キヤノン販売株式会社

発行日:2004/05/24

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
2004-05-24
キヤノン販売株式会社

更新履歴

バージョン	更新日付	事由	更新者	検査者	承認者
v1.0	2003/12/12	初期バージョン	土居	関田	広田
v1.01	2003/12/27	開発者の内部レビューによる修正	土居	関田	広田
v1.02	2004/01/16	評価者の OR の指摘を反映 TRN-EOR-0001-00 から TRN-EOR-0005-00	土居	関田	広田
v1.03	2004/02/06	評価者の OR の指摘を反映 TRN-EOR-0006-00 から TRN-EOR-0008-00	土居	関田	広田
v1.04	2004/02/18	開発者の内部レビューによる修正	土居	関田	広田
v1.05	2004/04/08	評価者の OR の指摘を反映 TRN-EOR-0009-00 から TRN-EOR-0016-00	土居	関田	広田
v1.06	2004/04/23	開発者の内部レビューによる修正	土居	関田	広田
v1.07	2004/05/24	認証レビューに基づいた修正	土居	関田	広田

目 次

1 - ST 概説

本章では、ST 識別、ST 概要、CC 適合の主張について記述する。

1.1 - ST 識別

タイトル: 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

日付: 2004-05-24

バージョン: v1.07

作成者: キヤノン販売株式会社

TOE: SeL v1

TOE revision: rev 01

キーワード: ランチャー、識別認証、SeL

CC のバージョン: Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

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 1999 年 8 月バージョン 2.1（平成 13 年 1 月翻訳第 1.2 版）

CCIMB Interpretations - 0210

補足-0210

評価保証レベル: EAL1

1.2 - ST 概要

本 ST は、セキュリティーランチャーソフトウェアである「SeL v1」のセキュリティ仕様を定めた ST (Security Target) である。本ソフトウェアは、Microsoft Windows 2000 Professional SP4 または Microsoft Windows XP Professional Edition SP1 上の保護対象プログラムを、起動可能な状態に変換する前にユーザの識別、認証を行うことで、第三者による不正変換から防止するランチャーソフトウェアである。

1.3 - CC 適合の主張

この TOE は、下記の CC に適合している。
- 機能要件－CC パート2適合
- 保証要件－CC パート3適合
- 保証レベル－EAL1 適合

本 ST が適合している PP はない。

1.4 - 略語・用語

- 保護対象プログラム：本 TOE により、不正変換されないように保護されるファイル
- 管理者：管理者権限を付与されたユーザ
- 一般ユーザ：管理者権限を付与されていないユーザ

2 - TOE 記述

本章では、TOE 種別、TOE 概要、TOE 範囲、役割、および資産について記述する。

2.1 - TOE 種別

TOE は、第三者による保護対象プログラムの不正変換を防止するために、起動可能な状態に変換する前に識別認証を行うランチャーソフトウェアである。
本 TOE は、Microsoft Windows 2000 Professional SP4 および Microsoft Windows XP Professional Edition SP1（以下、OS と略す）上で動作するソフトウェアである。

2.2 - TOE 概要

TOE は、第三者による保護対象プログラムの不正変換を防止するために、起動可能な状態に変換する前に識別認証を行うランチャーソフトウェアである。

本 TOE は、社内 LAN のような外部のネットワークから隔てられた内部ネットワークで使用し、その使用場所への入退出が管理される環境において使用する。
本 TOE が利用されるのは、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である。そのような環境では、本来の利用者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の漏洩、改ざんの危険がある。

これを防止するため、あらかじめ業務アプリケーションの形式を、起動できない形式に変換する。TOE 外である「組替えファイル生成ソフト v1.0」により、指定した実行可能な形式 exe ファイルから、OS のファイルシステムからの実行不可能な形式 EX_ファイルに組替える。
本 TOE は、上記の EX_ファイルを保護対象プログラムとしたランチャーソフトウェアであり、変換の前に識別認証を行うことで、第三者による exe ファイルへの変換を防ぐことを目的としている。

TOE が変換を保護する保護対象プログラムとして、任意の1種類の EX_ファイルを指定することができる。
TOE は、保護対象プログラムを変換する前に、ユーザの識別認証を行う。識別認証が正しく行われると、保護対象プログラムを実行可能な形式に変換して、対象となる業務アプリケーションを起動する。
また TOE は、ユーザ識別認証のために必要な識別認証データを、暗号化して保存することにより、暴露から保護している。さらに TOE は、保護対象プログラムから変換された exe ファイルの終了時に、これを削除する。

TOE のセキュリティ機能には以下のものがある。それぞれの機能に関しては 2.3 章で述べる。

- 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
- 暗号化機能

尚、本 TOE は OS 上で動作するソフトウェアであり、OS やハードウェアに直接アクセスし、TOE 自体を改ざんするといった攻撃には対処しない。このような高度な攻撃に対しては、運用面において対処するものである。

2.3 - TOE 範囲

＜TOE の物理的範囲＞
SeL v1 以外のソフトウェア、ハードウェアは TOE 外である。以下に、SeL v1 を動作させるために必要なハードウェア、ソフトウェアコンポーネントについて説明する。

本 TOE の物理的範囲は、SeL v1 である。

- ハードウェア構成
  CPU、メモリ、ハードディスク：Microsoft Windows 2000 Professional SP4 または Microsoft Windows XP Professional Edition SP1 の動作環境に準ずる

- ソフトウェア構成
  OS：Microsoft Windows 2000 Professional SP4 または Microsoft Windows XP Professional Edition SP1
  SeL v1
  保護対象プログラム

＜TOE の論理的範囲＞

本 TOE の論理的範囲としては、以下のセキュリティ機能が挙げられる。

- ユーザ識別認証機能
  ユーザ名とパスワードによる識別認証を行う。

- メンテナンス機能（管理者権限を持つユーザの機能）
  ・ユーザ名の問い合わせ、登録、および削除
  ・パスワードの登録、改変、削除
  ・ユーザの役割の改変
  ・パスワード有効期限の設定

- パスワード変更機能
  一般ユーザは、自身のパスワードについてのみ改変可能である。

- 暗号化機能
  ユーザ識別認証のために必要な識別認証データを暗号化して、暴露から保護している。

2.4 - 役割

ここでは役割について記述する。
正規のユーザは、管理者権限を付与されているか、付与されていないかで、下記のどちらかの役割を持ち、それぞれ操作できる機能が異なる。

- 一般ユーザ:管理者権限を付与されていないユーザ
  ① 保護対象プログラムの実行可能な形式への変換
  ② パスワード変更機能
- 管理者:管理者権限を付与されたユーザ
  ① 上記の一般ユーザの機能 ①、②
  ② 2.3-TOE 範囲に記述されているメンテナンス機能

2.5 - 資産

本 TOE の資産は以下の通りである。

- 保護対象プログラム (EX_ ファイル)
- 識別認証データ:下記情報がリスト形式で格納されているデータ

{ユーザ名、パスワード、役割、パスワードを更新した日時}

3 - TOE セキュリティ環境

本章では、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1 - 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 およ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 およ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。

3.2 - 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。

3.3 - 組織のセキュリティ方針

この ST で取り上げられる組織のセキュリティ方針はない。

4 - セキュリティ対策方針

本章では、TOE セキュリティ対策方針、環境セキュリティ対策方針について記述する。

4.1 - TOE のセキュリティ対策方針

O.CRYPTO:　識別認証データの暗号化
TOE は、識別認証データを暗号化して、盗み見られることからの保護を保証する。

O.I&A:　識別認証
TOE は、正規ユーザ以外の者が、TOE の機能を利用して保護対象プログラムを変換できないように、正規ユーザのみを識別認証することを保証する。

4.2 - 環境のセキュリティ対策方針

OE.ADMIN:　管理者の資質
管理者は、悪意を持たない人物であり、TOEの操作についての十分な教育を受け、故意または不注意によりTOEの機能を妨げることはないようにする。

OE.AREA:　使用される場所
管理者は、TOEが動作するハードウェアを、入退出が制限されたオフィスに設置する。

OE.INSTALL:　TOE および保護対象プログラムのインストール
管理者のみが、TOEおよびTOEが保護する保護対象プログラムをインストールする。

OE.NETWORK:　ネットワークからの保護
各ユーザは、TOE及び資産が保存されるディレクトリを、ネットワーク内で共有しないようにする。
外部ネットワークから内部ネットワークへの攻撃は、適切な設定をされたファイアウォールで防がれるようにする。

OE.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し、適時変更するようにする。

5 - セキュリティ要件

本章では、TOE セキュリティ要件、IT 環境セキュリティ要件について記述する。

5.1 - TOE セキュリティ要件

本章では、TOE が満たすべき TOE セキュリティ要件について記述する。

5.1.1 - TOE セキュリティ機能要件

本章では、TOE が提供するセキュリティ機能要件を記述する。機能コンポーネントは、CC パート 2 で規定されているものを、そのまま引用して、下記の操作を施した。
選択、割付を行った場合は下線にて、繰返しを行ったコンポーネントの場合はコンポーネント名の後ろに＋n (n は数字) を付与して、操作を行った。

5.1.1.1 - 暗号サポート (FCS)

5.1.1.1.1 - 暗号操作 (FCS_COP.1)

下位階層: なし

TSF は、FIPS PUB 46-2 に合致する、特定された暗号アルゴリズム DES と暗号鍵長 56bit に従って、識別認証データの暗号化及び復号を実行しなければならない。[FCS_COP.1.1]

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

5.1.1.2 - 識別と認証 (FIA)

5.1.1.2.1 - 認証失敗時の取り扱い (FIA_AFL.1)

下位階層: なし

TSFは、パスワードを用いた一般ユーザの認証に関して、連続5回の不成功認証試行が生じたときを検出しなければならない。[FIA_AFL.1.1]
不成功の認証試行が定義した回数に達するか上回ったとき、TSFは、該当ユーザのアカウン

トのロック、および管理者による該当ユーザのパスワード変更によってアカウントロックの解除をしなければならない。FIA_AFL.1.2

依存性: FIA_UAU.1 認証のタイミング

5.1.1.2.2 - 秘密の検証 (FIA_SOS.1)

下位階層: なし

TSFは、秘密が以下の品質尺度に合致することを検証するメカニズムを提供しなければならない。FIA_SOS.1.1
【品質尺度】 6文字以上8文字以下の半角英数字。大文字と小文字は区別する。

依存性: なし

5.1.1.2.3 - アクション前の利用者認証 (FIA_UAU.2)

下位階層: FIA_UAU.1

TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。FIA_UAU.2.1

依存性: FIA_UID.1 識別のタイミング

5.1.1.2.4 - 保護された認証フィードバック (FIA_UAU.7)

下位階層: なし

TSFは、認証を行っている間、*(アスタリスク)だけを利用者に提供しなければならない。
FIA_UAU.7.1

依存性: FIA_UAU.1 認証のタイミング

5.1.1.2.5 - アクション前の利用者識別 (FIA_UID.2)

下位階層: FIA_UID.1

TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。FIA_UID.2.1

依存性: なし

5.1.1.3 - セキュリティ管理 (FMT)

5.1.1.3.1 - TSF データの管理(FMT_MTD.1+0)

下位階層: なし

TSF は、自身のパスワードを改変する能力を一般ユーザに制限しなければならない。
FMT_MTD.1.1

依存性: FMT_SMR.1 セキュリティ役割
FMT_SMF.1 管理機能の特定

5.1.1.3.2 - TSF データの管理 (FMT_MTD.1+1)

下位階層: なし

TSF は、以下の TSF データを以下の操作する能力を管理者に制限しなければならない。
FMT_MTD.1.1

依存性: FMT_SMR.1 セキュリティ役割
FMT_SMF.1 管理機能の特定

表 5-1 管理者が行う TSF データに対する操作

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

機能	TSF データ	操作
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

5.1.1.3.3 - 時限付き許可 (FMT_SAE.1)

下位階層: なし

TSF は、パスワードの有効期限に対する有効期限の時間を特定する能力を、管理者に制限しなければならない。FMT_SAE.1.1

これらセキュリティ属性の各々について、TSF は、示されたセキュリティ属性に対する有効期限の時間後、パスワードの再設定を行えなければならない。FMT_SAE.1.2

依存性: FMT_SMR.1 セキュリティ役割
FPT_STM.1 高信頼タイムスタンプ

5.1.1.3.4 - 管理機能の特定(FMT_SMF.1)

下位階層: なし

TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない:下記の表5-2の「管理対象とすべきアクション」の項目において、下線を引いた管理用セキュリティ機能FMT_SMF.1.1

依存性:なし

表 5-2 機能要件から参照された管理用セキュリティ機能

機能要件	管理対象とすべきアクション	実現する機能要件
FCS_COP.1	なし	なし
FIA_AFL.1	a) 不成功の認証試行に対する閾値の管理 b) 認証失敗の事象においてとられるアクションの管理	a) なし b) FMT_MTD.1+1
FIA_SOS.1	a) 秘密の検証に使用される尺度の管理	なし
FIA_UAU.2	管理者による認証データの管理;このデータに関係する利用者による認証データの管理	FMT_MTD.1+0 FMT_MTD.1+1
FIA_UAU.7	なし	なし
FIA_UID.2	a) 利用者識別情報の管理	FMT_MTD.1+1
FMT_MTD.1+0	a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること	なし
FMT_MTD.1+1	a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること	なし
FMT_SAE.1	a) 有効期限がサポートされるはずのセキュリティ属性のリストを管理すること; b) 有効期限の時間が過ぎた時にとられるアクション	a) なし b) なし
FMT_SMF.1	なし	なし
FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理	なし
FPT_RVM.1	なし	なし
FPT_STM.1	a) 時間の管理	なし

5.1.1.3.5 - セキュリティ役割 (FMT_SMR.1)

下位階層: なし

TSF は、役割管理者、一般ユーザを維持しなければならない。[FMT_SMR.1.1]
TSF は、利用者を役割に関連づけなければならない。[FMT_SMR.1.2]

依存性: FIA_UID.1 識別のタイミング

5.1.1.4 - TSF の保護 (FPT)

5.1.1.4.1 – TSP の非バイパス性 (FPT_RVM.1)

下位階層: なし

TSFは、TSC内の各機能の動作進行が許可される前に、TSP実施機能が呼び出され成功することを保証しなければならない。FPT_RVM.1.1

依存性:なし

5.1.1.4.2 - 高信頼タイムスタンプ(FPT_STM.1)

下位階層: なし

TSF は、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。
FPT_STM.1.1

依存性:なし

5.1.2 - 最小機能強度レベル

本 ST では、最小機能強度レベルを主張しない。

5.1.3 - TOE セキュリティ保証要件

本章では、TOE のセキュリティ保証要件を記述する。
この TOE の保証要件は、EAL1 である。すべての保証要件コンポーネントは、CC パート 3 で規定されている EAL1 のコンポーネントをそのまま使用する。

表 5-3 評価保証レベル: EAL(1)

保証要件クラス	保証要件コンポーネント
ACM	ACM_CAP.1
ADO	ADO_IGS.1
ADV	ADV_FSP.1, ADV_RCR.1
AGD	AGD_ADM.1, AGD_USR.1
ATE	ATE_IND.1

5.2 - IT 環境のセキュリティ要件

本章では、IT 環境が満たすべきセキュリティ要件について記述する。

5.2.1 - IT 環境のセキュリティ機能要件

本 TOE では、IT 環境のセキュリティ機能要件を必要としない。

5.2.2 - IT 環境のセキュリティ保証要件

本 TOE では、IT 環境のセキュリティ保証要件を必要としない。

5.3 - 非 IT 環境のセキュリティ要件

本 TOE では、非 IT 環境のセキュリティ要件を必要としない。

6 - TOE 要約仕様

この章では、TOE の要約仕様を記述する。

6.1 - TOE セキュリティ機能

ここでは、TOE セキュリティ機能について記述する。

6.1.1 - TOE セキュリティ機能の記述

表 6-1 セキュリティ機能と対応するコンポーネント

セキュリティ機能	機能要件コンポーネント
SF.CRYPTO	FCS_COP.1, FPT_RVM.1
SF.I&A	FIA_UAU.7, FIA_AFL.1, FIA_UID.2, FIA_UAU.2, FPT_RVM.1, FPT_STM.1
SF.CHANGE_PW	FIA_SOS.1, FMT_MTD.1+0, FMT_SMF.1
SF.MAINTENANCE	FIA_SOS.1, FMT_SAE.1, FMT_SMR.1, FMT_MTD.1+1, FIA_AFL.1, FMT_SMF.1

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、暗号化および復号を行う。
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。

SF.I&A:　識別と認証

TOE は、保護対象プログラムが正規ユーザ以外に変換されないよう、ユーザ名およ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 は利用者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、パスワードを更新した日時と照会することで期限を確認する。現在のタイムスタンプとパスワードを更新した日時を比

較し、期限切れの場合、パスワードの再設定を要求する。TOE は、OS を利用して現在のタイムスタンプを提供している。

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。

SF.MAINTENANCE:　　メンテナンス機能

TOE は、管理者、一般ユーザの 2 つの役割を維持する。
TOE は、識別認証に関する設定を行う。これは、管理者が使用することのできる機能である。管理者に許可された機能を表 6-2 にまとめる。

表 6-2　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

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。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。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変更することにより、ロックを解除する。ユーザのパスワードを変更する際、ロック解除時のパスワード変更を除き、新しいパスワードは、現パスワードと同一のものは不許可とする。

6.2 - 保証手段

この章では、TOE のセキュリティ保証手段を記述する。以下のセキュリティ保証手段は、5.1.3 節で記述した TOE セキュリティ保証要件を満たすものである。

表 6-3 保証手段と対応するコンポーネント

保証要件コンポーネント	保証手段
ACM_CAP.1	本 ST および TOE
ADO_IGS.1	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
ADV_FSP.1	セキュリティーランチャーソフトウェア SeL v1 機能仕様書 v1.05
ADV_RCR.1	セキュリティーランチャーソフトウェア SeL v1 機能仕様書 v1.05
AGD_ADM.1	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
AGD_USR.1	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
ATE_IND.1	TOE

7 - PP 主張

この章では、PP 主張について記述する。

7.1 - PP 参照

参照した PP はない。

7.2 - PP 修正

修正した PP はない。

7.3 - PP 追加

PP への追加はない。

8 - 根拠

本章では、セキュリティ対策方針根拠、セキュリティ要件根拠、TOE 要約仕様根拠について記述する。

8.1 - セキュリティ対策方針根拠

本節では、セキュリティ対策方針が、TOE セキュリティ環境で規定した脅威、前提条件に対抗していることを示す。

表 8-1 セキュリティ対策方針と対抗する脅威、組織のセキュリティ方針および前提条件の対応表

	A.AREA	A.INSTALL	A.Competent_Admin	A.NETWORK	A.PASSWORD	A.Well_Behaved_Admin	T.ID_PASS	T.UNAUTH
O.CRYPTO							×	
O.I&A								×
OE.ADMIN			×			×		
OE.INSTALL		×						
OE.AREA	×							
OE.NETWORK				×				
OE.PASSWORD					×			

8.1.1 - 組織のセキュリティ方針に関する根拠

本 ST で取り上げられる組織のセキュリティ方針はない。

8.1.2 - 脅威に関する根拠

T.ID_PASS:　識別認証データの盗み見　は、以下の対策方針によって対抗される。
O.CRYPTO:　識別認証データの暗号化

TOE は、TOE 内に保存している識別認証データを O.CRYPTO により暗号化している。よって、識別認証データが、低い攻撃能力しか持たない第三者に知られることはない。

T.UNAUTH:　許可されないユーザの使用は、以下の対策方針によって対抗される。
O.I&A:　識別認証

TOE は、O.I&A によりユーザが TOE を利用する前に識別認証されることを保証する。よって、低い攻撃力しか持たない第三者が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ことはない。

8.1.3 - 前提条件に関する根拠

A.AREA:　使用される場所 は、以下の対策方針によって実現される。
OE.AREA:　使用される場所

OE.AREA により、TOE が動作するハードウェアは入退出が制限されたオフィスに設置される。

A.INSTALL:　インストールは、以下の対策方針によって実現される。
OE.INSTALL:　TOE および保護対象プログラムのインストール

OE.INSTALL により、TOE と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。

A.Competent_Admin:　適切な管理者は、以下の対策方針によって実現される。
OE.ADMIN:　管理者の資質

OE.ADMIN により、十分な能力を持つ管理者により、TOE のセキュリティは管理される。

A.NETWORK:　　ネットワーク は、以下の対策方針によって実現される。
OE.NETWORK:　　ネットワークからの保護

OE.NETWORK により、TOE 及び資産が保存されるディレクトリは、ネットワーク内で共有されない。また、適切に設定されたファイアウォールにより、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る。

A.PASSWORD:　　パスワードの管理 は、以下の対策方針によって実現される。
OE.PASSWORD:　　パスワードの管理

OE.PASSWORD により、ユーザは TOE にアクセスするためのパスワードを本人以外に漏洩せず、第三者のなりすましを防ぐ。

A.Well_Behaved_Admin:　　信頼できる管理者 は、以下の対策方針によって実現される。
OE.ADMIN:　　管理者の資質

OE.ADMIN により、故意または不注意により、TOE のセキュリティを危うくすることは無い。

8.2 - セキュリティ要件根拠

8.2.1 - TOE セキュリティ機能要件根拠

TOE セキュリティ機能要件と TOE セキュリティ対策方針の対応関係を表 8-2 に示す。

表 8-2 TOE セキュリティ要件と TOE セキュリティ対策方針の対応表

	O.CRYPTO	O.I&A
FCS_COP.1	×	
FIA_AFL.1		×
FIA_SOS.1		×
FIA_UAU.2		×
FIA_UAU.7		×
FIA_UID.2		×
FMT_MTD.1+0		×
FMT_MTD.1+1		×
FMT_SAE.1		×
FMT_SMF.1		×
FMT_SMR.1		×
FPT_RVM.1		×
FPT_STM.1		×

O.CRYPTO:　識別認証データの暗号化は、以下のセキュリティ要件によって実現される。
FCS_COP.1:　暗号操作

このセキュリティ対策方針は、FCS_COP.1 で実現できる。
FCS_COP.1 は、識別認証データを暗号化することで、盗み見られることを防ぎ、秘密性を保持する。

O.I&A:　識別認証は、以下のセキュリティ要件によって実現される。
FIA_AFL.1:　認証失敗時の取り扱い
FIA_UAU.2:　アクション前の利用者認証
FIA_UAU.7:　保護された認証フィードバック
FIA_UID.2:　アクション前の利用者識別
FIA_SOS.1:　秘密の検証
FMT_MTD.1+0:　TSF データの管理
FMT_MTD.1+1:　TSF データの管理
FMT_SAE.1:　時限付き許可
FMT_SMF.1:　セキュリティ管理機能の特定
FMT_SMR.1:　セキュリティ役割
FPT_RVM.1:　TSP の非バイパス性
FPT_STM.1:　高信頼タイムスタンプ

このセキュリティ対策方針は、FIA_AFL.1、FIA_SOS.1、FIA_UAU.2、FIA_UAU.7、FIA_UID.2、FMT_MTD.1+0、FMT_MTD.1+1、FMT_SAE.1、FMT_SMF.1、FMT_SMR.1、FPT_RVM.1、FPT_STM.1 で実現できる。

FIA_UAU.2 と FIA_UID.2 は入力されたユーザ名とパスワードによって、正当なユーザか否かを識別認証する。FPT_RVM.1 は、識別認証がバイパスされることを防止する。FIA_UAU.7 は、識別認証時に入力されるパスワードをアスタリスク(*)で画面に表示し、入力中の画面からパスワードが漏洩しないように保護する。FIA_AFL.1 は、識別認証の失敗が規定回数に達した時に、該当ユーザのアカウントをロックする。ロックの解除は、該当ユーザのパスワード変更により行う。FIA_SOS.1 は、設定するパスワードに対して、定められた品質尺度に合致することを検証する。これらにより識別認証の機能を強める。FMT_SAE.1 は、パスワードに対する有効期限を設定する能力を管理者に制限し、有効期限が設定された場合、FPT_STM.1 は、OS から高信頼タイムスタンプを取得し、これを提供することで有効期限の管理を行う。識別認証が成功すると、FMT_SMR.1 は、管理者、一般ユーザという、2 つの役割を維持する。この役割ごとに、TSF データに対して実行できる操作が異なり、FMT_MTD.1+0、FMT_MTD.1+1 は TSF データと役割、および可能な操作を規定している。
FMT_SMF.1 は、各 TSF が実行できる、TOE のセキュリティ管理機能を明示している。

8.2.2- セキュリティ保証要件根拠

SeL v1 は、Microsoft Windows 2000 Professional SP4 または Microsoft Windows XP Professional Edition SP1 上で動作するソフトウェアの不正変換を防止する製品である。保護対象プログラムの不正変換を試みる第三者は、低い攻撃能力しか持たない。よって EAL1 の選択は妥当なものであるといえる。

8.2.3 - セキュリティ要件依存性

セキュリティ要件のコンポーネントの依存性を、表 8-3 に示す。表の左側が選択されたコンポーネント、右側が依存するコンポーネントである。除去されたコンポーネントは（ ）で示す。

表 8-3 セキュリティ要件依存性の対応表

セキュリティ要件	依存性
機能要件	
FCS_COP.1	(FDP_ITC.1)または(FCS_CKM.1), (FCS_CKM.4),(FMT_MSA.2)
FIA_AFL.1	FIA_UAU.1
FIA_SOS.1	-
FIA_UAU.2	FIA_UID.1
FIA_UAU.7	FIA_UAU.1
FIA_UID.2	-
FMT_MTD.1+0	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1+1	FMT_SMR.1, FMT_SMF.1
FMT_SAE.1	FMT_SMR.1, FPT_STM.1
FMT_SMF.1	-
FMT_SMR.1	FIA_UID.1
FPT_RVM.1	-
FPT_STM.1	-

セキュリティ要件	依存性
保証要件	
ACM_CAP.1	-
ADO_IGS.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1
ADV_RCR.1	-
AGD_ADM.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1
ATE_IND.1	ADV_FSP.1, AGD_ADM.1, AGD_USR.1

依存性除去の理由:
FCS_COP.1 から FDP_ITC.1 または FCS_CKM.1, FCS_CKM.4,FMT_MSA.2 への依存性が満たされていないことについて、問題がない根拠を以下に示す。

本 TOE では、暗号鍵を別ファイルではなく TOE 自体に保持しており、これは第三者によって容易に知り得るものではなく、セキュアに維持管理している。よって暗号鍵をインポートまたは生成・破棄する必要はない。また固定鍵であるため、暗号鍵のセキュリティ属性のチェックを行うこともない。よって、これらの機能は本 TOE では不要なものである。
従って、これらのセキュリティ要件への依存関係は不要である。

また、以下の様に、本 ST で選択した機能要件は、相互サポートを行っている。

本 TOE では、保護対象プログラムの不正変換を防止するため、識別認証機能（FIA）を持つ。識別認証データは登録・改変・削除が可能となるように、セキュリティ管理（FMT）にて管理している。また識別認証データは暴露から保護するべく、暗号サポート（FCS）して保存している。これらは全体として相互サポートの構造をとっている。

バイパス防止：FPT_RVM.1 により、FIA_UIA.2 と FIA_UAU.2 による識別認証に成功しない限り、他の全ての機能を使用できないことが保証される。

改ざん防止：TSF データである識別認証データは、暗号化されて保存される。更に、本 TOE が想定する攻撃者は低い攻撃力しか持たないので、TSF の改ざんを行うような能力は持っていない。これらにより、改ざんは防止されている。

非活性化防止：本 TOE では、セキュリティ機能を非活性するような機能は持っていないので、非活性化は防止されている。従って、これらを検知しなくてもセキュリティ上問題は無く、監査機能も不要である。

8.2.4 - 最小機能強度レベル根拠

本 ST では、最小機能強度は主張しないため、根拠は記述しない。

8.3 - TOE 要約仕様根拠

8.3.1 - セキュリティ機能根拠

TOE のセキュリティ機能と、TOE の機能要件コンポーネントの対応を表 8-4 に示す。

表 8-4 TOE のセキュリティ機能と TOE の機能要件コンポーネントの対応表

	FCS_COP.1	FIA_AFL.1	FIA_SOS.1	FIA_UAU.2	FIA_UAU.7	FIA_UID.2	FMT_MTD.1+0	FMT_MTD.1+1	FMT_SAE.1	FMT_SMF.1	FMT_SMR.1	FPT_RVM.1	FPT_STM.1
SF.CRYPTO	×											×	
SF.I&A		×		×	×	×						×	×
SF.CHANGE_PW			×				×			×			
SF.MAINTENANCE		×	×					×	×	×	×		

FCS_COP.1:　暗号操作 は、以下のセキュリティ機能によって実現される。
　　SF.CRYPTO:　暗号化

　　SF.CRYPTO は FIPS PUB 46-2 に合致する DES 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。
　　従って、SF.CRYPTO により、FCS.COP.1 は実現できる。

FIA_AFL.1:　認証失敗時の取り扱い は、以下のセキュリティ機能によって実現される。
　　SF.I&A:　識別と認証
　　SF.MAINTENANCE:　メンテナンス機能

　　SF.I&A は、一般ユーザが連続 5 回の認証失敗をした時に、該当ユーザのアカウントをロックする。
　　ロックの解除は、管理者が該当ユーザのパスワードを変更することで行う。
　　従って、SF.I&A と SF.MAINTENANCE により、FIA_AFL.1 は実現できる。

FIA_SOS.1:　秘密の検証 は、以下のセキュリティ機能によって実現される。
SF.CHANGE_PW:　パスワードの変更
SF.MAINTENANCE:　メンテナンス機能

SF.CHANGE_PW および SF.MAINTENANCE は、ユーザの識別認証に使用するパスワードが、6 文字以上 8 文字以下の半角英数字（大文字と小文字を区別）の品質尺度を満たすことを検証するメカニズムを提供する。
従って、SF.CHANGE_PW と SF.MAINTENANCE により、FIA_SOS.1 を実現できる。

FIA_UAU.2:　アクション前の利用者認証 は、以下のセキュリティ機能によって実現される。
SF.I&A:　識別と認証

SF.I&A は、ユーザの認証前に、いかなる操作も許可しないことを保証する。
従って、SF.I&A により FIA_UAU.2 が実現できる。

FIA_UAU.7:　保護された認証フィードバック は、以下のセキュリティ機能によって実現される。
SF.I&A:　識別と認証

SF.I&A は、ユーザのパスワード入力時に、*（アスタリスク）以外のフィードバックを行わない。
従って、SF.I&A により、FIA_UAU.7 を実現できる。

FIA_UID.2:　アクション前の利用者識別 は、以下のセキュリティ機能によって実現される。
SF.I&A:　識別と認証

SF.I&A は、ユーザの識別前に、いかなる操作も許可しないことを保証する。
従って、SF.I&A により、FIA_UID.2 を実現できる。

FMT_MTD.1+0:　TSF データの管理は、以下のセキュリティ機能によって実現される。
SF.CHANGE_PW:　パスワードの変更

SF.CHANGE_PW は、一般ユーザが改変できるパスワードは、一般ユーザ自身のパスワードに限定する。
従って、SF.CHANGE_PW により、FMT_MTD.1+0 を実現できる。

FMT_MTD.1+1: TSF データの管理は、以下のセキュリティ機能によって実現される。
SF.MAINTENANCE: メンテナンス機能
SF.MAINTENANCE は、以下の能力を管理者に限定する。

表 8-5 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

従って、SF.MAINTENANCE により、FMT_MTD.1+1 を実現できる。

FMT_SAE.1: 時限付き許可 は、以下のセキュリティ機能によって実現される。
SF.MAINTENANCE: メンテナンス機能

SF.MAINTENANCE は、ユーザの使用するパスワードに有効期限を設定する能力を、管理者に限定する。
従って、SF.MAINTENANCE により、FMT_SAE.1 を実現する。

FMT_SMF.1:　セキュリティ管理機能の特定は、以下のセキュリティ機能によって実現される。

SF.CHANGE_PW:　パスワードの変更
SF.MAINTENANCE:　メンテナンス機能

以下に、本 TOE で選択している機能要件、その管理対象、実現するセキュリティ機能の表を示す。

表 8-6 機能要件から参照された管理用セキュリティ機能を、実現するセキュリティ機能

機能要件	管理対象とすべきアクション	実現するセキュリティ機能
FCS_COP.1	なし	なし
FIA_AFL.1	a) 不成功の認証試行に対する閾値の管理 b) 認証失敗の事象においてとられるアクションの管理	a) なし b) SF.MAINTENANCE
FIA_SOS.1	a) 秘密の検証に使用される尺度の管理	なし
FIA_UAU.2	管理者による認証データの管理;このデータに関係する利用者による認証データの管理	SF.CHANGE_PW SF.MAINTENANCE
FIA_UAU.7	なし	なし
FIA_UID.2	a) 利用者識別情報の管理	SF.MAINTENANCE
FMT_MTD.1+0	a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること	なし
FMT_MTD.1+1	a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること	なし
FMT_SAE.1	a) 有効期限がサポートされるはずのセキュリティ属性のリストを管理すること; b) 有効期限の時間が過ぎた時にとられるアクション	a) なし b) なし
FMT_SMF.1	なし	なし
FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理	なし
FPT_RVM.1	なし	なし
FPT_STM.1	a) 時間の管理	なし

以下に、管理対象とすべきアクションはあるが、TOE が管理機能を持たない機能要件について、その根拠を示す。

FIA_AFL.1：
a) 不成功の認証に対する閾値の管理
閾値は 5 回固定であるため、この回数を管理する機能は存在しない。

FIA_SOS.1:
a) 秘密の検証に使用される尺度の管理
パスワードの文字数チェックは行うが、尺度を変更する機能は存在しない。
FMT_MTD.1+0、FMT_MTD.1+1：
a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること
本 TOE では、役割は固定であるので、これを管理する機能は存在しない。

FMT_SAE.1：
a) 有効期限がサポートされるはずのセキュリティ属性のリストを管理すること；
b) 有効期限が過ぎたときにとられるアクション
有効期限をサポートするセキュリティ属性のリストは固定である。また、有効期限を過ぎたときにとられるアクションは、パスワードの再設定のみである。よってこれらを管理する機能は存在しない。

FMT_SMR.1：
a) 役割の一部をなす利用者のグループの管理
本 TOE では役割は固定であるので、これを管理する機能は存在しない。

FPT_STM.1：
a) 時間の管理
OS の機能を利用するため、本 TOE には機能が存在しない。

本 TOE では、セキュリティ管理機能として下記の 2 つのセキュリティ機能のみが存在する。
SF.CHANGE_PW は、一般ユーザが改変できるパスワードは、ユーザ自身の物のみに限定する。
SF.MAINTENANCE は、識別認証に関する設定を行うためのメンテナンス機能であり、管理者が使用することのできる機能である。
従って、SF.CHANGE_PW と SF.MAINTENANCE により、FMT_SMF.1 は実現される。

FMT_SMR.1:　　セキュリティ役割 は、以下のセキュリティ機能によって実現される。
SF.MAINTENANCE:　　メンテナンス機能

SF.MAINTENANCE は、ユーザの役割を維持する。
・管理者

・一般ユーザ
従って、SF.MAINTENANCE は、FMT_SMR.1 を実現する。

FPT_RVM.1: TSP の非バイパス性は、以下のセキュリティ機能によって実現される。
SF.CRYPTO: 暗号化
SF.I&A: 識別と認証

SF.I&A は、TOE の起動時に他の機能に先立って動作する。SF.I&A に成功しない限りは他の全機能を使用することができない。また、SF.I&A で用いる識別認証データは、SF.CRYPTO によって暗号化されて保持されるので、攻撃者からは保護されている。
従って、SF.CRYPTO と SF.I&A により、FPT_RVM.1 を実現する。

FPT_STM.1: 高信頼タイムスタンプは、以下のセキュリティ機能によって実現される。
SF.I&A: 識別と認証

SF.I&A は、パスワードの有効期限を確認するのに必要なタイムスタンプ情報を OS から取得して提供する。
従って、SF.I&A により、FPT_STM.1 を実現する。

8.3.2 - 機能強度根拠

本 ST では存在しない。

8.3.3 - セキュリティ機能のコンビネーション

本 TOE では、保護対象プログラムの不正変換を防止するため、SF.I&A (識別と認証) を持つ。識別認証データは登録・改変・削除が可能となるように、SF.MAINTENANCE (メンテナンス機能) にて管理している。一般ユーザの自身のパスワードは、SF.CHANGE_PW (パスワードの変更) によって変更できる。また識別認証データは暴露から保護するべく、SF.CRYPTO (暗号化) して保存している。これらは全体として相互サポートの構造をとっている。

8.3.4 - 保証手段の根拠

各保証手段と、EAL1 の保証要件コンポーネントの対応関係を表 8-7 に示す。

表 8-7 保証手段と TOE の保証要件コンポーネントの対応表

	ACM_CAP.1	ADO_IGS.1	ADV_FSP.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ATE_IND.1
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		×			×		
本 ST および TOE	×						
セキュリティーランチャーソフトウェア SeL v1 機能仕様書 v1.05			×	×			
TOE							×
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						×	

ACM_CAP.1: 本 ST および TOE は、TOE のバージョンのリファレンスを記述している。よって ACM_CAP.1 は、本 ST および TOE の提出により実現される。

ADO_IGS.1: 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 は、設置、生成、及び立上げ手順 について記述している。
よって ADO_IGS.1 は、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 により実現される。

ADV_FSP.1: セキュリティーランチャーソフトウェア SeL v1 機能仕様書 v1.05 は、TOE の非形式的機能仕様を記述している。
よって ADV_FSP.1 は、セキュリティーランチャーソフトウェア SeL v1 機能仕様書 v1.05 によって実現される。

ADV_RCR.1: セキュリティーランチャーソフトウェア SeL v1 機能仕様書 v1.05 は、非形式的対応の実証 を機能仕様一覧にて記述している。
よって ADV_RCR.1 は、セキュリティーランチャーソフトウェア SeL v1 機能仕様書 v1.05 によって実現される。

AGD_ADM.1: 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 は、管理者向けのガイダンスを記述している。
よって、AGD_ADM.1 は、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 によって実現される。

AGD_USR.1: 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 は、利用者向けのガイダンスを記述している。
よって AGD_USR.1 は、利用者ガイダンス は、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 によって実現される。

ATE_IND.1: テストのために TOE を提供する。
よって ATE_ IND.1 は、本 TOE および評価者の用意するテスト証跡資料により実現される。