セキュリティプラットフォーム evolution /SV CC
セキュリティターゲット

第 2.08版

作成日：2010 年5月27日

ハミングヘッズ株式会社

変更履歴

日付	版	修正概要	修正者
2009/09/01	2.00	新規作成	ハミングヘッズ株式会社
2009/12/18	2.01	CD/DVD の write 制限に関する修正	ハミングヘッズ株式会社
2010/01/18	2.02	ライティングソフトのバージョンに関する修正	ハミングヘッズ株式会社
2010/01/26	2.03	ガイダンスの版数に関する修正	ハミングヘッズ株式会社
2010/02/19	2.04	用語定義に関する修正	ハミングヘッズ株式会社
2010/03/02	2.05	用語定義に関する修正	ハミングヘッズ株式会社
2010/03/26	2.06	版数およびバージョンに関する修正	ハミングヘッズ株式会社
2010/04/14	2.07	用語定義に関する修正	ハミングヘッズ株式会社
2010/05/26	2.08	ドメインコントローラの記述修正	ハミングヘッズ株式会社

【目次】

1 ST 概説

本章では、ST 参照、TOE 参照、TOE 概要、および TOE 記述について記述する。

1.1 ST 参照

タイトル : セキュリティプラットフォーム evolution /SV CC セキュリティターゲット
バージョン : 第 2.08 版
作成日 : 2010 年 5 月 27 日
作成者 : ハミングヘッズ株式会社

1.2 TOE 参照

TOE : セキュリティプラットフォーム evolution /SV CC
バージョン : Ver.2.0.9.4
開発者 : ハミングヘッズ株式会社

※ セキュリティプラットフォーム evolution /SV CC は以下の製品の総称である。また、以下の製品のバージョンは上記バージョンと同一である。

- セキュリティプラットフォーム クライアント ベーシック evolution /SV
- セキュリティプラットフォーム サーバ ベーシック evolution /SV
- セキュリティプラットフォーム トレーサオプション
- セキュリティプラットフォーム クライアント イントラネットオプション
- セキュリティプラットフォーム サーバ イントラネットオプション
- セキュリティプラットフォーム クライアント エンクリプションオプション
- セキュリティプラットフォーム サーバ エンクリプションオプション
- セキュリティプラットフォーム クライアント ストレージエンクリプションオプション
- セキュリティプラットフォーム サーバ ストレージエンクリプションオプション

1.3 用語

1.3.1 本 ST における用語

本 ST で用いる用語を表 1-1 に定義する。

表 1-1 本 ST で用いる用語定義

用語	定義内容
SeP	セキュリティプラットフォームの略称。
SeP サーバ	SeP のサーバ製品がインストールされたサーバマシン。
SeP クライアント	SeP のクライアント製品がインストールされたクライアントマシン。
信頼領域	社の内部とする領域である。ドメインに登録されている SeP クライアントのブートハードディスク、管理者により指定されたファイルサーバの共有フォルダ(記憶媒体は NTFS または FAT ファイルシステム)。また、信頼領域(社内 URL)の Web ページへの添付時にブラウザが使用する領域。
リリースフォルダ	社の内部とする領域である。社外に提供するファイルを一旦入れるフォルダであり、パスは管理者が定義する。リリースフォルダが定義されると、他の領域に優先してリリースフォルダとして扱われる。
メール添付	ファイルを送信するためメーラ上に読み込むこと。
Web ページへの添付	ブラウザでファイルを読み込みアップロードすること。
外部媒体	マシンの外部インターフェースで取り外し可能な NTFS または FAT ファイルシステムの記憶媒体、または CD/DVD/ブルーレイディスク。
非信頼領域	社の外部とする領域であり、信頼領域でもリリースフォルダでもない領域(記憶媒体は NTFS または FAT ファイルシステム、または CD/DVD/ブルーレイディスク)、また、メール添付時にメーラが使用する領域、非信頼領域(SV 化 URL)の Web ページへの添付時にブラウザが使用する領域は非信頼領域として扱われる。なお、非信頼領域は管理者が定義することも可能であり、信頼領域上に非信頼領域が定義されると、非信頼領域として扱われる。
信頼領域(社内 URL)	ファイルを添付した際に SV 暗号化を行わないように管理者により指定された URL。
非信頼領域(SV 化 URL)	ファイルを添付した際に SV 暗号化を行うように管理者により指定された URL。
持ち出し操作	非信頼領域へのファイル操作、メールへのペースト操作、信頼領域(社内 URL)以外の Web ページへの添付およびペースト操作(移動については

用語	定義内容
	ドライブを跨ぐ場合。)。
ファイル操作	ファイルのコピー、移動、保存、メール添付・送信・ペースト操作、Web ページへの添付・送信・ペースト操作。
SV 暗号ファイル	SV 暗号機能により暗号化されたファイル。信頼領域から非信頼領域に持ち出した際に平文から自動的に変換される。元の信頼領域に戻すことによってのみ自動的に復号される。
自走式暗号ファイル	自走式暗号機能により暗号化されたファイル。作成者により設定されたパスワードにより復号される自己復号型暗号ファイル。リリースフォルダから非信頼領域に持ち出した際に平文から変換される。
操作履歴	TOE が出力する、アプリケーションの操作についての記録。
履歴データ	クライアントからサーバへアップロードされた操作履歴のデータで、トレーサで収集前の状態のもの。
集積履歴データ	トレーサで収集した操作履歴のデータで、CSV 出力前の状態のもの。
トレーサ	操作履歴を収集して CSV 形式で閲覧できるようにするための TOE の管理者向けツール。
CSV	データをカンマ(,)で区切って並べたファイル形式(Comma Separated Values)。
LAN	ローカルエリアネットワーク(Local Area Network)の略称。
モバイル	社内 LAN から切り離された状態。
第三者	社外の不特定多数の者。
USB	ユニバーサルシリアルバス(Universal Serial Bus)の略称。
FD	フロッピーディスク(Floppy Disk)の略称。

1.4 TOE 概要

1.4.1 TOE の使用方法とセキュリティ機能の概要

TOE は、情報漏洩対策ソフトウェア製品であり、意図した受け取り手以外の第三者に社内のデータが漏洩することを防ぐ目的のものである。TOE は、Windows ドメイン環境で利用するサーバークライアント型製品である。SeP サーバ製品は、サーバマシンにインストールする。SeP クライアント製品は、一般利用者が使用するマシンにインストールする。SeP サーバおよび SeP クライアントで利用できるセキュリティ機能は以下の通りである。

<SeP サーバ固有機能>

(1) 監査機能(管理者向け機能)

管理者はトレーサを用いて、操作履歴を収集し、汎用ソフトで閲覧できるようにCSV形式で出力する機能である。また、サーバ設定ツールの設定履歴を閲覧できる。

(2) 管理機能

管理者が TOE の動作を管理するための機能である。

<SeP クライアント固有機能>

(1) ストレージ暗号機能

モバイル端末の盗難・置忘れ対策のため、ハードディスクを暗号化する機能である。

<SeP サーバおよび SeP クライアント共通機能>

(1) SV 暗号機能

保護資産が存在する信頼領域から非信頼領域への許可されたファイル操作の際に、ファイルの自動暗号化を行う機能である。暗号化されたファイル(SV 暗号ファイル)は信頼領域に戻されると自動的に復号される。なお、Web ページに対しては URL によってファイルの添付を禁止し、データをメールまたは信頼領域以外の Web ページにペーストすることも禁止する。

(2) Write 制限機能

持ち出し操作を許可するアプリケーションを限定する機能である。

(3) 自走式暗号機能

一般利用者が正規の業務として保護資産を社外へ提供するための機能である。外部への窓口であるリリースフォルダを経由してファイルを出す際に、パスワードの設定が強制され、ファイルは自走式暗号ファイルに変換される。

(4) 監査機能(操作履歴出力機能)

アプリケーションの操作履歴を出力する機能である。

1.4.2 TOE 種別

TOE は、情報漏洩対策ソフトウェア製品である。

1.4.3 TOE の動作に必要な環境

TOE の動作環境を図 1-1 に示す。

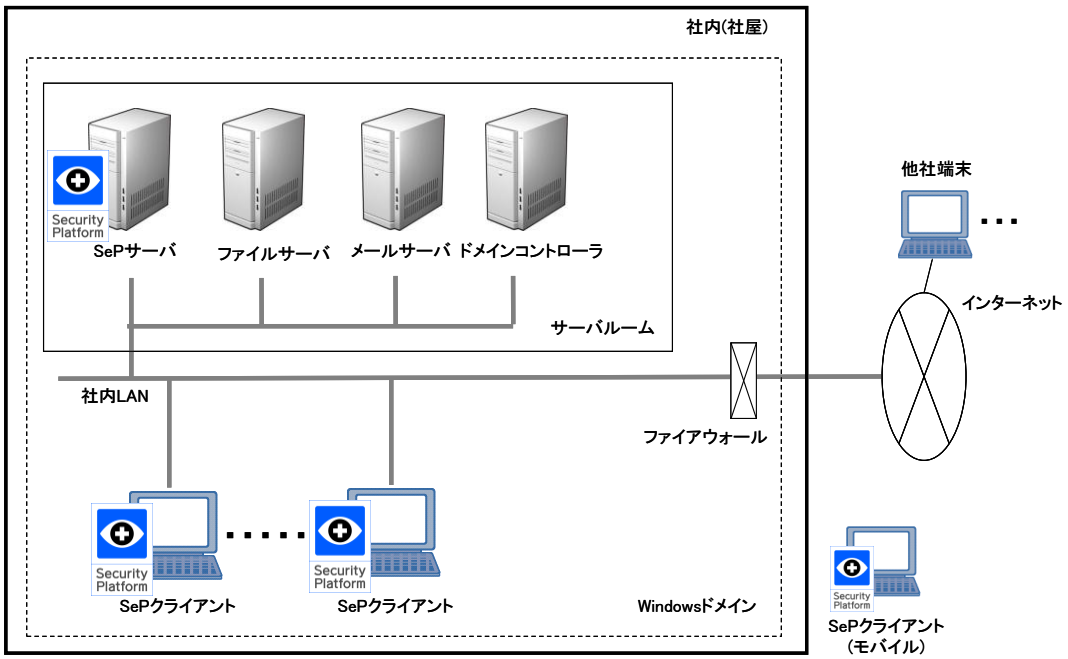

図 1-1 TOE の動作環境

動作環境の構成要素について以下に説明する。

(1) 社屋

社屋は入退館管理され、第三者は入館できない。

(2) サーバルーム

各種サーバ(SeP サーバ、ドメインコントローラ、メールサーバ、ファイルサーバ)が設置される。入退室管理され、管理者のみが各種サーバの管理を行うことができる。

(3) 社内 LAN

各種サーバ(SeP サーバ、ドメインコントローラ、メールサーバ、ファイルサーバ)およびクライアントを接続する。ファイアウォールを介してインターネットに接続される。

(4) ファイアウォール

ファイル転送可能なプロトコルとして SMTP と HTTP/HTTPS プロトコルのみの通信を双方向に許可する。

(5) SeP サーバ

TOE がインストールされ、管理者が TOE の管理機能および管理者向け監査機能(トレーサ)を利用する。

(6) ファイルサーバ

共有ファイルが保存される(TOE の利用のためには必須ではない)。

(7) メールサーバ

メールの利用を可能にする(TOE の利用のためには必須ではない)。

(8) ドメインコントローラ

Windows ドメインの管理を行う。OS は Windows Server 2003 (SP1)を使用する。

(9) SeP クライアント

TOE がインストールされ、一般利用者が利用する。LAN から切り離して、社外で利用されることがある。管理者は、一般利用者が管理者権限で利用できないように Windows の設定を行っている。

必要システム

(1) SeP サーバ

・ ハードウェア

CPU 1GHz 以上(2GHz 以上推奨)

メモリ 512MB 以上(2GB以上推奨)

HDD インストール: 850MB 以上の空き容量
別途履歴保存用の空き容量が必要
(クライアント 1 台当り 150～400KB/日を目安)

・ OS

Windows Server 2008, Enterprise Edition (SP1) 32bit 版

(2) SeP クライアント

・ ハードウェア

CPU 1GHz 以上

メモリ 1GB 以上

HDD 16GB 以上の空き容量
履歴保存用の空き容量が必要
(モバイルで使用する場合は 150～400KB/日を目安)

・ OS

Windows 7 Enterprise 32bit 版

1.5 TOE 記述

1.5.1 TOE の物理的範囲

TOE の物理的範囲を図 1-2 の青太枠に示す。

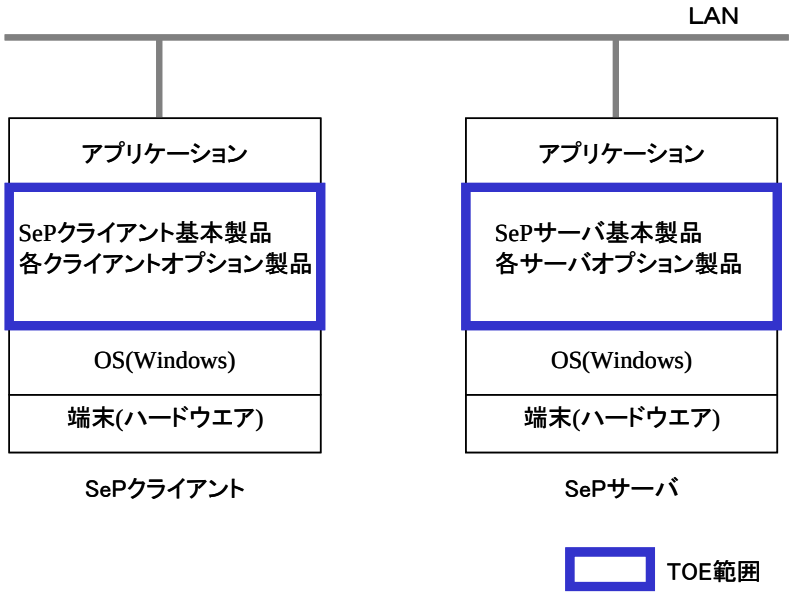

図 1-2. TOE のコンポーネント

各マシンにおける TOE のソフトウェアコンポーネントは以下の通りである。図 1-2 において、以下に示す TOE のソフトウェアコンポーネント以外のハードウェアおよびソフトウェアコンポーネントは TOE の範囲外である。

(1) SeP サーバ

セキュリティプラットフォーム サーバ ベーシック evolution /SV
(サーバ設定ツール、動作管理ツールを含む)
セキュリティプラットフォーム トレーサオプション
セキュリティプラットフォーム サーバ イントラネットオプション
セキュリティプラットフォーム サーバ エンクリプションオプション
セキュリティプラットフォーム サーバ ストレージエンクリプションオプション

(2) SeP クライアント

セキュリティプラットフォーム クライアント ベーシック evolution /SV
セキュリティプラットフォーム クライアント イントラネットオプション
セキュリティプラットフォーム クライアント エンクリプションオプション
セキュリティプラットフォーム クライアント ストレージエンクリプションオプション

TOE を構成するガイダンス文書を表1-2 に示す。本 TOE のガイダンスは全て管理者用である。

表1-2 TOE を構成するガイダンス文書

ガイダンス文書名
SeP マニュアル for ベーシック 第二十八版
SeP マニュアル ベーシック 別冊 1 SeP 正規表現 第一版
SeP マニュアル ベーシック 別冊 2 監視除外アプリケーション履歴機能 第三版
SeP マニュアル ベーシック 別冊 3 履歴絞込み機能 第二版
SeP マニュアル ベーシック 別冊 4 ファイル日時保持機能 第一版
SeP マニュアル ベーシック 別冊 5 SeP モジュール保護強化機能 第三版
SeP マニュアル ベーシック 別冊 6 暗号化ファイルの拡張子及びアイコンの変換 第三版
SeP マニュアル ベーシック 別冊 7 メール添付時 RTF/ZIP ファイル埋め込み機能 第三版
SeP マニュアル ベーシック 別冊 8 NAT 対応(ポートフォワード環境向け) 第一版
SeP マニュアル ベーシック 別冊 9 監視除外継承機能 第一版
SeP マニュアル ベーシック 別冊 10 AES 対応 第一版
SeP マニュアル ベーシック 別冊 11 暗号機能の作業フォルダ指定機能 第一版
SeP マニュアル ベーシック 別冊 12 マシン指定 Windows モード機能 第二版
SeP マニュアル ベーシック 別冊 13 Windows モードで動作するファイルのセキュリティ属性を管理しない機能 第二版
SeP マニュアル ベーシック 別冊 14 Office2007 対応 第二版
SeP マニュアル ベーシック 別冊 15 SeP クライアントアップデート機能 第二版
SeP マニュアル ベーシック 別冊 16 履歴データの暗号強化機能 第一版
SeP マニュアル ベーシック 別冊 17 ファイルサイズ履歴出力機能 第一版
SeP マニュアル ベーシック 別冊 18 アプリケーション管理制限機能 第二版
SeP マニュアル ベーシック 別冊 19 監視除外アプリケーションでのカプセルファイルオープン機能 第二版
SeP マニュアル ベーシック 別冊 20 圧縮(LZH 形式)フォルダの使用制限機能 第一版
SeP マニュアル ベーシック 別冊 21 クライアント蓄積履歴破棄機能 第一版
SeP マニュアル ベーシック 別冊 22 アクティブウインドウ履歴出力機能 第三版
SeP マニュアル ベーシック 別冊 23 管理監査ログ出力機能 第二版
SeP マニュアル ベーシック 別冊 24 印刷ジョブ履歴出力機能 第二版
SeP マニュアル for ベーシック evolution /SV 第二十六版
SeP マニュアル ベーシック evolution /SV 別冊 1 クリップボード動作指定アプリケーション 第四版
SeP マニュアル ベーシック evolution /SV 別冊 2 オフライン SV 暗号・復号設定 第二版
SeP マニュアル ベーシック evolution /SV 別冊 3 暗号化ファイルシステム(EFS)対応 第二版
SeP マニュアル ベーシック evolution /SV 別冊 4 添付ファイル操作で信頼領域とするアプリケーション指定

ガイダンス文書名
第八版
SeP マニュアル ベーシック evolution /SV 別冊 5 Write 制限機能 第九版
SeP マニュアル ベーシック evolution /SV 別冊 6 リリース形式固定/ 選択フォルダ 第十四版
SeP マニュアル ベーシック evolution /SV 別冊 7 自走式暗号ファイル・カプセル化ファイルの SV 暗号化 第一版
SeP マニュアル ベーシック evolution /SV 別冊 8 exe ファイルの添付時 SV 暗号化 第一版
SeP マニュアル ベーシック evolution /SV 別冊 9 画面キャプチャーの SV 暗号化 第一版
SeP マニュアル ベーシック evolution /SV 別冊 10 CD/DVD ライティングソフトの SV 機能 第六版
SeP マニュアル ベーシック evolution /SV 別冊 11 リモート信頼領域判定除外マシン指定機能 第一版
SeP マニュアル ベーシック evolution /SV 別冊 12 SV 禁止機能 第一版
SeP マニュアル ベーシック evolution /SV 別冊 13 圧縮フォルダの SV 機能対応 第二版
SeP マニュアル ベーシック evolution /SV 別冊 14 SV 暗号ファイルの属性継承を Windows 準拠とする機能 第一版
SeP マニュアル ベーシック evolution /SV 別冊 15 非信頼領域(同ドライブ)保存操作時 SV 機能 第三版
SeP マニュアル ベーシック evolution /SV 別冊 16 非信頼領域(同ドライブ)間クリップボード禁止機能 第一版
SeP マニュアル ベーシック evolution /SV 別冊 17 メール転送時 SV 化機能 第四版
SeP マニュアル ベーシック evolution /SV 別冊 18 USB の接続制限機能/接続・切断履歴出力機能 第四版
SeP マニュアル for イントラネットオプション 第八版
SeP マニュアル for イントラネットオプション 別冊 1 Netscape7.1Navigator セキュリティ情報未取得時の動作 第一版
SeP マニュアル for イントラネットオプション 別冊 2 セキュリティタグ機能の無効化 第一版
SeP マニュアル for イントラネットオプション 別冊 3 アップロード履歴出力機能 第二版
SeP マニュアル for イントラネットオプション 別冊 4 監視 Web ページ機能の一般 Web メール対応 第二版
SeP マニュアル for イントラネットオプション 別冊 5 SharePoint 対応 第三版
SeP マニュアル for イントラネットオプション 別冊 6 HTTP リクエスト制限機能 第二版
SeP マニュアル for トレーサオプション 第十一版
SeP マニュアル for トレーサオプション 別冊 1 収集機能強化 第一版
SeP マニュアル for トレーサオプション 別冊 2 エラーログ出力 第二版
SeP マニュアル for トレーサオプション 別冊 3 時刻単位指定機能 第一版
SeP マニュアル for エンクリプションオプション 第九版
SeP マニュアル for エンクリプションオプション 別冊 1 自走式暗号機能 第六版
SeP マニュアル for エンクリプションオプション 別冊 2 ZIP ファイル化機能 第三版
SeP マニュアル for ストレージエンクリプションオプション 第九版

ガイダンス文書名
SeP マニュアル for ストレージエンクリプションオプション 別冊 1 ストレージ暗号機能(フォルダ・ディレクトリ暗号、状態表示、履歴出力) 第一版
SeP マニュアル for ストレージ暗号復号ツール 第二版
セキュリティプラットフォームマニュアル 追加・更新・削除履歴一覧 2010 年 3 月 5 日
ご注意・制限事項 第十版
セキュアな運用ガイダンス 第 2.06 版
ご注意(Windows XP SP2 以上の環境でセキュリティプラットフォームをご使用する際のご注意) 2010 年 3 月 5 日
ご注意(セキュリティプラットフォームストレージエンクリプションオプションご使用のお客様へ) 2007 年 1 月 31 日
ご注意(セキュリティプラットフォームストレージエンクリプションオプションご使用のお客様へ 暗号化(復号)中の電源管理について) 2009 年 11 月 18 日
ご注意(セキュリティプラットフォームストレージエンクリプションオプションご使用のお客様へ デュアルブートのマシンをご使用の場合について) 2009 年 11 月 18 日
ご注意(セキュリティプラットフォーム履歴データの暗号強化機能をご使用のお客様へ) 2007 年 6 月 25 日
ご注意(セキュリティプラットフォームリリース形式選択フォルダ機能をご使用のお客様へ) 2008 年 3 月 4 日
お願い(ファイルマネジャーワンをご使いのお客様へ) 2005 年 7 月 11 日
内容物確認リスト 第 1.04 版

1.5.2 TOE の論理的範囲

TOE の論理的範囲を図 1-3 の青太枠に示す。

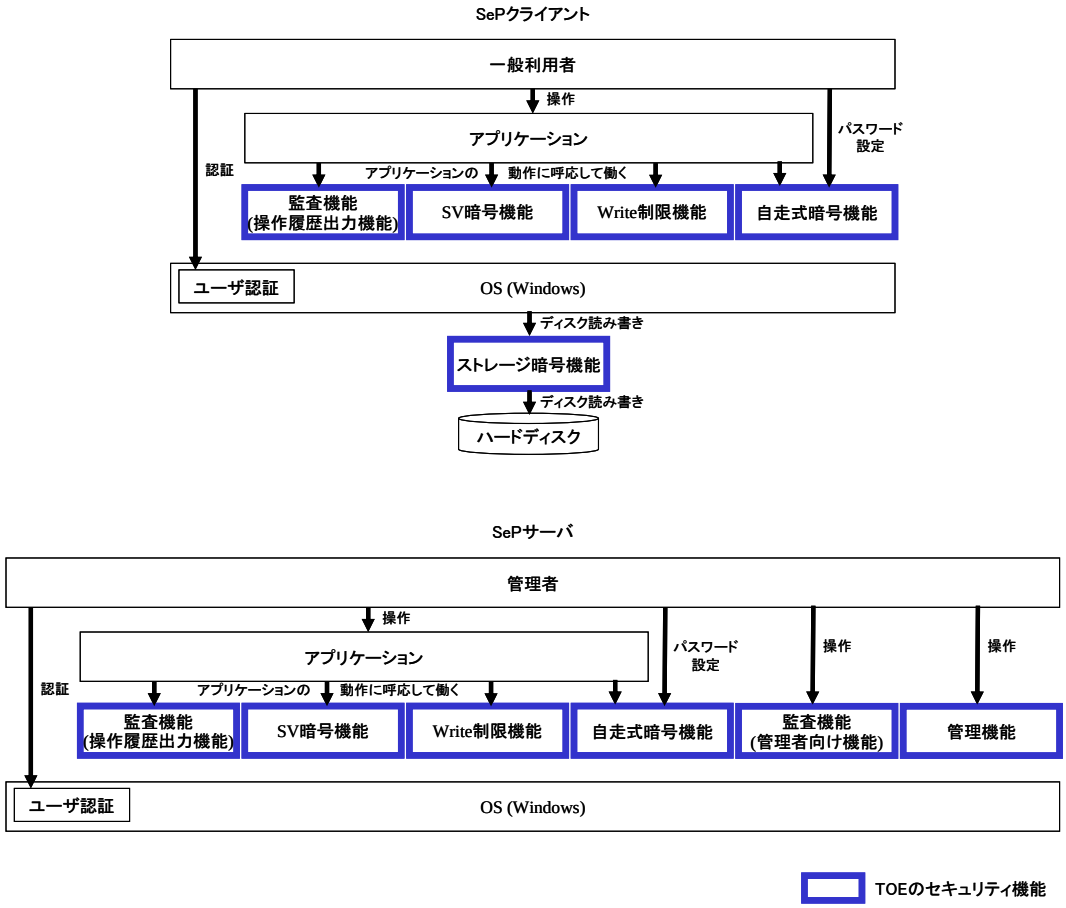

図 1-3　TOE 論理的範囲

SeP クライアントでは、監査機能(操作履歴出力機能)、SV 暗号機能、Write 制限機能、自走式暗号機能、ストレージ暗号機能が動作する。監査機能(操作履歴出力機能)、SV 暗号機能、Write 制限機能、自走式暗号機能は一般利用者が操作するアプリケーションの動作に呼応して動作する。一般利用者は自走式暗号ファイルを復号するためのパスワードを設定する。ストレージ暗号機能は OS がセクタ単位でハードディスクにアクセスする際に働く。なお、利用者のユーザ認証は Windows ドメインのユーザ認証による。

SeP サーバでは、ストレージ暗号機能を除く SeP クライアント機能に加え、管理者が利用する監査機能(管理者向け機能)、管理機能が動作する。

1.5.2.1 TOE の利用者

TOE に関連する利用者とその役割を次に記述する。

(1) 管理者

管理者は、TOE のインストールを行う。SeP サーバで、管理機能を利用して TOE の管理、および監査機能(管理者向け機能)を用いて操作履歴の管理を行う。各種サーバの管理を行う。

(2) 一般利用者

一般利用者は、SeP クライアントにおいてアプリケーションを用いて保護資産に対して操作を行う。

1.5.2.2 TOE 保護資産

一般利用者が業務で利用するクライアントマシンおよびファイルサーバマシン上のデータ。

1.5.2.3 TOE が提供する機能

図 1-3 に示す TOE のセキュリティ機能について以下に説明する。

TOE のセキュリティ機能の内、一般利用者が意識的に利用するのは、自走式暗号機能のみである。他の機能(SV 暗号機能、Write 制限機能、ストレージ暗号機能、監査機能(操作履歴出力機能))は、一般利用者がアプリケーションを操作した際に、アプリケーションの動作に呼応して働くものであり、一般利用者が直接意識して利用するものではない。

一般利用者および管理者がマシンを利用する際のユーザ認証は、Windows ドメインのユーザ認証による。

社外ネットワークからのアタックは、ファイアウォールやウイルス対策ソフトなどによって予防されているため、これらローカルハードディスクやファイルサーバ上に存在する限りにおいては、外部からのアタックによってファイルが漏洩する恐れはない。

一般利用者は、Windowsドメイン上のクライアントマシンで操作し、ローカルハードディスクおよびファイルサーバ上のファイルを利用して業務を行う。業務上、一般利用者はファイルを外部媒体(USB メモリ、FD など)やメールやインターネットなどの通信手段を利用して社内の他の一般利用者や他社に提供する。つまり、保護資産は他者に渡される際に、信頼領域から非信頼領域へ持ち出される。一般のマシン環境においては、一般利用者がファイルをコピーした外部媒体を紛失したり、ファイルを添付したメールを誤送したりすることにより情報漏洩が発生する恐れがある。

(1)SV 暗号機能により、一般利用者がファイルを信頼領域から非信頼領域に持ち出した際(例えば、外部媒体へのコピーやメールへの添付、Web ページへの添付)に、ファイルを強制的かつ自動的に暗号化する。反対に、この暗号ファイル(SV 暗号ファイル)は、信頼領域に戻すことによってのみ平文ファイルに戻すことができる。SV 暗号ファイルの復号は、非信頼領域から信頼領域

に戻した際に強制的かつ自動的に行われる。本機能により、一般利用者は、社内の他の利用者に通信手段や外部媒体を従来通り利用して、ファイルを安全に提供することができる。一方、社外においては、暗号ファイルの内容を閲覧することは不可能であるため、万一ファイルを誤送したり、ファイルがコピーされた外部媒体を紛失したりしても情報漏洩を防ぐことができる。なお、(2)Write 制限機能により、非信頼領域に持ち出すために利用されるアプリケーションが限定される。また、Web ページに対しては URL によってファイルの添付が禁止され、データをメールまたは信頼領域以外の Web ページにペーストすることが禁止される。

(1)SV 暗号機能が働いていると、閲覧可能な状態で社外にファイルを提供することができない。一般利用者は、正当な業務として閲覧可能な状態で社外にファイルを提供する必要がある場合、そのファイルを管理者がリリースフォルダと定義したフォルダに一旦入れることによって、それが可能になる。一般利用者が、リリースフォルダを経由して社外にファイルを提供する際に、受け取り手がパスワードにて復号可能な暗号化をファイルに施すことが強制される((3)自走式暗号機能)。これにより、ファイルの誤送などにより本来の提供先以外にファイルが渡り情報が漏れることを防ぐことができる。

一般利用者は、正当な業務としてクライアントマシンを LAN から切り離して社外で利用することがある。一般利用者は、社外でクライアントマシンを紛失し、これを取得した悪意の第三者がハードディスクを物理的に抜き取り、第三者のマシンに接続してその内容を閲覧することにより、情報漏洩が発生する恐れがある。これに対し、(4)ストレージ暗号機能により、TOE が稼動していないマシンでは、ハードディスクの内容を閲覧できないようにできる。

なお、TOE がインストールされたマシンにおける操作は、(5)監査機能により、全て記録される。これにより、管理者は、リリースフォルダを経由して、どのファイルが、いつ、だれによって閲覧可能な状態で外部に提供されたかを含め、一般利用者のクライアントでの操作について把握することができる。

以下に TOE の各セキュリティ機能について個別に説明する。

(1) SV 暗号機能(SeP サーバ、SeP クライアント共通)

一般利用者が保護資産を外部へ持ち出すことを強制的に制限する機能である。保護資産が存在する信頼領域から非信頼領域への許可されたファイル操作の際に、ファイルを自動的かつ強制的に暗号化する。暗号化されたファイル(SV 暗号ファイル)は、信頼領域に戻されると自動的に復号される。なお、Web ページに対しては、URL によってファイルの添付を禁止し、信頼領域のデータをメールまたは信頼領域以外の Web ページにペーストすることも禁止する。

(2) Write 制限機能(SeP サーバ、SeP クライアント共通)

非信頼領域に持ち出すためのアプリケーションを限定する機能である。本 ST では、持ち出

しに利用できるアプリケーションを、Explorer、Outlook2007(SP2)、InternetExplorer8 に限定する。

(3) 自走式暗号機能(SeP サーバ、SeP クライアント共通)

一般利用者が正規の業務として保護資産を社外へ提供する必要がある場合、対象ファイルをパスワードにより暗号化(自走式暗号化)できる機能である。これにより、提供時の誤送などによる情報漏洩を防止できる。一般利用者が、ファイルを社外に提供する際は、管理者が定義したリリースフォルダにファイルを一旦入れ、そこから外部媒体にコピーしたり、メールに添付したりする。リリースフォルダからファイルを出す際に、パスワード入力パネルが強制的に表示され、パスワードを設定することにより自走式暗号ファイルに変換される。

(4) ストレージ暗号機能(SeP クライアント)

セクタ単位でハードディスクを暗号化する機能である。初期暗号化完了後は、OS からのハードディスク上のデータの読み込み時にデータを復号し、書き込み時に暗号化する。保護資産が存在するマシンの盗難・置き忘れ対策となる。

(5) 監査機能

・操作履歴出力機能(SeP サーバ、SeP クライアント共通)

SeP サーバおよび SeP クライアントでのアプリケーション操作を操作履歴として出力し、一定のタイミングで SeP サーバへ操作履歴をアップロードする機能である。

・管理者向け機能(SeP サーバ)

管理者が SeP サーバにて蓄積されている操作履歴を収集し、CSV 形式のファイルに出力する機能である。本機能により、管理者は、一般利用者が保護資産に対して行った操作を後に把握することが可能である。また、サーバ設定ツールの設定履歴も後に把握することができる。

(6) 管理機能(SeP サーバ)

管理者が SeP サーバで利用可能な機能である。管理者は、サーバ設定ツールを用いて、SeP の機能の設定を行う。また、管理者は、動作管理ツールを用いて、SeP クライアントの TOE の機能(ストレージ暗号機能を除く)を停止・再開することができる。

2 適合主張

本章では、CC 適合主張、PP 主張、パッケージ主張及び適合根拠について記述する。

2.1 CC 適合主張

本 ST は、以下の通り CC 適合を主張する。
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 2006 年 9 月 バージョン 3.1 改訂第 1 版(翻訳第 1.2 版)
パート 2:セキュリティコンポーネント 2007 年 9 月 バージョン 3.1 改訂第 2 版(翻訳第 2.0 版)
パート 3:セキュリティ保証コンポーネント 2007 年 9 月 バージョン 3.1 改訂第 2 版(翻訳第 2.0 版)
CC パート 2 適合
CC パート 3 適合

2.2 PP 主張

この ST が適合している PP はない。

2.3 パッケージ主張

本 ST は、以下の通りパッケージ適合を主張する。
パッケージ: EAL3 適合

2.4 適合根拠

本 ST は PP 適合を主張していないので、PP 適合根拠はない。

3 セキュリティ課題定義

本章では、脅威、組織のセキュリティ方針および前提条件について記述する。

3.1 脅威

TOE の脅威エージェントの考察は以下のとおりである。

管理者は、信頼できる人物であり、TOE の利用に関して不正を行うことはない。一方、一般利用者は、悪意をもって保護資産を持ち出したり、TOE を攻撃したりすることは考えられないが、クライアントマシンの操作において過失を行うことが考えられる。

サーバマシンは、社内 LAN に接続した社内のみでの使用に限定される。一方クライアントマシン及び外部媒体は、社内での使用以外に社外に持ち出されることもある。

社外に持ち出されたクライアントマシン及び外部媒体、社外に送信されたファイルは、紛失や誤送などの過失により、第三者により不正に利用されることが考えられる。

T.USER_ERROR（一般利用者の過失）

保護資産を一般利用者が正当な相手に提供する際に、一般利用者による保護資産が入った外部媒体の紛失、または保護資産の誤送信により第三者がその情報を取得し、情報漏洩が発生すること。

T.STOLEN（第三者による盗み）

保護資産を一般利用者が正当な相手に提供する際に、第三者が外部媒体を盗む、または通信回線を盗聴することによりその情報を取得し、情報漏洩が発生すること。

T.LOST_PC（クライアントマシンの紛失）

第三者がモバイルのクライアントマシンのハードディスクを物理的に抜き取り、その内容を読み取ることにより、情報漏洩が発生すること。

3.2 組織のセキュリティ方針

なし。

3.3 前提条件

前提条件を以下に示す。

A.MANAGE_SAFE_PLACE（サーバの安全な設置）

サーバマシンに物理的にアクセスしうるのは管理者のみである。また、サーバマシンにログオンし、管理上の操作を行えるのは管理者のみである。

A.USER_RESTRICT（利用者の制限）

第三者は社内に立ち入ることはできない。

A.CLIENT_MACHINE（クライアントマシンの管理）

一般利用者が利用するクライアントマシンは、管理者により管理されており、全て TOE がインストールされる。一般利用者は、管理者の管理外のクライアントマシンを社内で利用することはできない。

A.USER_AUTHENTICATION（利用者の認証）

あるユーザアカウントでクライアントマシンにログオンし、操作できるのはそのユーザアカウントの正当な利用者のみである。

A.UNJUST_SOFTWARE（不正ソフトウェア対策）

クライアントマシンおよびサーバマシンには、ウイルス対策ソフトウェアが導入されるとともに、ウイルス対策ソフトウェアのパターンファイルや、OS のセキュリティ対策用修正ソフトウェアが適切に適用される。

A.NETWORK（ネットワーク環境）

社内 LAN には外部ネットワークから不正にアクセスされない。また、社内 LAN と外部ネットワーク間はファイル転送可能なプロトコルとしてSMTPとHTTP/HTTPSプロトコルのみを双方向に許可する。

A.OPERATOR_MANAGEMENT（管理者の管理）

管理者は、信頼できる者であり、不正な操作を行なわない。

4 セキュリティ対策方針

本章では、TOE のセキュリティ対策方針、運用環境のセキュリティ対策方針及びセキュリティ対策方針根拠について記述する。

4.1 TOE のセキュリティ対策方針

TOE のセキュリティ対策方針を以下に示す。

O.ENCRYPTION(提供ファイルの暗号化)

TOE は、非信頼領域に持ち出すためのアプリケーション、持ち出し操作を限定し、正当な受け取り手のみが閲覧可能となるように SV 暗号もしくは自走式暗号で提供ファイルを暗号化しなければならない。さらに自走式暗号の場合は、管理者が定めた品質尺度のパスワードが設定されるようにチェックしなければならない。また、TOE は非信頼領域への保護資産の許可されていない持ち出しの試行や、非信頼領域への保護資産の許可された持ち出し行為を管理者が監査できるようにしなければならない。

O.DISC_ ENCRYPTION(ハードディスクの暗号化)

TOE は、クライアントマシンのハードディスクを暗号化しなければならない。また、TOE はクライアントマシンのハードディスクの暗号化状態を管理者が監査できるようにしなければならない。

4.2 運用環境のセキュリティ対策方針

運用環境のセキュリティ対策方針を以下に示す。

OE.MANAGE_PC_PLACE(サーバマシンの安全な設置)

管理者は、管理者のみが入室可能なように入退室管理された室内にサーバマシンを設置しなければならない。また、管理者は、管理者のみがサーバマシンにログオンできるようにユーザアカウントの管理をしなければならない。管理者は、サーバマシンにアクセスするためのパスワードを記憶し、他人に漏らしてはならない。管理者は、パスワードを推測・解析されにくい設定にし、適切な間隔で変更しなければならない。

OE.USER_RESTRICT(利用者の制限)

組織の責任者は、社屋を入退館管理し、第三者が入館できないようにしなければならない。

OE.CLIENT_MACHINE(クライアントマシンの管理)

管理者は、一般利用者が利用するクライアントマシンを TOE がインストールされた状態にして

支給する。また、他のマシンの持ち込みを制限する社内規定などを設けて、他のマシンは社内 LAN にアクセスできないようにしなければならない。

OE.USER_AUTHENTICATION（利用者の認証）

管理者は Windows ドメインを構築し、Windows のドメインユーザアカウントにより利用者の識別認証が行われるようにしなければならない。また、管理者は、一般利用者に対して以下の指導をしなければならない。

- クライアントマシンにアクセスするためのパスワードを記憶して、他人に漏らさない。
- パスワードを推測・解析されにくい設定にし、適切な間隔で変更する。
- 離席する場合は、ログオフするか、スクリーンをロックする。

OE.UNJUST_SOFTWARE（不正ソフトウェア対策）

管理者は、サーバマシンにウイルス対策ソフトウェアをインストールし、ウイルスパターンファイルを常に最新に更新しなければならない。また、管理者は、OS のセキュリティ対策修正ソフトウェアを適切に適用しなければならない。管理者は、一般利用者がクライアントマシンについて同様の対策を行うよう一般利用者を指導しなければならない。

OE.NETWORK（ネットワーク環境）

管理者は、外部ネットワークからは許可された通信のみが社内 LAN に到達するように、また、社内 LAN と外部ネットワーク間はファイル転送可能なプロトコルとして SMTP と HTTP/HTTPS プロトコルのみを双方向に許可するように、適切にファイアウォールを設定しなければならない。

OE.OPERATOR_MANAGEMENT（管理者の管理）

組織の責任者は、不正を行わない信頼できる管理者が選任されるようにしなければならない。また、組織の責任者は、管理者が正しく TOE を運用できるように教育を受けさせなければならない。

OE.INFORM_PASSWORD（パスワードの伝達）

正当な業務として社外の相手にデータファイルを提供する際に、送り手となる一般利用者が、受け取り手がそのファイルの閲覧に必要なパスワードを、そのファイルとは別に確実に正しい相手に伝達するように、管理者は一般利用者を指導しなければならない。

OE.LOG_MANAGE（ログの管理）

管理者は、操作履歴の収集を行うために必要なハードディスクの空き容量が常に確保されるよう、定期的に操作履歴の収集・バックアップを行わなければならない。また、管理者は、SeP クライアントマシンから一定期間内に操作履歴がアップロードされるよう、一般利用者が SeP クライアント

マシンをLANから切り離して使用する場合には定期的にLANに接続するように指導しなければならない。

4.3 セキュリティ対策方針根拠

セキュリティ対策は、本章で規定した脅威に対抗するためのものである。あるいは、TOE の前提条件と組織のセキュリティ方針を実現するためのものである。セキュリティ対策方針と対抗する脅威及び対応する組織のセキュリティ方針及び前提条件の対応関係を表 4-1 に示す。

表 4-1 セキュリティ対策方針とセキュリティ課題定義の対応関係

	O.ENCRYPTION	O.DISC_ENCRYPTION	OE.MANAGE_PC_PLACE	OE.USER_RESTRICT	OE_CLIENT_MACHINE	OE_USER_AUTHENTICATION	OE_UNJUST_SOFTWARE	OE.NETWORK	OE.OPERATOR_MANAGEMENT	OE.INFORM_PASSWORD	OE.LOG_MANAGE
T.USER_ERROR	×									×	×
T.STOLEN	×									×	×
T.LOST_PC		×									×
A.MANAGE_SAFE_PLACE			×								
A.USER_RESTRICT				×							
A.CLIENT_MACHINE					×						
A.USER_AUTHENTICATION						×					
A.UNJUST_SOFTWARE							×				
A.NETWORK								×			
A.OPERATOR_MANAGEMENT									×		

表 4-1 により、各セキュリティ対策方針は1つ以上の脅威、及び前提条件に対応している。

次に、各脅威がセキュリティ対策方針で対抗できること、また前提条件がセキュリティ対策方針で実現できることを説明する。

○脅威

脅威に対して想定される全ての攻撃方法に対抗する対策方針の正当化を以下に示す。

T.USER_ERROR(一般利用者の過失)

この脅威は、一般利用者が過失(外部媒体紛失、誤送信)を行うことにより保護資産を第三者が取得し情報漏洩が発生することである。この脅威に有効な対抗策について以下に述べる。

a. 保護資産が入った外部媒体を一般利用者が正当な受け取り手に提供する経路においてこれを紛失し、それを入手した第三者が情報を暴露する

この脅威には、外部媒体に保護資産を格納しないように制御する、または正当な受け取り手のみが閲覧可能な形式で外部媒体に格納することで対抗することができる。

O.ENCRYPTION は、非信頼領域に持ち出せるアプリケーション、持ち出し操作を限定し、許可されたアプリケーションおよび持ち出し操作では外部媒体に保存される保護資産を SV 暗号もしくは自走式暗号により暗号化して、正当な受け取り手のみが暗号化ファイルを復号できるようにし、さらにパスワードの入力が必要な自走式暗号の場合は、管理者が定めた品質尺度のパスワードが設定されるようにチェックし、また、非信頼領域への保護資産の許可されていない持ち出しの試行や、非信頼領域への保護資産の許可された持ち出し行為を管理者が監査できるようにする対策方針である。OE.INFORM_PASSWORD は、受け取り手が自走式暗号ファイルを復号するために必要なパスワードを、送り手が自走式暗号ファイルとは別に確実に受け取り手に知らせるようにする対策方針である。OE.LOG_MANAGE は、監査ログが SeP サーバに収集され、管理者が常に監査を行うことができるようにする対策方針である。

従って、外部媒体に保護資産を格納しないように制御するアプリケーション、持ち出し操作の限定(O.ENCRYPTION)、正当な受け取り手のみが閲覧可能な形式で外部媒体に格納する SV 暗号(O.ENCRYPTION)、自走式暗号(O.ENCRYPTION / OE.INFORM_PASSWORD)、これらの機能の監査(O.ENCRYPTION / OE_LOG_MANAGE)の組み合わせにより、この脅威を十分に軽減することができる。

b. 一般利用者が正当な受け取り手に保護資産を送信する際に、誤って第三者に送信し、第三者がその情報を暴露する

この脅威には、保護資産を送信しないように制御する、または正当な受け取り手のみが閲覧可能な形式で送信することで対抗することができる。

O.ENCRYPTION は、非信頼領域に持ち出せるアプリケーション、持ち出し操作を限定し、許可されたアプリケーション、および持ち出し操作では送信される保護資産を SV 暗号もしくは自走式暗号により暗号化して、正当な受け取り手のみが暗号化ファイルを復号できるように

し、さらにパスワードの入力が必要な自走式暗号の場合は、管理者が定めた品質尺度のパスワードが設定されるようにチェックし、また、非信頼領域への保護資産の許可されていない持ち出しの試行や、非信頼領域への保護資産の許可された持ち出し行為を管理者が監査できるようにする対策方針である。OE.INFORM_PASSWORD は、受け取り手が自走式暗号ファイルを復号するために必要なパスワードを、送り手が自走式暗号ファイルとは別に確実に受け取り手に知らせるようにする対策方針である。OE.LOG_MANAGE は、監査ログが SeP サーバに収集され、管理者が常に監査を行うことができるようにする対策方針である。

従って、保護資産を送信しないように制御するアプリケーション、持ち出し操作の限定（O.ENCRYPTION）、正当な受け取り手のみが閲覧可能な形式で送信する SV 暗号（O.ENCRYPTION）、自走式暗号（O.ENCRYPTION / OE.INFORM_PASSWORD）、これらの機能の監査（O.ENCRYPTION / OE_LOG_MANAGE）の組み合わせにより、この脅威を十分に軽減することができる。

以上、a、b いずれの攻撃方法に対抗することは、T.USER_ERROR に対抗することである。従って、それぞれの攻撃方法に対する対抗策として該当する、O.ENCRYPTION、OE.INFORM_PASSWORD、および OE.LOG_MANAGE によって、T.USER_ERROR に対抗できる。

T.STOLEN（第三者による盗み）

この脅威は、一般利用者が正当な業務として保護資産を特定の受け取り手に提供する経路において、第三者が外部媒体を盗む、または通信回線を盗聴することにより情報漏洩が発生することである。この脅威に有効な対抗策について以下に述べる。

a. 保護資産が入った外部媒体を一般利用者が正当な受け取り手に提供する経路において、第三者が外部媒体を盗みその情報を暴露する

この脅威には、外部媒体に保護資産を格納しないように制御する、または正当な受け取り手のみが閲覧可能な形式で外部媒体に格納することで対抗することができる。

O.ENCRYPTION は、非信頼領域に持ち出せるアプリケーション、持ち出し操作を限定し、許可されたアプリケーションおよび持ち出し操作では外部媒体に保存される保護資産を SV 暗号もしくは自走式暗号により暗号化して、正当な受け取り手のみが暗号化ファイルを復号できるようにし、さらにパスワードの入力が必要な自走式暗号の場合は、管理者が定めた品質尺度のパスワードが設定されるようにチェックし、また、非信頼領域への保護資産の許可されていない持ち出しの試行や、非信頼領域への保護資産の許可された持ち出し行為を管理者が監査できるようにする対策方針である。OE.INFORM_PASSWORD は、受け取り手が自走式暗号ファイルを復号するために必要なパスワードを、送り手が自走式暗号ファイルとは別

に確実に受け取り手に知らせるようにする対策方針である。OE.LOG_MANAGE は、監査ログが SeP サーバに収集され、管理者が常に監査を行うことができるようにする対策方針である。

従って、外部媒体に保護資産を格納しないように制御するアプリケーションおよび持ち出し操作の限定(O.ENCRYPTION)、正当な受け取り手のみが閲覧可能な形式で外部媒体に格納する SV 暗号(O.ENCRYPTION)、自走式暗号(O.ENCRYPTION / OE.INFORM_PASSWORD)、これらの機能の監査(O.ENCRYPTION / OE_LOG_MANAGE)の組み合わせにより、この脅威を十分に軽減することができる。

b. 一般利用者が正当な受け取り手に保護資産を送信した際に、その経路において第三者が情報を盗聴し暴露する

この脅威には、保護資産を送信しないように制御する、または正当な受け取り手のみが閲覧可能な形式で送信することで対抗することができる。

O.ENCRYPTION は、非信頼領域に持ち出せるアプリケーション、持ち出し操作を限定し、許可されたアプリケーション、持ち出し操作では送信される保護資産を SV 暗号もしくは自走式暗号により暗号化して、正当な受け取り手のみが暗号化ファイルを復号できるようにし、さらにパスワードの入力が必要な自走式暗号の場合は、管理者が定めた品質尺度のパスワードが設定されるようにチェックし、また、非信頼領域への保護資産の許可されていない持ち出しの試行や、非信頼領域への保護資産の許可された持ち出し行為を管理者が監査できるようにする対策方針である。OE.INFORM_PASSWORD は、受け取り手が自走式暗号ファイルを復号するために必要なパスワードを、送り手が自走式暗号ファイルとは別に確実に受け取り手に知らせるようにする対策方針である。OE.LOG_MANAGE は、監査ログが SeP サーバに収集され、管理者が常に監査を行うことができるようにする対策方針である。
従って、保護資産を送信しないように制御するアプリケーション、持ち出し操作の限定(O.ENCRYPTION)、正当な受け取り手のみが閲覧可能な形式で送信する SV 暗号(O.ENCRYPTION)、自走式暗号(O.ENCRYPTION / OE.INFORM_PASSWORD)、これらの機能の監査(O.ENCRYPTION / OE_LOG_MANAGE)の組み合わせにより、この脅威を十分に軽減することができる。

以上、a、bいずれの攻撃方法に対抗することは、T.STOLEN に対抗することである。従って、それぞれの攻撃方法に対する対抗策として該当する、O.ENCRYPTION、OE.INFORM_PASSWORD、および OE.LOG_MANAGE によって、T.STOLEN に対抗できる。

T.LOST_PC(クライアントマシンの紛失)

この脅威は、第三者がハードディスクを物理的に抜き取り、その内容を読み取ることである。この脅威に有効な対抗策について以下に述べる。

a. 第三者がハードディスクを物理的に抜き取り、その内容を読み取る

この脅威には、ハードディスク内の保護資産をクライアントマシンの正当な利用者のみが読み取ることができるようにすることで対抗することができる。

O.DISC_ENCRYPTIONはハードディスク内のデータを暗号化して、クライアントマシンの正当な利用者のみが復号できるようにし、また、クライアントマシンのハードディスクの暗号化状態を管理者が監査できるようにする対策方針である。OE.LOG_MANAGE は、監査ログがSeP サーバに収集され、管理者が常に監査を行うことができるようにする対策方針である。

従って、クライアントマシンの正当な利用者のみが読み取ることができるようにするハードディスクの暗号化(O.DISC_ENCRYPTION)、この機能の監査(O.DISC_ENCRYPTION / OE.LOG_MANAGE)の組み合わせにより、この脅威を十分に軽減することができる。

以上、a の攻撃方法に対抗することは、T.LOST_PC に対抗することである。従って、それぞれの攻撃方法に対する対抗策として該当する、O.DISC_ENCRYPTION および OE.LOG_MANAGE によって、T.LOST_PC に対抗できる。

○前提条件

A.MANAGE_SAFE_PLACE(サーバの安全な設置)

この前提条件は、サーバマシンへのアクセスに関するものである。有効な対策方針について以下に述べる。

a. サーバマシンへの物理的アクセスの制限

サーバマシンに物理的にアクセスしうるのは管理者のみである。OE.MANAGE_PC_PLACE は、管理者のみが入室可能な室内に設置し、サーバマシンへの物理的アクセスを管理者のみに限定することである。従って、この方針に応じるための運用環境のセキュリティ対策方針としては、OE.MANAGE_PC_PLACE である。

b. サーバマシンへのログオンの制限

サーバマシンにログオンし、管理上の操作を行えるのは管理者のみである。OE.MANAGE_PC_PLACE は、管理者のみがパスワードを知りうるようにし、サーバマシン

へのログオンを管理者のみに限定することである。従って、この方針に応じるための運用環境のセキュリティ対策方針としては、OE.MANAGE_PC_PLACE である。

以上、上記 a、b に応じることは、A.MANAGE_SAFE_PLACE に応じることである。従って、それぞれの要求に応じる対抗策として該当する、OE.MANAGE_PC_PLACE の達成によって A.MANAGE_SAFE_PLACE が実現される。

A.USER_RESTRICT(利用者の制限)

この前提条件は、社内の立ち入りに関するものである。有効な対策方針について以下に述べる。

a. 第三者の社内への立ち入り制限

第三者は社内に立ち入ることはできない。OE.USER_RESTRICT は、社屋を入退館管理し、第三者が入館できないようにすることである。従って、この方針に応じるための運用環境のセキュリティ対策方針としては、OE.USER_RESTRICT である。

以上、上記 a に応じることは、A.USER_RESTRICT に応じることである。従って、それぞれの要求に応じる対抗策として該当する、OE.USER_RESTRICT の達成によって A.USER_RESTRICT が実現される。

A.CLIENT_MACHINE(クライアントマシンの管理)

この前提条件は、管理外のクライアントマシンの使用制限に関するものである。有効な対策方針について以下に述べる。

a. TOE のインストール

一般利用者が利用するクライアントマシンは、管理者により管理されており、全て TOE がインストールされる。OE.CLIENT_MACHINE は、一般利用者が利用するクライアントマシンを TOE がインストールされた状態にして支給することである。従って、この方針に応じるための運用環境のセキュリティ対策方針としては、OE.CLIENT_MACHINE である。

b. 管理外マシンの使用制限

一般利用者は、管理者の管理外のクライアントマシンを社内で利用することはできない。OE.CLIENT_MACHINE は、管理外のマシンの持ち込みを制限する社内規定などを設けて、管理外のマシンは社内 LAN にアクセスできないようにすることである。従って、この方針

に応じるための運用環境のセキュリティ対策方針としては、OE.CLIENT_MACHINE である。

以上、上記 a、b に応じることは、A.CLIENT_MACHINE に応じることである。従って、それぞれの要求に応じる対抗策として該当する、OE.CLIENT_MACHINE の達成によって A.CLIENT_MACHINE が実現される。

A.USER_AUTHENTICATION（利用者の認証）

この前提条件は、利用者の認証に関するものである。有効な対策方針について以下に述べる。

a. ログオンの制限

あるユーザアカウントでクライアントマシンにログオンできるのは、そのユーザアカウントの正当な利用者のみである。OE.USER_AUTHENTICATION は、Windows ドメインを構築し、正当な利用者のみがパスワードを知りうるようにし、クライアントマシンへのログオンを正当な利用者のみに限定することである。従って、この方針に応じるための運用環境のセキュリティ対策方針としては、OE.USER_AUTHENTICATION である。

b. ログオン中の他者の利用制限

クライアントマシンにログオンした状態でそのマシンを操作できるのは、そのユーザアカウントの正当な利用者のみである。OE.USER_AUTHENTICATION は、正当な利用者の離席後速やかに画面をロックするようにし、クライアントマシンの操作を正当な利用者のみに限定することである。従って、この方針に応じるための運用環境のセキュリティ対策方針としては、OE.USER_AUTHENTICATION である。

以上、上記 a、b に応じることは、A.USER_AUTHENTICATION に応じることである。従って、それぞれの要求に応じる対抗策として該当する、OE.USER_AUTHENTICATION の達成によって A.USER_AUTHENTICATION が実現される。

A.UNJUST_SOFTWARE（不正ソフトウェア対策）

この前提条件は、コンピュータウイルス及びセキュリティ対策用修正ソフトウェアに関するものである。有効な対策方針について以下に述べる。

a. ウイルス対策ソフトウェアの導入

サーバマシンおよびクライアントマシンに、ウイルス対策ソフトウェアを導入する。OE.UNJUST_SOFTWARE は、サーバマシンおよびクライアントマシンに、ウイルス対策ソフトウェアを導入することである。従って、この方針に応じるための運用環境におけるセキュリティ対策方針は、OE.UNJUST_SOFTWARE である。

b. パターンファイル、及びセキュリティ対策用修正ソフトウェアの適切な適用

ウイルス対策ソフトウェアのパターンファイル、及びセキュリティ対策用修正ソフトウェアの適用について、常に最新のものが適用される。OE.UNJUST_SOFTWARE は、常に最新のウイルス対策ソフトウェアのパターンファイル及びセキュリティ対策用修正ソフトウェアを適用することである。従って、この方針に応じるための運用環境におけるセキュリティ対策方針は、OE.UNJUST_SOFTWARE である。

以上、上記 a、b 全てに応じることは、A.UNJUST_SOFTWARE に応じることである。したがって、それぞれの要求に応じる対抗策として該当する、OE.UNJUST_SOFTWARE の達成によって A.UNJUST_SOFTWARE が実現される。

A.NETWORK（ネットワーク環境）

この前提条件は、ネットワーク環境の構築に関するものである。有効な対策方針について以下に述べる。

a. 社内 LAN と外部ネットワークとの接続の制限

社内 LAN と外部ネットワークとの接続は、外部ネットワークからの不正な通信を防ぎ、また、社内 LAN と外部ネットワーク間はファイル転送可能なプロトコルとして SMTP と HTTP/HTTPS プロトコルのみを双方向に許可する装置（ファイアウォール）を介して接続する。OE.NETWORK は、社内 LAN と外部ネットワークを外部ネットワークからの不正な通信を防ぐ装置（ファイアウォール）を介して接続し、社内 LAN と外部ネットワーク間はファイル転送可能なプロトコルとして SMTP と HTTP/HTTPS プロトコルのみを双方向に許可することである。従って、この方針に応じるための運用環境のセキュリティ対策方針は、OE.NETWORK である。

以上、上記の a に応じることは、A.NETWORK に応じることである。従って、それぞれの要求に応じる対抗策として該当する、OE.NETWORK の達成によって A.NETWORK が実現される。

A.OPERATOR_MANAGEMENT（管理者の管理）

この前提条件は、管理者の選任に関するものである。有効な対策方針について以下に述べる。

a. 信頼できる者の選任

管理者については、社員の中から選任され、その役割及び責任を良く理解し、職務に忠実で決して悪意を抱かない者とする。OE.OPERATOR_MANAGEMENT は、悪意を抱かない者を管理者に選任することである。従って、この方針に応じるための運用環境のセキュリティ対策方針は、OE.OPERATOR_MANAGEMENT である。

以上、上記 a に応じることは、A.OPERATOR_MANAGEMENT に応じることである。従って、それぞれの要求に応じる対抗策として該当する、OE.OPERATOR_MANAGEMENT の達成によって A.OPERATOR_MANAGEMENT が実現される。

5 拡張コンポーネント定義

5.1 拡張コンポーネント定義

本ST はCC パート2 及びCC パート3 に適合しているので、拡張コンポーネントはない。

6 セキュリティ要件

本章では、セキュリティ機能要件、セキュリティ保証要件及びセキュリティ要件根拠について記述する。機能要件を詳細化した箇所は下線で示す。

なお、本章で使用する用語の定義は、以下のとおりである。

表6-1. サブジェクトの用語定義

用語	定義
アプリケーション監視サブジェクト	一般利用者が操作したアプリケーションの動作を捕捉し、これを代行するTOEの処理部分

表6-2. 情報の用語定義

用語	定義
ファイル操作情報	ファイル操作に関する情報で、ファイル操作の対象となるデータ、ファイル操作を行うアプリケーション、ファイル操作先に関する情報を含む

表6-3. セキュリティ属性の用語定義

用語	定義
アプリケーション情報	アプリケーションを識別する情報
書き込み先のパス	ファイルのコピー、移動、保存先のNTFSまたはFATファイルシステムのパス、またはCD/DVD/ブルーレイディスクのドライブ
送信先情報	ファイルの送信先のIPアドレスと使用ポート
添付先URL	ファイルの添付先のURL
添付元のパス	ファイルの添付元のNTFSまたはFATファイルシステムのパス、またはCD/DVD/ブルーレイディスクのドライブ
ペースト先情報	データのペースト先のアプリケーションおよびURL

表6-4. その他の用語定義

用語	定義
マシン名	マシンのNetBIOS名
ファイル名	ファイル名

パス	絶対パスからファイル名を除いたもの
ウインドウタイトル	アプリケーションのウインドウのタイトル
アプリケーション名	アプリケーションのEXE名
操作	操作の種別を示す名称(暗号化の有無を含む)
ユーザ名	Windowsユーザアカウント
日時	年月日時分秒
備考	操作により異なる補足の情報

6.1 セキュリティ機能要件

本章では、CC パート 2 で規定されている機能要件コンポーネントを直接使用する。

○セキュリティ監査(FAU)

FAU_GEN.1 監査データ生成

下位階層: なし

依存性: FPT_STM.1高信頼タイムスタンプ

FAU_GEN.1.1 TSFは、以下の監査対象事象の監査記録を生成できなければならない:

a) 監査機能の起動と終了;

b) 監査の[選択: 最小、基本、詳細、指定なし: から**1**つのみ選択]レベルのすべての監査対象事象;及び

c) [割付: 上記以外の個別に定義した監査対象事象]。

[選択: 最小、基本、詳細、指定なし: から **1** つのみ選択]:指定なし
[割付: 上記以外の個別に定義した監査対象事象]:以下の通り

表 6-5. TOE の監査対象事象

機能要件	TOE の監査対象事象
FCS_COP.1	成功及び暗号操作の種別(※1)
FDP_IFF.1	持ち出し操作の拒否
FMT_SMF.1	サーバ設定ツールの起動と設定変更

※1 操作の種別:

SV 暗号の場合:暗号化時、「(SV-暗号)」と付記。

自走式暗号の場合:暗号化時、「(SV-リリース選択自走式暗号 OUT)」と付記。

ストレージ暗号の場合:初期暗号化時、「ストレージ暗号(開始)」、「ストレージ暗号(終了)」と記載。全復号時、「ストレージ復号(開始)」、「ストレージ復号(終了)」と記載。

FAU_GEN.1.2 **TSF**は、各監査記録において少なくとも以下の情報を記録しなければならない:

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報(該当する場合)、事象の結果(成功または失敗);及び

b) 各監査事象種別に対して、**PP/ST**の機能コンポーネントの監査対象事象の定義に基づいた、[割付: その他の監査関連情報] 。

[割付: その他の監査関連情報]:

FMT_SMF.1 のサーバ設定ツールの設定変更については、サーバ設定の設定内容。

FCS_COP.1、FDP_IFF.1、FMT_SMF.1 のサーバ設定ツールの起動については、マシン名、ファイル名、パス、ウィンドウタイトル、アプリケーション名、備考。

FAU_SAR.1 監査レビュー

下位階層: なし

依存性: FAU_GEN.1監査データ生成

FAU_SAR.1.1 **TSF**は、[割付: 許可利用者]が、[割付: 監査情報のリスト]を監査記録から読み出せるようにしなければならない。

[割付: 許可利用者]:管理者

[割付: 監査情報のリスト]:

FMT_SMF.1 のサーバ設定ツールの設定変更については、サーバ設定の設定内容、ユーザ名、日時。

FCS_COP.1、FDP_IFF.1、FMT_SMF.1 のサーバ設定ツールの起動については、マシン名、ファイル名、パス、ウィンドウタイトル、アプリケーション名、操作(持ち出し操作の拒否、暗号化の識別含む)、ユーザ名、日時、備考。

FAU_SAR.1.2 **TSF**は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しな

ければならない。

FAU_SAR.3 選択可能監査レビュー

下位階層: なし

依存性: FAU_SAR.1監査レビュー

FAU_SAR.3.1 **TSF**は、[割付: 論理的な関連の基準]に基づいて、FCS_COP.1、FDP_IFF.1、FMT_SMF.1のサーバ設定ツールの起動についての監査データの[割付:選択方法、及び/または 並べ替え方法]を適用する能力を提供しなければならない。

[割付: 論理的な関連の基準]: 下表の関連の基準
[割付: 割付:選択方法、及び/または 並べ替え方法]: 下表の方法

表 6-6. 監査データの選択方法および並び替え方法

関連の基準	方法
ユーザ別、マシン別	分類して出力
操作、日時	選択して出力

○暗号サポート(FCS)

FCS_CKM.1 暗号鍵生成

下位階層: なし

依存性: [FCS_CKM.2暗号鍵配付、または
FCS_COP.1暗号操作]
FCS_CKM.4暗号鍵破棄

FCS_CKM.1.1 **TSF**は、以下の[割付: 標準のリスト]に合致する、指定された暗号鍵生成アルゴリズム[割付: 暗号鍵生成アルゴリズム]と指定された暗号鍵長[割付: 暗号鍵長]に従って、暗号鍵を生成しなければならない。

[割付: 標準のリスト]:FIPS 140-2, Annex C

[割付: 暗号鍵生成アルゴリズム]:決定論的擬似乱数生成法

[割付: 暗号鍵長]:下表の暗号鍵長

表6-7. 暗号鍵生成における暗号鍵長

暗号操作のリスト	暗号鍵長
SV暗号ファイルの暗号化または復号	256bits
自走式暗号ファイルの暗号化または復号	256bits
ストレージ暗号の暗号化または復号	256bits

FCS_COP.1 暗号操作

下位階層: なし

依存性: [FDP_ITC.1セキュリティ属性なし利用者データインポート、または
FDP_ITC.2セキュリティ属性を伴う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

FCS_COP.1.1 **TSF**は、[割付: 標準のリスト]に合致する、特定された暗号アルゴリズム[割付: 暗号アルゴリズム]と暗号鍵長[割付: 暗号鍵長]に従って、[割付: 暗号操作のリスト]を実行しなければならない。

[割付: 標準のリスト]:FIPS 197

[割付: 暗号アルゴリズム]:下表の暗号アルゴリズム

[割付: 暗号鍵長]:下表の暗号鍵長

[割付: 暗号操作のリスト]:下表の暗号操作リスト

表6-8. 暗号操作の暗号アルゴリズムと暗号鍵長

暗号操作のリスト	暗号アルゴリズム	暗号鍵長
SV暗号ファイルの暗号化または復号	AES	256bits
自走式暗号ファイルの暗号化または復号	AES	256bits
ストレージ暗号の暗号化または復号	AES	256bits

○利用者データ保護(FDP)

FDP_IFC.1 サブセット情報フロー制御

下位階層: なし

依存性: FDP_IFF.1単純セキュリティ属性

FDP_IFC.1.1 TSFは、[割付: ***SFP***によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こすサブジェクト、情報及び操作のリスト]に対して[割付: 情報フロー制御***SFP***]を実施しなければならない。

[割付: ***SFP*** によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こすサブジェクト、情報及び操作のリスト]:
サブジェクト:アプリケーション監視サブジェクト
情報:ファイル操作情報
操作:持ち出し操作
[割付: 情報フロー制御 ***SFP***]:Write 制限 SFP

FDP_IFF.1 単純セキュリティ属性

下位階層: なし

依存性: FDP_IFC.1サブセット情報フロー制御
FMT_MSA.3静的属性初期化

FDP_IFF.1.1 TSFは、以下のタイプのサブジェクト及び情報セキュリティ属性に基づいて、[割付: 情報フロー制御***SFP***]を実施しなければならない。: [割付: 示された***SFP***下において制御されるサブジェクトと情報のリスト、及び各々に対応する、セキュリティ属性]

[割付: 情報フロー制御 ***SFP***]:Write 制限 SFP
[割付: 示された ***SFP*** 下において制御されるサブジェクトと情報のリスト、及び各々に対応する、セキュリティ属性]:
サブジェクト, 属性
アプリケーション監視サブジェクト, 許可(拒否)するアプリケーション情報のリスト、(非)信頼領域のリストまたは許可(拒否)する送信先情報のリスト

情報, 属性
ファイル操作情報, アプリケーション情報、書き込み先のパスまたは送信先情報または添付先

URL またはペースト先情報、添付元のパス

FDP_IFF.1.2 TSFは、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない：[割付：各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係]。

[割付：各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係]：

情報の属性とサブジェクトの属性を比較し、情報のアプリケーション情報が許可アプリケーション情報を示しているか、書き込み先のパスが信頼領域を示しているかまたは送信先情報が許可送信先情報を示している場合は情報フローを許可し、情報のアプリケーション情報が拒否アプリケーション情報を示しており、かつ、書き込み先のパスが非信頼領域を示しているかまたは送信先情報が拒否送信先情報を示している場合は情報フローを禁止する。この持ち出し操作に対し、サブジェクトの属性が未設定の場合は情報フローは許可される。

許可アプリケーションによる持ち出し操作が Web ページへの添付で、情報の添付先 URL が信頼領域(社内 URL)または非信頼領域(SV 化 URL)を示している場合は、情報フローを許可し、それ以外の場合は禁止する。この持ち出し操作に対し、サブジェクトの属性が未設定の場合は情報フローは禁止される。ただし、添付元のパスがリリースフォルダの場合、情報フローは許可される。

持ち出し操作が Web ページへのペーストで、情報のペースト先情報が信頼領域(社内 URL)を示している場合は、情報フローを許可し、それ以外の場合は禁止する。この持ち出し操作に対し、サブジェクトの属性が未設定の場合は情報フローは禁止される。

持ち出し操作がメールへのペーストの場合は、情報フローを禁止する。この持ち出し操作に対し、サブジェクトの属性が未設定の場合は情報フローは禁止される。

FDP_IFF.1.3 TSFは、[割付：追加の情報フロー制御***SFP***規則]を実施しなければならない。

[割付：追加の情報フロー制御 ***SFP*** 規則]：なし

FDP_IFF.1.4 TSFは、以下の規則、[割付：セキュリティ属性に基づいて情報フローを明示的に許可する規則]に基づいて、情報フローを明示的に許可しなければならない。

[割付：セキュリティ属性に基づいて情報フローを明示的に許可する規則]：なし

FDP_IFF.1.5 TSFは、以下の規則、[割付：セキュリティ属性に基づいて情報フローを明示的に拒否する規則]に基づいて、情報フローを明示的に拒否しなければならない。

[割付: セキュリティ属性に基づいて情報フローを明示的に拒否する規則]:なし

○識別と認証(FIA)

FIA_SOS.1 秘密の検証

下位階層: なし

依存性: なし

FIA_SOS.1.1 TSFは、秘密が[割付: 定義された品質尺度]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。

[割付: 定義された品質尺度]:管理者が設定した品質尺度(10-64 文字、英数混合)、使用可能文字:英字大文字([A-Z]26 文字), 英字小文字([a-z]26 文字),数字([0-9]10 文字)

○セキュリティ管理(FMT)

FMT_SMF.1 管理機能の特定

下位階層: なし

依存性: なし

FMT_SMF.1.1 TSFは、以下の管理機能を実行することができなければならない。:[割付: ***TSF***によって提供される管理機能のリスト]

[割付: ***TSF***によって提供される管理機能のリスト]:

- 管理者が SV 暗号機能、Write 制限機能、自走式暗号機能、監査機能(操作履歴出力機能)の停止／起動を実施する機能
- 管理者が TSF データ(SV 暗号機能の有効/無効、Write 制限機能の有効/無効、自走式暗号機能の有効/無効、リリースフォルダの定義、パスワードの長さの範囲、パスワードの英数混合の指定、ストレージ暗号機能の有効/無効)、セキュリティ属性(許可(または拒否)するアプリケーション情報、(非)信頼領域または許可(または拒否)する送信先情報)を問い合わせ／改変する機能
- 管理者が履歴データ、集積履歴データを削除する機能

表6-9. CC パート2「管理」の節との対応

機能要件	管理要件	TOE	妥当性
FAU_GEN.1	なし	なし	
FAU_SAR.1	監査記録に対して読み出しアクセス権のある利用者グループの維持(削除、改変、追加)	なし	Windows のユーザ管理によるため
FAU_SAR.3	なし	なし	
FCS_CKM.1	なし	なし	
FCS_COP.1	なし	なし	
FDP_IFC.1	なし	なし	
FDP_IFF.1	明示的なアクセスに基づく決定に使われる属性の管理	サーバ設定ツールにて、許可(拒否)アプリケーション情報、(非)信頼領域および許可(拒否)送信先情報を設定する	
FIA_SOS.1	秘密の検証に使用される尺度の管理	サーバ設定ツールにて、許可されるパスワードの長さ、英数混合を設定する	
FMT_SMF.1	なし	なし	
FPT_STM	時間の管理	なし	Windows の時間管理によるため

FPT_STM.1 高信頼タイムスタンプ

下位階層: なし

依存性: なし

FPT_STM.1.1 TSFは、高信頼タイムスタンプを提供できなければならない。

6.2 セキュリティ保証要件

セキュリティ保証要件を記述する。

本 TOE の評価保証レベルは EAL3 である。全てのセキュリティ保証要件は CC パート3に規定されているセキュリティ保証コンポーネントを直接使用する。

表 6-10. 保証クラスと保証コンポーネント

保証クラス	保証コンポーネント
ADV: 開発	ADV_ARC.1 セキュリティアーキテクチャ記述
	ADV_FSP.3 完全な要約を伴う機能仕様
	ADV_TDS.2 アーキテクチャ設計
AGD: ガイダンス文書	AGD_OPE.1 利用者操作ガイダンス
	AGD_PRE.1 準備手続き
ALC: ライフサイクル サポート	ALC_CMC.3 許可の管理
	ALC_CMS.3 実装表現のCM範囲
	ALC_DEL.1 配付手続き
	ALC_DVS.1 セキュリティ手段の識別
	ALC_LCD.1 開発者によるライフサイクルモデルの定義
ASE: セキュリティ ターゲット評価	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST概説
	ASE_OBJ.2 セキュリティ対策方針
	ASE_REQ.2 派生したセキュリティ要件
	ASE_SPD.1 セキュリティ課題定義
	ASE_TSS.1 TOE要約仕様
ATE: テスト	ATE_COV.2 カバレージの分析
	ATE_DPT.1テスト: 基本設計
	ATE_FUN.1機能テスト
	ATE_IND.2 独立テスト - サンプル
AVA: 脆弱性評定	AVA_VAN.2 脆弱性分析

6.3 セキュリティ要件根拠

6.3.1 セキュリティ機能要件根拠

セキュリティ機能要件とTOEのセキュリティ対策方針の対応関係を表6-11に示す。この表で示す通り、各 TOE セキュリティ対策方針は少なくとも1つのセキュリティ機能要件により実現される。また各セキュリティ機能要件は少なくとも1つの TOE セキュリティ対策方針に対抗している。

表 6-11. TOE セキュリティ対策方針とセキュリティ機能要件の対応

	O.ENCRYPTION	O.DISC_ENCRYPTION
FAU_GEN.1	×	×
FAU_SAR.1	×	×
FAU_SAR.3	×	×
FCS_CKM.1	×	×
FCS_COP.1	×	×
FDP_IFC.1	×	
FDP_IFF.1	×	
FIA_SOS.1	×	
FMT_SMF.1	×	×
FPT_STM.1	×	×

次に、各 TOE セキュリティ対策方針が、セキュリティ機能要件により実現できることを説明する。

O.ENCRYPTION（提供ファイルの暗号化）

この TOE セキュリティ対策方針は、非信頼領域に持ち出すためのアプリケーション、持ち出し操作を限定し、正当な受け取り手のみが閲覧可能となるように SV 暗号もしくは自走式暗号で提供ファイルを暗号化し、自走式暗号の場合は管理者が定めた品質尺度のパスワードが設定されるようチェックすることを求めている。また、非信頼領域への保護資産の許可されていない持ち出しの試行や、非信頼領域への保護資産の許可された持ち出し行為を管理者が監査できるようにすることを求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下の通りである。

a. 非信頼領域に持ち出すためのアプリケーションを限定する

TOE は、非信頼領域に持ち出すことが可能なアプリケーション、持ち出し操作を限定し、それ以外の持ち出し操作を禁止する。FDP_IFC.1 および FDP_IFF.1 は、アプリケーションと持ち出し操作先によってその操作を許可または禁止する機能要件である。従って、この対

策に該当するセキュリティ機能要件は、FDP_IFC.1 および FDP_IFF.1 である。

b. SV 暗号もしくは自走式暗号により提供ファイルを暗号化する

TOE は、利用者が他者に渡すファイルを暗号化しなければならない。その際、暗号鍵を生成し、暗号化する必要がある。FCS_CKM.1 は標準の暗号鍵生成アルゴリズムを用いて暗号鍵を生成する機能要件である。FCS_COP.1 は標準の暗号化・復号アルゴリズムを用いて暗号化・復号を行う機能要件である。従って、この対策に該当するセキュリティ機能要件は、FCS_CKM.1、および FCS_COP.1 である。

c. 自走式暗号の場合、管理者が定めた品質尺度のパスワードが設定されるようチェックする

TOE は、自走式暗号の場合、送り手が設定するパスワードが管理者が定めた品質尺度に適合しているかチェックする必要がある。FIA_SOS.1 はパスワードが管理者が定めた品質尺度に適合しているかチェックする機能要件である。従って、この対策に該当するセキュリティ機能要件は、FIA_SOS.1 である。

d. 非信頼領域へ許可されていない持ち出しの試行を監査する

TOE は、許可されていないアプリケーションによる非信頼領域への持ち出しの試行を把握するために、監査機能を有する必要がある。FAU_GEN.1、FPT_STM.1 は高性能タイムスタンプを使用した監査記録を生成し、FAU_SAR.1,FAU_SAR.3 は管理者のみが監査情報を監査しやすい形式でレビューする機能要件である。FMT_SMF.1 は管理者が不要となった履歴データおよび履歴集積データを削除する機能要件である。FAU_GEN.1 で規定した監査事象のうち、FDP_IFF.1（持ち出し操作の拒否）の監査事象を生成することにより、許可されていないアプリケーションによる非信頼領域への持ち出しの試行を監査することができる。FMT_SMF.1（サーバ設定ツールの起動と設定変更）の監査事象を生成することにより、許可されていないアプリケーションや非信頼領域の設定変更を把握することができる。したがって、この対策に該当するセキュリティ機能要件は FAU_GEN.1（監査事象：FDP_IFF.1、FMT_SMF.1）、FPT_STM.1、FAU_SAR.1、FAU_SAR.3、FMT_SMF.1 である。

e. 非信頼領域へ持ち出された保護資産を監査する

TOE は、非信頼領域へ持ち出された保護資産について後に追跡可能なように監査機能を有する必要がある。FAU_GEN.1、FPT_STM.1 は高性能タイムスタンプを使用した監査記録を生成し、FAU_SAR.1,FAU_SAR.3 は管理者のみが監査情報を監査しやすい形式でレビューする機能要件である。FMT_SMF.1 は管理者が不要となった履歴データおよび履歴集積データを削除する機能要件である。非信頼領域への持ち出しの許可の処理の後には、必ず暗号化機能が動作するため、FAU_GEN.1 で規定した監査事象のうち、FDP_COP.1 の監査事象を生成することにより、社内(信頼領域)でのみ復号可能な形式(SV 暗号)または

社外(非信頼領域)で復号可能な形式(自走式暗号)で非信頼領域へ持ち出された保護資産を監査することができる。TOE は、ファイルの暗号化と同時に、暗号鍵の生成を行うため、FCS_COP.1 のログを FCS_CKM.1 のログと見なすことができる。暗号機能が失敗した場合は、エラーパネルを表示して持ち出し操作を拒否するため、提供ファイルが非セキュアな状態で非信頼領域に持ち出されることはなく、監査対象とする必要はない。また、自走式暗号で非信頼領域へ持ち出す際には秘密の尺度のテストを行うが、拒否に際してエラーパネルを表示し、品質尺度に適合した秘密が入力されるまで、ファイルの持ち出し操作を拒否するため、提供ファイルが非セキュアな状態で非信頼領域に持ち出されることはなく、監査対象とする必要はない。FMT_SMF.1(サーバ設定ツールの起動と設定変更)の監査事象を生成することにより、自走式暗号の秘密の品質尺度の設定変更を把握することができる。したがって、この対策に該当するセキュリティ機能要件は FAU_GEN.1(監査事象:FCS_COP.1、FMT_SMF.1)、FPT_STM.1、FAU_SAR.1、FAU_SAR.3、FMT_SMF.1 である。

f. 管理機能を有する

TOE は、SV 暗号機能、Write 制限機能、自走式暗号機能、監査機能に関する管理機能を有する必要がある。FMT_SMF.1 は、上記機能の起動・停止の管理、Write 制限機能の設定の管理、上記機能の TSF データの管理を管理者が行う機能要件である。従って、この対策に該当するセキュリティ機能要件は、FMT_SMF.1 である。

以上、a、b、c、d、e、f すべての対策を満たすことにより、O.ENCRYPTION を満たすことができる。従って、それぞれの対策に必要な機能要件に該当する FCS_CKM.1、FCS_COP.1、FIA_SOS.1 、FDP_IFC.1 、FDP_IFF.1 、FAU_GEN.1 、FAU_SAR.1 、FAU_SAR.3 、FPT_STM.1、および FMT_SMF.1 の達成により O.ENCRYPTION を実現できる。

O.DISC_ENCRYPTION(ハードディスクの暗号化)

この TOE セキュリティ対策方針は、クライアントマシンのハードディスクを暗号化することを求めている。また、クライアントマシンのハードディスクの暗号化状態を管理者が監査できるようにすることを求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下の通りである。

a. ハードディスクを暗号化する

TOE は、クライアントマシンのハードディスクを暗号化しなければならない。ハードディスクの初期暗号化を行う際には、暗号鍵を生成する必要がある。FCS_CKM.1 は標準の暗号鍵生成アルゴリズムを用いて暗号鍵を生成する機能要件である。FCS_COP.1 は標準の暗号化・復号アルゴリズムを用いて暗号化・復号を行う機能要件である。従って、この対策に該当するセキュリティ機能要件は、FCS_CKM.1、および FCS_COP.1 である。

b. 社外に持ち出されうるクライアントマシンのハードディスクの暗号化状態を監査する

TOE は、社外に持ち出されうるクライアントマシンのハードディスクの暗号化状態を把握するために監査機能を有する必要がある。FAU_GEN.1、FPT_STM.1 は高性能タイムスタンプを使用した監査記録を生成し、FAU_SAR.1,FAU_SAR.3 は管理者のみが監査情報を監査しやすい形式でレビューする機能要件である。FMT_SMF.1 は管理者が不要となった履歴データおよび履歴集積データを削除する機能要件である。FAU_GEN.1 で規定した監査事象のうち、FDP_COP.1 の監査事象を生成することにより、初期暗号化の開始・完了、全復号の開始・完了を知ることができ、どのクライアントマシンのハードディスクが暗号化された状態であり、どのクライアントマシンのハードディスクが暗号化されていない状態であるかを監査することができる。TOE は、初期暗号化の開始時に暗号鍵を生成するため、FCS_COP.1 のログを FCS_CKM.1 のログと見なすことができる。TOE では、初期暗号化後のファイルの読み書きに伴う暗号化・復号は通常成功する。失敗する可能性としては暗号鍵情報を含む管理情報が破損した場合が考えられるが、この場合、データが復号した状態で読み取れなくなるため、マシンが正常に起動しなくなる恐れがあるが、情報漏洩には繋がらない。そのため暗号化・復号の失敗を監査対象にする必要はない。従って、この対策に該当するセキュリティ機能要件は、FAU_GEN.1（監査事象：FCS_COP.1）、FPT_STM.1、FAU_SAR.1、FAU_SAR.3、および FMT_SMF.1 である。

c. 管理機能を有する

TOE は、ストレージ暗号機能、監査機能に関する管理機能を有する必要がある。FMT_SMF.1 は、監査機能の起動・停止の管理、上記機能の TSF データの管理を管理者が行う機能要件である。従って、この対策に該当するセキュリティ機能要件は、FMT_SMF.1 である。

以上、a、b、c すべての対策を満たすことにより、O.DISC_ENCRYPTION を満たすことができる。従って、それぞれの対策に必要な機能要件に該当する FCS_CKM.1、FCS_COP.1、FAU_GEN.1、FAU_SAR.1、FAU_SAR.3、FPT_STM.1、および FMT_SMF.1 の達成により O. DISC_ENCRYPTION を実現できる。

6.3.2 セキュリティ機能要件依存性

セキュリティ要件のコンポーネントの依存性を表 6-12 に示す。

表 6-12. セキュリティ要件のコンポーネントの依存性

項番	TOE で使用されているコンポーネント	CC パート 2 で規定されている依存コンポーネント	TOE の依存コンポーネント	依存性が満たされていないコンポーネント	妥当性
1	FAU_GEN.1	FPT_STM.1	FPT_STM.1	なし	
2	FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	なし	
3	FAU_SAR.3	FAU_SAR.1	FAU_SAR.1	なし	
4	FCS_CKM.1	[FCS_CKM.2 または FCS_COP.1]	FCS_COP.1	なし	
		FCS_CKM.4	なし	FCS_CKM.4	※1
5	FCS_COP.1	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1]	FCS_CKM.1	なし	
		FCS_CKM.4	なし	FCS_CKM.4	※1
6	FDP_IFC.1	FDP_IFF.1	FDP_IFF.1	なし	
7	FDP_IFF.1	FDP_IFC.1	FDP_IFC.1	なし	
		FMT_MSA.3	なし	FMT_MSA.3	※2
8	FIA_SOS.1	なし	なし	なし	
9	FMT_SMF.1	なし	なし	なし	
10	FPT_STM.1	なし	なし	なし	

※1 FCS_CKM.4 に対する依存性の欠如の妥当性について

SV 暗号機能、自走式暗号機能において、暗号鍵は復号のため暗号化されてファイルに保持されるので破棄の必要はない（ファイルの削除により暗号鍵も削除される）。また、TOE の運用中はストレージ暗号化された状態を維持する必要があるため暗号鍵は破棄しない（ストレージ暗号機能の暗号鍵は、TOE のアンインストール時にディスクの復号が完了されると、ディスクは暗号化された状態にはなく、暗号鍵は再利用されないため明示的に破棄する必要はない）。よって、この依存関係は不要である。

※2 FMT_MSA.3 に対する依存性の欠如の妥当性について

本 TOE では情報のセキュリティ属性は自動的に付加されるものであり、かつその値自体が許可的/制限的な性質を持つものではないため、デフォルト値の管理を行う必要はない。

よって、この依存関係は不要である。

6.3.3 セキュリティ保証要件根拠

セキュリティ保証要件根拠を以下に示す。

本製品は、社内のデータが正当な受け取り手以外の第三者の手に渡り、これを暴露されることにより情報漏洩が発生することを防止するための商用製品である。EAL3 は、TOE における開発段階のセキュリティ対策の分析(系統だったテストの実施と分析、および開発環境や開発生産物の管理状況の評価)、セキュリティ機能を安全に使用するための十分なガイダンス情報の分析を含み、商用製品の評価として妥当な選択であるといえる。

7 TOE 要約仕様

本章では、TOEが提供するセキュリティ機能の要約仕様について述べる。

7.1 TOE セキュリティ機能

表 7-1 に TOE セキュリティ機能とセキュリティ機能要件(SFR)との対応関係について示す。ここで示される通り、本節で説明するセキュリティ機能は 6.1 節に記述される全ての SFR を満たすものである。

表7-1 TOEセキュリティ機能とセキュリティ機能要件の対応関係

	SF.AUDIT	SF.SV_ENCRYPTION	SF.WRITE_CONTROL	SF.PASS_ENCRYPTION	SF.STORAGE_ENCRYPTION	SF.ADMIN
FAU_GEN.1	×					
FAU_SAR.1	×					
FAU_SAR.3	×					
FCS_CKM.1		×		×	×	
FCS_COP.1		×		×	×	
FDP_IFC.1		×	×			
FDP_IFF.1		×	×			
FIA_SOS.1				×		
FMT_SMF.1	×					×
FPT_STM.1	×					

7.1.1 監査機能(SF.AUDIT)

監査機能は、利用者が行ったファイル操作を操作履歴として記録し、管理者がサーバでその操作履歴を収集して閲覧できる状態にできる機能である。利用者が SeP クライアントで行ったファイル操作はSePクライアントにて操作履歴として出力される。SePクライアントで出力された操作履

歴は管理者が定めたタイミングで SeP サーバにアップロード(送信)される。管理者は SeP サーバ上でトレーサを用いて、SeP サーバに蓄積された操作履歴を収集し、汎用ソフトで閲覧できるよう CSV 形式で出力することができる。また、操作履歴とは別に、管理者が SeP サーバで行ったサーバ設定ツールの設定を記録する。

7.1.1.1 対応する SFR の実現方法

(1) FAU_GEN.1 監査データ生成

監査機能は TOE が起動している間働いている。TOE は Windows 起動時に起動され、Windows シャットダウン時に終了する。TOE は起動時、終了時に「Windows 起動」「Windows 終了」の操作履歴を出力する。これを監査機能の起動と終了の監査記録と読み替えることができる。

TOE の操作履歴には、マシン名、ファイル名、パス、ウィンドウタイトル、アプリケーション名、操作名、ユーザ名、日時、備考の情報が含まれる。

SV 暗号化の対象となる操作には次のものがある。操作:ファイルコピー、ファイル移動、別名保存、メール添付。操作の結果 SV 暗号化された場合は操作名の後ろに「(SV-暗号)」と付加される。SV 暗号化しない操作、または SV 暗号解除(平文化)した場合には操作名のみが出力される。

Web ページへのファイルの添付が禁止された場合は、「拒否-メール添付」と出力される。

メールまたは Web ページへのクリップボードのペーストが禁止された場合は、「拒否-クリップボード」と出力される。

Write 制限機能により、ファイルの書き込みによる持ち出し操作が禁止された場合は操作欄に「拒否-ファイル書き込み(SV-Write 制限)」と出力され、通信による持ち出し操作が禁止された場合は操作欄に「拒否-ファイル転送(SV-Write 制限)」と出力される。

リリースフォルダから自走式暗号化してファイルが持ち出された場合には、操作名に「(SV-リリース選択自走式暗号 OUT)」と付加される。

ストレージ暗号化機能により、初期暗号化を行った場合、操作名欄に「ストレージ暗号(開始)」、「ストレージ暗号(終了)」と出力される。また、全復号を行った場合、操作名欄に「ストレージ復号(開始)」、「ストレージ復号(終了)」と出力される。

サーバ設定ツールを起動した際に、操作名欄に「プロセス起動」、アプリケーション欄にサーバ設定ツールの exe 名が記録される。

また、操作履歴とは別に、サーバ設定ツールの設定履歴として、サーバ設定ツールで設定ボタンを押した際に、設定内容が記録される。この際、設定内容、日時、ユーザ名が記録される。前回の設定内容と比較することで、変更分を知ることができる。

(2) FAU_SAR.1 監査レビュー

SeP サーバにインストールされるトレーサを用いて、管理者は SeP サーバに集積された操

作履歴を汎用的な表計算ソフトなどで表示できるように CSV 形式に変換して出力することができる。CSV に出力した際、次の項目順で出力される。マシン名、ファイル名、パス、ウィンドウタイトル、アプリケーション名、操作（持ち出し操作の拒否、暗号化の識別含む）、ユーザ名、日時、備考。

サーバ設定ツールの設定記録は、サーバ設定ツールを実行した SeP サーバ上にてテキストファイルで出力されるため、汎用的なソフトで閲覧できる。出力される項目は、設定内容、日時、ユーザ名である。

(3) FAU_SAR.3 選択可能監査レビュー

SeP サーバにインストールされるトレーサを用いて、管理者が SeP サーバに集積された操作履歴を CSV 形式に変換して出力する際、以下のような分類、選択、またはその組み合わせを選択することができる。

表 7-2. 操作履歴の分類と選択

関連の基準	方法
ユーザ別、マシン別	分類して出力
操作、日時	選択して出力

(4) FPT_STM.1 高信頼タイムスタンプ

TOE は、Windows からタイムスタンプを取得して利用する。

(5) FMT_SMF.1 管理機能の特定

SeP サーバにインストールされるトレーサを用いて、管理者は SeP サーバにクライアントからアップロードされた履歴データ、およびトレーサによって収集された集積履歴データを削除することができる。

7.1.2 SV 暗号機能(SF.SV_ENCRYPTION)

SV 暗号機能は、信頼領域から非信頼領域にファイルを持ち出した際に、自動的かつ強制的にファイルを暗号化する機能である。非信頼領域から信頼領域に暗号化ファイル(SV 暗号ファイル)を戻すと自動的に復号する。

7.1.2.1 対応する SFR の実現方法

(1) FCS_CKM.1 暗号鍵生成

本機能では以下の暗号鍵生成アルゴリズムに従って暗号鍵を生成する。
[標準のリスト]:FIPS 140-2, Annex C
[暗号鍵生成アルゴリズム]:決定論的擬似乱数生成法
[暗号鍵長]:256bits (AES)

(2) FCS_COP.1 暗号操作
本機能では以下の暗号アルゴリズムを用いて暗号化および復号を行う。
[標準のリスト]:FIPS 197 (AES)
[暗号アルゴリズム]:下表の暗号アルゴリズム
[暗号鍵長]:下表の暗号鍵長

表 7-3. SV 暗号機能の暗号アルゴリズムと暗号鍵長

暗号アルゴリズム	暗号鍵長
AES	256bits

信頼領域から非信頼領域への以下のファイル操作の際にファイルを暗号化する。
ファイル操作:コピー、移動、別名保存、メールに添付、Web ページに添付。
非信頼領域から信頼領域への以下のファイル操作の際にファイルを復号する。
ファイル操作:コピー、移動、別名保存、メールの添付ファイルを保存、Web ページの添付ファイルを保存。

(3) FDP_IFC.1 サブセット情報フロー制御、FDP_IFF.1 単純セキュリティ属性
アプリケーション監視サブジェクトは、持ち出し操作が Web ページへの添付の際にファイル操作情報の情報フローを実施しようとすると、ファイル操作情報の添付先 URL が信頼領域(社内 URL)または非信頼領域(SV 化 URL)を示している場合は、情報フローを許可し、それ以外の場合は禁止する。この持ち出し操作に対し、サブジェクトの属性が未設定の場合は情報フローは禁止される。ただし、添付元のパスがリリースフォルダの場合、情報フローは許可される。

アプリケーション監視サブジェクトは、持ち出し操作が Web ページへのペーストの際にファイル操作情報の情報フローを実施しようとすると、ファイル操作情報のペースト先情報が信頼領域(社内 URL)を示している場合は、情報フローを許可し、それ以外の場合は禁止する。この持ち出し操作に対し、サブジェクトの属性が未設定の場合は情報フローは禁止される。

アプリケーション監視サブジェクトは、持ち出し操作がメールへのペーストの際にファイル操作情報の情報フローを実施する場合、情報フローを禁止する。この持ち出し操作に対し、サブジェクトの属性が未設定の場合は情報フローは禁止される。

7.1.3 Write 制限機能(SF.WRITE_CONTROL)

Write 制限機能は、本機能の拒否アプリケーションでの非信頼領域へのファイルの持ち出し操作を禁止する機能である。

7.1.3.1 対応する SFR の実現方法

(1) FDP_IFC.1 サブセット情報フロー制御、FDP_IFF.1 単純セキュリティ属性

アプリケーション監視サブジェクトは、アプリケーションが持ち出し操作によるファイル操作情報の情報フローを実施しようとすると、ファイル操作情報のアプリケーション情報と書き込み先のパスまたは送信先情報を、サブジェクトのセキュリティ属性であるサーバ設定情報の許可(または拒否)アプリケーションのリストと信頼領域および非信頼領域の設定または許可(または拒否)するポート・IP アドレスの設定と比較して、ファイル操作情報のアプリケーション情報と書き込み先のパスまたは送信先情報が、許可アプリケーションであるか信頼領域への書き込みまたは許可先への送信であれば許可し、拒否アプリケーションで非信頼領域への書き込みまたは拒否先への送信であれば拒否する。なお、サブジェクトのセキュリティ属性が未設定の場合は情報フローを許可する。

7.1.4 自走式暗号機能(SF.PASS_ENCRYPTION)

自走式暗号機能は、ファイルを暗号化して社外の受け取り手に渡すための機能である。ファイルを社外の受け取り手に渡すための窓口であるリリースフォルダからファイルを持ち出す際に、パスワードの入力が求められ、自走式暗号化が強要される。受け取り手は送り手が設定したパスワードを入力することによって自走式暗号ファイルを復号できる。

7.1.4.1 対応する SFR の実現方法

(1) FCS_CKM.1 暗号鍵生成

本機能では以下の暗号鍵生成アルゴリズムに従って暗号鍵を生成する。

[標準のリスト]:FIPS 140-2, Annex C

[暗号鍵生成アルゴリズム]:決定論的擬似乱数生成法

[暗号鍵長]:256bits (AES)

(2) FCS_COP.1 暗号操作

本機能では以下の暗号アルゴリズムを用いて暗号化および復号を行う。

[標準のリスト]:FIPS 197 (AES)

[暗号アルゴリズム]:下表の暗号アルゴリズム

[暗号鍵長]:下表の暗号鍵長

表 7-4. 自走式暗号機能の暗号アルゴリズムと暗号鍵長

暗号アルゴリズム	暗号鍵長
AES	256bits

自走式暗号ファイルの作成は次のように行う。自走式暗号化して社外の受け取り手に渡すファイルを管理者が定めたリリースフォルダに入れる。リリースフォルダから出す(外部媒体へコピー、メールに添付など)と、パスワードの入力を求めるパネルが表示される。品質尺度に適合したパスワードを入力することによりファイルは自走式暗号化される。
受け取り手は、実行形式である自走式暗号化ファイルを実行する(マウスでダブルクリック)と、パスワードの入力を求められる。送り手が設定したパスワードを入力することで自走式暗号ファイルは解凍(平文化)される。

(3) FIA_SOS.1 秘密の検証

自走式暗号ファイル作成の際に入力されたパスワードは以下の品質尺度に適合しているかチェックされ、適合している場合には自走式暗号ファイルが作成され、不適合の場合は再入力を求める。
【定義された品質尺度】:管理者が設定した品質尺度(10-64 文字、英数混合)、使用可能文字:英字大文字([A-Z]26 文字), 英字小文字([a-z]26 文字),数字([0-9]10 文字)

7.1.5 ストレージ暗号機能(SF.STORAGE_ENCRYPTION)

ストレージ暗号機能は、クライアントマシンの盗難・紛失に備えてハードディスクを暗号化する機能である。

7.1.5.1 対応する SFR の実現方法

(1) FCS_CKM.1 暗号鍵生成

本機能では以下の暗号鍵生成アルゴリズムに従って暗号鍵を生成する。
【標準のリスト】:FIPS 140-2, Annex C
【暗号鍵生成アルゴリズム】:決定論的擬似乱数生成法
【暗号鍵長】:256bits (AES)

(2) FCS_COP.1 暗号操作

本機能では以下の暗号アルゴリズムを用いて暗号化および復号を行う。
【標準のリスト】:FIPS 197 (AES)
【暗号アルゴリズム】:下表の暗号アルゴリズム

[暗号鍵長]: 下表の暗号鍵長

表 7-5. ストレージ暗号機能の暗号アルゴリズムと暗号鍵長

暗号アルゴリズム	暗号鍵長
AES	256bits

管理者がサーバ設定ツール(管理ツール)でストレージ暗号機能を有効にすると、初期暗号化が開始され、内蔵ハードディスクの使用領域が暗号化される。

管理者がサーバ設定ツールでストレージ暗号機能を無効にすると、全復号が開始され、暗号化された内蔵ハードディスクの領域が復号される。

初期暗号化完了後、内蔵ハードディスクにファイルを書き込むとハードディスク上にデータは暗号化されて書き込まれる。アプリケーションまたは OS が内蔵ハードディスク上のファイルを読み込むとハードディスク上のデータは復号されて読み込まれる。

7.1.6 管理機能(SF.ADMIN)

管理機能は、管理者がセキュリティ機能のふるまいを設定するための機能であり、SeP サーバ上で使用できるサーバ設定ツールおよび動作管理ツールによって提供される。サーバ設定ツールによって、SV 暗号機能、Write 制限機能、自走式暗号機能、ストレージ暗号機能、各種設定が個別に可能である。動作管理ツールを用いて、SeP クライアントのセキュリティ機能(ストレージ暗号機能を除く)を停止・再開することができる。

7.1.6.1 対応する SFR の実現方法

(1) FMT_SMF.1 管理機能の特定

管理者はSePサーバ上で使用する動作管理ツールを用いて、クライアントのセキュリティ機能である、SV 暗号機能、Write 制限機能、自走式暗号機能、監査機能(操作履歴出力機能)を停止することができる。

管理者は SeP サーバ上で使用する動作管理ツールを用いて、停止させたクライアントのセキュリティ機能を再開することができる。

管理者は SeP サーバ上で使用するサーバ設定ツールを用いて以下の設定を問い合わせし、変更することができる。

- SV 暗号機能の有効/無効
- 信頼領域(非信頼領域)の定義
- Write 制限機能の有効/無効
- Write 制限機能の許可(拒否)アプリケーション
- Write 制限機能の許可(拒否)するポート・IP アドレス

- 自走式暗号機能の有効/無効
- リリースフォルダの定義
- パスワードの長さの範囲
- パスワードの英数混合の指定
- ストレージ暗号機能の有効/無効

※ 自走式暗号機能で利用される FIA_SOS.1 により要求されるパスワードの品質尺度の設定は、パスワードの長さの範囲、パスワードの英数混合の指定の設定により実現される。Write 制限機能で利用される FDP_IFF.1 による要求は、Write 制限機能の許可(または拒否)するアプリケーションの設定、信頼領域(許可する領域)および非信頼領域(拒否する領域)の設定および送信を許可(または拒否)するポート・IP アドレスの設定により実現される。