Defense Platform Business Edition CC

セキュリティターゲット

第 1.41版

作成日：2016 年 11 月14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
2014/12/24	1.00	新規作成	ハミングヘッズ株式会社
2015/2/4	1.01	指摘箇所修正	ハミングヘッズ株式会社
2015/2/9	1.02	1.5.2.3 (1)判定機能および FDP_IFF.1(4)の修正	ハミングヘッズ株式会社
2015/2/20	1.03	指摘箇所修正	ハミングヘッズ株式会社
2015/3/3	1.04	指摘箇所修正	ハミングヘッズ株式会社
2015/3/12	1.05	指摘箇所修正	ハミングヘッズ株式会社
2015/3/15	1.06	指摘箇所修正	ハミングヘッズ株式会社
2015/3/16	1.07	指摘箇所修正	ハミングヘッズ株式会社
2015/3/18	1.08	指摘箇所修正	ハミングヘッズ株式会社
2015/3/19	1.09	指摘箇所修正	ハミングヘッズ株式会社
2015/3/20	1.10	指摘箇所修正	ハミングヘッズ株式会社
2015/4/6	1.11	指摘箇所修正	ハミングヘッズ株式会社
2015/4/13	1.12	指摘箇所修正	ハミングヘッズ株式会社
2015/4/17	1.13	指摘箇所修正	ハミングヘッズ株式会社
2015/4/22	1.14	指摘箇所修正	ハミングヘッズ株式会社
2015/5/20	1.15	指摘箇所修正	ハミングヘッズ株式会社
2015/6/15	1.16	TOE のバージョン変更	ハミングヘッズ株式会社
2015/7/21	1.17	指摘箇所修正	ハミングヘッズ株式会社
2015/8/20	1.18	指摘箇所修正	ハミングヘッズ株式会社
2015/9/2	1.19	T.CONNECTION の削除	ハミングヘッズ株式会社
2015/9/10	1.20	TOE のバージョン変更、指摘箇所修正	ハミングヘッズ株式会社
2015/9/28	1.21	マニュアルの版数変更、指摘箇所の修正	ハミングヘッズ株式会社
2015/10/26	1.22	指摘箇所修正	ハミングヘッズ株式会社
2015/11/4	1.23	指摘箇所修正	ハミングヘッズ株式会社
2015/11/18	1.24	指摘箇所修正	ハミングヘッズ株式会社
2015/12/2	1.25	指摘箇所修正	ハミングヘッズ株式会社
2016/3/9	1.26	指摘箇所修正	ハミングヘッズ株式会社
2016/3/11	1.27	指摘箇所修正	ハミングヘッズ株式会社
2016/4/1	1.28	指摘箇所修正	ハミングヘッズ株式会社
2016/4/22	1.29	指摘箇所修正	ハミングヘッズ株式会社

日付	版	修正概要	修正者
2016/5/12	1.30	指摘箇所修正	ハミングヘッズ株式会社
2016/5/20	1.31	指摘事項修正	ハミングヘッズ株式会社
2016/6/21	1.32	信頼されるプログラムの見直しによる修正	ハミングヘッズ株式会社
2016/7/20	1.33	指摘事項修正	ハミングヘッズ株式会社
2016/8/5	1.34	指摘事項修正	ハミングヘッズ株式会社
2016/9/6	1.35	指摘事項修正	ハミングヘッズ株式会社
2016/9/16	1.36	ガイダンスの版数変更	ハミングヘッズ株式会社
2016/10/4	1.37	指摘事項修正	ハミングヘッズ株式会社
2016/10/17	1.38	指摘事項修正	ハミングヘッズ株式会社
2016/10/26	1.39	指摘事項修正	ハミングヘッズ株式会社
2016/11/8	1.40	ガイダンスの版数変更	ハミングヘッズ株式会社
2016/11/14	1.41	ガイダンスの版数変更	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 : Defense Platform Business Edition CC セキュリティターゲット
バージョン : 第 1.41 版
作成日 : 2016 年 11 月 14 日
作成者 : ハミングヘッズ株式会社

1.2 TOE 参照

TOE : Defense Platform Business Edition CC
バージョン : Ver.3.6.1.5
開発者 : ハミングヘッズ株式会社

※ Defense Platform Business Edition 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。

(1) ディフェンスプラットフォーム ビジネスエディション クライアント
(2) ディフェンスプラットフォーム ビジネスエディション サーバ

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
DeP	Defense Platform の略称。
DeP サーバ	ディフェンスプラットフォーム ビジネスエディション サーバの略称。
DeP クライアント	ディフェンスプラットフォーム ビジネスエディション クライアントの略称。

用語	定義内容
DeP サーバ PC	DeP サーバがインストールされたサーバマシン。
DeP クライアント PC	DeP クライアントがインストールされたクライアントマシン。
管理者	TOE および動作環境の管理を行う者。
PC 使用者	DeP クライアント PC を使用する者。
マルウェア	不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称。インターネットなどを利用し、標的のコンピュータに侵入して、システムやアプリケーションの破壊、改ざんを行ったり、ユーザデータの搾取を行ったりする。
プログラム	アプリケーション、スクリプト、マクロ、拡張モジュール。
動作履歴	プログラムの動作について TOE が出力する記録。
トレーサツール	動作履歴を収集して 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。
履歴データ	DeP クライアントから DeP サーバへアップロードされた動作履歴のデータで、トレーサツール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動作履歴のデータで、CSV 出力前の状態のもの。
ホワイトリスト	管理者が定義する、許可する動作のリスト。定義には、以下の項目が指定できる。 ・動作を行うプログラム ・動作の種類 ・動作対象 各項目は一意の値、複数、すべてといった指定ができる。指定されたプログラムによる指定された動作対象への指定された動作は許可される。
プログラム領域	Program Files フォルダ以下の、各プログラムが固有で使用するフォルダ。
アプリケーション領域	各ユーザフォルダの AppData フォルダ以下の、各プログラムが固有で使用するフォルダ。
プログラムレジストリ	HKEY_CURRENT_USER¥SOFTWARE および HKEY_LOCAL_MACHINE¥SOFTWARE 以下の、各プログラムが固有で使用するレジストリ。
プログラム自身のファイル	プログラム領域から実行されたプログラムが使用する、そのプログラム用のプログラム領域内のファイル。
プログラム自身のレジストリ	プログラム領域から実行されたプログラムが使用する、そのプログラム用のプログラムレジストリ。
実行可能ファイル	・EXE ファイル

用語	定義内容
	・DLL ファイル ・SYS ファイル ・COM ファイル ・LIB ファイル
保護対象ファイル	以下のいずれかのファイル ・システムドライブ直下のファイル ・システムドライブの¥windows¥System32 フォルダおよびシステムドライブの¥windows¥SysWow64 フォルダ内のファイル ・プログラム領域内のファイル(動作を行ったプログラム自身のファイルは除く) ・実行可能ファイル(動作を行ったプログラムのアプリケーション領域内のファイルは除く) ・MBR
保護対象レジストリ	動作を行ったプログラム自身のレジストリを除くレジストリ。
保護対象メモリ	動作を行ったプログラム以外のプログラムが、実行時に使用するメモリ。
保護対象	保護対象ファイル、保護対象レジストリ、保護対象メモリの総称。
ユーザデータ	DeP サーバ PC および DeP クライアント PC 上に存在するデータ。
デバイスドライバ	入出力デバイスを制御するドライバソフトウェア。
IPsec	暗号化セキュリティサービスを使用することで、IP ネットワーク上でのセキュリティで保護されたプライベートな通信を保証する、オープンスタンダードのフレームワーク。
IP セキュリティポリシー	IPsec ポリシー。Windows 上に IETF(インターネット技術標準化委員会)の開発した業界基準に基づいて実装された IPsec を設定する為のポリシー。
UEFI	Unified Extensible Firmware Interface の略称。BIOS に代わる PC の標準ファームウェアインターフェイス。
セキュアブート	ファームウェアにより、PC 起動時の各ブートプログラムおよび OS の署名チェックが行われ、署名が有効な場合のみ OS が起動する仕組み。

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、ホワイトリスト型のマルウェア対策ソフトウェア製品である。増加し続けるマルウェアから

守るべき対象(システムやプログラムを構成するファイルやレジストリ、それらが使用中のメモリ)は有限で、不変で、現実的に制御可能な範囲であり、それらに対するプログラムの動作も有限である。また、通信によるユーザデータの送信といった、情報漏えいにつながるプログラムの動作も有限である。保護対象以外への書き込み、自身の PC 内での通信処理は許容される。TOE は、許容された動作以外の動作を拒否することで、マルウェアによる、システムやプログラムの破壊、改ざん、通信を使用した情報の漏えいを防ぐ目的のものである。また、プログラムによる動作をすべて拒否すると、業務ソフトなどの動作も止めてしまう可能性があるが、組織の管理者が許容範囲を定義するホワイトリストを作成することで、業務ソフトなどの動作を止めずに、マルウェアによる、システムやプログラムの破壊、改ざん、通信を使用した情報の漏えいを防ぐことができる。

従来のマルウェアを特定する方式(ブラックリスト方式)とは違い、すべてのプログラムの動作を網羅的に捕捉し、TOE およびホワイトリストによる定義で許可された動作以外は拒否する方式(ホワイトリスト方式)を取っているのが特徴であり、それによって未知のマルウェアにも対抗することができる。

TOE は、サーバークライアント型製品である。DeP サーバ製品は、サーバマシンにインストールする。DeP クライアント製品は、PC 使用者が使用するクライアントマシンにインストールする。

DeP サーバ PC および DeP クライアント PC で利用できるセキュリティ機能は以下の通りである。

<DeP サーバ PC 固有機能>

(1) 監査機能(管理者向け機能)

管理者がトレーサを用いて、動作履歴を収集し、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。また、管理者が許可してもよいとするプログラムや動作を定義するホワイトリストを作成する。

<DeP サーバ PC および DeP クライアント PC 共通機能>

(1) 判定機能

検知したプログラムの動作を判定し、許可してもよい動作以外を拒否する機能である。

(2) 監査機能(動作履歴出力機能)

プログラムの動作履歴を出力する機能である。

1.4.2 TOE 種別

TOE は、ホワイトリスト型のマルウェア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 の動作に必要な環境を図 1-1 に示す。

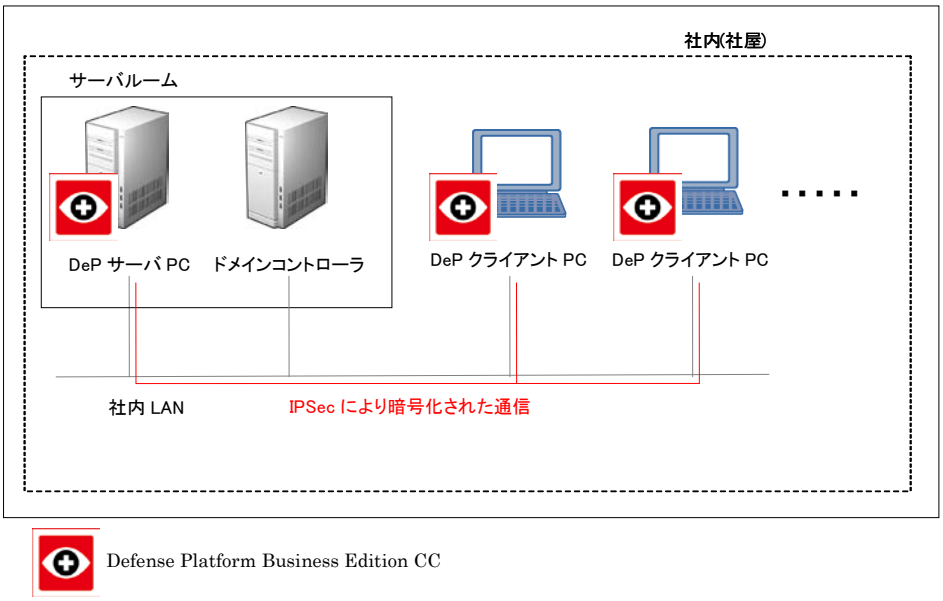

図 1-1 TOE の動作に必要な環境

TOE の動作に必要な環境の構成要素について以下に説明する。

(1) サーバルーム

ドメインコントローラ、DeP サーバ PC が設置される。入退室管理され、管理者のみがドメインコントローラ、DeP サーバ PC の管理を行うことができる。

(2) 社内 LAN

ドメインコントローラ、DeP サーバ PC および DeP クライアント PC を接続する。DeP サーバ PC と DeP クライアント PC 間の通信は、Windows の IP セキュリティポリシーの設定により通信パケットが暗号化された状態で行われる。

(3) ドメインコントローラ

Windows ドメインの管理を行う。

(4) DeP サーバ PC

TOE がインストールされ、管理者が TOE の管理機能および監査機能(管理者向け機能)を利用する。DeP クライアント PC との通信が暗号化されるように Windows の IP セキュリティポリシーが適用される。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ている。OS およびデバイスドライバ以外のドライバソフトウェアがインストールされていない。既定のブートプログラム以外が動作しないように、ファームウェアを UEFI モードに設定し、セキュアブートを有効にしている。ファームウェアにアップデートが適用されている。

(5) DeP クライアント PC

TOE がインストールされ、PC 使用者が利用する。管理者は、PC 使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。DeP サーバ PC との通信が暗号化されるように Windows の IP セキュリティポリシーが適用される。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ている。OS およびデバイスドライバ以外のドライバソフトウェアがインストールされていない。既定のブートプログラム以外が動作しないように、ファームウェアを UEFI モードに設定し、セキュアブートを有効にしている。ファームウェアにアップデートが適用されている。

※ 上記は TOE を使用する為の必要最低限の環境であり、社内 LAN がファイアウォールなどを介してインターネットにつながっている一般的な環境でも TOE を使用することができる。

必要システム

(1) DeP サーバ PC

・ ハードウェア

CPU 1.4GHz 以上の x64 プロセッサ(2GHz 以上推奨)

メモリ 2GB 以上

HDD インストール:880MB 以上

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 2012 R2 Standard 64bit

(2) DeP クライアント PC

・ ハードウェア

CPU 1GHz 以上の x64 プロセッサ

メモリ 2GB 以上

HDD インストール:150MB 以上

・ OS

Windows 8.1 Enterprise 64bit

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。

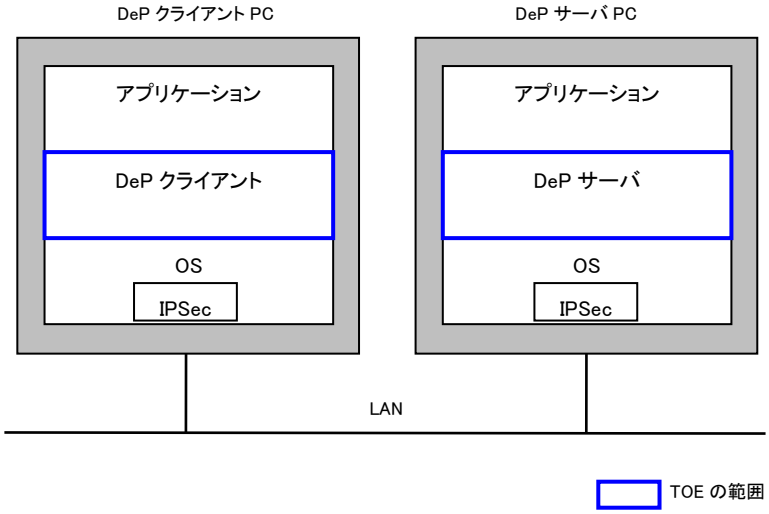

図 1-2. TOE のコンポーネント

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) DeP サーバ PC
ディフェンスプラットフォーム ビジネスエディション サーバ
(2) DeP クライアント PC
ディフェンスプラットフォーム ビジネスエディション クライアント

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
ディフェンスプラットフォーム ビジネスエディション マニュアル 機能編(第 23 版)
ディフェンスプラットフォーム ビジネスエディション マニュアル インストール・初期設定編(第 7 版)
ディフェンスプラットフォーム ビジネスエディション トレーサ マニュアル(第 10 版)
ディフェンスプラットフォーム ビジネスエディション リアルタイム履歴通知 マニュアル(第 10 版)
DeP 履歴抽出ツール マニュアル(第 6 版)
ディフェンスプラットフォーム ビジネスエディション マニュアル 追加・更新・削除履歴一覧(2016 年 7 月 20 日版)

ガイダンス文書名
Defense Platform Business Edition CC セキュアな運用ガイダンス(第 1.31 版)
Defense Platform Business Edition CC 内容物確認リスト（第 1.15 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。

DeP クライアント PC では、監査機能(動作履歴出力機能)、判定機能が動作する。監査機能(動作履歴出力機能)、判定機能はプログラムの動作に呼応して動作する。

DeP サーバ PC では、DeP クライアント PC で動作する機能に加え、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。管理者は管理機能により、DeP の動作を管理し、全ての DeP クライアント PC に配信されるホワイトリストを作成する。

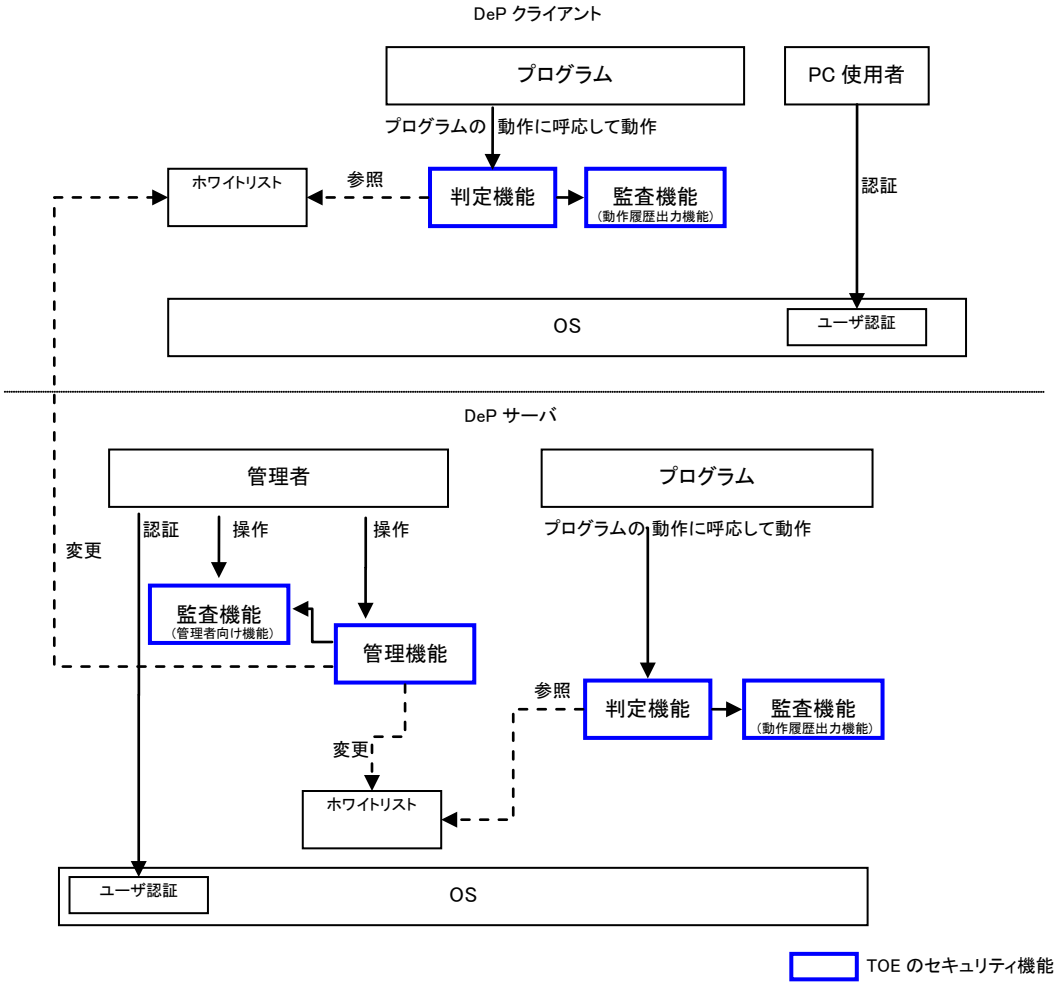

図 1-3　TOE 論理的範囲

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。DeP サーバ PC で、管理機能を利用して TOE の管理、ホワイトリストの作成(許可する動作の定義)、および監査機能(管理者向け機能)を用いて動作履歴の管理を行う。また、動作環境の管理(マシンの設置、Windows ドメインの構築、入退出の管理、ユーザアカウントの管理、セキュリティ対策用修正ソフトウェアの適用、ドライバソフトウェアのインストール状況の管理、UEFI モードおよびセキュアブートの設定およびファームウェアのアップデートの適用)、設定(Windows のログオンパスワードの設定、Windows の IP セキュリティポリシーの設定)を行う。

(2) PC 使用者

PC 使用者は、DeP クライアント PC で業務を行う。

1.5.2.2 TOE 保護資産

DeP サーバ PC および DeP クライアント PC 上の以下のデータ。

(1) 破壊、改ざんから保護するデータ
  (ア) 保護対象ファイル
  (イ) 保護対象レジストリ
  (ウ) 保護対象メモリ
(2) 漏えいから保護するデータ
  (ア) ユーザデータ

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((1)判定機能、(2)監査機能(動作履歴出力機能))は、プログラムの動作に呼応して働くものであり、PC 使用者が直接意識して利用するものではない。

プログラムが図 1-4 に示すような対象動作(保護対象への書き込み、外部へのユーザデータの送信(TCP/IP プロトコルおよび UDP/IP プロトコルによる送信))を行った場合に、(1)判定機能により、その動作が検知される。図 1-5、図 1-6 に示すように、(1)判定機能は、ホワイトリストを参照し、その動作の許可/拒否を判定し、許可もしくは拒否する。その際に、(2)監査機能(動作履歴出力機能)によりプログラムの対象動作とその動作の許可/拒否が記録される。

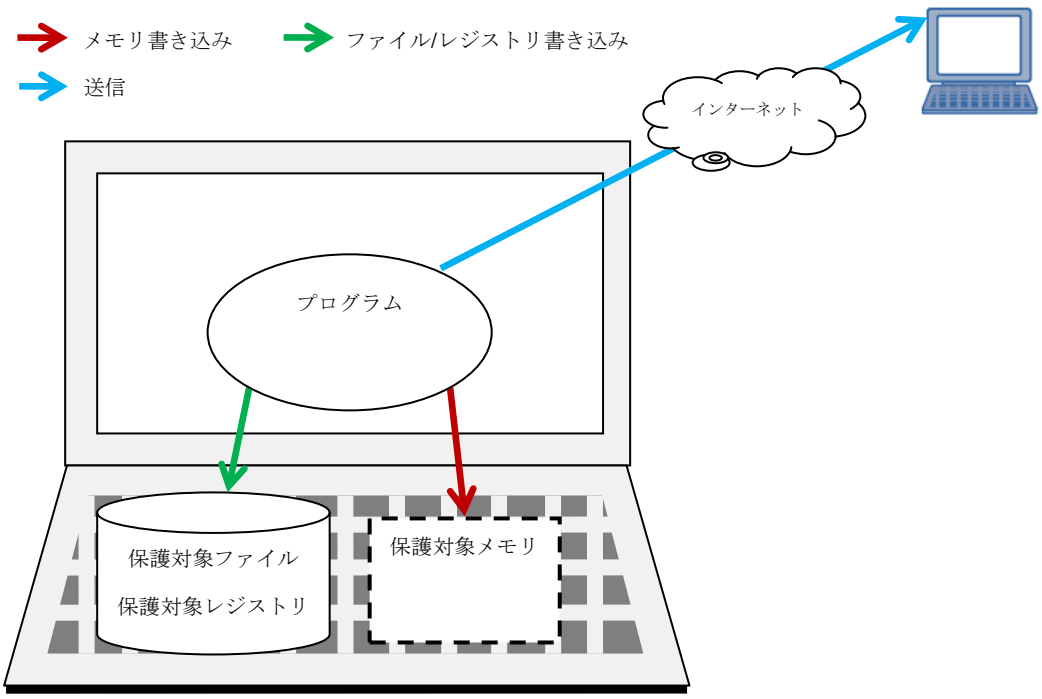

図 1-4 監視すべきプログラムの動作一覧

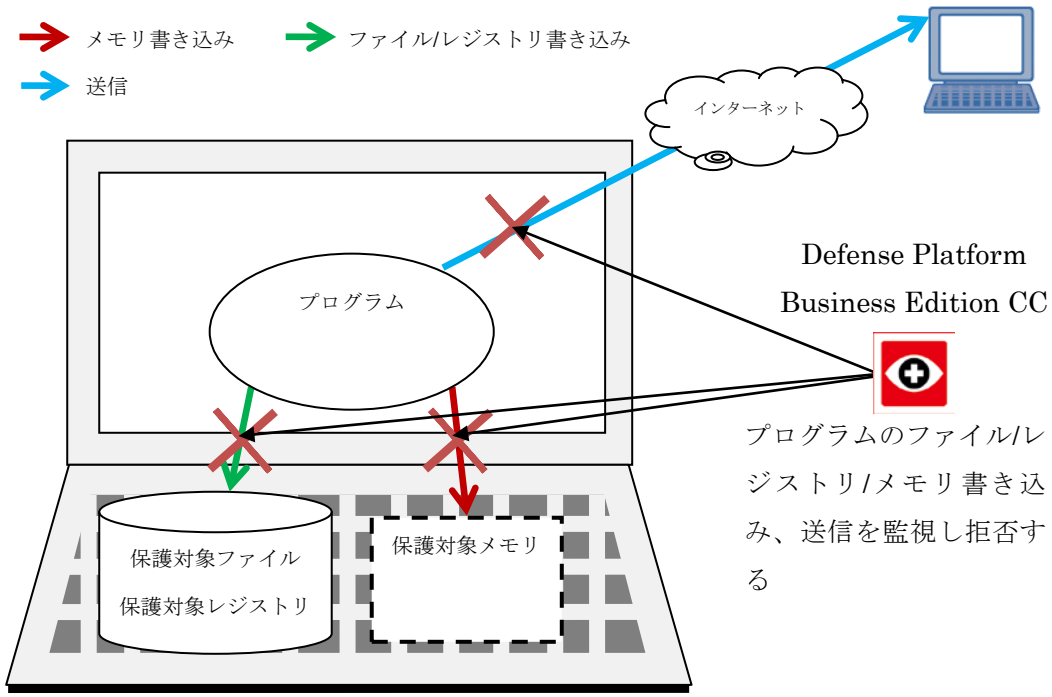

図 1-5 プログラムの監視と拒否

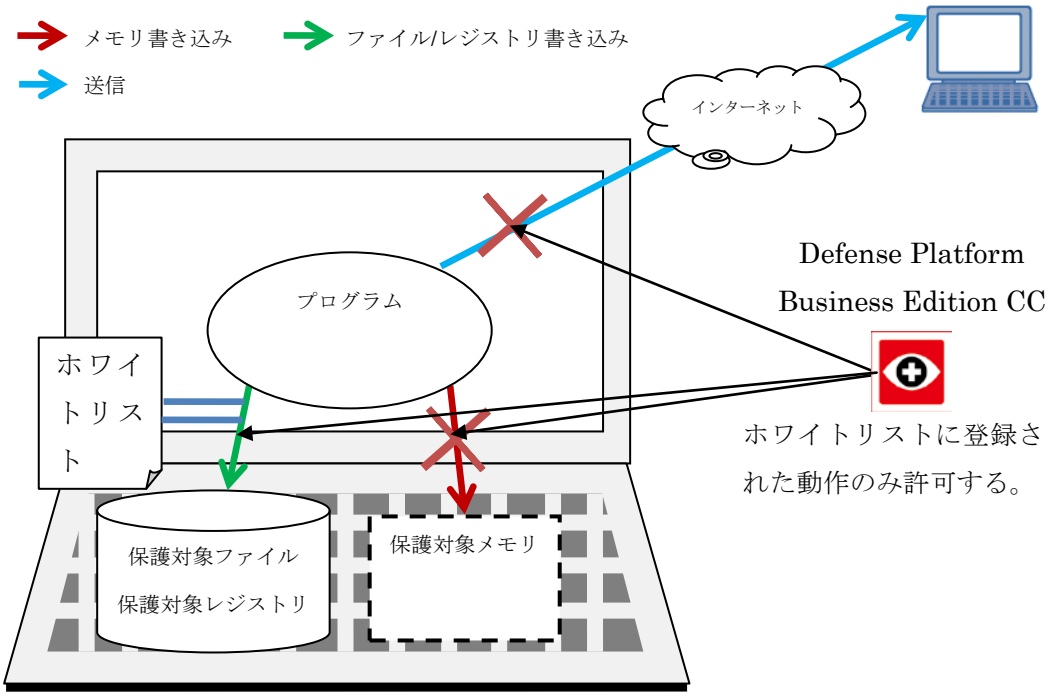

図 1-6 ホワイトリストによる動作の許可

管理者は、(3)管理機能を使用し、TOE の設定やホワイトリストの作成を行う。また、(2)監査機能(管理者向け機能)を使用してプログラムの動作や TOE の設定の変更について把握することができる。

PC 使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。

Windows ドメインによる時刻補正機能により、DeP サーバ PC および DeP クライアント PC の時刻が補正される。

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) 判定機能(DeP サーバ PC、DeP クライアント PC 共通)

判定機能は、検知したプログラムの動作の許可、拒否の判定を行う機能である。

プログラムの種類によっては、次のように、動作が定義されたものを、動作を行ったプログラムとして扱うことで、細かい制御ができるようにする。

A) インタプリタのように渡されたファイル(スクリプト)により動作が変わる以下のプログラムの場合は、渡されたファイル(スクリプト)をプログラムとして動作判定を行う。

1. 渡されたファイルによって動作の変わるプログラム(ファイルをプログラムとして判定)

コマンドプロンプト、WindowsScriptHost、Rundll32 ユーティリティプログラ

ム

2. Web 上の以下のスクリプトによって動作の変わるプログラム(URL をプログラムとして判定)
   InternetExplorer、Chrome、Firefox
   スクリプト:JavaScript、Silverlight

B) プラグインのように、外部の拡張モジュールを使用した動作を行うプログラムの場合は、拡張モジュールをプログラムとして動作判定を行う。

C) Office マクロによる動作の場合は、マクロを含むドキュメントファイルをプログラムとして動作判定を行う。

検知した動作の許可、拒否の判定にはホワイトリストを使用する。検知した動作がホワイトリストに定義された動作の場合は許可し、それ以外は拒否する。

(2) 監査機能

a. 動作履歴出力機能(DeP サーバ PC、DeP クライアント PC 共通)
   判定機能により検知された動作を動作履歴として出力し、一定のタイミングで DeP サーバ PC へ動作履歴をアップロードする機能である。

b. 管理者向け機能(DeP サーバ PC)
   管理者が DeP サーバ PC にて蓄積されている動作履歴を収集し、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、プログラムが保護資産に対して行った動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。

(3) 管理機能(DeP サーバ PC)

管理者が DeP サーバ PC 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、DeP の機能の設定を行う。また、管理者は DeP サーバ PC と全 DeP クライアント PC 上で有効になるホワイトリストの作成を行う。

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 2012 年 9 月 バージョン 3.1 改訂第 4 版 翻訳第 1.0 版
パート 2: セキュリティ機能コンポーネント 2012 年 9 月 バージョン 3.1 改訂第 4 版 翻訳第 1.0 版
パート 3: セキュリティ保証コンポーネント 2012 年 9 月 バージョン 3.1 改訂第 4 版 翻訳第 1.0 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

脅威を以下に示す。

T.WRITE_RESOURCE

プログラムが、管理者の許可なく保護対象を書き換える。

T.INFORMATION_LEAKAGE

プログラムが、管理者の許可なく外部にユーザデータをTCP/IPプロトコルおよびUDP/IPプロトコルにより送信する。

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_AUTHENTICATION

PC 使用者の使用するユーザアカウントはクライアントマシンの管理者権限を持たない。

A.NETWORK

サーバ/クライアント間の DeP 通信は、Windows の IP セキュリティポリシーにより通信パケットが暗号化された状態で行われる。

A.OPERATOR_MANAGEMENT

管理者は、信頼される者であり、不正な操作を行なわない。

A.UNJUST_SOFTWARE

クライアントマシンおよびサーバマシンには OS のセキュリティ対策用修正ソフトウェアおよびファームウェアのアップデートが適切に適用される。

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.REFUSE_WRITE

TOE は、プログラムが保護対象に書き込みを行った際に検知し、その動作がホワイトリストに定義されていなければ拒否しなければならない。また、TOE はプログラムによる保護対象への書き込み動作を管理者が監査できるようにしなければならない。また、TOE は DeP クライアント PC 上の監査データを不正な削除や改ざんから保護しなければならない。

O.REFUSE_SEND

TOE は、プログラムが外部へユーザデータの TCP/IP プロトコルおよび UDP/IP プロトコルによる送信を行った際に検知し、その動作がホワイトリストに定義されていなければ拒否しなければならない。また、TOE はプログラムによる外部へのユーザデータの TCP/IP プロトコルおよび UDP/IP プロトコルによる送信動作を管理者が監査できるようにしなければならない。また、TOE は DeP クライアント PC 上の監査データを不正な削除や改ざんから保護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

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 DeP サーバ PC を設置しなければならない。また、管理者は、管理者のみが DeP サーバ PC 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、DeP サーバ PC 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_AUTHENTICATION

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 PC 使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 PC 使用者の使用するユーザア

カウントに DeP クライアント PC の管理者権限を持たないように設定しなければならない。

OE.NETWORK

管理者は、DeP サーバ PC および DeP クライアント PC に適用される Windows の IP セキュリティポリシーの設定を行い、DeP サーバ PC と DeP クライアント PC 間の DeP 通信パケットが暗号化されるようにしなければならない。

OE.OPERATOR_MANAGEMENT

組織の責任者は、不正を行わない信頼され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.LOG_MANAGE

管理者は、DeP サーバ PC への動作履歴のアップロードが行われる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、定期的に動作履歴の収集を行い、集積履歴データを外部の機器にバックアップし、削除を行わなければならない。

OE. UNJUST_SOFTWARE

管理者は、DeP サーバ PC に OS のセキュリティ対策用修正ソフトウェアおよびファームウェアのアップデートを適切に適用しなければならない。管理者は、DeP クライアント PC についてファームウェアのアップデートを適切に適用し、PC 使用者が DeP クライアント PC について OS のセキュリティ対策用修正ソフトウェアを適切の適用するように PC 使用者を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.REFUSE_WRITE	O.REFUSE_SEND	OE.MANAGE_PC_PLACE	OE_USER_AUTHENTICATION	OE.NETWORK	OE.OPERATOR_MANAGEMENT	OE.UNJUST_SOFTWARE	OE.LOG_MANAGE
T.WRITE_RESOURCE	×		×					×
T.INFORMATION_LEAKAGE		×	×					×
A.MANAGE_SAFE_PLACE			×					
A.USER_AUTHENTICATION				×				
A.NETWORK					×			
A.OPERATOR_MANAGEMENT						×		
A.UNJUST_SOFTWARE							×	

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.WRITE_RESOURCE

この脅威は、プログラムが、管理者の許可なく保護対象に対して書き込みを行うことにより、システムもしくはアプリケーションが本来の正常な動作を行えなくなることである。この脅威に有効な対抗策について以下に述べる。

a. プログラムが、管理者の許可なく保護対象に対して書き込みを行い、システムやアプリケーシ

ョン本来の正常な動作を阻害する。

この脅威には、プログラムが保護対象に書き込み動作を行った際に、その動作がホワイトリストに定義されていない場合に拒否することで対抗することができる。ホワイトリストには、「書き込みを行ったプログラム」と「書き込み対象」の組み合わせによって動作を許可するかを、管理者によって定義することができる。つまり、ホワイトリストの定義を参照することにより、管理者が許可していない、プログラムによる保護対象への書き込みを拒否することができるので、上記の手段で脅威に対抗することができる。

O.REFUSE_WRITE は、プログラムによる保護対象への書き込みの試みを検知し、その動作がホワイトリストで定義されていなければ拒否する。また、保護対象への書き込みの試みを管理者が監査でき、DeP クライアント PC 上の監査ログを不正な削除や改ざんから守るようにする対策方針である。OE.MANAGE_PC_PLACE は DeP サーバ PC にアクセスし得るのを管理者のみにすることで、DeP サーバ PC 上の監査ログを不正な削除や改ざんから守るようにする対策方針である。OE.LOG_MANAGE は、監査ログが DeP サーバ PC にアップロードされ、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、保護対象への書き込みの許可、拒否を判定する判定機能(O.REFUSE_WRITE)、判定機能の監査(OE.LOG_MANAGE)、監査ログの保護(O.REFUSE_WRITE、OE.MANAGE_PC_PLACE) の組み合わせにより、この脅威を除去することができる。

以上、a の攻撃方法に対抗することは、T.WRITE_RESOURCE 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.REFUSE_WRITE、OE.MANAGE_PC_PLACE および OE.LOG_MANAGE によって、T.WRITE_RESOURCE に対抗できる。

T.INFORMATION_LEAKAGE

この脅威は、プログラムが、管理者の許可なく外部にユーザデータを TCP/IP プロトコルおよび UDP/IP プロトコルにより送信することで情報が漏えいすることである。この脅威に有効な対抗策について以下に述べる。

a. プログラムが、管理者の許可なく外部にユーザデータTCP/IPプロトコルおよびUDP/IPプロトコルにより送信する。

この脅威には、プログラムが、外部へのユーザデータの TCP/IP プロトコルおよび UDP/IP プロトコルによる送信動作を行った際に、その動作がホワイトリストに定義されていない場合に拒否することで対抗することができる。ホワイトリストには、「送信を行ったプログラム」と「送信先」の組み合わせによって動作を許可するかを、管理者によって定義することができる。つまり、ホワイトリストの定義を参照することにより、管理者が許可していない、プログラムによる外

部へのTCP/IPプロトコルおよびUDP/IPプロトコルによる送信を拒否することができるので、上記の手段で脅威に対抗することができる。

O.REFUSE_SEND はプログラムによる、外部へのユーザデータの TCP/IP プロトコルおよび UDP/IP プロトコルによる送信の試みを検知し、その動作がホワイトリストに定義されていなければ拒否する。また、外部へのユーザデータのTCP/IPプロトコルおよびUDP/IPプロトコルによる送信の試みを管理者が監査でき、DePクライアントPC上の監査ログを不正な削除や改ざんから守るようにする対策方針である。OE.MANAGE_PC_PLACE は DeP サーバ PC にアクセスし得るのを管理者のみにすることで、DeP サーバ PC 上の監査ログを不正な削除や改ざんから守るようにする対策方針である。OE.LOG_MANAGE は、監査ログが DeP サーバPCにアップロードされ、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、プログラムによる外部へのデータの TCP/IP プロトコルおよび UDP/IP プロトコルによる送信の許可、拒否を判定する判定機能(O.REFUSE_SEND)、判定機能の監査(OE.LOG_MANAGE) 、監査ログの保護 (O.REFUSE_SEND 、OE.MANAGE_PC_PLACE) の組み合わせにより、この脅威を除去することができる。

以上、a の攻撃方法に対抗することは、T.INFORMATION_LEAKAGE 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.REFUSE_SEND、OE.MANAGE_PC_PLACE および OE.LOG_MANAGE によって、T.INFORMATION_LEAKAGE に対抗できる。

○前提条件

A.MANAGE_SAFE_PLACE

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、管理者が DeP サーバ PC を管理者のみが入室可能な室内に設置し、DeP サーバ PC 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、管理者が管理者のみがパスワードを知りうるようにし、DeP サーバ PC 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_AUTHENTICATION

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. 権限の制限

PC 使用者の利用するユーザアカウントはクライアントマシンの管理者権限を持たない。OE.USER_AUTHENTICATION は、管理者が Windows ドメインを構築し、PC 使用者が利用するユーザアカウントに、DeP クライアント PC の管理者権限を持たないようにする。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、上記の a 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.NETWORK

この前提条件は、サーバ/クライアント間のネットワーク通信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/クライアント間の通信の暗号化

DeP サーバ PC と DeP クライアント PC 間の通信は暗号化される。OE.NETWORK は、管理者が、DeP サーバ PC および DeP クライアント PC に適用される Windows の IP セキュリティポリシーを設定し、DeP サーバ PC と DeP クライアント PC 間の通信パケットが暗号化されるようにする。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

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. 信頼される者の選任

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、組織の責任者が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。

A.UNJUST_SOFTWARE

この前提条件は、セキュリティ対策用修正ソフトウェアおよびファームウェアのアップデート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. セキュリティ対策用修正ソフトウェアおよびファームウェアのアップデートを適切に適用する

セキュリティ対策用修正ソフトウェアおよびファームウェアのアップデートの適用について、常に最新のものが適用される。OE. UNJUST_SOFTWARE は、常に最新のセキュリティ対策用修正ソフトウェアおよびファームウェアのアップデート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のセキュリティ対策方針は、OE. UNJUST_SOFTWARE である。

以上、上記 a に応じることは、A.UNJUST_SOFTWARE 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. UNJUST_SOFTWARE の達成によって A.UNJUST_SOFTWARE 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
動作判定サブジェクト	プログラムの動作を捕捉し、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
ファイル書き込み情報	保護対象ファイルへの書き込みを行うプログラムを識別する情報と書き込み先ファイルパス
レジストリ書き込み情報	保護対象レジストリへの書き込みを行うプログラムを識別する情報と書き込み先レジストリパスおよび値の名前
メモリ書き込み情報	保護対象メモリへの書き込みを行うプログラムを識別する情報と書き込み先メモリを所有するプログラムの実行ファイルパス
書き込み情報	ファイル書き込み情報、レジストリ書き込み情報、メモリ書き込み情報の総称
送信情報	送信を行うプログラムを識別する情報と送信先のIPアドレス(およびドメイン名)および使用ポート番号

表6-3. サブジェクトのセキュリティ属性の用語定義

用語	定義
プログラムを識別する情報	プログラムを識別するのに必要な以下の情報 ・デスクトップアプリの場合 実行ファイルパス、実行ファイルの会社名 ・ストアアプリの場合 表示名、実行ファイル名、パッケージ名、コマンドライン、会社名 ・拡張モジュールの場合

用語	定義
	実行ファイルパス、実行ファイルの会社名、モジュールファイルパス ・スクリプトもしくはマクロの場合 実行ファイルパス、実行ファイルの会社名、スクリプトもしくはマクロを実行するモジュールファイルパス、スクリプトのURLもしくはマクロを含むドキュメントファイルパス
許可する書き込み情報	管理者がホワイトリストに定義した以下のいずれかの情報 ・保護対象ファイルへの書き込みを行うプログラムを識別する情報と書き込み先ファイルパス（もしくは「MBR」） ・保護対象レジストリへの書き込みを行うプログラムを識別する情報と書き込み先レジストリキーパスおよび値の名前 ・保護対象メモリへの書き込みを行うプログラムを識別する情報と書き込み先メモリを所有するプログラムの実行ファイルパス
許可する送信情報	管理者がホワイトリストに定義した以下の情報 ・送信を行うプログラムを識別する情報と送信先のIPアドレス(およびドメイン名)および使用ポート番号
許可する動作情報	許可する書き込み情報、許可する送信情報の総称

表6-4. 情報のセキュリティ属性の用語定義

用語	定義
プログラム情報	プログラムを識別するのに必要な以下の情報 ・デスクトップアプリの場合 実行ファイルパス、実行ファイルの会社名 ・ストアアプリの場合 表示名、実行ファイル名、パッケージ名、コマンドライン、会社名 ・拡張モジュールの場合 実行ファイルパス、実行ファイルの会社名、モジュールファイルパス ・スクリプトもしくはマクロの場合

用語	定義
	実行ファイルパス、実行ファイルの会社名、スクリプトもしくはマクロを実行するモジュールファイルパス、スクリプトのURLもしくはマクロを含むドキュメントファイルパス
書き込み先ファイルパス	保護対象ファイルの作成、コピー、移動、保存、削除先のNTFSまたはFATファイルシステムのパス(MBRへの書き込みの場合は「MBR」)
書き込み先レジストリパス	保護対象レジストリの作成、変更、削除先のパスおよび値の名前
書き込み先プログラム	書き込み先保護対象メモリを所有するプログラムの実行ファイルパス
書き込み先情報	書き込み先ファイルパス、書き込み先レジストリパス、書き込み先プログラムの総称
送信先情報	送信先のIPアドレス(およびドメイン名)および使用ポート番号

表6-5. 操作の用語定義

用語	定義
ファイル書き込み操作	保護対象ファイルの作成、保護対象ファイルへのデータ書き込み、保護対象ファイルの削除
レジストリ書き込み操作	保護対象レジストリキーの作成、保護対象レジストリキーの削除、保護対象レジストリキーの値の作成、保護対象レジストリキーの値の変更、保護対象レジストリキーの値の削除
メモリ書き込み操作	保護対象メモリへのデータの書き込み
書き込み操作	ファイル書き込み操作、レジストリ書き込み操作、メモリ書き込み操作の総称
送信操作	TCP/IPプロトコルおよびUDP/IPプロトコルを使用した外部へユーザデータの送信を行う操作

表6-6. 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	ファイルシステム(NTFS、FAT)における拡張子

用語	定義
	を含むファイル名
フォルダパス	ファイルシステム(NTFS、FAT)における絶対パスからファイル名を除いたもの
レジストリパス	レジストリキーのパス
レジストリ名	レジストリキーの値の名前
ポート番号	通信に使用するポート番号
IPアドレス(ドメイン)	接続元、接続先もしくは送信先IPアドレス(およびドメイン名)
追加情報	操作によって異なる補足の情報
プログラム名	プログラムのファイル名
日時	年月日時分秒
親プロセス名	操作を行ったプログラムを起動したプログラムの実行ファイル名
起動ドライブ情報	プログラムが起動したドライブの種別 ローカルドライブ、リムーバブル、CD/DVD、ネットワークドライブのいずれか
モジュールパス	操作を行ったプログラムが拡張モジュールの場合の拡張モジュールのファイルパス
インタプリタ名	操作を行ったプログラムがスクリプトの場合のインタプリタ名
スクリプト名	操作を行ったプログラムがスクリプトの場合のスクリプトのファイルパスもしくはURL
メールアドレス・件名	操作を行ったプログラムがメーラから起動された場合の添付されていたメールの差出人のメールアドレスおよびメールの件名
アプリケーションの種別	操作を行ったプログラムがインストーラの場合は「インストーラ」、アンインストーラの場合は「アンインストーラ」、ストアアプリのインストーラの場合は「ストアアプリのインストーラ」、ストアアプリの場合は「ストアアプリ」
起動元情報	操作を行ったプログラムがエクスプローラから起動された場合は「エクスプローラ」、スタートアップによって起動された場合は「スタートアップ」
起動方法	操作を行ったプログラムがユーザ操作によって起

用語	定義
	動された場合は「手動」、それ以外の場合は「自動」
システムアプリケーション情報:備考	システムアプリケーション(XCOPY、ROBOCOPY、NETSHなど)を用いて操作を行った場合に、そのシステムアプリケーションの名前と操作対象の情報
ストアアプリの表示名	操作を行ったプログラムがストアアプリの場合、そのストアアプリの表示名
プログラム詳細情報	操作を行ったプログラムに関する以下の項目 ※情報が存在しない項目は空とする ・プロセスID、親プロセス名、バージョン、ファイルサイズ、更新日時、会社名、デジタル署名の有無、起動ドライブ情報、ハッシュ値、モジュールパス、インタプリタ名、スクリプト名、メールアドレス・件名、アプリケーションの種別、起動元情報、起動方法、システムアプリケーション情報:備考、ストアアプリの表示名
ユーザ名	Windowsドメインのユーザ名
動作名	操作の種別を示す名称(判定結果(許可/拒否)を含む)

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 6-7. TOE の監査対象事象

機能要件	TOE の監査対象事象
FDP_IFF.1(1)	プログラムによる書き込み操作の許可/拒否
FDP_IFF.1(2)	プログラムによる送信操作の許可/拒否
FMT_SMF.1	サーバ設定ツールによる設定値(許可する動作情報)の問い合わせ、改変、削除

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*]:以下の通り

表 6-8. その他の監査記録情報

機能要件、監査対象事象	監査記録情報
FMT_SMF.1 のサーバ設定ツールによる設定値(許可する動作情報)の改変、削除	サーバ設定の設定内容
FMT_SMF.1 のサーバ設定ツールによる設定値(許可する動作情報)の問い合わせ	マシン名、追加情報、プログラム名、ユーザ名、バージョン
FDP_IFF.1(1)のファイル書き込み操作	マシン名、ファイル名、フォルダパス、追加情報、プログラム名、プログラム詳細情報、ユーザ名
FDP_IFF.1(1)のレジストリ書き込み操作	マシン名、レジストリパス、レジストリ名、追加情報、プログラム名、プログラム詳細情報、ユーザ名

機能要件、監査対象事象	監査記録情報
FDP_IFF.1(1)のメモリ書き込み操作	マシン名、書き込み先プログラムのファイル名、書き込み先プログラムのパス、プログラム名、プログラム詳細情報、ユーザ名
FDP_IFF.1(2)	マシン名、ポート番号、IP アドレス(ドメイン)、追加情報、プログラム名、プログラム詳細情報、ユーザ名

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*]:すべての監査情報

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、FMT_SMF.1のサーバ設定ツールによる設定値(許可する動作情報)の問い合わせ、FDP_IFF.1(1)、FDP_IFF.1(2)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:*選択方法、及びまたは 並べ替え方法*]:下表の方法

表 6-9. 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
ユーザ名、マシン名	分類して出力
動作名、日時	選択して出力

FAU_STG.1 保護された監査証跡格納

下位階層: なし

依存性: FAU_GEN.1 監査データ生成

FAU_STG.1.1 TSF は、DePクライアントPC上の監査証跡に格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2 TSFは、DePクライアントPC上の監査証跡に格納された監査記録への不正な改変を[選択: *防止*、*検出*: から1 つのみ選択]できなければならない。

[選択: *防止*、*検出*: から 1 つのみ選択]:防止

○利用者データ保護(FDP)

FDP_IFC.1(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(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:動作判定サブジェクト
情報:書き込み情報
操作:書き込み操作
[割付:*情報フロー制御 SFP*]:書き込み制御 SFP

FDP_IFF.1(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(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*]: 書き込み制御 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*]: 以下の通り

表 6-10. サブジェクトのリストと対応するセキュリティ属性

サブジェクト	セキュリティ属性
動作判定サブジェクト	許可する書き込み情報のリスト

表 6-11.情報のリストと対応するセキュリティ属性

情報	セキュリティ属性
書き込み情報	プログラム情報
	書き込み先情報

FDP_IFF.1.2(1) 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*]: 以下の通り

表 6-12.セキュリティ属性に基づく情報フロー制御のルール

情報	情報のセキュリティ属性	サブジェクト	サブジェクトのセキュリティ属性	操作	情報フロー制御のルール
書き込み情報	・プログラム情報 ・書き込み先情報	動作判定サブジェクト	・許可する書き込み情報のリスト	書き込み操作	プログラム情報と書き込み先情報の組み合わせが許可する書き込み情報のリストに含まれない場合は操作を拒否する。

FDP_IFF.1.3(1) 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(1) 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(1) 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

FDP_IFC.1(2) 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(2) 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:動作判定サブジェクト
情報:送信情報
操作:送信操作

[割付:*情報フロー制御 SFP*]:送信制御 SFP

FDP_IFF.1(2) 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(2) 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*]:送信制御 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*]:以下の通り

表 6-13. サブジェクトのリストと対応するセキュリティ属性

サブジェクト	セキュリティ属性
動作判定サブジェクト	許可する送信情報のリスト

表 6-14.情報のリストと対応するセキュリティ属性

情報	セキュリティ属性
送信情報	プログラム情報
	送信先情報

FDP_IFF.1.2(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*]:以下の通り

表 6-15.セキュリティ属性に基づく情報フロー制御のルール

情報	情報のセキュリティ属性	サブジェクト	サブジェクトのセキュリティ属性	操作	情報フロー制御のルール
送信情報	・プログラム情報 ・送信先情報	動作判定サブジェクト	・許可する送信情報のリスト	送信操作	プログラム情報と送信先情報の組み合わせが許可する送信情報のリストに含まれない場合は操作を拒否する。

FDP_IFF.1.3(2) 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(2) 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(2) 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

○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*]:

- 管理者がセキュリティ属性(許可する動作情報)を問い合わせ、改変、削除する機能
- 管理者が履歴データ、集積履歴データを削除する機能

表6-16. 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	—	—
FAU_SAR.1	a) 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)。	a) なし	a) Windows によりユーザの管理を行っているため
FAU_SAR.3	なし	—	—
FAU_STG.1	なし	—	—
FDP_IFC.1(1)	なし	—	—
FDP_IFF.1(1)	a) 明示的なアクセスに基づく決定に使われる属性の管理。	a) サーバ設定ツールにて、許可する書き込み情報を設定する	—
FDP_IFC.1(2)	なし	—	—
FDP_IFF.1(2)	a) 明示的なアクセスに基づく決定に使われる属性の管理。	a) サーバ設定ツールにて、許可する送信情報を設定する	—
FMT_SMF.1	なし	—	—
FPT_STM.1	a) 時間の管理。	a) なし	a) Windows ドメインにより時刻管理を行っているため

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 6-17. 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6-18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 6-18. 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.REFUSE_WRITE	O.REFUSE_SEND
FAU_GEN.1	×	×
FAU_SAR.1	×	×
FAU_SAR.3	×	×
FAU_STG.1	×	×
FDP_IFC.1(1)	×	
FDP_IFC.1(2)		×
FDP_IFF.1(1)	×	
FDP_IFF.1(2)		×
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.REFUSE_WRITE

この TOE セキュリティ対策方針は、プログラムが保護対象に書き込みを行った際に検知し、その動作がホワイトリストに定義されていなければ拒否することを求めている。また、プログラムによる保護対象に対する書き込み動作を管理者が監査できるようにすることを求めている。さらに、DeP クライアント PC 上の監査データを不正な削除や改ざんから保護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. プログラムが保護対象に書き込みを行った際に検知し、その動作がホワイトリストに定義されていなければ拒否する

TOE は、プログラムが保護対象に書き込みを行った際に、その動作を検知し、その動作がホワイトリストに定義されていなければ拒否する。FDP_IFC.1(1)および FDP_IFF.1(1)は、保護対象への書き込み動作が、「許可する書き込み情報のリストに含まれない動作」の場合に、その動作を拒否する機能要件である。「許可する書き込み情報のリストに含まれない動作」は

「ホワイトリストに定義されていない動作」を示す。よって、保護対象への書き込み動作が、「ホワイトリストに定義されていない動作」の場合に、その動作を拒否する。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(1)および FDP_IFF.1(1)である。

b. プログラムによる保護対象への書き込み動作を監査し、DeP クライアント PC 上の監査データを不正な削除や改ざんから保護する

TOE は、プログラムによる保護対象への書き込み動作を把握するために、監査機能を有する必要がある。さらに、DeP クライアント PC 上の監査データを不正な削除や改ざんから保護する必要がある。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。FAU_STG.1 は DeP クライアント PC 上で生成した監査データを不正な削除および改変から保護する機能要件である。因みに、DeP サーバ PC 上の監査データは OE.MANAGE_PC_PLACE によって物理的に保護される。FAU_GEN.1 で規定した監査事象のうち、FDP_IFF.1(1)(プログラムによる書き込み操作の許可/拒否)の監査事象を生成することにより、保護対象への書き込み動作を監査することができる。FMT_SMF.1(サーバ設定ツールによる設定値(許可する書き込み情報)の問い合わせ、改変、削除)の監査事象を生成することにより、許可する書き込み情報の設定変更を把握することができる。ただし、監査記録時の時刻は Windows のシステム時刻を使用しているが、TOE によるシステム時刻の変更の監査は行っていない。しかし、Windows の特権使用の監査ポリシーにより、システム時刻の変更のイベントログ出力が行われる為、イベントログを参照することで、時刻の変更を監査することができる。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 : FDP_IFF.1(1)、FMT_SMF.1)、FAU_STG.1、FPT_STM.1、FAU_SAR.1、FAU_SAR.3 である。

c. 管理機能を有する

TOE は、監査機能および判定機能に関する管理機能を有する必要がある。FMT_SMF.1 は、判定機能の許可する書き込み情報の設定の管理機能、監査機能の履歴データ、集積履歴データの管理機能、これらの管理機能を管理者が実行することができる機能要件である。従って、この対策に該当するセキュリティ機能要件は、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.REFUSE_WRITE 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 FAU_GEN.1、FAU_SAR.1、FAU_SAR.3、FAU_STG.1、FDP_IFC.1(1)、FDP_IFF.1(1)、FMT_SMF.1 および FPT_STM.1 の達成により O.REFUSE_WRITE を実現できる。

O.REFUSE_SEND

この TOE セキュリティ対策方針は、プログラムが外部へユーザデータの TCP/IP プロトコルおよび UDP/IP プロトコルによる送信を行った際に検知し、その動作がホワイトリストに定義されていな

ければ拒否することを求めている。また、プログラムによる外部へのユーザデータのTCP/IPプロトコルおよび UDP/IP プロトコルによる送信動作を管理者が監査できるようにすることを求めている。さらに、DeP クライアント PC 上の監査データを不正な削除や改ざんから保護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. プログラムが外部へユーザデータの TCP/IP プロトコルおよび UDP/IP プロトコルによる送信を行った際に検知し、その動作がホワイトリストに定義されていなければ拒否する

TOE は、プログラムが外部へユーザデータの TCP/IP プロトコルおよび UDP/IP プロトコルによる送信を行った際に、その動作を検知し、その動作がホワイトリストに定義されていなければ拒否する。FDP_IFC.1(2)および FDP_IFF.1(2)は、外部へのユーザデータの TCP/IP プロトコルおよび UDP/IP プロトコルによる送信動作が、「許可する送信情報のリストに含まれない動作」の場合に、その動作を拒否する機能要件である。「許可する送信情報のリストに含まれない動作」は「ホワイトリストに定義されていない動作」を示す。よって、外部へのユーザデータの TCP/IP プロトコルおよび UDP/IP プロトコルによる送信動作が、「ホワイトリストに定義されていない動作」の場合に、その動作を拒否する。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(2)および FDP_IFF.1(2)である。

b. プログラムによる外部へのユーザデータの TCP/IP プロトコルおよび UDP/IP プロトコルによる送信動作を監査し、DeP クライアント PC 上の監査データを不正な削除や改ざんから保護する

TOE は、プログラムによる外部へのユーザデータの TCP/IP プロトコルおよび UDP/IP プロトコルによる送信動作を把握するために、監査機能を有する必要がある。さらに、DeP クライアント PC 上の監査データを不正な削除や改ざんから保護する必要がある。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。FAU_STG.1 は DeP クライアント PC 上で生成した監査データを不正な削除および改変から保護する機能要件である。因みに、DeP サーバ PC 上の監査データは OE.MANAGE_PC_PLACE によって物理的に保護される。FAU_GEN.1 で規定した監査事象のうち、FDP_IFF.1(2)(プログラムによる送信操作の許可/拒否)の監査事象を生成することにより、外部へのユーザデータの TCP/IP プロトコルおよび UDP/IP プロトコルによる送信動作を監査することができる。FMT_SMF.1(サーバ設定ツールによる設定値(許可する送信情報)の問い合わせ、改変、削除)の監査事象を生成することにより、許可する送信情報の設定変更を把握することができる。ただし、監査記録時の時刻は Windows のシステム時刻を使用しているが、TOE によるシステム時刻の変更の監査は行っていない。しかし、Windows の特権使用の監査ポリシーにより、システム時刻の変更のイベントログ出力が行われる為、イベントログを参照することで、時刻の変更を監査することができる。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:FDP_IFF.1(2)、FMT_SMF.1)、

FAU_STG.1、FPT_STM.1、FAU_SAR.1、FAU_SAR.3 である。

c. 管理機能を有する

TOE は、監査機能および判定機能に関する管理機能を有する必要がある。FMT_SMF.1 は、判定機能の許可する送信情報の設定の管理機能、監査機能の履歴データ、集積履歴データの管理機能、これらの管理機能を管理者が実行することができる機能要件である。従って、この対策に該当するセキュリティ機能要件は、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.REFUSE_SEND 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 FAU_GEN.1、FAU_SAR.1、FAU_SAR.3、FAU_STG.1、FDP_IFC.1(2)、FDP_IFF.1(2)、FMT_SMF.1 および FPT_STM.1 の達成により O.REFUSE_SEND 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 6-19 に示す。

表 6-19. 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	FAU_STG.1	FAU_GEN.1	FAU_GEN.1	なし	—
5	FDP_IFC.1(1)	FDP_IFF.1	FDP_IFF.1(1)	なし	—
6	FDP_IFC.1(2)	FDP_IFF.1	FDP_IFF.1(2)	なし	—
8	FDP_IFF.1(1)	FDP_IFC.1	FDP_IFC.1(1)	なし	—
		FMT_MSA.3	なし	FMT_MSA.3	※1
9	FDP_IFF.1(2)	FDP_IFC.1	FDP_IFC.1(2)	なし	—
		FMT_MSA.3	なし	FMT_MSA.3	※1
11	FMT_SMF.1	なし	なし	なし	—
12	FPT_STM.1	なし	なし	なし	—

※1　FMT_MSA.3 に対する依存性の欠如の妥当性について

TOE において、情報のセキュリティ属性は、情報が本来持つセキュリティ属性しか存在せず、TOE によって管理することが可能なセキュリティ属性ではない為、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、許可されていないプログラムの動作を禁止することで、マルウェアの可能性のあるプログラムによって、システムやアプリケーションのファイルやレジストリ、実行中のメモリが書き換えられ、正常に動作しなくなったり、マシン上の情報が漏えいしたりすることを防止する商用製品である。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.JUDGE	SF.ADMIN
FAU_GEN.1	×		
FAU_SAR.1	×		
FAU_SAR.3	×		
FAU_STG.1	×		
FDP_IFC.1(1)		×	
FDP_IFC.1(2)		×	
FDP_IFF.1(1)		×	
FDP_IFF.1(2)		×	
FMT_SMF.1			×
FPT_STM.1	×		

7.1.1 監査機能(SF.AUDIT)

監査機能は、判定機能により検知された動作を動作履歴として記録し、DeP サーバ PC にアップロードされ、管理者が DeP サーバ PC でその動作履歴を収集して閲覧できる状態にできる機能である。判定機能により検知された、プログラムが行った動作は動作履歴として出力される。各 PC で出力された動作履歴は管理者が定めたタイミングで DeP サーバ PC にアップロードされる。管理者は DeP サーバ PC 上でトレーサを用いて、DeP サーバ PC に蓄積された動作履歴を収集し、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、動作履歴とは別に、管理者が DeP サーバ PC で行ったサーバ設定ツールによる設定の変更を記録する。

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」の動作履歴を出力する。Windows の動作履歴を出力することにより、監査機能の起動と終了の監査履歴が取られる。

TOE の動作履歴には、すべての動作においてマシン名、プログラム名、動作名、日時、ユーザ名が含まれる。ファイル書き込み動作ではファイル名、フォルダパス、追加情報、プログラム詳細情報が含まれる。レジストリ書き込み動作ではレジストリパス、レジストリ名、追加情報、プログラム詳細情報が含まれる。メモリ書き込み動作では書き込み先プログラム、プログラム詳細情報が含まれる。TCP/IP プロトコルおよび UDP/IP プロトコルを使用した外部へのユーザデータの送信動作ではポート番号、IP アドレス(ドメイン) 、追加情報、プログラム詳細情報が含まれる。起動動作では追加情報、バージョンが含まれる。

判定機能の対象になるプログラムの動作には次のものがある。動作:プログラムによる書き込み操作、プログラムによる送信操作。動作判定の結果、拒否された場合は動作名の前に「拒否-」と付加される。許可された場合には動作名のみが出力される。

サーバ設定ツールを使用し、セキュリティ属性を改変、削除した際に、サーバ設定の変更履歴を出力する。サーバ設定の変更履歴には、日時、変更内容が含まれる。

サーバ設定ツールを起動すると設定が表示され、サーバ設定ツールの起動を示す動作履歴を出力する。サーバ設定ツールを起動することで、セキュリティ属性の問い合わせができる。サーバ設定ツールの起動を示す動作履歴を出力することにより、セキュリティ属性の問い合わせの監査履歴が取られる。

(2) FAU_SAR.1 監査レビュー

DeP サーバ PC にインストールされるトレーサを用いて、管理者は DeP サーバ PC に集積された動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(もしくはレジストリ名、書き込み先プログラムのファイル名、ポート番号)、フォルダパス(もしくはレジストリパス、書き込み先プログラムのパス、IP アドレス(およびドメイン名))、追加情報、プログラム名、動作名(判定機能による判定結果(許可/拒否)含む)、ユーザ名、日時、プログラム詳細情報(もしくはバージョン情報)。

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 DeP サーバ PC 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

DeP サーバ PC にインストールされるトレーサを用いて、管理者が DeP サーバ PC に集積された動作履歴を 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. 動作履歴の分類と選択

関連の基準	方法
ユーザ名、マシン名	分類して出力
動作名、日時	選択して出力

(4) FAU_STG.1 保護された監査証跡格納

TOE は、DeP クライアント PC 上に蓄積された動作履歴のファイルに対して、他のプログラムが削除や書き込みを行えないように排他制御を行い、DeP サーバ PC にアップロードされるまで不正な削除および改変から保護する。

(5) FPT_STM.1 高信頼タイムスタンプ

TOE は、Windows ドメインの時刻補正機能により補正されている日時情報を Windows から取得し、動作履歴の日時に利用する。

7.1.2 判定機能(SF.JUDGE)

判定機能は、プログラムが対象の動作(保護対象への書き込み、外部へのユーザデータの送信(TCP/IP プロトコルおよび UDP/IP プロトコルによる送信))を行った際に、その動作を検知し、TOE で予め定義されている基準もしくはホワイトリストを参照して、その動作を許可もしくは拒否する機能である。

7.1.2.1 対応する SFR の実現方法

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

TOE は、OS が提供するファイル操作命令、レジストリ操作命令、メモリ操作命令を捕捉することで、プログラムによる保護対象への書き込みを検知し、許可か拒否の判定を行う。書き込みを行ったプログラムと書き込み先(ファイルパスもしくはレジストリパスもしくはプログラム)の組み合わせが、管理者がサーバ設定ツールで設定した許可する書き込み情報のリストに含まれない場合は拒否する。

(2) FDP_IFC.1(2) サブセット情報フロー制御、FDP_IFF.1(2) 単純セキュリティ属性

TOE は、OS が提供する通信命令を捕捉することで、プログラムによる外部へのユーザデ

ータの送信(TCP/IP プロトコルおよび UDP/IP プロトコルによる送信)を検知し、許可か拒否の判定を行う。送信を行ったプログラムと送信先(IP アドレスと使用ポート)の組み合わせが、管理者がサーバ設定ツールで設定した許可する送信情報のリストに含まれない場合は拒否する。

7.1.3 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、DeP サーバ PC 上で使用できるサーバ設定ツールによって提供される。サーバ設定ツールによって、判定機能の各種設定が個別に可能である。また、DeP サーバ PC 上で使用できるトレーサによって履歴データ、集積履歴データを削除することができる。

7.1.3.1 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 DeP サーバ PC 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、変更、削除することができる。

- 許可する書き込み情報のリスト
  プログラムを識別する情報と対象操作(ファイル書き込み、レジストリ書き込み、メモリ書き込み)と許可する書き込み先情報の組み合わせを指定する。
- 許可する送信情報のリスト
  プログラムを識別する情報と対象操作(送信)と許可する送信先情報の組み合わせを指定する。

プログラムを識別する情報は表 7-3 に示すように、ファイルパス、会社名、モジュールパス、スクリプト名の組み合わせにより指定する。ただし、ストアアプリの場合は、表示名、実行ファイル名、パッケージ名、コマンドライン、会社名の組み合わせを指定する。

対象操作は、ファイル書き込み、レジストリ書き込み、メモリ書き込み、送信のいずれかを指定する。

許可する書き込み先情報および許可する送信先情報は表 7-4 に示す値を指定する。

各設定項目は正規表現が使用できる。

表7-3. プログラムを識別する情報の設定項目

プログラムの種類	ファイルパス	会社名	モジュールパス	スクリプト名
デスクトップア	実行ファイルパ	実行ファイル	指定なし	指定なし

プログラムの種類	ファイルパス	会社名	モジュールパス	スクリプト名
プリ	ス	の会社名		
拡張モジュール	実行ファイルパス	実行ファイルの会社名	モジュールファイルパス	指定なし
スクリプト	実行ファイルパス	実行ファイルの会社名	スクリプトを実行するモジュールファイルパス	スクリプトのURL
マクロ	実行ファイルパス	実行ファイルの会社名	マクロを実行するモジュールファイルパス	マクロを含むドキュメントファイルパス
ファイル※	指定なし	指定なし	指定なし	動作が定義されたファイルパス

※ 以下のプログラム上で動作する、動作が定義されたファイル
コマンドプロンプト、WindowsScriptHost、Rundll32 ユーティリティプログラム

表7-4. 許可する操作対象の設定項目

情報	設定項目
許可する書き込み先情報	・保護対象ファイルへの書き込みの場合 書き込み先ファイルパス（もしくは「MBR」） ・保護対象レジストリへの書き込みの場合 書き込み先レジストリキーパスおよび値の名前 ・保護対象メモリへの書き込みの場合 書き込み先メモリを所有するプログラムの実行ファイルパス
許可する送信先情報	送信先のIPアドレス(およびドメイン名)および使用ポート番号

※ 判定機能で利用される FDP_IFF.1(1)による要求は、許可する書き込み情報のリストの設定により実現される。
判定機能で利用される FDP_IFF.1(2)による要求は、許可する送信情報のリストの設定により実現される。

管理者は DeP サーバ PC 上で使用するトレーサを用いて、履歴データ、集積履歴データを削除することができる。

本セキュリティターゲット（以下 本書）及びその中に記載されているディフェンスプラットフォーム ビジネスエディション サーバ、ディフェンスプラットフォーム ビジネスエディション クライアントは、ハミングヘッズ株式会社（以下ハミングヘッズ）が提供するライセンスの所有者に対してのみ供給され、同ライセンスの許可する条件のもとでのみ使用または複製することが許されます。