認 証 報 告 書

独立行政法人情報処理推進機構
理事長　富田　達夫

原紙押印済

評価対象

申請受付日（受付番号）	平成27年1月13日 (IT認証5526)
認証番号	C0532
認証申請者	ハミングヘッズ株式会社
TOEの名称	Defense Platform Business Edition CC
TOEのバージョン	Ver.3.6.1.5
PP適合	なし
適合する保証パッケージ	EAL3
開発者	ハミングヘッズ株式会社
評価機関の名称	一般社団法人ITセキュリティセンター 評価部

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。

平成28年12月9日

技術本部
セキュリティセンター 情報セキュリティ認証室
技術管理者　山里　拓己

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① 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 バージョン3.1 リリース4
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 リリース4

評価結果：合格

「Defense Platform Business Edition CC」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

この認証報告書は、ハミングヘッズ株式会社が開発した「Defense Platform Business Edition CC、Ver.3.6.1.5」（以下「本 TOE」という。）について一般社団法人 IT セキュリティセンター 評価部（以下「評価機関」という。）が平成 28 年 11 月 16 日に完了した IT セキュリティ評価に対し、その内容の認証結果を申請者であるハミングヘッズ株式会社に報告するとともに、本 TOE に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書とともに提供されるセキュリティターゲット（以下「ST」という。）を併読されたい。特に本 TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、ST において詳述されている。

本認証報告書は、本 TOE を購入する調達者を読者と想定している。本認証報告書は、本 TOE が適合する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本 TOE の機能、運用条件の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 保証パッケージ

本 TOE の保証パッケージは、EAL3 である。

1.1.2 TOEとセキュリティ機能性

本 TOE は、Windows 8.1 Enterprise 64bit または Windows Server 2012 R2 Standard 64bit を搭載した PC 用の、ホワイトリスト型のマルウェア対策製品である。

本 TOE は、マルウェアの典型的な動作である潜伏活動やネットワーク送信に着目し、それを防止するために、管理者が許可設定したホワイトリストに基づいて、プログラムの動作の許可と拒否を制御するセキュリティ機能を提供する。

本 TOE にあらかじめ設定しておく情報は、管理者の許可するプログラムの動作であるため、個別のマルウェアを検出するための情報を設定・更新する必要はない。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で評価が行われた。本 TOE が想定する脅威及び前提については次項のとおりである。

1.1.2.1 脅威とセキュリティ対策方針

本 TOE は、以下の脅威を想定しており、それに対抗するセキュリティ機能を提供する。

一般に、PC がマルウェアに感染すると、ファイルの改ざんや情報漏えいなど、様々な悪影響がある。

本 TOE は、マルウェアの活動を防止するために、マルウェアの典型的な動作である潜伏活動やネットワーク送信に着目し、管理者の許可していないシステムファイルや実行中のプログラム等への書き込みとネットワーク送信を防止するセキュリティ機能を提供する。これによりマルウェアによる様々な悪影響を未然に防止する。

1.1.2.2 構成要件と前提条件

本 TOE は、次のような構成及び前提で運用することを想定する。

- 本 TOE の運用環境は、Windows Server 2012 R2 Standard 64bit を搭載したサーバ PC と、Windows 8.1 Enterprise 64bit を搭載したクライアント PC で構成された、Windows ドメインの環境を想定する。
- 本 TOE を搭載する PC は、セキュアブートの設定がされており、OS に標準搭載されていない追加の API を提供するカーネル内ソフトウェアが導入されていない構成を想定する。
- 本 TOE を搭載する PC のファームウェア及び OS は、安全性を保つために、それらの更新を適用する運用がされていることを想定する。

1.1.3 免責事項

本 TOE は、以下の脅威には対抗していない。

- 本 TOE は、利用者のファイルの改ざんの脅威は想定していない。
- 本 TOE は、TCP/IP と UDP/IP 以外のプロトコルによるネットワーク送信の脅威は想定していない。対応していないプロトコルには、ICMP も含まれる。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価・認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって本 TOE に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 28 年 11 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、所見報告書、及び関連する評価証拠資料を検証し、本 TOE の評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。認証機関が指摘した問題点は、すべて解決され、かつ、TOE の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 TOE識別

本 TOE は、以下のとおり識別される。

TOE名称：	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

TOE 名称は以下の製品の総称であり、TOE には以下の製品すべてが含まれる。また、以下の製品のバージョンは、すべて、上記のバージョンと同一である。

・ディフェンスプラットフォーム ビジネスエディション クライアント
（以下「DeP クライアント」という。）
・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
（以下「DeP サーバ」という。）

製品が評価･認証を受けた本 TOE であることを、利用者は、製品を格納した CD-ROM のラベルで確認することができる。

3 セキュリティ方針

本章では、本 TOE が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

本 TOE は、マルウェア対策を目的とした製品である。本 TOE は、マルウェアの典型的な動作である、システムファイルや実行中のプログラム等への潜伏とネットワーク送信に着目し、マルウェアの動作を防止するセキュリティ機能を提供する。

マルウェアの動作防止にあたっては、マルウェア毎の個別の情報設定が不要となるように、管理者の許可するプログラムの動作を設定するホワイトリスト方式を採用する。

3.1 セキュリティ機能方針

本 TOE は、3.1.1 に示す脅威に対抗するセキュリティ機能を具備する。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

本 TOE は、表 3-1 に示す脅威を想定し、これに対抗する機能を備える。

表3-1 想定する脅威

識別子	脅威
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。 注1）本脅威は、マルウェアの潜伏活動に着目したものであり、「保護対象」はシステムファイルや実行中のプログラム等である。利用者のファイルは含まない。詳細は「11 用語」を参照。 注2）本TOEは、OSのブートメカニズムが「セキュアブート」で保護されていることを前提としている。しかし、MBR領域を書き換えるマルウェアを検出するために、「保護対象」にはMBR領域も含まれている。 注3）管理者が書き換えを許可することのできる「保護対象」に、本TOEのホワイトリストは含まれていない。 ホワイトリスト等のTOEが使用するデータは、本TOEが、自己保護のために、OSのAPIを捕捉して他プログラムによる書き換えを防止している。

識別子	脅威
T.INFORMATION_LEAKAGE	プログラムが、管理者の許可なく外部にデータをTCP/IPプロトコルおよびUDP/IPプロトコルにより送信する。

3.1.1.2 脅威に対するセキュリティ機能方針

本 TOE は、表 3-1 に示す脅威に対し、以下のセキュリティ機能方針で対抗する。なお、各セキュリティ機能の詳細は、5 章に示す。

(1) 脅威「T. WRITE_RESOURCE」「T.INFORMATION_LEAKAGE」への対抗

TOE は「判定機能」で本脅威に対抗し、その機能の運用を「管理機能」と「監査機能」で補助する。

TOE の「判定機能」は、OS の API を捕捉してプログラムの動作を監視し、管理者の設定したホワイトリストに基づいて、「保護対象」への書き込み及び TCP/IP と UDP/IP によるネットワーク送信の許可と拒否を制御する。

TOE の「管理機能」は、管理者に対して、判定機能で参照するホワイトリストの設定と、監査機能で蓄積された監査記録を削除する機能を提供する。

TOE の「監査機能」は、判定機能による許可と拒否、及び、管理機能によるホワイトリストの設定の監査記録を生成し、それを管理者が読み出す機能を提供する。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

本 TOE の利用に当たって要求される組織のセキュリティ方針はない。

4 前提条件と評価範囲の明確化

本章では、想定する読者が本 TOE の利用の判断に有用な情報として、本 TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

本 TOE を運用する際の前提条件を表 4-1 に示す。これらの前提条件が満たされない場合、本 TOE のセキュリティ機能が有効に動作することは保証されない。

表4-1 前提条件

識別子	前提条件
A.MANAGE_SAFE_PLACE	サーバPC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PC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PCの管理者権限を持たない。
A.NETWORK	サーバPCとクライアント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PCおよびサーバPCにはOSのセキュリティ対策用修正ソフトウェア及びPCのファームウェアのアップデートが適切に適用される。 注) PCのファームウェアのアップデートは、「セキュアブート」の実装上の欠陥を悪用するマルウェアを排除するために必要である。

4.2 運用環境と構成

本 TOE の一般的な運用環境を図 4-1 に示す。

なお、本構成に示されている、TOE 以外のハードウェア及び連携するソフトウェアの信頼性は、本評価の範囲ではない（十分に信頼できるものとする）。

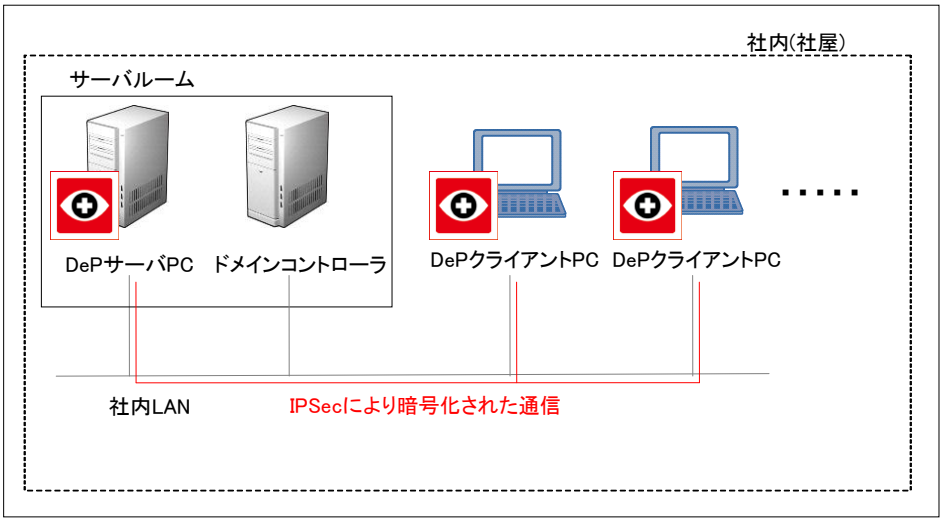

図4-1 TOEの運用環境

図 4-1 で、TOE は、DeP サーバ PC と DeP クライアント PC に搭載されるソフトウェアである。運用環境の構成品を以下に示す。

(1) DeP サーバ PC

DeP サーバ PC は、TOE のサーバ部分（DeP サーバ）を搭載した PC である。管理者が TOE の設定と監査記録の集中管理を行うために使用する。

・ 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 2012 R2 Standard 64bit

※セキュアブートが有効で、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こと。

(2) DeP クライアント PC

DeP クライアント PC は、TOE のクライアント部分（DeP クライアント）を搭載した一般利用者用の PC である。

・ 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 以上の空き容量

・ OS　Windows 8.1 Enterprise 64bit

※セキュアブート有効で、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こと。

(3) ドメインコントローラ

ドメインコントローラは、Windows ドメインの管理を行うサーバである。

本評価では、Windows Server 2003 R2 Standard Edition SP1、Windows Server 2012 R2 Standard 64bit を搭載する PC を使用。

4.3 運用環境におけるTOE範囲

本 TOE の提供するセキュリティ機能には、以下の制約がある。

(1) 静的なファイル内容の監視

本 TOE は、プログラムの実行中の動作を監視する方式を採用している。そのため、プログラムを実行せずに、静的なファイルの中に含まれているマルウェアを検出することはできない。

(2) 許可設定されたプログラムの悪用

本 TOE は、許可設定されたプログラムを悪用する攻撃には対応できない。例えば、Web サーバのネットワーク送信が許可されている場合に、Web サーバへの SQL インジェクション等の攻撃によって、Web サーバから情報が流出する脅威には対応できない。管理者が許可設定したプログラムの安全性は、管理者の責任である。

(3) カーネルモードのマルウェアの対処

本 TOE は、カーネルモードで動作するマルウェアによって、TOE の機能が改ざんされたり回避されたりすることを防止するしくみは提供していない。カーネルモードで動作するマルウェアを排除するために OS の維持管理をするのは、管理者の責任である。

(4) OS のブートメカニズムの保護

OS のブートメカニズムの保護は、本 TOE を搭載する PC が提供する「セキュアブート」に依存する。その機能が安全に動作するように、PC のファームウェアや OS を維持管理するのは、管理者の責任である。

(5) OS に標準搭載されていない追加 API

OS に標準搭載されていない、追加したドライバソフトウェアが提供する API は、本 TOE による監視の対象外である。そのようなドライバソフトウェアを使用しないように､本 TOE を搭載する PC の構成条件を順守することは、管理者の責任である。

(6) 監査記録の保護

本 TOE は、監査記録を格納する領域が十分にあることを前提としており、監査記録を格納する領域があふれた場合の保証はしていない。監査記録を格納する領域があふれないように、監査記録を定期的に削除することは、管理者の責任である。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成を説明する。

5.1 TOE境界とコンポーネント構成

本 TOE は以下のセキュリティ機能で構成される。

- DeP サーバ : 判定機能、監査機能（動作履歴出力機能）、監査機能（管理者向け機能）、管理機能
- DeP クライアント : 判定機能、監査機能（動作履歴出力機能）

以下、各セキュリティ機能の概要について説明する。

(1) 判定機能

本機能は、プログラムの動作を監視して、ホワイトリストに基づいて監視対象の動作の許可と拒否を制御する機能である。監視対象の動作を以下に示す。

・「保護対象」への書き込み（詳細は「11 用語」を参照）
・TCP/IP プロトコルおよび UDP/IP プロトコルによるネットワーク送信

プログラムの動作の監視と制御は、監視対象の動作を実施する OS の API を捕捉することで実現する。

ホワイトリストでは、許可するプログラムの識別情報として、プログラムのパス名を指定する他に、コンマンドプロンプトが実行するファイル名、InternetExploreが実行するJavaScriptを含むURL、Microsoft Officeが実行するマクロを含むファイル名等を指定することもできる。

(2) 監査機能（動作履歴出力機能）

本機能は、判定機能の監査記録を生成し、DeP サーバに蓄積する機能である。

DeP クライアントで生成された判定機能の監査記録は、一時的に DeP クライアント上に保存され、OS のログオフ時に DeP サーバに送信された後に削除される。

DeP クライアントに保存された監査記録は、DeP サーバに送信されるまでの間、TOE が OS の API を監視して改変や削除ができないように保護する。

(3) 監査機能（管理者向け機能）

本機能は、DeP サーバ上の管理者向けの監査機能であり、以下の 2 つの機能が含まれる。

- DeP サーバに蓄積された判定機能の監査記録を収集して、CSV 形式で出力する機能。
- DeP サーバでのホワイトリストの設定変更の監査記録を生成・蓄積し、テキスト形式で出力する機能。

(4) 管理機能

本機能は、DeP サーバ上の管理者向けの管理機能であり、以下の 2 つの機能が含まれる。

- ホワイトリストの設定変更
- DeP サーバ上に蓄積された監査記録の削除

管理者が DeP サーバで設定した情報は、DeP クライアントに送信され反映される。

5.2 IT環境

本 TOE は Windows Server 2012 R2 Standard 64bit、Windows 8.1 Enterprise 64bit を搭載した PC 上で動作する。

本 TOE の提供するセキュリティ機能が改ざん・バイパスされないように保護するしくみは、本 TOE 自身による保護機能と本 TOE を搭載する PC や OS の提供する保護機能で実現されている。本 TOE が、PC や OS に依存する主な保護機能を以下に示す。

・ブートメカニズムを悪用するマルウェアの防御
・バッファオーバフローを悪用するマルウェアの防御
・カーネル内モジュールの保護
・DeP サーバと DeP クライアント間の通信の保護
・管理者と一般利用者の権限管理

なお、バッファオーバフローを悪用するマルウェアは、OS の提供する防御機能に加えて、本 TOE による保護機能によっても防御されている。

6 製品添付ドキュメント

本 TOE に添付されるドキュメントの識別を以下に示す。TOE の利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

- ディフェンスプラットフォーム ビジネスエディション 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)
- 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）

7 評価機関による評価実施及び結果

7.1 評価機関

評価を実施した一般社団法人 IT セキュリティセンター 評価部は、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）の相互承認に加盟している認定機関（独立行政法人製品評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

7.2 評価方法

評価は、CC パート 3 の保証要件について、CEM に規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告された。評価報告書では、本TOEの概要と、CEMのワークユニットごとの評価内容及び判断結果を説明する。

7.3 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成 27 年 1 月に始まり、平成 28 年 11 月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成 27 年 8 月、9 月、11 月、平成 28 年 8 月及び 11 月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付・開発セキュリティの各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成 27 年 9 月、11 月、平成 28 年 4 月、8 月及び 11 月に開発者サイトで開発者のテスト環境を使用し、開発者テストのサンプリングチェック及び評価者テストを実施した。さらに、平成 27 年 9 月、11 月、平成 28 年 8 月及び 11 月に評価機関内のテスト環境を使用し、評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.4 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

7.4.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価者が評価した開発者テストの内容を以下に説明する。

(1) 開発者テスト環境

開発者が実施したテストの構成を図 7-1 に示す。

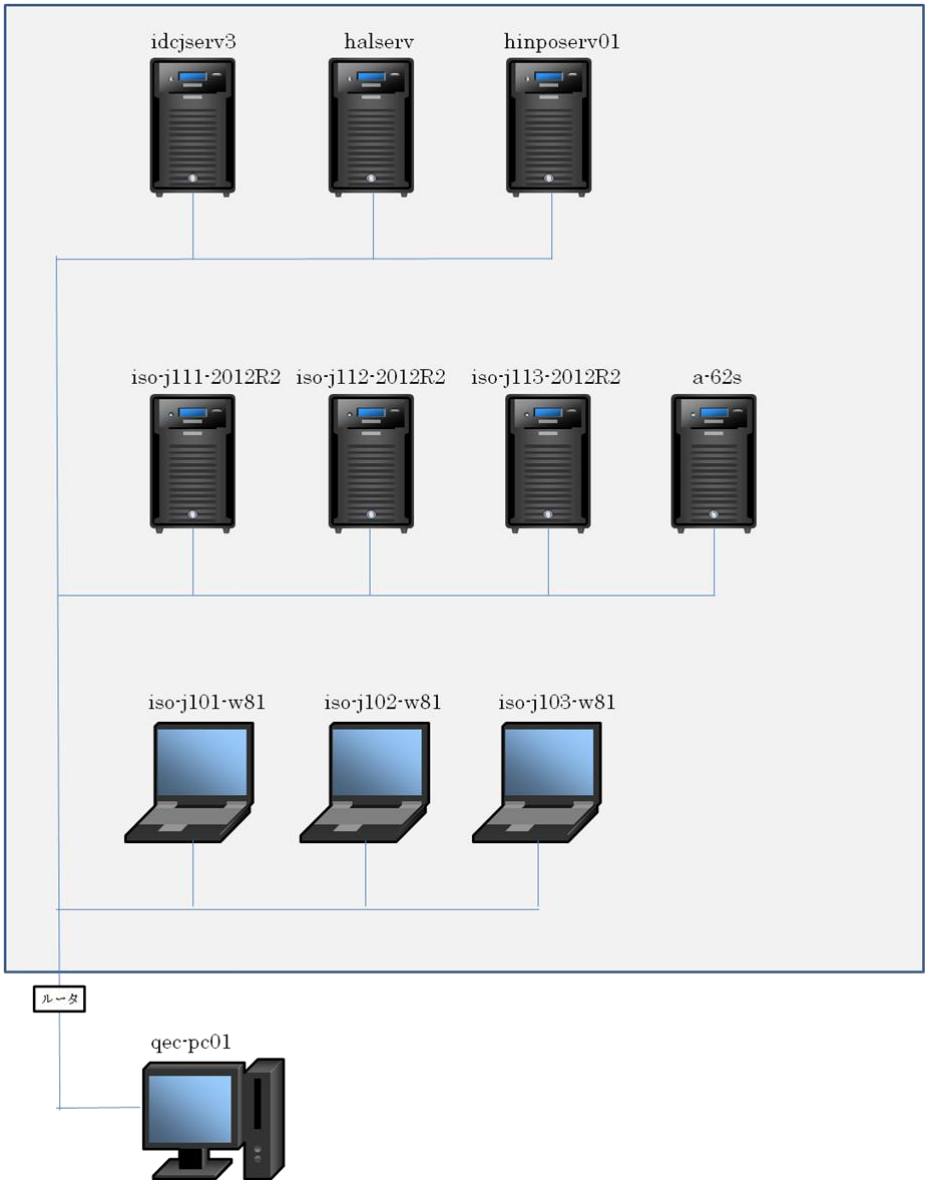

図7-1　開発者テストの構成図

開発者テストの構成要素を表7-1に示す。

表7-1　開発者テストの構成要素

分類	構成品	概要
DeP サーバPC (TOE搭載)	iso-j111-2012R2 iso-j112-2012R2 iso-j113-2012R2	DePサーバPCとして、自動検査及び手動検査で使用 ・Windows Server 2012 R2 Standard 64bit搭載PC ・TOE（DePサーバ） ・自動検査ツール: Intelligence Platform 4.0.2.58 ※その他、検査内容に応じて表7-2のテストツール搭載
	a-62s	DePサーバPCとして、手動検査で使用 ・Windows Server 2012 R2 Standard 64bit搭載PC ・TOE（DePサーバ） ※その他、検査内容に応じて表7-2のテストツール搭載
DeP クライアントPC (TOE搭載)	iso-j101-w81 iso-j102-w81 iso-j103-w81	DePクライアントPCとして、自動検査及び手動検査で使用 ・Windows 8.1 Enterprise 64bit搭載PC ・TOE（DePクライアント） ・自動検査ツール: Intelligence Platform 4.0.2.58 ※その他、検査内容に応じて表7-2のテストツール搭載
ドメインコントローラ	idcjserv3	ドメインコントローラとして使用 ・Windows Server 2003 R2 Standard Edition SP1搭載PC ・ドメインコントローラ: OS付属
Webサーバ	halserv	Webサーバとして使用 ・Windows Server 2008 R2 Standard搭載PC ・Webサーバ: OS付属
自動検査ツール管理	hinposerv01	自動検査ツールの管理（結果格納）用に使用 ・Windows Server 2003 R2 Standard Edition SP1搭載PC
	qec-pc01	自動検査ツールの管理（集中管理）用に使用 ・Windows 7 Professional搭載PC ・自動検査ツール: Intelligence Platform 4.0.2.58

開発者がテストしたTOEは、2章のTOE識別と同一の識別を持つ。

開発者テストは本 ST において識別されている TOE 構成と同一の TOE テスト環境で実施されている。

⑵ 開発者テスト概説

開発者テストの概説は以下のとおりである。

a) テスト概要

開発者テストの概要は、以下のとおりである。

＜開発者テスト手法＞

- OS の API を使用するテスト用のプログラムやアプリケーションプログラムを動作させて、それらのふるまいや TOE の監査記録を確認する。
- TOE が参照しているメモリ上の設定情報を取り出すためのテストツールを用いて、TOE 内部のデータを確認する。
- TOE の提供する管理画面を操作して TOE のふるまいを確認する。

＜開発者テストツール＞

開発者テストにおいて利用したツールを表 7-2 に示す。

表7-2　開発テストツール

ツール名称	概要
Webブラウザ (Internet Explorer 11, Google Chrome 44, Mozilla Firefox ESR31)	ホワイトリストに指定可能なスクリプト（JavaScript, Silverlight）の判定機能の確認に使用
Microsoft Office Professional Plus 2013	ホワイトリストに指定可能なOfficeマクロの判定機能の確認に使用
開発者作成プログラム（判定機能用 9種類）	監視対象のAPIを発行するプログラム。判定機能の確認に使用
開発者作成プログラム（保護機能用 6種類）	TOEの自己保護メカニズムやバイパス防止メカニズムの確認に使用
Netcat Ver1.11	任意のデータを送信するツール。TOEの自己保護メカニズムの確認に使用
Driver Walker 3.0.301.0	ドライバの動作状況の確認に使用
開発者作成ツール（テスト補助 2種類）	テストの自動化、メモリ上の設定情報の確認に使用

＜開発者テストの実施内容＞

テスト用のプログラムやアプリケーションプログラムを動作させて、監視対象の OS の API に対して、TOE のセキュリティ機能が仕様どおりに動作することを確認した。

なお、テストのための一連の操作は、自動検査ツールを用いて自動で実施したテスト項目と、手動で実施したテスト項目がある。

b) 開発者テストの実施範囲

開発者テストは開発者によって79項目（自動検査30項目、手動検査49項目）実施された。カバレージ分析によって、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証された。深さ分析によって、TOE設計に記述されたすべてのサブシステムとサブシステムインタフェースが十分にテストされたことが検証された。

c) 結果

評価者は、開発者テストの実施方法、実施項目の正当性を確認し、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

7.4.2 評価者独立テスト

評価者は、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実行されることを再確認するサンプルテストを実施するとともに、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることをより確信するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

評価者が実施した独立テストの構成は、1 項目のテストを除き、図 7-1 の開発者テストと同一の構成に、表 7-3 及び表 7-4 の独立テストツールを追加した構成である。残りの 1 項目のテストは、後述する侵入テスト環境で実施された。

独立テストは、本 ST において識別されている TOE の構成と同じ環境で実施された。

なお、独立テスト環境の構成品やテストツールは、開発者が独自に開発したものも含まれているが、それらの妥当性確認及び動作試験は、評価者によって実施されている。

(2) 独立テスト概説

評価者の実施した独立テストは以下のとおりである。

a) **独立テストの観点**

評価者が､開発者テスト及び提供された評価証拠資料から考案した独立テストの観点を以下に示す。

＜独立テストの観点＞

① 開発者が厳格に確認していないふるまいを確認する。

② 開発者の作成したテストツールによる確認を別の方式で確認する。

③ 実際のマルウェアを動作させた場合のふるまいを確認する。

④ サンプリングテストでは､以下の観点で開発者テストの項目を抽出する。

・すべてのセキュリティ機能と外部インタフェースを確認する。
・テストツールなどのテスト手法の異なるものを確認する。
・開発者が自動検査ツールで行ったテストを、手動で再確認する。

b) **独立テスト概要**

評価者が実施した独立テストの概要は以下のとおりである。

＜独立テスト手法＞

独立テストは、開発者テストと同じテスト手法で実施された。

＜独立テストツール＞

独立テストツールは、開発者テストと同じツールに、表 7-3 及び表 7-4 のツールを追加して使用した。

表7-3　独立テストで追加したツール

ツール名称	概要
ネットワーク送信アプリケーション ・Tera Term Ver.4.90 ・TWSNMPマネージャ Ver.4.4.2 ・LimeChat Ver.2.40 ・ChotServer Ver.0.652	ネットワーク送信の判定機能の確認に使用。 ・telnetプロトコル ・snmpプロトコル ・IRCクライアント ・IRCサーバ
一般のアプリケーション ・TeraPad v1.09 ・Wise Registry Cleaner 8.81.551 ・Thunderbird v38.3.0	開発者が開発したテストプログラムによる確認を、一般のアプリケーションプログラムを使用して確認。 ・ファイル書き込み ・レジストリ書き込み ・メール送信

開発者作成ツールの改造（判定機能用 1種類）	ファイルへの不正な書き込みを行うコードを、アプリケーションプログラムに注入する開発者作成ツールにおいて、コード注入対象のアプリケーションプログラムをregedit.exeに変更したもの。

表7-4　独立テストで追加したツール（実際のマルウェア）

区分	種類	名称
ウィルス	スクリプト	VBS/Internal
	ファイル	W32/Dizan
		W32/Sality
	マクロ	W97M/Relax
ワーム	E-mail	VBS/Freelink
		W32/Badtrans
		W32/Mylife
	E-mail、ファイル共有ソフト	W32/Banwarum
	ファイル共有ソフト	W32/Antinny
	インスタントメッセンジャー	W32/Neeris
		W32/Pykspa
		W32/Sohanad
	ネットワーク共有	W32/Allaple
		W32/Mumu
	ネットワーク共有、リムーバブルディスク	W32/Pesin
	ネットワークサービスの脆弱性悪用	W32/Korgo
		W32/Randex
		W32/Sasser
トロイの木馬	ランサムウェア	W32/CryptoLocker

＜独立テストの実施内容＞

評価者は、独立テストの観点に基づいて、54 項目（自動検査 30 項目、手動検査 24 項目）のサンプリングテストと、9 項目の追加の独立テストを実施した。

独立テストの観点とそれに対応した主なテスト内容を表 7-5 に示す。

表 7-5 実施した主な独立テスト

観点	テスト概要
観点①	TOEの履歴の収集機能を操作し、監査記録が収集されるフォルダやファイル名が仕様どおりであることを確認する。
	開発者がテストしていない、telnet, snmp, ircのプロトコルによるネットワーク送信を実施しても、TOEが仕様どおりに動作することを確認する。
	開発者がテストしていない、任意のTCPポートを使用したネットワーク送信を実施しても、TOEが仕様どおりに動作することを確認する。 ※本テスト項目だけは、侵入テスト環境で実施された。
観点②	開発者が開発したテストツールによるテストを、一般のアプリケーションプログラムで実施しても、TOEが仕様どおりに動作することを確認する。
	開発者テストツールを改造し、別のアプリケーションにコード注入を実施しても、TOEが仕様どおりに動作することを確認する。
観点③	実際のマルウェアを実行し、TOEが仕様どおりにマルウェアの動作を防止することを確認する。

c) 結果

評価者が実施したすべての独立テストは正しく完了し、評価者は TOE のふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが一致していることを確認した。

7.4.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

① TOEのガイダンスによる環境設定の指示が不十分な場合、一般利用者の権限でTOEの設定変更やTOEの機能の回避ができる可能性がある。

② TOEのサーバとクライアント間の通信に、別のPCからデータを送信すると、誤動作する可能性がある。

③ TOEのホワイトリストの設定で正規表現が使用されている場合、ディレクトリトラバーサルを引き起こす可能性がある。

b) **侵入テストの概要**

評価者は、潜在的な脆弱性が悪用される可能性を検出するために、以下の侵入テストを実施した。

＜侵入テスト環境＞

侵入テスト環境を図 7-2 に示す。

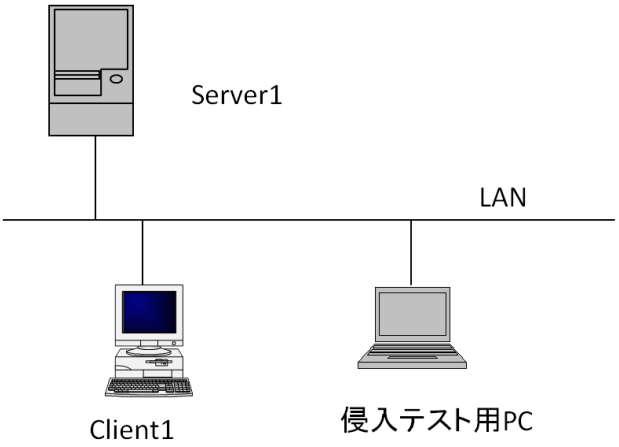

図7-2　侵入テスト環境

侵入テストの環境の構成要素、および侵入テストで使用したツールの詳細を表 7-6 に示す。

表7-6　侵入テスト構成

構成品	概要
Server1 (TOE搭載)	DePサーバPC兼ドメインコントローラとして使用 ・Windows Server 2012 R2 Standard 64bit搭載PC ・TOE（DePサーバ） ・Microsoft Office Standard 2007
Client1 (TOE搭載)	DePクライアントPCとして使用 ・Windows 8.1 Enterprise 64bit搭載PC ・TOE（DePクライアント） ・netcat 1.12: データの送受信を行うツール
侵入テスト用PC	Server1及びClient1とのデータの送受信に使用 ・Windows 8.1 64bit搭載PC ・netcat 1.12: データの送受信を行うツール

＜侵入テストの実施項目＞

懸念される脆弱性と対応する侵入テスト内容を表 7-7 に示す。

表7-7　侵入テスト概要

脆弱性	テスト概要
脆弱性①	・一般利用者がTOEのアンインストール用ツールを実行しようとしても実行できないことを確認する。 ・一般利用者がWindowsのタスクスケジューラでタスクを作成できないことを確認する。 ・Windowsをセーフモードで起動した場合、一般利用者ではログインできないことを確認する。
脆弱性②	DePサーバとDePクライアントが、設定情報や監査記録をやりとりしているポートに対して、侵入テストPCからデータを送信しても悪影響がないことを確認する。
脆弱性③	ホワイトリストで正規表現を用いてパス名やURLを設定した状態で、ディレクトリトラバーサルを引き起こす可能性のある文字列を含むコマンドの実行やURLの参照を行っても、正規表現がマッチせずに拒否されることを確認する。

c) **結果**

評価者が実施した侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

7.5　評価構成について

本評価の前提となる TOE の構成条件は、6 章に示したガイダンスに記述されているとおりである。本 TOE を安全に使用するために、TOE の管理者は、当該ガイダンスの記述のとおりに、TOE 及び TOE をインストールする OS を設定しなければならない。これらの設定値をガイダンスと異なる値に変更した場合には、本評価による保証の対象ではない。

7.6 評価結果

評価者は、評価報告書をもって本 TOE が CEM のワークユニットすべてを満たしていると判断した。

評価では以下について確認された。

セキュリティ機能要件： コモンクライテリア パート２ 適合
セキュリティ保証要件： コモンクライテリア パート３ 適合

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

EAL3 パッケージのすべての保証コンポーネント

評価の結果は、第 2 章に記述された識別に一致する TOE によって構成されたもののみに適用される。

7.7 評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

8 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。認証機関は、本 ST 及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

8.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本 TOE が CC パート 3 の EAL3 に対する保証要件を満たすものと判断する。

8.2 注意事項

本評価において、CC/CEM の範囲で保証するのは、3 章及び 5 章で説明したセキュリティ機能である。本 TOE がすべてのマルウェアに対して有効であることを保証するものではない。

本 TOE の管理者には、インストールするソフトウェアの中に追加の API を提供するカーネルモジュールが含まれていないことや、管理者が許可設定するプログラムの安全性を判断するといった運用管理が求められる。

本 TOE に興味のある調達者は、「1.1.3 免責事項」、「4.3 運用環境における TOE 範囲」及び「7.5 評価構成について」の記載内容を参照し、本 TOE の制約事項や評価対象範囲が、各自の想定する運用条件に合致しているかどうか注意が必要である。

9 附属書

特になし。

10 セキュリティターゲット

本 TOE のセキュリティターゲット[12]は、本報告書とは別文書として以下のとおり本認証報告書とともに提供される。

Defense Platform Business Edition CC セキュリティターゲット, 第 1.41 版, 2016 年 11 月 14 日, ハミングヘッズ株式会社

11 用語

本報告書で使用された CC に関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用された TOE に関する略語を以下に示す。

DeP	Defense Platform（ディフェンスプラットフォーム）
MBR	Master Boot Record（マスターブートレコード）

本報告書で使用された用語の定義を以下に示す。

DePクライアント	TOEのクライアント部分「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
DePサーバ	TOEのサーバ部分「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
保護対象	本TOEが書き込みを制御する対象であり、下記のレジストリ、メモリ、ファイル等が該当する。なお、本TOEがOSのAPIを捕捉したときに、そのAPIを実行したプログラムが「監視対象プログラム」であり、それ以外のプログラムが「他プログラム」である。 ・他プログラムのレジストリ ・他プログラムが実行中に使用するメモリ ・他プログラム及びシステム用の以下のファイル - 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フォルダ内ファイル - システムドライブの¥windows¥SysWow64フォルダ内ファイル - Program Filesフォルダ以下の、他プログラム用フォルダ内のファイル - 実行可能ファイル（COM、DLL、EXE、LIB、SYS形式のファイル）。ただし、AppDataフォルダ以下の、監視対象プログラム用フォルダ内のファイルは除く - MBR

ホワイトリスト　許可するプログラムの動作のリスト。本TOEの管理者が以下の項目を設定する。
・プログラムの識別情報（ファイル名等）
・動作の種類（ファイル書き込み、レジストリ書き込み、メモリ書き込み、ネットワーク送信のいずれかを指定）
・動作対象（書き込み対象のファイル名、ネットワーク送信先のIPアドレスとポート番号など）

12 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 平成27年6月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-001, (平成24年11月, 翻訳第1.0版)

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能コンポーネント, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-002, (平成24年11月, 翻訳第1.0版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証コンポーネント, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-003, (平成24年11月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] 情報技術セキュリティ評価のための共通方法: 評価方法, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-004, (平成24年11月, 翻訳第1.0版)

[12] Defense Platform Business Edition CC セキュリティターゲット, 第1.41版, 2016年11月14日, ハミングヘッズ株式会社

[13] ハミングヘッズ株式会社Defense Platform Business Edition CC評価報告書, 第1.15版, 2016年11月16日, 一般社団法人ITセキュリティセンター 評価部