認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司

原紙押印済

評価対象

申請受付日（受付番号）	**平成21年9月2日** (IT**認証**9262)
認証番号	C0256
認証申請者	**ハミングヘッズ株式会社**
TOE**の名称**	**セキュリティプラットフォーム** evolution /SV CC
TOE**のバージョン**	Ver.2.0.9.4
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22年6月17日

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 改訂第2版 (翻訳第2.0版)
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 改訂第2版　(翻訳第2.0版)

評価結果：合格

「セキュリティプラットフォーム evolution /SV CC」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「セキュリティプラットフォーム evolution /SV CC」（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。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者であるハミングヘッズ株式会社に報告するとともに、本TOEに関心を持つ利用者や運用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、本書と共に、対応するSTを併読されたい。本TOEの動作条件や運用のための前提についての詳細、本TOEが対抗する脅威へのセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件、及びセキュリティ仕様の概要と十分性の根拠は、STにおいて詳述されている。

本認証報告書は、市販される本TOEを購入する一般消費者を読者と想定している。本認証報告書は、本TOEに対して適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

1.1.1 評価保証レベル

本TOEが適合を主張する評価保証レベルは、EAL3適合である。

1.1.2 PP適合

適合するPPはない。

1.2 評価製品

1.2.1 製品名称

本TOEは、以下の製品のセキュリティ機能である。

製品名称： 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

なお、「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り、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。

・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 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

・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

1.2.2 製品概要

TOEは、Windows 7またはWindows Server 2008を搭載したPC用の情報漏洩対策ソフトウェア製品であり、利用者がファイルを持ち出す際に意図した受け取り手以外の第三者にファイルが漏洩することを防止する目的のものである。TOEは、Windowsドメイン環境で利用するサーバ・クライアント型製品であり、モバイル環境での使用にも対応している。管理者はTOEのサーバ部分を使用して一般利用者が使用するTOEのクライアント部分を集中管理する。

TOEは、情報漏洩を防止するためのセキュリティ機能として、一般利用者が外部媒体やWeb及び電子メールでファイルを持ち出す際に、持ち出しのできるアプリケーションと操作を限定して許可された持ち出しファイルを強制的に暗号化する機能、及び、クライアントPCのハードディスク全体を暗号化する機能を備えている。また、TOEは、それらのセキュリティ機能を管理するために、管理機能と監査機能を提供する。

1.2.3 TOE範囲とセキュリティ機能

TOEの動作環境を図1-1に示す。図1-1で、TOEは、SePサーバ及びSePクライアントにインストールされているソフトウェア部分である。TOEは、SePサーバ及びSePクライアントの利用者がファイルを持ち出す際に、意図した受け取り手以外の第三者にファイルが漏洩することを防止するためのセキュリティ機能を提供する。

TOEの提供する機能の範囲を図1-2に示す。図1-2で、TOEの提供する機能は「TOEのセキュリティ機能」として示されている部分であり、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、監査機能（操作履歴出力機能と管理者向け機能）、管理機能が含まれている。各機能は実際には、WindowsのDLL、カーネル内ドライバ、又は、Windows上のプログラムとして実装されている。

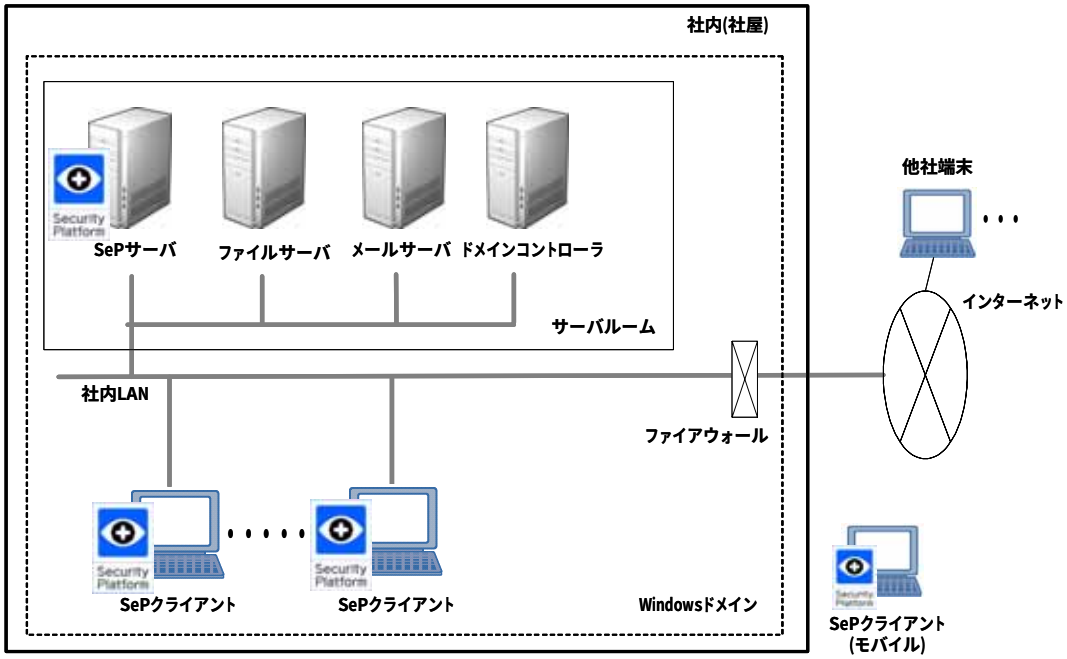

図1-1　TOEの動作環境

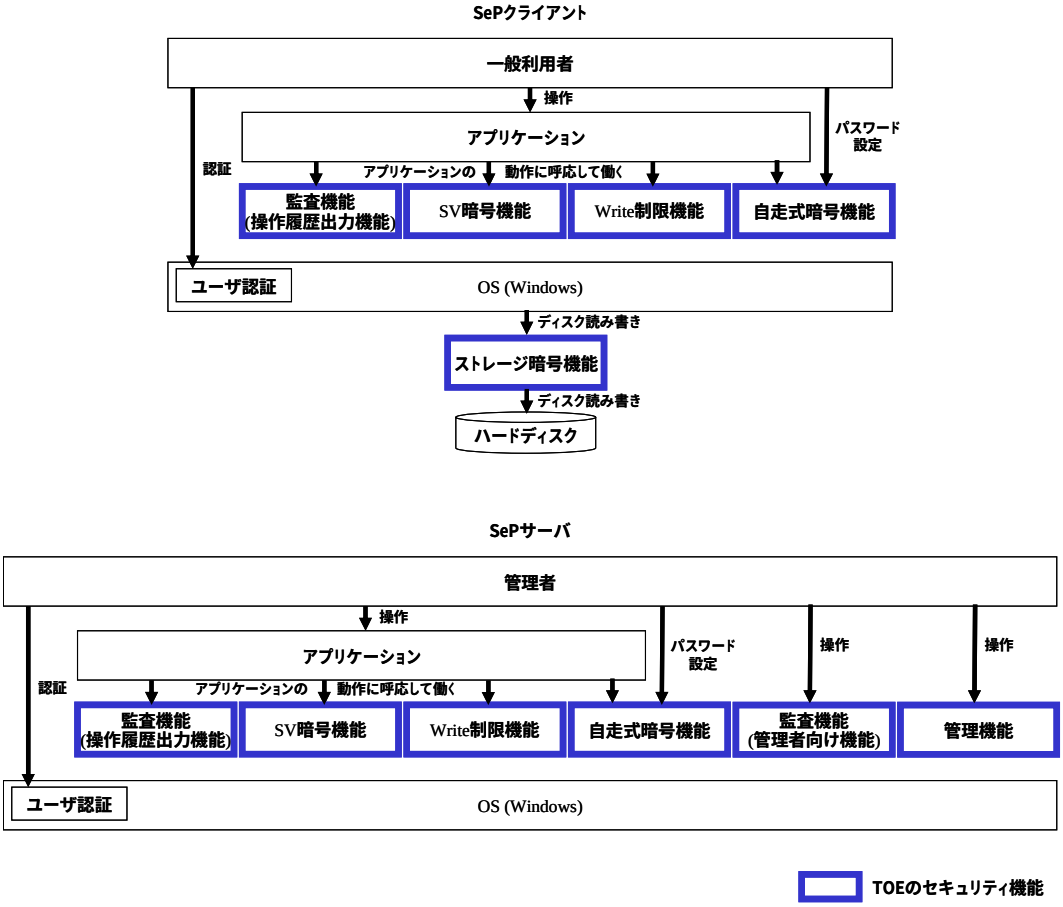

図1-2　TOEの論理的範囲

TOEの主目的は、アプリケーションの実行を監視して、利用者の過失によるファイルの持ち出しを制限し、持ち出しが許可されたファイルは強制的に暗号化することにより、正当な受け取り手以外が持ち出されたファイルを閲覧できないようにすることである。それを実現するために、TOEは、アプリケーションが実行するOSライブラリ呼び出しやシステムコールを捕捉し、実行の制限や暗号処理を行っている。

TOEの各セキュリティ機能の概要は以下のとおりである。

(1) Write制限機能

Write制限機能は、ファイルの持ち出しを行うアプリケーションを限定する。本評価では、持ち出しに利用できる許可アプリケーションを、Explorer、Outlook2007(SP2)、InternetExplorer8に限定する。

(2) SV暗号機能、自走式暗号機能

SV暗号機能と自走式暗号機能は、許可アプリケーションで持ち出すファイルを強制的に暗号化する。暗号化には次の2種類があり、利用者が送信相手に応じて使い分ける。

・SV暗号ファイル(SV暗号機能による暗号化)

TOEの導入された環境だけで使用できる暗号化ファイルである。ファイルを信頼領域（TOEの導入された環境内の指定された領域）からそれ以外の非信頼領域に持ち出すと自動的に暗号化され、暗号化されたファイルは信頼領域に戻すと自動的に復号される。パスワードの入力は必要としない。

・自走式暗号ファイル(自走式暗号機能による暗号化)

TOEの導入されていない環境でも復号できる暗号化ファイルである。利用者は、自走式暗号化を行うために、信頼領域のファイルを管理者の指定するリリースフォルダに一旦格納する。格納したファイルをリリースフォルダから非信頼領域に持ち出すと、強制的にパスワードの入力が求められ、実行形式の自走式暗号ファイルに変換される。受け取り手は、自走式暗号ファイルを実行し、送り手の設定したパスワードを入力することによって復号できる。

また、SV暗号機能には、暗号化の他に、WebページのURLによってファイルのアップロードを制限したり、Webブラウザやメールソフトウェアにファイルの内容をペーストする操作を制限したりする機能も含まれている。

(3) ストレージ暗号機能

ストレージ暗号機能は、OSのハードディスク入出力に暗号処理を適用し、ハードディスク全体を暗号化する。これにより、利用者は全く意識することな

くハードディスク全体が常時暗号化され、モバイル端末の盗難や紛失時に、ハードディスクから内容が直接読み出されることを防止する。

(4) 監査機能

監査機能は、SePサーバ及びSePクライアントで、ファイルの持ち出し操作の履歴を出力する。また、SePサーバで、管理者がそれらの履歴を収集・閲覧するための機能を提供する。これにより管理者は、ファイルの持ち出し状況を把握することができる。

(5) 管理機能

管理機能は、管理者がSePサーバでTOEの設定を行う機能を提供する。設定内容は、SePサーバ及びSePクライアントに反映される。これにより、管理者は、SePサーバ及びSePクライアントを集中管理することができる。

なお、モバイル環境で使用するSePクライアントは、TOEの設定を行う際には、SePサーバのLANに接続する必要がある。また、定期的にSePサーバのLANに接続し、履歴情報をSePサーバで収集する必要がある。

1.3 評価の実施

認証機関が運営するITセキュリティ評価･認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

① 本TOEのセキュリティ設計が適切であること。
② 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。
③ 本TOEがセキュリティ設計に基づいて開発されていること。
④ 上記①、②、③を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「セキュリティプラットフォーム evolution /SV CC セキュリティターゲット」（以下「本ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1 ([5][8]のいずれか) 附属書A、CCパート2（[6][9]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「セキュリティプラット

フォーム evolution /SV CC Ver.2.0.9.4 評価報告書」（以下「評価報告書」という。）[13]に示されている。なお、評価方法は、CEM（[11][12]のいずれか）に準拠する。

1.4 評価の認証

認証機関は、評価機関が作成した、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、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。評価は、平成22年6月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 TOE概要

2.1 セキュリティ課題と前提

TOEが解決すべき課題と、必要とする前提を以下に示す。

2.1.1 脅威

本TOEは、表2-1に示す脅威を想定し、これに対抗する機能を備える。

表2-1 想定する脅威

識別子	脅　威
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。

(注)
・保護資産は、信頼領域上のファイルである。
・保護資産の送信の対象プロトコルは、SMTP、HTTP、HTTPSである。
・一般利用者に対して、脅威の対象は過失による行為である。一般利用者が、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、脅威として想定されていない。

2.1.2 組織のセキュリティ方針

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。

2.1.3 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表2-2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2-2　TOE使用の前提条件

識別子	前提条件
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。

(注) A.NETWORKのプロトコルの記述は、TOEが送信ファイルを暗号化するSMTP、HTTP、HTTPS以外のプロトコルについて、TOE導入PCから外部へのファイル送信ができないように、ファイアウォールで制限することを意図している。

2.1.4　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。なお、これらのドキュメントはすべて管理者用であり、一般利用者に対しては管理者から周知されることを意図している。

下記ドキュメントの内、「セキュアな運用ガイダンス」には、本TOEをSTに記載されているとおりの動作をするように設定し運用するための手順や注意事項がまとめられており、他ドキュメントは必要に応じて参照するよう構成されている。

TOEの管理者は、前提条件を満たすため、最低限「セキュアな運用ガイダンス」についての十分な理解と遵守が要求される。

表2-3　ガイダンス文書一覧

ガイダンス文書名
セキュアな運用ガイダンス 第2.06版
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 第八版

ガイダンス文書名
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 ﾗｲﾃｨﾝｸﾞｿﾌﾄの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(同ﾄﾞﾗｲﾌﾞ)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(同ﾄﾞﾗｲﾌﾞ)間ｸﾘｯﾌﾟﾎﾞｰﾄﾞ禁止機能 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 ｲﾝﾄﾗﾈｯﾄｵﾌﾟｼｮﾝ 第八版
SeP マニュアル for ｲﾝﾄﾗﾈｯﾄｵﾌﾟｼｮﾝ 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 ｲﾝﾄﾗﾈｯﾄｵﾌﾟｼｮﾝ 別冊2 ｾｷｭﾘﾃｨﾀｸﾞ機能の無効化 第一版
SeP マニュアル for ｲﾝﾄﾗﾈｯﾄｵﾌﾟｼｮﾝ 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 ｲﾝﾄﾗﾈｯﾄｵﾌﾟｼｮﾝ 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 ｲﾝﾄﾗﾈｯﾄｵﾌﾟｼｮﾝ 別冊5 SharePoint 対応 第三版
SeP マニュアル for ｲﾝﾄﾗﾈｯﾄｵﾌﾟｼｮﾝ 別冊6 HTTPﾘｸｴｽﾄ制限機能 第二版
SeP マニュアル for ﾄﾚｰｻｵﾌﾟｼｮﾝ 第十一版
SeP マニュアル for ﾄﾚｰｻｵﾌﾟｼｮﾝ 別冊1 収集機能強化 第一版
SeP マニュアル for ﾄﾚｰｻｵﾌﾟｼｮﾝ 別冊2 エラーログ出力 第二版
SeP マニュアル for ﾄﾚｰｻｵﾌﾟｼｮﾝ 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 ｽﾄﾚｰｼﾞｴﾝｸﾘﾌﾟｼｮﾝｵﾌﾟｼｮﾝ 第九版
SeP マニュアル for ｽﾄﾚｰｼﾞｴﾝｸﾘﾌﾟｼｮﾝｵﾌﾟｼｮﾝ 別冊1 ｽﾄﾚｰｼﾞ暗号機能(ﾌｫﾙﾀﾞ･ﾃﾞｨﾚｸﾄﾘ暗号、状態表示、履歴出力) 第一版
SeP マニュアル for ｽﾄﾚｰｼﾞ暗号復号ツール 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

ガイダンス文書名
ご注意･制限事項 第十版
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

2.1.5 構成条件

本TOEは、Windowsを搭載したPC用のソフトウェアである。本評価は以下のハードウェア及びソフトウェア上での動作を対象とする。なお、本構成に示されるハードウェア及びソフトウェアの信頼性は本評価の範囲外である。

(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

・ 許可アプリケーション　Explorer、Outlook2007(SP2)、InternetExplorer8

(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　インストール: 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

・ 許可アプリケーション　Explorer、Outlook2007(SP2)、InternetExplorer8

(3) ドメインコントローラ

・Windows 7及びWindows Server 2008を含むWindowsドメインを管理可能なサーバ。本評価では、Windows 2003 Active Directoryを搭載するPCを使用。

なお、図1-1に示したTOEの動作環境の内、ファイルサーバとメールサーバは、TOEの動作に必須ではなく、利用環境の必要に応じて導入する。

2.2 セキュリティ対策

TOEは、具備したセキュリティ機能により以下のように2.1.1の脅威に対抗する。

(1) 脅威T.USER_ERRORと脅威T.STOLEN

脅威T.USER_ERROR(一般利用者の過失)と脅威T.STOLEN(第三者による盗み)は、Write制限機能とSV暗号機能に含まれる制限機能でファイルを持ち出すアプリケーションと持ち出し操作を限定し、許可されたファイル持ち出しについては、SV暗号機能または自走式暗号機能でファイルを暗号化することで対抗する。各機能の概要を以下に示す。

① 持ち出しファイルの暗号化

脅威に対抗するためのメインとなる機能である。

TOEは、SV暗号機能により、許可アプリケーションが信頼領域から非信頼領域にファイルを持ち出す際に、自動的かつ強制的にファイルをSV暗号化する。SV暗号ファイルは、信頼領域に戻すと自動的に復号される。

TOEは、自走式暗号機能により、許可アプリケーションがリリースフォルダから非信頼領域にファイルを持ち出す際に、強制的にファイルを自走式暗号化する。その際に、利用者にパスワードの入力を要求し、管理者の設定した品質尺度に合うパスワードだけが受け入れられる。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。

これらの機能により、一般利用者の過失または第三者による盗みによって、持ち出されたファイルを意図しない受け取り手が入手したとしても、持ち出したファイルは正当な受け取り手のみが閲覧できるように暗号化されるので、情報漏洩を防止することができる。

② 持ち出しアプリケーションと操作の制限

脅威に対抗するためのメインとなる持ち出しファイルの暗号化をサポートする機能である。

TOEは、Write制限機能により、許可アプリケーション以外のアプリケーションについて、非信頼領域へのファイルの書き込みと、許可されていない通信先へのTCP/IP通信を禁止する。これにより、ファイルの暗号化が行われるアプリケーション以外で、ファイルを持ち出すことが制限されるので、脅威T.USER_ERRORと脅威T.STOLENの対抗に貢献する。

TOEは、SV暗号機能により、許可アプリケーションが信頼領域からファイルを持ち出す操作を次のように制限する。ファイルのWebページへの添付をURLによって禁止する。また、ファイル内容のペースト操作に対して、メールへのペーストと信頼領域以外のWebページへのペーストを禁止する。これらにより、ファイルの暗号化が行われる操作以外で、ファイルを持ち出すことが制限されるので、脅威T.USER_ERRORと脅威T.STOLENの対抗に貢献する。

(2) 脅威T.LOST_PC

脅威T.LOST_PC(クライアントマシンの紛失)は、ストレージ暗号機能で、ハードディスク全体を暗号化することで対抗する。TOEは、ストレージ暗号機能により、初期設定時にハードディスク全体を暗号化し、初期設定後はOSがハードディスクのデータを読み込むときに復号し、書き込むときに暗号化する。これにより、ハードディスクを抜き取って内容を読み出しても、内容は暗号化されているため、情報漏洩を防止することができる。

なお、前提条件A.USER_AUTHENTICATION(利用者の認証)により、OSには適切なパスワードが設定され、OSのログオンは正当な利用者に限定される。そのため、攻撃者がOSにログインしてハードディスクの内容を参照することは防止される。

(3) セキュリティ機能のサポート

TOEは、(1)(2)で述べた脅威に対抗するセキュリティ機能をサポートするために、管理機能と監査機能を提供する。管理者は、管理機能でセキュリティ機能に必要な設定を行い、監査機能でセキュリティ機能の実施状況を把握することができる。各機能の概要を以下に示す。

①管理機能

TOEは、セキュリティ機能の設定を行う機能を提供する。管理者はSePサーバで設定を行い、設定された内容はSePサーバ及びSePクライアントに反映される。設定項目は次のとおりである。

・信頼領域(非信頼領域)の定義、リリースフォルダの定義
・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IPアドレスとポート

・機能の有効/無効
(Write制限機能、SV暗号機能、自走式暗号機能、ストレージ暗号機能)
・パスワードの品質尺度(長さ、英数混合の指定)

②監査機能

TOEは、セキュリティ機能の履歴を出力し、定期的にSePサーバに収集する。また、SePサーバで収集した履歴を閲覧する機能を提供する。出力する履歴は次のとおりである。

・Write制限機能とSV暗号機能で禁止された操作
・SV暗号機能と自走式暗号機能で暗号化された操作
・ストレージ暗号機能の初期設定と解除
・管理機能の設定操作

3 評価機関による評価実施及び結果

3.1 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ている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

3.2 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21年9月に始まり、平成22年6月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成21年12月に開発・製造・出荷現場へ赴き、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22年3月及び同年4月に開発者サイトで開発者のテスト環境を使用し、開発者が実施した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。

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

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

3.3 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。

3.3.1 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。評価した開発者テストの概要を以下に示す。

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3-1　開発者テストの構成図に示す。また、

開発者テストで使用された機器構成を表3-1に示す。

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。

ただし、開発者テストでは、テストを効率よく行うために複数のSePサーバが設置され、テスト対象機器に実行すべきテストを指示して結果を収集する自動検査用集中管理ワークステーションが存在している。これらの違いは、TOEの動作に影響を及ぼさないことが評価者により確認されている。

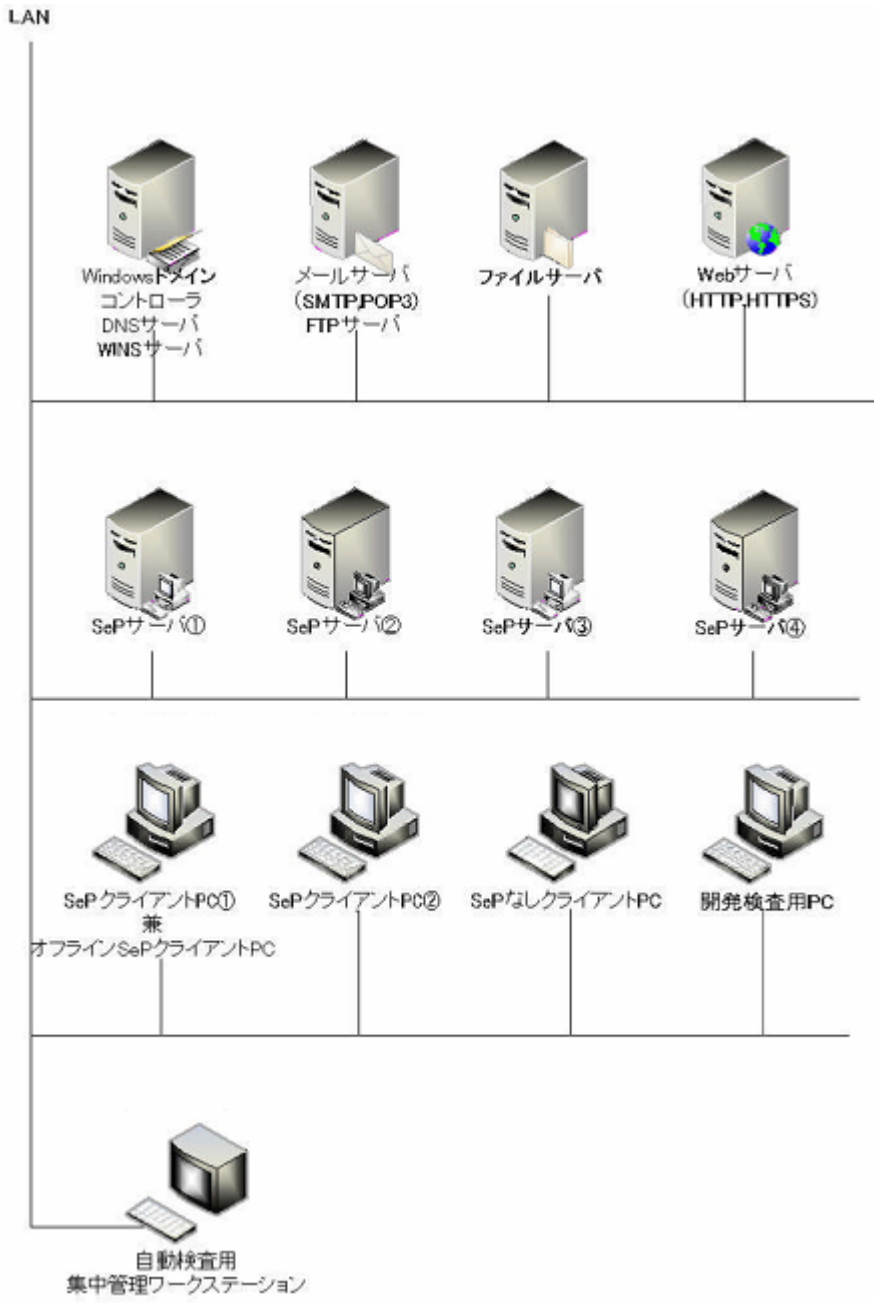

図3-1　開発者テストの構成図

表3-2　開発者テストの機器構成

マシン名(用途)	概要	構成
SePサーバ①	SePクライアントPCに提供するサーバ機能、及び、SeP クライアントと同機能の検査を行うSePサーバ	●ハードウェア（PC） ・CPU：Intel Core2 Duo E7400 @ 2.80GHz ・メモリ：2GB ・HDD：365GB（空容量345GB） ●ソフトウェア ・TOE ・Windows Server 2008 Enterprise (SP1) 32bit版 ・AVG File Server Edition 0.9.785 ・遠隔操作用ソフトウェア（UltraVNC） ・自動検査ツール（インテリジェンスプラットフォーム） ・アプリケーション： Microsoft Office Professional Plus 2007、2007 Microsoft Office Suite SP2、Adobe Reader 9、FFFTP 1.96d、Mozilla Firefox 2.0.0.10、Mozilla Thunderbird 2.0.0.6
SePサーバ②	SePクライアントPCに提供するサーバ機能、及び、SePクライアントと同機能の検査を行うSePサーバ	●ハードウェア（PC） ・CPU：Intel Core2 Duo E7500@ 2.93GHz ・メモリ：2GB ・HDD：33GB（空容量13GB） ●ソフトウェア ・TOE ・Windows Server 2008 Enterprise (SP1) 32bit版 ・AVG File Server Edition 0.9.785 ・遠隔操作用ソフトウェア（UltraVNC） ・自動検査ツール（インテリジェンスプラットフォーム） ・アプリケーション： Microsoft Office Professional Plus 2007、2007 Microsoft Office Suite SP2、Adobe Reader 9
SePサーバ③	SePクライアントと同機能の検査を行うSeP	●ハードウェア（PC） ・CPU：Intel Core2 Duo E7500 @ 2.93GHz ・メモリ：2GB

	サーバ	・HDD：148GB（空容量133GB） ●ソフトウェア ・Internet Explorer 8.0 ・他はSePサーバ②と同じ
SePサーバ④	他のSePサーバとは異なるライセンスの媒体で導入したSePサーバ	●ハードウェア（PC） ・CPU：Intel Core2 Duo E7500 @ 2.93GHz ・メモリ：2GB ・HDD：148GB（空容量134GB） ●ソフトウェア ・TOE(他SePサーバとは異なる媒体で導入) ・Internet Explorer 8.0 ・他はSePサーバ②と同じ
SePクライアントPC①	SePクライアント機能の検査を行うPC （オフラインの場合を含む）	●ハードウェア（PC） ・CPU：Intel Core2 Duo E7500 @ 2.93GHz ・メモリ：2GB ・HDD：128GB（空容量110GB） ●ソフトウェア ・TOE ・Windows 7 Enterprise 32bit版 ・AVG Anti-Virus 9.0.700 ・遠隔操作用ソフトウェア（UltraVNC） ・自動検査ツール（インテリジェンスプラットフォーム） ・アプリケーション： Microsoft Office Professional Plus 2007、2007 Microsoft Office Suite SP2、Internet Explorer 8.0、Windows Media Player 12.0.7600.16385、Windows DVD メーカー 6.1.7600.16385、Windows Media Center 6.1.7600.16385、Windows ディスクイメージ書き込みツール6.1.7600.16385、Mozilla Firefox 2.0.0.10、Mozilla Thunderbird 2.0.0.6、Adobe Reader 9、FFFTP 1.96d
SePクライアントPC②	SePクライアント機能の検査を行うPC	●ハードウェア（PC） ・CPU：Intel Core2 Duo E7500 @ 2.93GHz ・メモリ：2GB ・HDD：31GB（空容量20GB） ●ソフトウェア ・TOE

		・Windows 7 Enterprise 32bit版 ・AVG Anti-Virus 9.0.700 ・遠隔操作用ソフトウェア（UltraVNC） ・自動検査ツール（インテリジェンスプラットフォーム） ・アプリケーション： Microsoft Office Professional Plus 2007、2007 Microsoft Office Suite SP2、Internet Explorer 8.0 、 Windows Media Player 12.0.7600.16385、Windows DVD メーカー 6.1.7600.16385 、 Windows Media Center 6.1.7600.16385、Windows ディスクイメージ書き込みツール6.1.7600.16385、Adobe Reader 9、B's Recorder; Ver 10.00.000
開発検査用PC	暗号アルゴリズムや暗号鍵の検査を行うPC	●ハードウェア（PC） ・CPU：Intel Core2 Duo E7250 @ 2.00GHz ・メモリ：2GB ・HDD：31GB（空容量20GB） ●ソフトウェア ・TOE ・Windows 7 Enterprise 32bit版 ・AVG Anti-Virus 9.0.700 ・遠隔操作用ソフトウェア（UltraVNC） ・自動検査ツール（インテリジェンスプラットフォーム） ・OpenSSL 0.9.8j ・アプリケーション： Microsoft Office Professional Plus 2007、2007 Microsoft Office Suite SP2、Internet Explorer 8.0 、 Windows Media Player 12.0.7600.16385、Windows DVD メーカー 6.1.7600.16385 、 Windows Media Center 6.1.7600.16385、Windows ディスクイメージ書き込みツール6.1.7600.16385
SePなしクライアントPC	SeP がインストールされていないPC	・Windows 7 Enterprise 32bitを搭載したPC ・TOEなし ・AVG Anti-Virus 9.0.700 ・遠隔操作用ソフトウェア（UltraVNC） ・自動検査ツール（インテリジェンスプラッ

		トフォーム） ・アプリケーション： Microsoft Office Professional Plus 2007、2007 Microsoft Office Suite SP2
ドメインコントローラ	ドメインコントローラ	・Windows Server 2003 SP 1 を搭載したPC ・OS標準搭載のWindows Active Directoryを使用
メールサーバ、FTPサーバ	メールサーバ、FTPサーバ	・Windows 2000 Advanced Serverを搭載したPC ・OS標準搭載のメールサーバ、FTPサーバのソフトウェアを使用
ファイルサーバ	ファイルサーバ	・Windows Server 2003 SP 2を搭載したPC ・OS標準の共有フォルダ設定
Webサーバ	Webサーバ	・Windows 2000 Advanced Server SP4を搭載したPC ・Webサーバソフトウェアは、ドミノR5、ノーツR5
自動検査用集中管理ワークステーション	自動検査を行う際の集中管理システム用ワークステーション	・Windows Vista Ultimateを搭載したPC ・遠隔操作用ソフトウェア（UltraVNC） ・自動検査ツール（インテリジェンスプラットフォーム）の集中管理ツール

2) 開発者テスト概説

開発者の実施したテストは以下のとおり。

a. テスト概要

開発者テストで実施されたテストの概要は以下のとおり。

①自動テスト

キー入力やマウス操作を自動的に行い、期待される画面遷移や表示内容を自動的に比較する自動検査ツールを使用して以下のテストを実施した。

・アプリケーションでファイルを扱う各種操作を行い、アプリケーションの画面遷移とエラー表示、出力ファイル内のデータから、持ち出しの制限や暗号化が正しく行われていることを確認する。(注：暗号化のアルゴリズムが正しく実装されていることは、別途、手動テストで確認している。)

・自走式暗号ファイルの暗号化と復号の際のパスワードに各種文字列を入力し、出力されるエラー表示により、パスワードの条件チェックが正しく行われていることを確認する。

②手動テスト

自動化ツールを使用せずに、手動で以下のテストを実施した。

・光学メディア（CD/DVD/ブルーレイディスク）に対しても、持ち出しの制限や暗号化が正しく行われていることを確認する。

・TOEの管理機能を操作してストレージ暗号の設定と解除を行い、開発用のツールでHDDに書き込まれている暗号化状態を示す管理情報を表示させ、HDDの暗号化が正しく行われていることを確認する。また、OSやアプリケーションの各種操作でHDDの読み書きを行い、OSやアプリケーションの動作に影響を与えることなく、暗号化と復号が行われることを確認する。

・SV暗号、自走式暗号、ストレージ暗号について、開発用デバッガを使用して暗号鍵と暗号化前後のデータを取得し、TOEの暗号化データとインターネットで入手できる暗号ツールOpenSSLで暗号化したデータを比較し、暗号アルゴリズムが正しく実装されていることを確認する。

・TOEが生成する暗号鍵を書き出す処理を追加したテスト用モジュールを使用してTOEの生成した暗号鍵を抽出し、乱数により異なる暗号鍵が生成されていることを確認する。

・TOEの管理機能を操作して設定情報の作成や変更を行い、開発用のツールで設定ファイル等の内容を表示し、設定情報が正しく反映されていることを確認する。

・TOEの監査機能を使用して、各種セキュリティ機能の出力した履歴の内容を表示し、履歴が正しく出力されていること、及び、管理者向けの機能が正しく動作することを確認する。

・TOEの操作とOSの起動・終了やログインを行い、TOEの表示やTOEの出力する履歴により、OS再起動を伴う設定など、OSの起動・終了やログインに依存するTOEの処理が正しく行われていることを確認する。

・タスクマネージャ等を使用して、TOEプロセスの起動状況や終了時の動作を確認する。

b. 実施テストの範囲

テストは開発者によって、自動テスト52項目、手動テスト182項目、合計234項目実施されている。（注：1項目には条件を変えた複数のテストが含まれている。）

カバレージ分析が実施され、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ている。深さ分析が実施され、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ている。

特に、許可アプリケーションについては、ファイルを操作するメニュー、マウス、キーボードのショートカット操作が網羅的にテストされたことが検

証されている。

c. 結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。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、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

3.3.2 評価者独立テスト

評価者は、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の再確認のための独立テストを実施した。評価者が実施した独立テストの概要を以下に示す。

1) 評価者独立テスト環境

評価者が実施したテストの構成は、開発者テストと同様の構成である。

評価者が実施したテストの構成を図3-1に示す。評価者テストは本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。

2) 評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

a. 独立テストの観点

評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点での独立テストを考案した。

①開発者テストのサンプルを使用したテスト

TOEが、開発者がテストしたとおりにふるまうことの確信を得るためのテストである。開発者の実施した自動テスト52項目について、全件を自動で再実施した。また、その自動テストが正しいことの確認、及び、手動テストの確認のために、Windows 7対応のために追加・変更された機能が重点的に含まれると共に、すべてのセキュリティ機能とすべてのインタフェース及びサブシステムインタフェースが含まれるように考慮し、自動テスト52項目から17項目、手動テスト182項目から81項目、合計98項目のテスト項目を選択し、手動で実施した。

②評価者が考案したテスト

開発者テストをふまえ、TOEが仕様のとおりにふるまうことの確信を得るためのテストである。開発者がテストしていないパラメタ値や、開発者が厳密に確認していないふるまいを考慮し、22項目のテストを考案した。

b. 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。

①開発者テストのサンプルを使用したテスト

開発者テストと同じテスト手法を用いた。

②評価者が考案したテスト

開発者テストと同じテスト手法を用い、以下を変更して実施した。

・許可・拒否アプリケーションと許可・拒否通信IPアドレス及びポート番号の設定の組合せ、キーボードとマウスの組合せによるファイルコピーや移動操作等、開発者がテストしていないテスト条件の追加。

・SePクライアントとSePサーバ間の通信データ仕様、SePクライアントでの受信タイミングや受信条件、オフライン環境やTOEがインストールされていない環境での確認等、開発者が厳密に確認していないふるまいの確認項目の追加。

・PC内蔵の光学メディアドライブに加えて、開発者がテストしていないUSB接続の外付け光学メディアドライブのテストの追加。

なお､通信データの確認にあたっては､インターネットで入手できるツールであるWiresharkを搭載したPCをネットワークに接続して、SePクライアントとSePサーバの間の通信データをモニタした。

c. 結果

実施したすべての評価者独立テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

3.3.3 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の可能性について必要と思われる侵入テストを考案し実施した。評価者侵入テストの概要を以下に示す。

1) 評価者侵入テスト概説

評価者の実施した侵入テストは以下のとおり。

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 パスワード入力において、制限を越えるデータを入力すると、TOEが予期しない動作をする可能性がある。

② TOEをアンインストールしたり、TOE動作に影響を与えるファイルを削除したり、TOEプロセスを終了させたりすることにより、セキュリティ機能が適用されずバイパスされる可能性がある。
③ Windowsのサービスとして動作しているTOE部分が、何らかの原因で異常終了すると、サービスが再起動するまでの間に、利用者操作にセキュリティ機能が適用されずバイパスされる可能性がある。
④ TOEの意図していない通信ポートを使用して、TOEの動作に悪影響を与えたり、セキュリティ機能をバイパスしたりする可能性がある。
⑤ SePクライアントをLANに接続された状態で、SePサーバを停止すると、SePクライアントのTOEが予期しない動作をする可能性がある。
⑥ OSが一度も認識していないデバイスをプラグアンドプレイで認識させると、そのデバイスに対してTOEが予期しない動作をする可能性がある。
⑦ ファイルの暗号化処理を途中で打ち切った場合、暗号化されない情報が残存し、平文のまま情報が持ち出される可能性がある。
⑧ 光学メディアドライブに対して、OSの特殊設定やOS内インタフェースにより、セキュリティ機能が適用されずバイパスされる可能性がある。

b. 実施テストの範囲

評価者は、潜在的な脆弱性が悪用される可能性があるかを決定するため、以下の侵入テストを実施した。

① 自走式暗号ファイルの暗号化と復号のパスワード入力において、GUIの制限により、制限を越えるデータの入力ができないことを確認する。
② 一般利用者権限で、TOEのアンインストール、TOEの動作に影響を与えるファイルの削除、TOEプロセスの終了ができないことを確認する。
③ 異常終了時と同じ状態を実現するために、管理者権限でWindowsのタスクマネージャ機能でTOEサービスを強制終了させる。その後、自動的に再起動する間に、ファイルの持ち出し操作を行い、セキュリティ機能がバイパスされないことを確認する。
④ インターネットで入手できるポートスキャンツールNessusを使用して、SePサーバ及びSePクライアントの通信ポートを探索し、意図しない通信ポートが開放されていないことを確認する。
⑤ SePクライアントにログインした状態で、SePサーバをシャットダウンしても、SePクライアントの各種セキュリティ機能が正常に動作することを確認する。
⑥ OSに一度も認識されていないUSBメモリをSePクライアントに接続して初めて認識させた時に、USBメモリへファイルのコピーを行い、各種暗号化が正常に動作することを確認する。

⑦ USBメモリにファイルをコピーしている途中で、USBメモリを引き抜いてコピー動作を中断し、作業用ファイルなど平文のファイルが作成されていないことを確認する。

⑧ 光学メディアドライブのプロパティを変更しても許可アプリケーション（Explorer）による持ち出しファイルが暗号化されることを確認する。また、光学メディアドライブを扱うExplorer以外のアプリケーション（OSに標準添付されているWindows Media Player、Windows DVD メーカー、Windows Media Center、Windows ディスクイメージ書き込みツール）について、すべてのファイル持ち出し操作が禁止されることを確認する。

c. 結果

実施した評価者侵入テストでは、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。

3.4 評価結果

3.4.1 評価結果

評価報告書をもって、評価者は本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。

3.4.2 評価者コメント/勧告

消費者に喚起すべき評価者勧告はとくにない。

4 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正しく反映されていること。
③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが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。

5 結論

5.1 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。

5.2 注意事項

本TOEの脅威の対象は利用者の過失による行為であり、悪意を持った利用者の持ち出し行為は評価の対象外である。

TOEのセキュリティ機能のふるまいは、TOEの設定内容によって変化する。本評価の対象は、「2.1.4 製品添付ドキュメント」に記載した「セキュアな運用ガイダンス」に従ってTOEの導入と設定を行った場合に限定される。

TOEが対応可能な媒体や通信プロトコルには制約があり、「セキュアな運用ガイダンス」には、TOEをセキュアに運用するための注意事項が含まれている。TOEの管理者は、ガイダンスに従って、TOE外の環境の設定や、利用者への周知徹底を行う必要がある。

なお、消費者によっては、消費者の意図している運用とTOEの制約が合致しない可能性もあるので、注意が必要である。TOEの導入を検討している消費者は、導入決定前に「セキュアな運用ガイダンス」の内容を確認することが推奨される。

6 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用語の定義を以下に示す。

SeP	セキュリティプラットフォームの略。
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。
SV暗号	SV暗号ファイルの暗号化と復号を行うSeP独自の暗号処理。SVは、Safety Valve (安全弁) の略。
SV暗号ファイル	TOEを導入している環境内で、暗号化と復号が自動的に行われる暗号化ファイル。平文のファイルを信頼領域から非信頼領域に持ち出した際に自動的に変換される。暗号化されたファイルは、信頼領域に戻すと自動的に復号される。
Webページへの添付	Webブラウザでファイルを読み込み、HTTPまたはHTTPSプロトコルでアップロードすること。
外部媒体	USBメモリなどの取り外し可能な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。
信頼領域	社の内部とする領域であり、以下が含まれる。 ・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)。 ・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。
信頼領域(社内URL)	ファイルをWebページに添付した際に、SV暗号化を行わないように管理者により指定されたURL。
自走式暗号ファイル	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

	復号可能な実行形式の暗号化ファイル。平文のファイルをリリースフォルダから非信頼領域に持ち出した際に変換される。
第三者	社外の不特定多数の者。
非信頼領域	社の外部とする領域であり、以下が含まれる。 ・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)。 ・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。 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。
非信頼領域(SV化URL)	ファイルをWebページに添付した際に、SV暗号化を行うように管理者により指定されたURL。
ファイル操作	ファイルのコピー、移動、保存、メール添付と送信、Webページへの添付と送信。ファイル内容のメールへのペースト操作、Webページへのペースト操作。
ファイル内容のペースト	ファイルの内容をWindowsのクリップボードに格納し、そのデータをアプリケーションの入力にペーストすること。
ファイルの書き込み	ファイルのコピー、移動、保存。
メール添付	ファイルを送信するために、メールソフトウェア上に読み込むこと。
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ページへの添付やペースト操作。
リリースフォルダ	自走式暗号ファイルとして持ち出すファイルを一旦入れるフォルダ。パスは管理者が定義する。

7 参照

[1] 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 2010年5月27日 ハミングヘッズ株式会社

[2] ITセキュリティ評価及び認証制度の基本規程 平成19年5月 独立行政法人 情報処理推進機構 CCS-01

[3] ITセキュリティ認証申請手続等に関する規程 平成19年5月 独立行政法人 情報処理推進機構 CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程 平成19年5月 独立行政法人 情報処理推進機構 CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 1 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 2 September 2007 CCMB-2007-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 2 September 2007 CCMB-2007-09-003

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-001 (平成19年3月翻訳第1.2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2版 2007年9月 CCMB-2007-09-002 (平成20年3月翻訳第2.0版)

[10] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-003 (平成20年3月翻訳第2.0版)

[11] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 3.1 Revision 2 September 2007 CCMB-2007-09-004

[12] 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2版 2007年9月 CCMB-2007-09-004 (平成20年3月翻訳第2.0版)

[13] セキュリティプラットフォーム evolution /SV CC Ver.2.0.9.4 評価報告書 第1.6版 2010年6月3日 一般社団法人 ITセキュリティセンター 評価部