認 証 報 告 書

独立行政法人情報処理推進機構
理事長　藤江　一正

原紙押印済

評価対象

申請受付日（受付番号）	平成27年4月1日 (IT認証5544)
認証番号	C0493
認証申請者	京セラドキュメントソリューションズ株式会社
TOEの名称	TASKalfa 266ci, Data Security Kit (E), HD-7付きモデル
TOEのバージョン	System:2PY_2F7K.C02.011 Panel:2PX_707K.C02.010 FAX:2NM_5100.004.001
PP適合	なし
適合する保証パッケージ	EAL1
開発者	京セラドキュメントソリューションズ株式会社
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27年12月7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

「TASKalfa 266ci, Data Security Kit (E), HD-7付きモデル」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、京セラドキュメントソリューションズ株式会社が開発した「TASKalfa 266ci, Data Security Kit (E), HD-7 付きモデル、バージョン System: 2PY_2F7K.C02.011 Panel:2PX_707K.C02.010 FAX:2NM_5100.004.001」（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 27 年 11 月 19 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京セラドキュメントソリューション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、本書の付属書であ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、EAL1 である。

1.1.2 TOEとセキュリティ機能性

本 TOE は、コピー機能、スキャン送信機能、プリンター機能、FAX 機能、ボックス機能といった基本機能を有するデジタル複合機（以下「MFP」という。）である。

本 TOE は、それらの MFP の基本機能に加えて、基本機能で扱う文書データやセキュリティに影響する設定データ等を漏えいや改ざんから保護するセキュリティ機能を提供する。

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

脅威とセキュリティ対策方針の妥当性は、本評価の保証要件には含まれていない。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような環境で運用することを想定する。

本 TOE は、TOE のハードウェアやソフトウェアが、物理的な不正アクセスから保護されるように、管理された環境に設置されることを想定している。

1.1.3 免責事項

本評価では、以下の運用を行った場合、それ以降は本評価による保証の対象外となる。

- 「7.5 評価構成について」に記述されている設定条件の変更
- サービス担当者用の保守機能の使用

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 27 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]、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。また、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：	TASKalfa 266ci, Data Security Kit (E), HD-7付きモデル
バージョン：	System:2PY_2F7K.C02.011　Panel:2PX_707K.C02.010 FAX:2NM_5100.004.001
開発者：	京セラドキュメントソリューションズ株式会社

製品が評価･認証を受けた本 TOE であることを、利用者は以下の方法によって確認することができる。

製品のガイダンスの記載に従って、MFP の操作パネルに TOE 名称とバージョンの情報を表示させ、MFP の操作パネルに表示された以下の情報を確認する。

- MFP 名称：TASKalfa 266ci
- オプション名称：「Data Security Kit (E)」及び「HD-7」
- System、Panel、FAX の各バージョン

3 セキュリティ方針

TOE は、コピー機能、スキャン送信機能、プリンター機能、FAX 機能、ボックス機能といった MFP の基本機能を提供しており、利用者の文書データを TOE 内部に保存したり、ネットワークを介して利用者の端末や各種サーバとやりとりしたりする機能を有している。

TOE は、開発者が必要であると想定した以下のセキュリティ機能を提供する。

・利用者を識別認証する機能
・ボックスに保存された文書データのアクセスを制御する機能
・管理機能の使用を権限のある利用者に制限する機能
・TOE 内部に保存される文書データを暗号化する機能
・ネットワーク上のデータを保護する機能
・公衆回線から内部ネットワークへのデータ転送を防止する機能

各セキュリティ機能の詳細は 5 章に示す。なお、TOE は、監査ログ機能は提供していない。

3.1 セキュリティ機能方針

TOE の提供するセキュリティ機能について、脅威や組織のセキュリティ方針に対する妥当性は、本評価の保証要件には含まれていない。

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 の運用環境のセキュリティ対策方針を表 4-1 に示す。これらの運用環境のセキュリティ対策方針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　運用環境のセキュリティ対策方針

識別子	前提条件
OE.LOCATION	TOEは機器管理者による監視が可能な管理された環境で運用し、機器管理者による監視により、TOEを構成するハードウェアおよびソフトウェアに対する解析、改ざんを行う物理的な攻撃を防止しなければならない。
OE.NETWORK	TOEが設置される内部ネットワークは、ファイアウォールなどの機器を設置して、外部ネットワークからTOEへの攻撃を防止しなければならない。
OE.ADMIN	機器管理者は、信頼のできる人物を選出し、所属する組織のセキュリティ方針や運用ルールを遵守するよう、また製品ガイダンスの記載に従って適切な操作ができるように、十分な指導を受けなければならない。

4.2 運用環境と構成

本 TOE は、オフィスに設置されて、内部ネットワークに接続し、同様に内部ネットワークに接続されたクライアント PC から利用される。本 TOE の一般的な運用環境を図 4-1 に示す。

なお、図 4-1 には示されていないが、クライアント PC は、USB ポート経由で TOE と接続し、TOE のプリンター機能を使用することもできる。

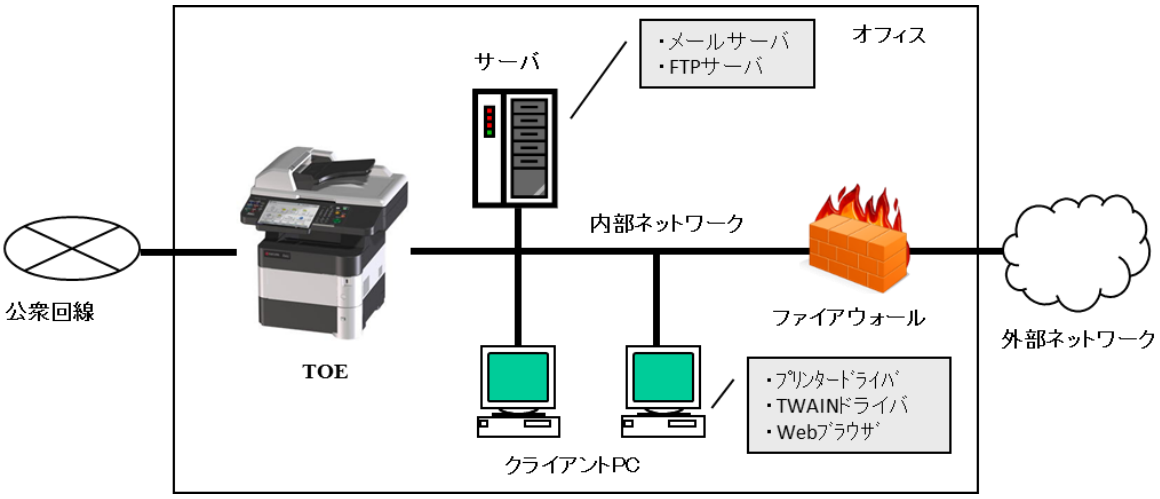

図 4-1　TOE の運用環境

TOE の運用環境において、TOE 以外の構成品を以下に示す。

(1) クライアント PC

利用者が、内部ネットワークまたは USB ポート経由で、TOE の提供する機能を利用するために使用する。以下のソフトウェアが必要である。

表4-2　クライアントPCのソフトウェア

種別	名称とバージョン
Webブラウザ	・Microsoft Internet Explorer 11.0
プリンタドライバ	・京セラドキュメントソリューションズ社 KX Driver
TWAINドライバ (スキャン送信機能)	・京セラドキュメントソリューションズ社 Kyocera TWAIN Driver

(2) サーバ（メールサーバ）

TOE 内の文書データをメール送信する機能を使用する場合に必要である。以下のサーバが必要である。

・メールサーバ：SMTP over TLS (TLS 1.2) に対応したもの

(3) サーバ（FTP サーバ）

TOE 内の文書データを FTP 送信する機能を使用する場合に必要である。以下のサーバが必要である。

・FTPサーバ：FTP over TLS (TLS 1.2) に対応したもの

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）。

4.3 運用環境におけるTOE範囲

TOE は、TOE に接続した USB メモリに格納した文書データの印刷や、TOE 内の文書データを USB メモリに格納する機能を提供している。USB メモリに格納された文書データの保護は、利用者の責任である。

FAX 送受信で保存される文書データは暗号化されない（詳細は 5 章の「SSD 暗号化機能」の説明を参照）。TOE の廃棄やリース返却の際には、注意が必要である。

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

TOE の構成を図 5-1 に示す。

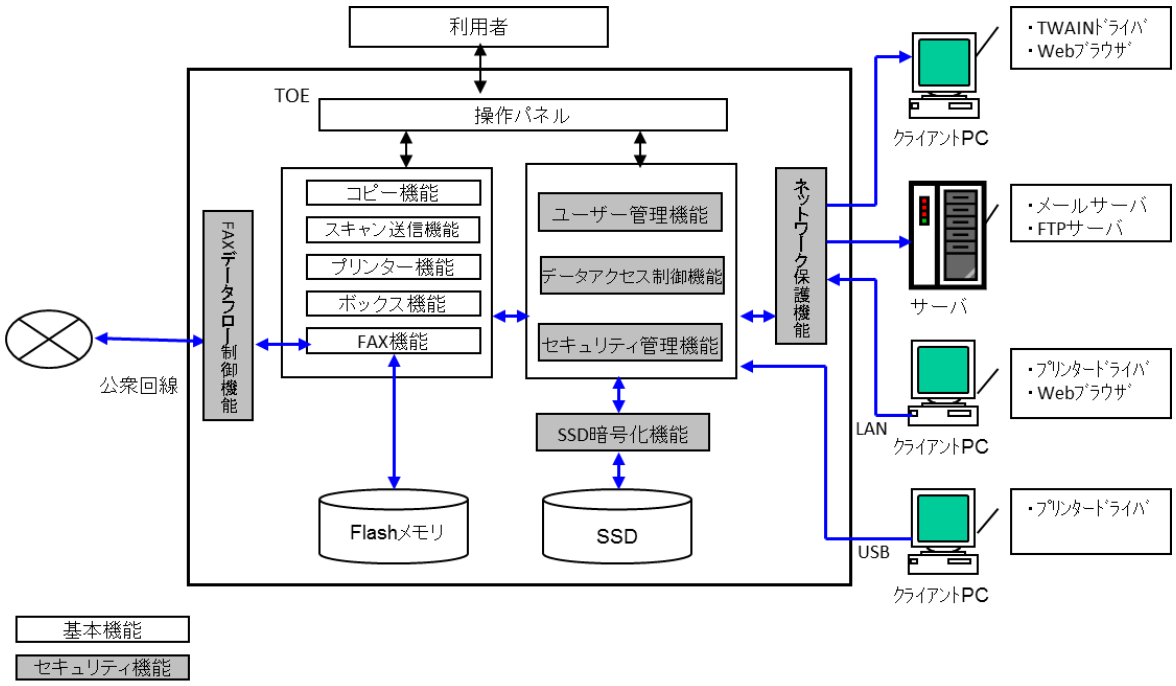

図 5-1　TOE の構成

図 5-1 で、網掛けした四角の中の機能は、セキュリティ機能である。以下、TOE のセキュリティ機能について説明する。

(1) ユーザー管理機能

本機能は、TOE の利用者を、ログインユーザー名とログインユーザーパスワードで識別認証する機能である。識別認証は、以下に示す利用者インタフェースのすべてに適用される。

・操作パネル
・クライアント PC (Web ブラウザ、プリンタドライバ、TWAIN ドライバ)

識別認証機能を補強するために、以下の機能を備えている。

- パスワードは 8 文字以上が要求される。
- 連続した認証失敗回数が機器管理者の設定値に達すると認証を停止する。
- 識別認証後、一定時間操作がない場合には、セッションを終了する。
- パスワードをダミー文字（*の表示）で隠匿する。

(2) データアクセス制御機能

本機能は、MFP の基本機能による文書データのアクセスを、権限のある利用者のみに制限する機能である。

アクセス制御は、文書データが保存されているボックスの所有者情報と共有設定情報に基づいて行われ、利用者本人が所有者であるボックスと共有設定されたボックス内の文書データへのアクセスだけが許可される。ただし、機器管理者は、ボックスに格納されたすべての文書データの操作が可能である。

(3) セキュリティ管理機能

本機能は、セキュリティ機能で使用されるデータの設定や変更を、識別認証された機器管理者だけに許可する機能である。ただし、一般利用者は、本人のログインユーザーパスワードの変更と、本人が所有者であるボックスの共有設定の変更が可能である。

(4) SSD 暗号化機能

本機能は、TOE 内部の SSD に保存するデータを暗号化する機能である。暗号化の対象の文書データは以下のものである。

・ボックスに保存される文書データ
・コピー機能やプリンター機能の処理の途中に一時的に保存される文書データ

なお、スキャン送信機能では、文書データを保存する処理はない。また、FAX 機能では、文書データは Flash メモリに保存され、暗号化されない。

暗号アルゴリズムは、256bit の AES である。暗号鍵は、TOE の導入時に機器管理者が設定する 8 文字の文字列と他の秘密情報を組み合わせて SHA-256 を用いて生成する。暗号鍵は、電源 ON 時に毎回同じ値が生成されて揮発メモリ上に格納され、電源 OFF によって消滅する。

(5) ネットワーク保護機能

本機能は、各種サーバやクライアント PC とネットワークを介して通信する際に、TLS による暗号化通信を行う機能である。

(6) FAX データフロー制御機能

公衆回線からのデータを、TOE を介して内部ネットワークに不正に転送することを防止する機能である。

5.2 IT環境

TOEは､内部ネットワークを介して各種サーバやクライアントPCと通信を行う。また、公衆回線を介してFAX通信を行う。

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。

表6-1 ガイダンス

名称	バージョン
Safety Guide (TASKalfa 266ci)	First edition 2013.11 302PZ5621001
Notice	2015.11 302P65699001
INSTALLATION GUIDE for Data Security Kit (E)	First edition 2015.1 303MS5650001
TASKalfa 266ci FIRST STEPS QUICK INSTALLATION GUIDE	First edition 2013.11 302PZ5601001
TASKalfa 266ci OPERATION GUIDE	Rev.1 2015.7 2PZKDEN001
TASKalfa 266ci FAX OPERATION GUIDE	First edition 2014.01 2PZKDEN500
Data Security Kit (E) OPERATION GUIDE	Rev.1 3MS2P6KDEN1 2015.11
Command Center RX USER GUIDE	Rev. 6 2015.8 CCRXKDEN06
Printer Driver User Guide	Rev.16.18 2013.10
KYOCERA Net Direct Print User Guide	Rev. 3.51 2014.5

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）と相互承認している認定機関（独立行政法人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 4 月に始まり、平成 27 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、10 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、評価者テストを実施した。

7.4 製品テスト

評価者は、評価の過程で示された証拠を検証した結果から、必要と判断された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

本評価では、開発者テストは保証要件に含まれていない。

7.4.2 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を確認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を図 7-1 に示す。

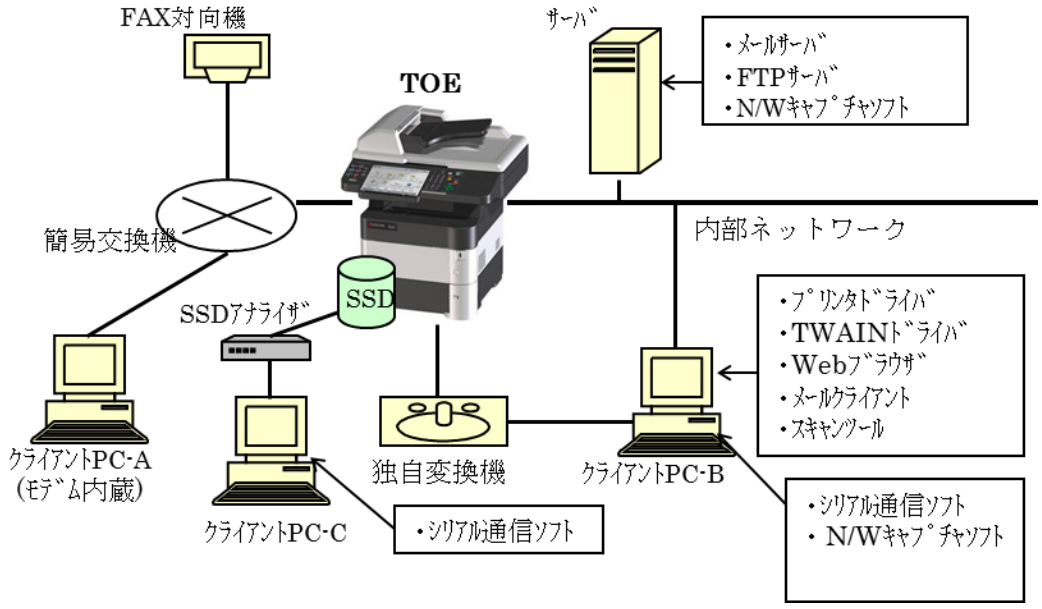

図7-1　独立テストの構成図

独立テストの構成要素を表 7-1 に示す。

表7-1　独立テストの構成要素

名称	詳細
TOE	TASKalfa 266ci ・Data Security Kit (E)とHD-7を装着

名称	詳細
サーバ	メールサーバ、FTPサーバとして使用 ・Windows Server 2003 SP2搭載PC ・メールサーバ：Pmail Server Manager 1.91 ・FTPサーバ：Microsoft Internet Information Services Version 8.5 ※上記の他に以下の開発テストツールを搭載 ・ネットワークキャプチャソフト：WireShark v1.12.2
クライアント PC-B	TOE利用者のクライアントPCとして使用 ・Windows 8.1 Enterprise搭載PC ・プリンタドライバ：KX Driver v6.2.1113 ・TWAINドライバ：Kyocera TWAIN Driver v2.0.5217 ・Webブラウザ：Internet Explorer 11.0 ・メールクライアント：Mozilla Thunderbird 38.1.0 ・スキャンツール：IrfanView v3.91 （本ツールは、TWAINドライバを使用して、TOEでスキャンした画像を取り込み、表示する） ※上記の他に以下の開発テストツールを搭載 ・シリアル通信ソフト：Tera Term Professional v4.78 ・ネットワークキャプチャソフト：WireShark v1.12.2
独自変換器	TOE内部の開発者用インタフェースを取り出す基板 ・京セラドキュメントソリューションズ社の独自基板
クライアント PC-C	SSDアナライザと接続し、TOE内のSSDの入出力データのモニタに使用 ・Windows 7 Professional SP1搭載PC ・シリアル通信ソフト：Tera Term Professional v4.78
SSDアナライザ	TOE内のSSDの入出力データを解析する装置 ・SATA Command Monitor
FAX対向機	TOEとのFAX送受信に使用 ・ECOSYS FS-C2626MFP (京セラドキュメントソリューションズ社のMFP)
簡易交換機	公衆回線を疑似的に実現する機器 ・X4108 Switch Simulator (AD SYSTEMS)
クライアント PC-A	公衆回線を経由した不正転送防止機能の確認に使用 ・Windows 7 Professional SP1搭載PC

評価者がテストしたTOEは、TOEの全機種であり、2章のTOE識別と同一の識別を持つ。

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、開発者から提供されたものを利用しており、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、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 すべてのセキュリティ機能を確認する。

② 暗号鍵生成アルゴリズムや暗号アルゴリズムが、仕様どおりのアルゴリズムであることを確認する。

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＞

TOEが提供している外部インタフェースから確認可能なふるまいについては、それを利用して、入力に対する応答、TOEの動作、通信データを確認する。

TOEが提供している外部インタフェースでは確認できないふるまいについては、開発者用インタフェースやSSDアナライザを使用して、TOE内部の動作を確認する。

＜独立テストツール＞

独立テストで利用したツールを表7-3に示す。

表7-3　独立テストツール

ツール名称	概要・利用目的
ネットワークキャプチャソフト (WireShark v1.12.2)	内部ネットワーク上の通信データをキャプチャする。通信プロトコルの確認に使用
SSDアナライザ＋モニタソフト(クライアントPC-C)	TOE内部のSSDのSATAインタフェースを流れるデータをキャプチャする。SSDの暗号化データの確認に使用
ハッシュ計算ツール GNU coreutils v5.97	TOEによる暗号鍵生成結果が正しいことを確認するための比較対象として使用
暗号化ツール OpenSSL 1.0.1h	TOEによる暗号化結果が正しいことを確認するための比較対象として使用
独自変換器＋シリアル通信ソフト(クライアントPC-B)	TOEの開発者用インタフェースを使用して、TOE内部でのテスト実行や、テスト結果の確認を行う

＜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、11 項目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 7-4 に示す。

表7-4 実施した主な独立テスト

観点	テスト概要
観点①	・操作パネル、クライアントPC(Webブラウザ、プリンタドライバ、TWAINドライバ)からのログインを行い、識別認証が仕様どおりに動作することを確認する。また、アカウントロックまでの認証失敗回数が、異なるインタフェースを使用しても通算され、仕様どおりに動作することを確認する。 ・ボックスの所有者情報の変更や文書データの移動を行い、文書データのアクセス制御が仕様どおりに動作することを確認する。 ・利用者に付与する管理者権限の変更を行い、管理機能のアクセス制御が仕様どおりに動作することを確認する。 ・TOE内部のSSDにファイルを作成し、その際のSSDへの書き込みデータが暗号化されていることを、SSDアナライザを使用して確認する。

	・TOEとクライアントPC(Webブラウザ、プリンタドライバ、TWAINドライバ)、FTPサーバ、メールサーバ間の通信データをモニタし、通信プロトコルがTLS 1.2であることを確認する。 ・公衆回線を経由してTOEに接続を試みても、FAX通信以外は接続できないことを確認する。
観点②	・開発者インタフェースを使用して、TOE内部の暗号鍵生成ライブラリを用いて暗号鍵の生成を行い、その結果を別途計算したSHA-256の結果と比較する。 ・開発者インタフェースを使用して、TOE内部のAES演算を行うハードウェアにデータの暗号化と復号を実行させ、その結果を別途計算したAESの結果と比較する。

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 想定外のネットワークインタフェースが悪用される懸念がある。

② 各種インタフェースに特殊な入力をすると、不正な処理が実行される懸念がある。

③ Web の各種の公知の脆弱性が該当する懸念がある。

④ 通信データを書き換えることにより、セキュリティ機能がバイパスされ、悪用される懸念がある。

⑤ 暗号化通信で弱い暗号方式が使われる懸念がある。

⑥ 印刷ジョブコマンドや PDF ファイルの処理に、公知の脆弱性が存在する懸念がある。

⑦ TOE 動作中の電源 OFF によって、セキュリティ機能が正常に動作しない懸念がある。

⑧ サービス担当者用インタフェースが悪用される懸念がある。

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＞

侵入テストは、独立テストの環境に、侵入テスト用の PC を追加した環境で実施した。侵入テストで使用したツールの詳細を表 7-5 に示す。

表7-5　侵入テストツール

名称		概要・利用目的
侵入テスト用PC		Windows VISTA Business SP2、Windows 8.1 Professionalを搭載したPCであり、以下の侵入テスト用ツールを動作させる。
	Nmap Ver.6.49BETA3	利用可能なネットワークポートを検出するツール
	Fiddler V4.5.1.5	WebブラウザとWebサーバ(TOE)の間の通信を仲介し、その間の通信データの参照と変更を行う
	Metasploit Version 4.6.2	PDFの脆弱性を検査するための検査データの作成に使用
	SSLScan kali-linux-1.1.0a-i386	SSL/TLSの暗号スイーツのサポート有無を確認するツール。Kali Linux付属のものを使用
	VMware Player 6.0.7	Kali Linuxの実行環境として使用
	OWASP ZAP 2.4.0	Webの一般的な脆弱性をスキャンするツール
	Java V8 Update 51	OWASP ZAPの実行環境として使用

＜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 7-6 に示す。

表7-6　侵入テスト概要

脆弱性	テスト概要
脆弱性①	・NmapをTOEに実施し、意図しないポートがオープンされていないことを確認する。
脆弱性②	・操作パネル、プリンタドライバ、Webブラウザ、TOEに接続したUSBメモリから、制限値を超える長さのデータや、SQL、OSコマンド、スクリプトなどの不正な処理が実行される可能性のある文字列を入力しても、不正な処理が実行されないことを確認する。
脆弱性③	・OWASP ZAPを使用してTOEのWebサーバ機能の脆弱性の探索を行い、公知の脆弱性が存在しないことを確認する。 ・WebブラウザでURLを直接指定しても、識別認証やアクセス制御がバイパスされないことを確認する。 ・Webのセッション管理情報を調査し、公知の脆弱性が疑われる方式ではないことを確認する。 ・シェルコマンドが実行される可能性のある文字列を入力しても、処理が実行されないことを確認する。
脆弱性④	・Fiddlerを使用して、WebブラウザからTOEへの通信データを書き換えても、アクセス制御がバイパスされないことを確認する。 ・Fiddlerを使用して、Webブラウザからは入力できないフィールドのデータを、長大なデータや特殊な文字コードに書き換えても、TOEが誤動作しないことを確認する。
脆弱性⑤	・SSLScanをTOEに実施し、弱い暗号方式を指定しても接続できないことを確認する。 ・WebブラウザからTOEにhttpプロトコルで接続を試みても、httpsプロトコルで接続されることを確認する。
脆弱性⑥	・悪用される可能性のある印刷ジョブコマンドや、不正な処理を含むPDFファイルをTOEに入力しても、処理が実行されないことを確認する。
脆弱性⑦	・TOE動作中に電源OFF・ONしても、以下のセキュリティ機能のふるまいが正常に動作することを確認する。 - アカウントロックまでの認証失敗回数の保持 - アカウントロック後の解除までの時間
脆弱性⑧	・サービス担当者用インタフェースを使用するためには、サービス担当者毎に設定するパスワードが必要であり、サービス担当者以外は使用できないことを確認する。

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 のセキュリティ機能を有効にし、安全に使用するために、TOE の機器管理者は、当該ガイダンスの記述のとおりに TOE 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。

TOE の構成条件には、TOE の提供している機能を使用禁止にする設定があり、例えば、以下のような設定値も含まれている。

・IPP以外の印刷プロトコルの無効化
・SNMPの無効化
・公衆回線を介したリモート診断の無効化
・FAX受信したデータのネットワーク送信やボックス保存の無効化

上記のように、TOE の提供している機能を使用禁止にする設定も含めて、TOE の構成条件である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くなるので、TOE の機器管理者は注意が必要である。

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。

・EAL1 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 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。
② 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。
③ 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。

8.1 認証結果

提出された評価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 EAL1 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 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 の評価対象範囲や運用上の要求事項が、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。

特に、保守機能を使用した場合、それ以降の運用での本 TOE のセキュリティ機能への影響については本評価の保証の範囲外となるため、保守の受け入れについては管理者の責任において判断されたい。

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。

TASKalfa 266ci, Data Security Kit (E), HD-7 付きモデル セキュリティターゲット, 第 1.04 版, 2015 年 11 月 19 日, 京セラドキュメントソリューションズ株式会社

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。

MFP	Multi-Function Printer (デジタル複合機)

本報告書で使用された用語の定義を以下に示す。

FAX機能	公衆回線を通して、FAX送受信を行う機能。FAX受信した文書データは自動的に印刷出力される。FAX送信は、操作パネルの操作で、紙文書を読み取って送信する
コピー機能	操作パネルの操作で、紙文書を読み取って複写印刷する機能
スキャン送信機能	TOEで紙文書を読み取って、FTPサーバ、メールサーバ、TOEに接続されたUSBメモリ、クライアントPC(TWAINドライバ)に送信する機能。読み取りの指示は、TWAINドライバへの送信の場合はTWAINドライバから行い、その他の場合は、TOEの操作パネルから行う
プリンター機能	クライアントPCから内部ネットワークまたはUSBポートを経由して、TOEが受信した文書データを印刷する機能。TOEが受信した文書データはいったんボックスに蓄積され、操作パネルからの指示で印刷出力される
ボックス	文書データを格納する領域。属性として、ボックスの所有者と共有設定の情報を持つ
ボックス機能	文書データをボックスに保存する機能。保存した文書データは印刷出力や削除等をすることができる。文書データの保存は、操作パネルでの紙文書の読み取り操作や、クライアントPC(プリンタドライバ)からの印刷依頼で行う。文書データの削除等は、TOEの操作パネルまたはクライアントPC(Webブラウザ)から操作可能である。ただし、文書データの印刷出力は、操作パネルだけが可能である

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] TASKalfa 266ci, Data Security Kit (E), HD-7 付きモデル セキュリティターゲット, 第1.04版, 2015年11月19日, 京セラドキュメントソリューションズ株式会社

[13] TASKalfa 266ci, Data Security Kit (E), HD-7 付きモデル 評価報告書, 第4.9版, 2015年11月19日, 一般社団法人ITセキュリティセンター 評価部