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21年9月24日** (IT**認証**9265)
認証番号	C0268
認証申請者	**京セラミタ株式会社**
TOE**の名称**	Data Security Kit (E) Software Type II
TOE**のバージョン**	V1.00J
PP**適合**	**なし**
適合する保証パッケージ	EAL3
開発者	**京セラミタ株式会社**
評価機関の名称	**株式会社電子商取引安全技術研究所 評価センター**

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9月28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

「Data Security Kit (E) Software Type II V1.00J」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

この認証報告書は、京セラミタ株式会社が開発した「Data Security Kit (E) Software Type II V1.00J」（以下「本TOE」という。）について株式会社電子商取引安全技術研究所 評価センター（以下「評価機関」という。）が平成22年9月15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ミタ株式会社に報告するとともに、本TOEに関心を持つ消費者や調達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を導入し運用する消費者サイトのシステム管理者等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、主としてコピー機能、スキャナ機能、プリンタ機能を有する複合機(Multi Function Printer：以下「MFP」という。)に対して、Data Security Kit (E)のライセンスを適用した後の、MFPを制御するファームウェアとセキュリティ演算を行う専用カスタムIC(ASIC)である。ライセンスが適用された後のファームウェアとASICがData Security Kit (E) Software Type II V1.00Jと称される。

本TOEは、HDD上の画像データを削除する際には、画像データが存在する領域を上書きするようにして、画像データの漏洩を防止する。

本TOEは、MFPの機能(コピー機能等)のためにHDDに一時的に画像データを保存する際には、画像データを暗号化してから保存するようにして、画像データの漏洩を防止する。

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。

1.1.2.1 脅威とセキュリティ対策方針

本TOEは、以下のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

・ MFPに搭載されているHDDが、運用時または廃棄・返却後に持ち出されて、MFPの機能(コピー機能等)のためにHDDに一時保存されている画像データが漏洩することを脅威と想定する。
ここで対象となるのは、利用者の意図とは無関係にMFPの機能のために保存される画像データ(例えば、コピー機能においてスキャンした画像データであり、印刷が終わるまで保存される)であり、利用者が意図的に保存する画像データは対象ではない。
この脅威に対抗するために、TOEは、HDDに画像データを保存する際には、画像データを暗号化してから保存する。

・ MFPに搭載されているHDDが、運用時または廃棄・返却後に持ち出されて、既に削除された画像データが復元され漏洩することを脅威と想定する。
ここでは、利用者が意図的に保存した画像データを削除した場合と、MFPの機能のために一時保存される画像データが自動的に削除される場合がともに対象となる。
この脅威に対抗するために、TOEはHDD上の画像データを削除する際には、画像データが存在する領域を上書きし再利用できなくすることで漏洩を防止する。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定している。

・ 本TOEは、以下の京セラミタ株式会社製MFPに搭載され使用される。

- TASKalfa 520i
- TASKalfa 420i

・ 本TOEを含むMFPは、企業やその部門等の組織により運営されるオフィスに設置されることを想定している。

・ この利用環境では、MFPの設置場所は従業員等の監視下となり、少なくとも明白に攻撃とわかるような行為は防止されることが想定される。ただし、MFPの構造上、HDDの取り外しは比較的容易であるために、防止しきれない可能性がある。

・ MFPがネットワークに接続される場合は、オフィス内のLANに接続されることを想定している。LANが外部ネットワーク(インターネット等、組織外のもの)と接続する場合も外部ネットワークからMFPにアクセスできないように管理される。

・ サービス担当者は信頼できることが想定される。

1.1.3 免責事項

本評価で保証されるのは、MFPに対してData Security Kit (E)のライセンスを適用することによって有効になる「上書きの機能」と「暗号化の機能」に限定される。

Data Security Kit (E)のライセンスを適用する前のMFPにも、一般的にはセキュリティ機能と認識される機能があるが、これらの機能は本評価では保証されない。

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セキュリティ認証申請手続等に関する規程」[2]、「ITセキュリティ評価機関承認申請手続等に関する規程」[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22年9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、本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：	Data Security Kit (E) Software Type II
バージョン：	V1.00J
開発者：	京セラミタ株式会社

正しいMFP及びファームウェアに Data Security Kit (E)のライセンスが適用されていること(アクティベートされていること)が、評価・認証を受けた本TOEであることの条件である。そのことを、利用者は以下の方法によって確認することができる。

・ MFPの確認

MFPの識別はMFP本体に記載されている。それをガイダンスに記載されているMFPのリストのいずれかと一致することを確認することで、正しいMFPであることの確認ができる。

・ ファームウェアの確認

ガイダンスに記載された手順に従い、MFPを操作してファームウェアのバージョンを印刷することができる。印刷されたバージョンを、ガイダンスに記載されているファームウェアの正しいバージョンと照合することで、正しいファームウェアであることの確認ができる。

・ Data Security Kit (E)のライセンスが適用されていること(アクティベートされていること)の確認

ライセンスが適用されている場合に表示されるアイコンについてガイダンスに記載されている。これに従い操作パネルを確認することで、ライセンスが適用されていることの確認ができる。

(補足) MFPの識別が決まれば、それによりASICの識別も一意に決まるように製造の管理がされている。そのため、正しいMFPであることの確認が正しいASICであることの確認となる。

3 セキュリティ方針

本章では、本TOEがセキュリティサービスとしてどのような方針あるいは規則のもと、機能を実現しているかを述べる。

本TOEはファームウェアとASICであり、MFPを制御することにより、コピー機能、スキャナ機能、プリンタ機能を実現する。これらの機能の実行の際に、必要に応じて画像データをHDDに一時保存する。このように、MFPの機能のために利用者の意図によらず保存されることを一時保存と呼ぶ。

一時保存された画像データは、これらの機能が終了して必要がなくなると自動的に削除される。

本TOEはまた、利用者の指示によって、画像ファイルをHDDに長期保存する機能も提供する。このように、利用者の意図により保存されることを長期保存と呼び、一時保存と区別する。

長期保存された画像データは、利用者からの指示がなければ削除されない。

本TOEは、MFPの機能(コピー機能等)のためにHDDに画像データを一時保存する際には、画像データを暗号化してから保存するようにして、画像データの漏洩を防止する。

本TOEは、一時保存された画像データや長期保存された画像データを削除する際には、画像データが存在する領域を上書きするようにして、画像データの漏洩を防止する。

(注) 長期保存されている画像データは、明示的に削除されない限りは漏洩を防止する対象とはみなさない。

3.1 セキュリティ機能方針

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.TEMP	**一時保存データへの不正アクセス** 攻撃者が、HDDを持ち出し、容易に入手可能なツールを利用して、HDD上に一時保存している画像データを不正に読み出して持ち出すかもしれない。
T.RESIDUAL	**残存データへの不正アクセス** 攻撃者が、HDDを持ち出し、容易に入手可能なツールを利用して、画像データの削除後もHDDに残存しているデータを不正に復元/解読し、読み出して持ち出すかもしれない。 (補足) 画像データの削除は、以下の両者が対象である。 ・一時保存された画像データを、TOEが自動的に削除する。 ・長期保存された画像データを、利用者に指示によりTOEが削除する。

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。

(1) 脅威「T.TEMP」への対抗

本TOEは、この脅威に対抗するために、HDD上に画像データを保存する際には、画像データを暗号化してから保存する。

(2) 脅威「T.RESIDUAL」への対抗

本TOEは、この脅威に対抗するために、HDD上の画像データを削除する際には、画像データが存在する領域を無意味なデータで上書きする。

なお、一時保存された画像データが読み出されるという脅威に対しては、脅威「T.TEMP」への対抗(上記)によって対抗されている。そのため、対抗が二重に行われることになる。

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が対応する組織のセキュリティ方針はない。

4 前提条件と使用環境

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使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.LOCATION	**運用環境におけるTOEの安全性の確保** MFPのハードウエアに対し行われるかもしれない攻撃によるTOEのセキュリティ侵害を防ぐため、相互監視が可能な管理された環境にて運用するものと想定する。ハードウエアに対する攻撃ではMFP内部を開き機器を接続し解析する、あるいはMFPの基板を交換するようなことを想定する。 (補足) MFP内部を開き機器を接続し解析する、あるいはMFPの基板を交換する等、明白に攻撃とわかるような行為は防止できるような相互監視のある環境で運用するということである。 ただし、上記のような明白な攻撃に較べ、MFPの構造上、HDDの取り外しは比較的容易であるために、相互監視では防止しきれない可能性がある。そのため、本前提条件が満たされても可能な攻撃手段とみなされ、脅威として挙げられている。
A.NETWORK	**TOEの外部ネットワークからの安全性** TOEは外部ネットワークの不正アクセスから保護された内部ネットワークに接続されて使用されるものと想定する。 (補足) TOEが搭載されるMFPが内部ネットワークに接続される場合の前提条件である。
A.CE	**サービス担当者の信頼性** TOEのサービス担当者は、信頼出来る人物であり、不正は行わないものと想定する。

4.2 使用環境と構成

本TOEは、以下の京セラミタ株式会社製MFPに搭載され使用される。

- TASKalfa 520i
- TASKalfa 420i

本TOEを含むMFPは、企業やその部門等の組織により運営されるオフィスに設置されることを想定している。本TOEの一般的な使用環境を図4-1に示す。

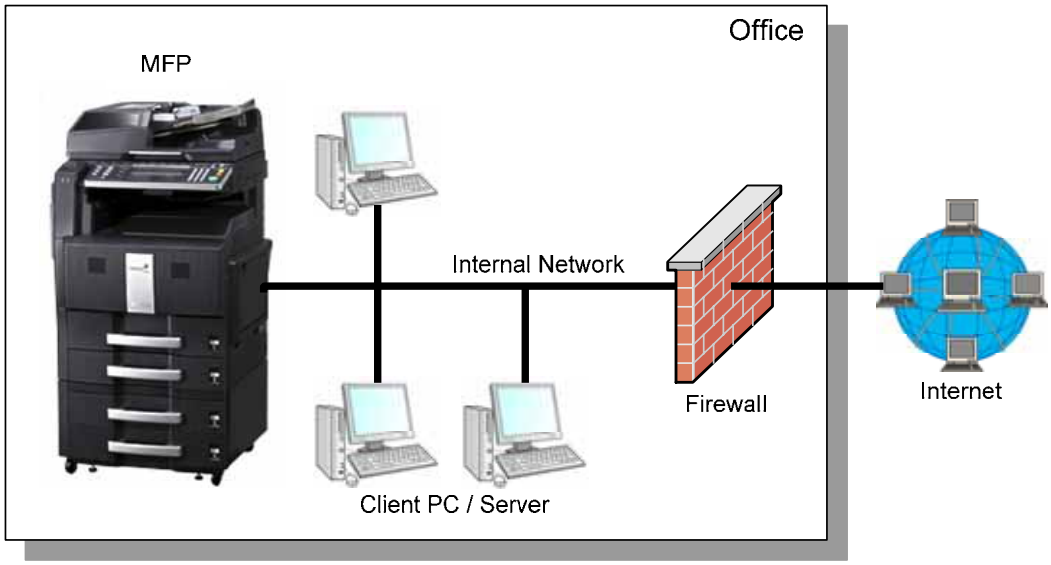

図4-1　TOEの使用環境

内部ネットワークへの接続は必須ではないが、内部ネットワークに接続してMFPの機能を使用するためには、クライアントPC及びサーバに、以下のソフトウェアが必要となる。(どれが必要かは、MFPのどの機能を使用するかによる。)

- ガイダンスで指定されているプリンタドライバ及びTWAINドライバ
- SMTPサーバ、SMBサーバ、FTPサーバ

ファイアウォールは、A.NETWORKを達成するためのものである。

なお、TOE以外のMFPの部分(ファームウェアとASICが除かれた部分)、内部ネットワークに接続されるクライアントPC及びサーバ、クライアントPC及びサーバで動作するソフトウェア、ファイアウォール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 使用環境におけるTOE範囲

本評価で保証されるのは、MFPに対してData Security Kit (E)を適用することによって有効になる以下のセキュリティ機能に限定される。

- MFPの機能(コピー機能等)のためにHDDに一時的に画像データを保存する際に、画像データを暗号化する機能
- HDD上の画像データを削除する際に、画像データが存在する領域を上書きする機能

Data Security Kit (E)を適用する前のMFPにも、一般的にはセキュリティ機能と認識される機能(例えば、長期保存された画像データへの許可されないアクセスを防ぐための識別・認証やアクセス制御)があるが、これらの機能は本評価では保証されない。

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（コンポーネント）について、目的と関連を説明する。

5.1 TOE境界とコンポーネント構成

TOEはMFPのファームウェアとASICであり、主要なコンポーネントは図5-1のように構成される。ファームウェアとASIC以外のMFPの部分はTOEの範囲ではない。

HDDへのアクセスを含めたMFPの制御をTOEが実施している。そのため、ユーザがMFPを利用することで発生する画像データのHDDへの保存やHDDからの削除は、すべてTOEによるHDDの制御で行われる。つまり、ユーザがMFPを利用することで発生する画像データに対しては、本評価で保証される上書き消去機能や暗号化機能が動作することは信頼できる。

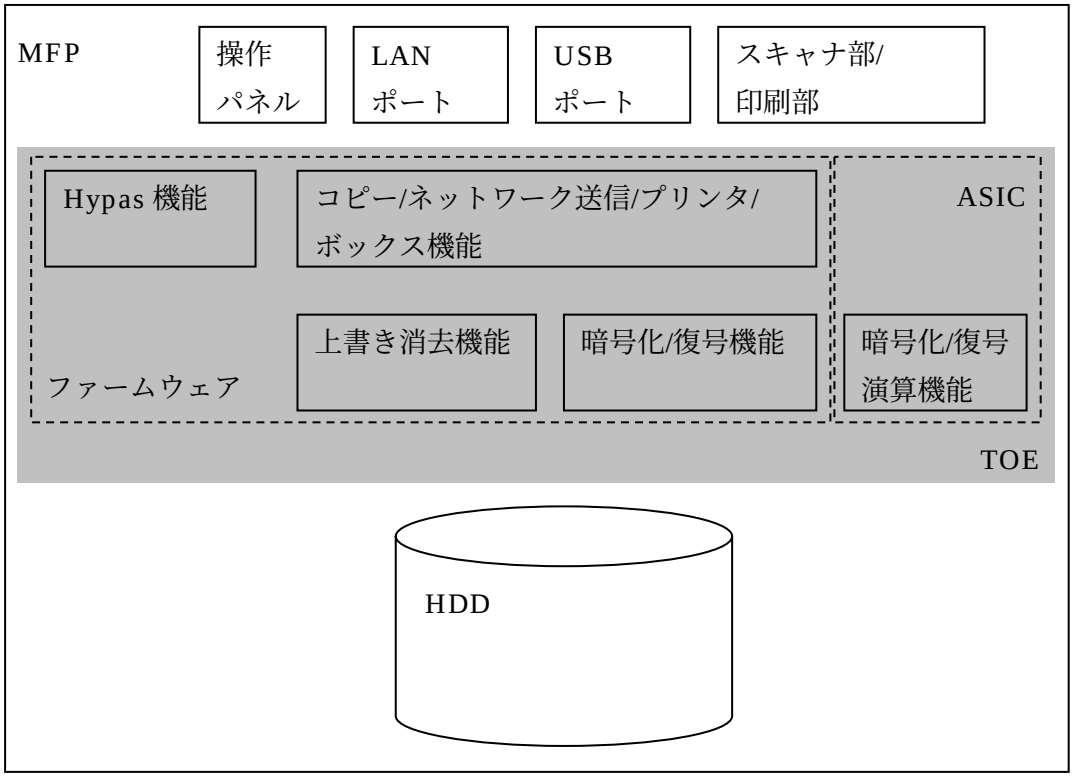

図5-1　TOE境界

TOEを構成する主要なコンポーネント(コピー/ネットワーク送信/プリンタ/ボックス機能、上書き消去機能、暗号化/復号機能、暗号化/復号演算機能、HyPAS機能)について説明する。

・ コピー/ネットワーク送信/プリンタ/ボックス機能

この機能はData Security Kit (E)のライセンスの適用とは無関係に利用でき

る機能であり、セキュリティ機能ではない。

以下のように、MFPの各機能を提供する。

- コピー機能

  操作パネルから入力/操作を行うことにより、画像データをスキャナデバイスから読み込み、印刷部から出力する。

- ネットワーク送信機能

  操作パネルから入力/操作を行うことにより、スキャナ部から読み込んだ画像データをLAN経由で送信する。

- プリンタ機能

  LAN上、またはUSB接続されたクライアントPCまたはサーバPCから操作することにより、送信された画像データを印刷部から出力する。

- ボックス機能

  操作パネルからの入力/操作を行うか、もしくは、LANまたはUSB接続されたクライアントPCまたはサーバPCから操作を行うことにより、入力された画像データをHDD上に長期保存する。長期保存された画像データは、印刷部から出力、クライアントPCまたはサーバPCへ転送、及び削除することができる。

これらの機能を提供する際には、HDDへの画像データの保存、HDDからの画像データの読み出し、HDD上の画像データの削除が行われる。

HDDに対するデータの読み書きは、「暗号化/復号機能」を通して行うことによって、HDDに書き込むデータは暗号化され、HDDから読み出すデータは復号される。

HDD上のデータの削除には、「上書き消去機能」を利用する。それによって、削除されたデータの復元は困難になる。

・ 暗号化/復号機能

この機能はData Security Kit (E)のライセンスの適用によって利用可能になる機能であり、セキュリティ機能である。

HDDに対して画像データを読み書きする機能である。

HDDに書き込む際には、FIPS PUB 197 に基づくAES暗号アルゴリズムにより暗号化を行う。HDDから読み込む際には、同アルゴリズムにより復号する。

暗号化/復号の演算は、「暗号化/復号演算機能」を利用して行う。

・ 暗号化/復号演算機能

この機能はData Security Kit (E)のライセンスの適用によって利用可能になる機能であり、セキュリティ機能である。

FIPS PUB 197 に基づくAES暗号アルゴリズムの演算を行う。

・ 上書き消去機能

この機能はData Security Kit (E)のライセンスの適用によって利用可能になる機能であり、セキュリティ機能である。

指定された画像データが存在するHDD上の領域に、無意味な文字列を上書きして復元が困難な状態にした上で画像データの管理情報を削除する。

・ HyPAS機能

この機能はData Security Kit (E)のライセンスの適用とは無関係に利用できる機能であるが、セキュリティ機能の部分を保護するという意味でセキュリティ機能に間接的に寄与している。

MFPにアプリケーションをインストールし、MFP上で動作させるための機能である。インストールされるアプリケーションはTOEには含まれない。

アプリケーションには限られた動作のみが許され、セキュリティの侵害となるような動作はできないようになっている。

5.2 IT環境

本TOEは、MFPに搭載されて動作する。MFPの構成要素で、特にTOEと関係するのは以下のものである。

・ ファームウェアを実行するための環境(CPUやメモリ)

・ 画像を光学的に読み取るためのスキャナ部

・ 印刷を行うための印刷部

・ 画像データを保存するためのHDD

・ 利用者、クライアントPC、サーバPCとのインタフェースを提供する操作パネル、LANポート、USBポート

クライアントPCまたはサーバPCは、LANポートまたはUSBポートを介して接続

され、プリンタ機能、ボックス機能を使うことができる。ネットワーク送信機能で送信される画像データを受け取ることもできる。

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。

・ 取扱説明書

名称	バージョン	仕向地
Data Security Kit (E) 使用説明書	Rev.2 2010.8	日本
お知らせ	303MS56320 2010.1	日本
Data Security Kit (E) 設置手順書	303MS56710 2008.12	日本
TASKalfa 420i/520i 使用説明書	302KR56010 初版 2009.7	日本

・ サービスマニュアル

名称	バージョン	仕向地
TASKalfa 420i/520i サービスマニュアル	2KSSM003 Rev.3 2010.5	日本

7 評価機関による評価実施及び結果

7.1 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。

7.2 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9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、平成22年1月、及び同年3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22年3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。

7.3 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。

7.3.1 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7-1に示す。

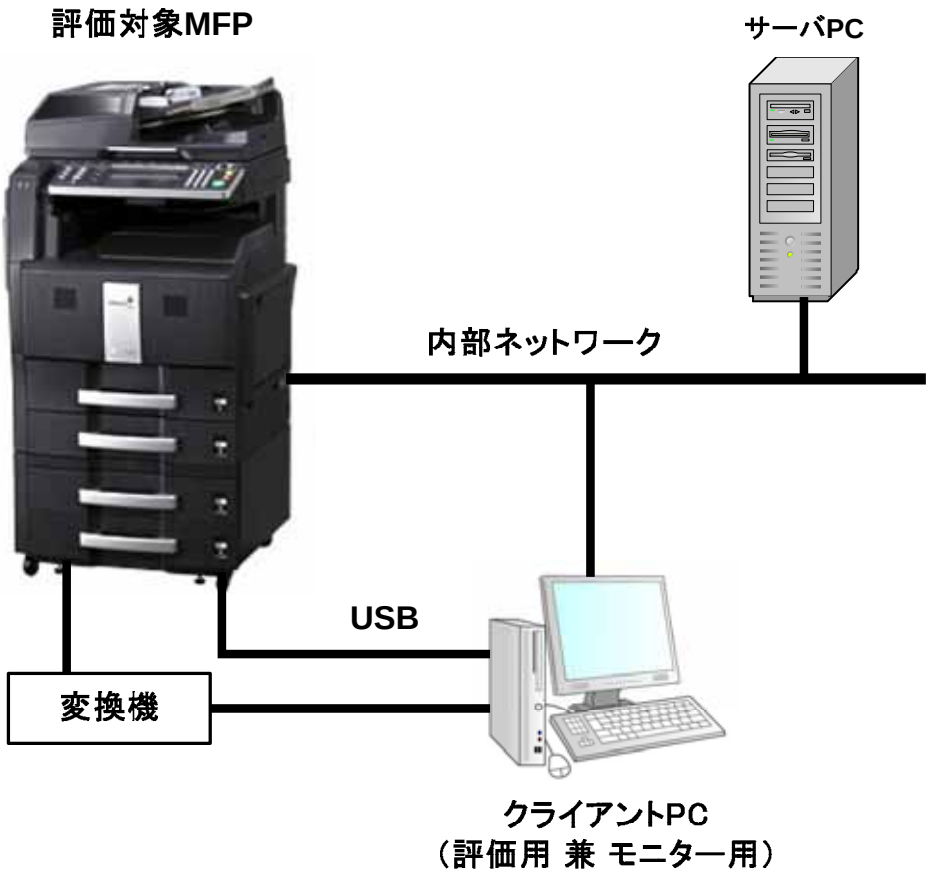

図7-1　開発者テストの構成図

・ TOE

　STで識別されているTOEに対して、テストのためのログ出力の機能が追加されたものが、評価対象MFPで使用された。

　追加された機能が、TOEの機能のふるまいに影響がないものであることが、評価者によるソースコードのレビューで確認された。

・ MFP(TOEの動作環境)

　TASKalfa 420i が使用された。

　TASKalfa 520iは、提供する機能はTASKalfa 420iと同一であるが、速度が異なる機種である。印刷の量が異なるテストを実施することによって、異なる速度の機種を使用した場合をカバーできることが評価者により判断された。そのため、STで示されたMFPの機種の全てがカバーされる。

・ プリンタドライバ、TWAINドライバ(TOEの動作環境)

　クライアントPCで、以下のものが使用された。

- Kyocera TASKalfa KX Ver 5.0.2130a
- Kyocera TWAIN Driver Ver 1.7.1106

　これらはガイダンスで指定されているものと一致するものである。ST

ではガイダンスで指定するものが必要としているため、STで示されたものと一致する。

・ SMTPサーバ、SMBサーバ、FTPサーバ (TOEの動作環境)
　サーバPCに、SMTP、SMB、FTPのプロトコルに対応するサーバソフトウェアが使用された。そのためSTで示されたものと一致する。

以上より、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。

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。

＜開発者テスト手法＞
TOEの外部インタフェースで確認できる機能(セキュリティ機能に関連する操作パネルの表示等)は、外部インタフェースの刺激と観察によってテストされたが、上書き消去と暗号化の機能はこの方法では十分な確信が得られないために以下の方法で補足された。

・ 暗号化が正しく行われていることの確認のための手法

TOEの機能によって暗号化されてHDDに書き込まれたデータを、デバッグ用の操作で復号されない状態で得る。
こうして得たデータを、TOEとは別のソフトウェアAESを用いて暗号化に使用したものと同じ鍵で復号して、暗号化される前のデータと一致することを確認する。

・ 上書き消去が正しく行われていることの確認のための手法

TOEに追加されるログ出力の機能では、上書き消去の前後のHDDの該当部分の内容を出力できるようにする。そのうえで、上書き消去が動作すべき操作を行い、出力されたログを観察する。

＜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7-1に示す。これらはTOEの機能のふるまいに影響がないことが評価者によって判断されている。
変換機、ケーブルに関しては、開発者により正しく動作することが確認されている。ソフトウェアAESについては、NISTから公開されている平

文/暗号文及び暗号鍵を使ったテストで信頼性が確認されている。

表7-1　開発テストツール

ツール名称	概要・利用目的
変換機、ケーブル	開発者用デバッグ機材。ログ出力の確認や、デバッグ用の操作を行う。
ソフトウェアAES	AESの暗号化・復号を行うソフトウェア。暗号化の機能の確認に使う。

＜開発者テストの実施＞

外部インタフェース及び出力されたログの観察結果に対しては、あらかじめ期待されたテスト計画書の値との比較が行われた。

デバッグ用の操作で得た暗号化データに対しては、ソフトウェアAESによって復号されて暗号化される前のデータとの照合が行われた。

b. 実施テストの範囲

テストは開発者によって103項目実施されている。

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。

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。

7.3.2 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は図7-1　開発者テストの構成図に示すとおりである。

評価者独立テストに使われたTOE及び環境は、開発者テストで使われたもの

と同じである。そのため、評価者独立テストは本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. 評価者独立テストの観点

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、以下の観点での評価者独立テストを考案した。

開発者テストのサンプリングは、以下のような方針で行われた。

- セキュリティ機能を実装するサブシステムのふるまいのテストをすべて選択する。
- セキュリティ機能を実装するサブシステムを呼び出してセキュリティ機能を提供する外部インタフェースについては、少なくとも外部インタフェースに抜けがなく、インタフェースの提供方法の違いもカバーするように選択する。

上書き消去の機能に対しては、特に他の動作との干渉が懸念されるため、開発者とは異なる条件やタイミングで上書き消去の機能が正しく動作することの確信を得るための独立テストを考案した。加えて、バッファオーバーフロー防止のメカニズムに対して、開発者によるテストとは異なる入力を与えるテストを考案した。

＜独立テストの観点＞

① 一時保存データに関するパラメタが開発者テストと異なるケースにおける、上書き消去も動作しないことを確認する。
② スリープ機能と干渉する場合における、上書き消去の正常動作を確認する。
③ MFPの機能の利用と干渉する場合における、上書き消去の正常動作を確認する。
④ 開発者によるテストとは異なる入力を与えて、バッファオーバーフロー防止のメカニズムの正常動作を確認する。

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。

＜独立テスト手法＞

独立テストは、開発テストと同じ手法で実施された。

＜独立テストツール＞

開発テストにおいて利用した表7-1のツールを用いた。

＜独立テストの実施＞

評価者により考案された独立テストの観点とその対応したテスト内容を表7-2に示す。

表7-2 実施した独立テスト

独立テストの観点	テスト概要
①	一時保存データが生成されないようにしてMFPの機能を利用して、上書き消去も動作しないことを確認する。
②	上書き消去の実行中に手動でスリープをONにして、上書き消去が正しく完了することを確認する。
③	上書き消去の実行中にコピーを実行して、上書き消去が正しく完了することを確認する。
④	イメージへの展開後に大きなサイズとなる画像データ、実際の画像サイズと整合しないサイズ情報をヘッダに持つ画像データの印刷を試みて、問題が起こらないことを確認する。

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。

7.3.3 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 想定されていないポートが開いていた場合、そこが侵入経路となる可能性がある。

② FTPサービスが適切に構成されていない場合､不正にデータにアクセスできる可能性がある。
③ HDDの残り容量が少ない状態において、資源の枯渇やタイムアウト等によりTOEのセキュリティ機能が誤動作する可能性がある。
④ 同じ画像データに対するジョブ(MFPの機能の利用)の入れ替えにより、ジョブの内容の整合が崩れ、TOEのセキュリティ機能が誤動作する可能性がある。
⑤ Webサーバ機能が適切に構成されていない場合､不正にデータにアクセスできる可能性がある。
⑥ セキュリティ機能のアクティベート情報を物理的に未アクティベート状態へ置き換えられ悪用できる可能性がある。
⑦ ファームウェアのアップデート機能により、TOEの改変ができる可能性がある。
⑧ ドメイン分離のメカニズムによって、HyPASアプリケーションから画像データの保存される領域にはアクセスはできないが、TOEがその通りにふるまうことの確信に至っていない。
⑨ セキュリティキットのアクティベート中に電源を切った場合に､正しくアクティベートができないことが、TOEの初期化の評価で疑われた。

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があるかを決定するため、以下の侵入テストを実施した。

＜侵入テスト環境＞

侵入テストは開発者テストと同じ環境で行われた｡ただし､ポートスキャンの実施のために Nmap 5.21 が追加で使われた。

＜脆弱性テストの実施＞

潜在的な脆弱性の探索において識別された懸念される脆弱性について、これと対応する評価者侵入テストを表7-3に示す｡評価者は、潜在的な脆弱性が悪用される可能性の有無を決定するため、以下の評価者侵入テストを実施した。

表7-3　侵入テスト概要

脆弱性	テスト概要
①	仕様にないポートが開いていないかどうかを､ポートスキャンツールを用いて確認する。
②	FTPサービスに接続してファイルの取得やディレクトリの移動を試み、HDD内の画像データに到達できないことを確認する。

脆弱性	テスト概要
③	多数のMFPの機能を実行して、HDDの残り容量が少ない状況とし、さらにMFPの機能を実行する。そのような場合でも上書き消去は正しく完了することを確認する。
	上記と同様にHDDの残り容量が少ない状態において、HDDの残り容量を超える画像データの保存を試みる。そのような場合でも、TOEの誤動作に結びつかないことを確認する。
④	実行待ちになっている同じ画像データに対するジョブ(MFPの機能の利用)を入れ替えることが、TOEの誤動作に結びつかないことを確認する。具体的には、ジョブを入れ替えた結果が「削除後に印刷」となるような場合が懸念の対象である。
⑤	TOEのWebサーバ機能に対して、ディレクトリトラバーサルが懸念される入力を与え、ディレクトリトラバーサルが起こらないことを確認する。
⑥	セキュリティ機能のアクティベート情報を物理的に未アクティベート状態に置き換えようとしても不正変更ができないことを確認する。
⑦	ベンダから正式に提供されているものとは異なる内容のファームウェアのデータを用意し、TOEの不正なアップデートを試みても拒否されることを確認する。
⑧	HyPASアプリケーションから画像データの保存される領域にアクセスを試みても、アクセスできないことを確認する。
⑨	セキュリティキットのアクティベート中に電源を切った場合でも、再度電源を入れた後に正常にアクティベートを続けら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。

7.4 評価構成について

TOEの動作環境としてのMFPは、STでは複数の機種が示されている。本評価では、その中の一つの機種が選択された。妥当性は評価者により判断されている。(「7.3.1 開発者テスト」参照。)

クライアントPCまたはサーバPCに導入されることが想定されるソフトウェアとして、プリンタドライバ、TWAINドライバ、SMTPサーバ、SMBサーバ、FTPサーバがある。これらは、STと一貫するものが用意された。

STでは明示されていないが、クライアントPCまたはサーバPCにはWebブラウザが導入されることも想定されている。Webブラウザからは TOEのセキュリティ機能に関係する操作がないという理由で、一つだけ(Internet Explorer ver6.0 sp1)が用意された。

7.5 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

評価では以下について確認された。

- PP適合：なし
- 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

評価の結果は、第2章で識別されたTOEについて、本章の評価された構成のみに適用される。

7.6 評価者コメント/勧告

評価は、「ファックス機能」または他のオプション機能が搭載されていない構成で実施された。「ファックス機能」または他のオプション機能を搭載する場合のセキュリティ機能の信頼性の判断は、本評価の対象外である。

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。

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

TOEが持つ機能のうち、何がセキュリティ機能として評価されたかについて注意を要する。詳細は「4.3 使用環境におけるTOE範囲」参照。

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、公表のため、本報告書とは別文書として、以下のとおり提供される。

京セラミタ Data Security Kit (E) Software Type II 日本版 セキュリティターゲット 第1.10版 2010年8月10日 京セラミタ株式会社

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。

AES	Advanced Encryption Standard
ASIC	Application Specific Integrated Circuit
HDD	Hard Disk Drive
MFP	Multi Function Printer
NIST	National Institute of Standards and Technology
USB	Universal Serial Bus

本報告書で使用された用語の定義を以下に示す。

一時保存	受け取った画像データをそのまま出力または転送せずに一時的にHDD上に保持したり、画像処理において一時的にHDD上に保持すること。利用者が意識することなくMFPの処理過程で自動的に行う。長期保存と対比。
上書き消去	HDD に保存された画像データの削除が指示された際に、画像データの実データ領域に対して無意味な文字列を上書きし、実データ領域を完全に消去した上で画像データの管理情報を削除することを指す。こうすることでデータ再利用を不可能な状態にすることができる。
画像データ	TOE利用者が、コピー機能、ネットワーク送信機能、プリンタ機能、及びボックス機能を利用した際に、MFP 内部で処理される画像情報のことを指す。

クライアントPC	ネットワークに接続されたTOEに対して、ネットワークに接続してTOEのサービス(機能)を利用する側のコンピュータのことを指す。
操作パネル	MFPの一番上部に設置され、液晶パネルで構成される。外部インタフェースであり、利用者は、操作パネルを通してTOEを利用することができる。
長期保存	画像データを、利用者が意識して保存操作を行い、HDD上に保持すること。一時保存と対比。
ネットワーク送信	スキャンされた画像データやボックスに保存された画像データを、クライアントPCに送信する機能。LAN経由で送信するPC送信と、E-mail経由で送信するE-mail送信、クライアントPCからの操作でセットされた原稿を取り込むTWAIN機能がある。

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19年5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

[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　平成19年5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 Part1: Introduction and general model Version 3.1 Revision 1 September 2006 CCMB-2006-09-001

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

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

[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1版 2006年9月 CCMB-2006-09-001　(平成19年3月翻訳第1.2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2版 2007年9月 CCMB-2007-09-002　(平成20年3月翻訳第2.0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2版 2007年9月 CCMB-2007-09-003　(平成20年3月翻訳第2.0版)

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

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

[12] 京セラミタ Data Security Kit (E) Software Type II 日本版 セキュリティターゲット 第1.10版 2010年8月10日 京セラミタ株式会社

[13] Data Security Kit (E) Software Type II (日本版) 評価報告書 第1.1版 2010年9月15日 株式会社電子商取引安全技術研究所 評価センター