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10月16日 (IT認証5567)
認証番号	C0549
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 6052ci, TASKalfa 5052ci, TASKalfa 4052ci, TASKalfa 3552ci, TASKalfa 6052ciG, TASKalfa 5052ciG, TASKalfa 4052ciG (KYOCERA), CS 6052ci, CS 5052ci, CS 4052ci, CS 3552ci (Copystar), 6006ci, 5006ci, 4006ci(TA Triumph-Adler/UTAX) Data Security Kit (E), FAX System 12 付きモデル
TOEのバージョン	システム: 2ND_20IS.C01.010HS パネル: 2ND_70IS.CI1.010 ファクス: 3R2_5100.002.005
PP適合	IEEE Std 2600.1-2009
適合する保証パッケージ	EAL3及び追加の保証コンポーネントALC_FLR.2
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29年5月25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 Common Criteria for Information Technology Security Evaluation
Version 3.1 Release 4

② Common Methodology for Information Technology Security Evaluation
Version 3.1 Release 4

評価結果：合格

「TASKalfa 6052ci, TASKalfa 5052ci, TASKalfa 4052ci, TASKalfa 3552ci, TASKalfa 6052ciG, TASKalfa 5052ciG, TASKalfa 4052ciG(KYOCERA), CS 6052ci, CS 5052ci, CS 4052ci, CS 3552ci(Copystar), 6006ci, 5006ci, 4006ci(TA Triumph-Adler/UTAX) Data Security Kit (E), FAX System 12 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 1
1.1　評価対象製品概要 1
1.1.1　保証パッケージ 1
1.1.2　TOEとセキュリティ機能性 1
1.1.2.1　脅威とセキュリティ対策方針 2
1.1.2.2　構成要件と前提条件 2
1.1.3　免責事項 2
1.2　評価の実施 3
1.3　評価の認証 3
2　TOE識別 4
3　セキュリティ方針 5
3.1　セキュリティ機能方針 6
3.1.1　脅威とセキュリティ機能方針 6
3.1.1.1　脅威 6
3.1.1.2　脅威に対するセキュリティ機能方針 7
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 8
3.1.2.1　組織のセキュリティ方針 8
3.1.2.2　組織のセキュリティ方針に対するセキュリティ機能方針 8
4　前提条件と評価範囲の明確化 10
4.1　使用及び環境に関する前提条件 10
4.2　運用環境と構成 10
4.3　運用環境におけるTOE範囲 12
5　アーキテクチャに関する情報 13
5.1　TOE境界とコンポーネント構成 13
5.2　IT環境 15
6　製品添付ドキュメント 16
7　評価機関による評価実施及び結果 18
7.1　評価機関 18
7.2　評価方法 18
7.3　評価実施概要 18
7.4　製品テスト 19
7.4.1　開発者テスト 19
7.4.2　評価者独立テスト 23
7.4.3　評価者侵入テスト 25
7.5　評価構成について 28
7.6　評価結果 29

7.7　評価者コメント/勧告 29
8　認証実施 30
8.1　認証結果 30
8.2　注意事項 30
9　附属書 31
10　セキュリティターゲット 31
11　用語 32
12　参照 33

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 6052ci, TASKalfa 5052ci, TASKalfa 4052ci, TASKalfa 3552ci, TASKalfa 6052ciG, TASKalfa 5052ciG, TASKalfa 4052ciG(KYOCERA), CS 6052ci, CS 5052ci, CS 4052ci, CS 3552ci(Copystar), 6006ci, 5006ci, 4006ci(TA Triumph-Adler/UTAX) Data Security Kit (E), FAX System 12 付きモデル、バージョン システム: 2ND_20IS.C01.010HS パネル: 2ND_70IS.CI1.010 ファクス: 3R2_5100.002.005」（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 29 年 5 月 8 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、10 章の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 及び追加の保証コンポーネント ALC_FLR.2 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

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。

TOE の保護資産である利用者の文書データ及びセキュリティに影響する設定データは、TOE の操作や、TOE が設置されているネットワーク上の通信データへのアクセスによって、不正に暴露されたり改ざんされたりする脅威がある。

それらの脅威に対抗するために、TOE は、識別認証、アクセス制御、暗号化などのセキュリティ機能を提供する。

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する。

本 TOE は、TOE の物理的部分やインタフェースが不正なアクセスから保護されるような環境に設置されることを想定している。また、TOE の運用にあたっては、ガイダンス文書に従って適切に設定し、維持管理しなければならない。

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 29 年 5 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 6052ci, TASKalfa 5052ci, TASKalfa 4052ci, TASKalfa 3552ci, TASKalfa 6052ciG, TASKalfa 5052ciG, TASKalfa 4052ciG(KYOCERA), CS 6052ci, CS 5052ci, CS 4052ci, CS 3552ci(Copystar), 6006ci, 5006ci, 4006ci(TA Triumph-Adler/UTAX) Data Security Kit (E), FAX System 12 付きモデル
バージョン：	システム: 2ND_20IS.C01.010HS パネル: 2ND_70IS.CI1.010 ファクス: 3R2_5100.002.005
開発者：	京セラドキュメントソリューションズ株式会社

TOE 名称は、MFP の機種名と必須オプションの名称で構成されている。

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。

MFP の機種名は、MFP 本体の表面に印字されている機種名が、以下のいずれかであることを確認する。

KYOCERA TASKalfa 6052ci, KYOCERA TASKalfa 5052ci,
KYOCERA TASKalfa 4052ci, KYOCERA TASKalfa 3552ci,
KYOCERA TASKalfa 6052ciG, KYOCERA TASKalfa 5052ciG,
KYOCERA TASKalfa 4052ciG,
Copystar CS 6052ci, Copystar CS 5052ci, Copystar CS 4052ci,
Copystar CS 3552ci,
TA Triumph-Adler 6006ci, TA Triumph-Adler 5006ci,
TA Triumph-Adler 4006ci,
UTAX 6006ci, UTAX 5006ci, UTAX 4006ci

必須オプションの名称と TOE のバージョンは、製品のガイダンスの記載に従って MFP を操作し、MFP の操作パネルに表示された以下の情報を確認する。

- オプション名称：「Data Security Kit (E)」及び「FAX System 12」
- システム、パネル、ファクスの各バージョン

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。

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 内部の HDD に蓄積したり、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、それらの機能を使用する際に、MFP 用の Protection Profile である IEEE Std 2600.1-2009 [14]（以下「PP」という。）で要求されているセキュリティ機能要件を満たすセキュリティ機能を提供する。TOE の提供するセキュリティ機能には、利用者の識別認証とアクセス制御、HDD に蓄積した文書データ及び設定データの暗号化と文書データ削除時の上書き消去、暗号化通信などが含まれており、保護資産である利用者の文書データ及びセキュリティに影響する設定データが、不正に暴露されたり改ざんされたりすることを防止する。

なお、TOE は以下の利用者役割を想定している。

・一般利用者

TOE が提供するコピー機能、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 の基本機能の利用者である。

・機器管理者

TOE のセキュリティ機能の設定を行うための特別な権限を持つ TOE の利用者である。

・TOE Owner

TOE 資産の保護や、TOE の運用環境のセキュリティ対策方針の実現に責任を持つ人物または組織である。

また、TOE の保護資産は以下のものである。

・User Document Data

利用者の文書データ。

・User Function Data

TOE によって処理される利用者の文書データやジョブに関連する情報。本 TOE では、MFP の基本機能を実行した際に生成されるジョブデータが該当する。

・TSF Confidential Data

セキュリティ機能で使用されるデータの中で、完全性と秘匿性が求められるデータ。本 TOE では、ログインユーザーパスワード、暗号鍵、監査ログが該当する。

・TSF Protected Data

セキュリティ機能で使用されるデータの中で、完全性だけが求められるデータ。本 TOE では、利用者のログインユーザー名とジョブの実行権限、文書データを保存するボックスの共有設定、ネットワーク設定など、TSF Confidential Data を除く、セキュリティ機能の各種設定値が該当する。

3.1 セキュリティ機能方針

TOE は、3.1.1 に示す脅威に対抗し、3.1.2 に示す組織のセキュリティ方針を満たす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。これらの脅威は、PP に記述されているものと同じである。

表3-1 想定する脅威

識別子	脅威
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons
T.DOC.ALT	User Document Data may be altered by unauthorized persons
T.FUNC.ALT	User Function Data may be altered by unauthorized persons
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons

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.DOC.DIS」「T.DOC.ALT」「T.FUNC.ALT」への対抗

これらは利用者データ（User Document Data と User Function Data）に対する脅威であり、TOE は、「ユーザー管理機能」、「ジョブ認可機能」、「データアクセス制御機能」、「上書き消去機能」及び「ネットワーク保護機能」で対抗する。

TOE の「ユーザー管理機能」は、識別認証が成功した利用者だけに TOE の利用を許可する。

TOE の「ジョブ認可機能」は、識別認証された利用者が、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 の基本機能を使用する際に、利用者に付与された実行権限をチェックし、権限のある利用者だけに基本機能の実行を許可する。

TOE の「データアクセス制御機能」は、MFP の基本機能で利用者データの操作をする際にアクセス制御を行い、利用者データに対してアクセス権限のある利用者だけにアクセスを許可する。

TOE の「上書き消去機能」は、文書データが削除される際に、文書データが格納されていた HDD 等の領域を上書き消去することで、残存情報の参照を防止する。

TOE の「ネットワーク保護機能」は、TOE とクライアント PC や各種サーバとの通信時に、暗号通信プロトコルを適用し、通信データを暗号化する。

以上の機能により、TOE は、TOE の権限外使用や通信データへの不正アクセスによって、保護対象の利用者データが漏えいしたり改ざんされたりすることを防止する。

(2) 脅威「T.PROT.ALT」「T.CONF.DIS」「T.CONF.ALT」への対抗

これらはセキュリティ機能で使用されるデータに対する脅威であり、TOE は、「ユーザー管理機能」、「セキュリティ管理機能」及び「ネットワーク保護機能」で対抗する。

TOE の「ユーザー管理機能」と「セキュリティ管理機能」は、セキュリティ機能で使用されるデータの参照と変更を、識別認証された機器管理者だけに許可する。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等の変更は可能である。

TOE の「ネットワーク保護機能」は、TOE とクライアント PC や各種サーバとの通信時に、暗号通信プロトコルを適用し、通信データを暗号化する。

以上の機能により、TOE は、TOE の権限外使用や通信データへの不正アクセスによって、保護対象のデータが漏えいしたり改ざんされたりすることを防止する。

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

3.1.2.1 組織のセキュリティ方針

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を表 3-2 に示す。これらの組織のセキュリティ方針は、P.HDD.ENCRYPTION が追加されていることを除いて、PP に記述されているものと同じである。

表3-2 組織のセキュリティ方針

識別子	組織のセキュリティ方針
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.
P.HDD.ENCRYPTION	To improve the confidentiality of the documents, User Data and TSF Data stored in HDD will be encrypted by the TOE.

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

TOE は、表 3-2 に示す組織のセキュリティ方針を満たす、以下のセキュリティ機能を具備する。なお、各セキュリティ機能の詳細は、5 章に示す。

(1) 組織のセキュリティ方針「P.USER.AUTHORIZATION」への対応

TOE は、「ユーザー管理機能」及び「ジョブ認可機能」で本方針を実現する。

TOE の「ユーザー管理機能」は、識別認証の成功した利用者だけに TOE の利用を許可する。

TOE の「ジョブ認可機能」は、識別認証された利用者が、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 の基本機能を使用する際に、利用者に付与された実行権限をチェックし、権限のある利用者だけに基本機能の実行を許可する。

(2) 組織のセキュリティ方針「P.SOFTWARE.VERIFICATION」への対応

TOE は、「自己テスト機能」で本方針を実現する。

TOE の「自己テスト機能」は、暗号鍵を使用した HDD 暗号化機能が正常に動作することを、起動時に検証する。また、機器管理者の指示により、TSF 実行コードの完全性を検証する。

(3) 組織のセキュリティ方針「P.AUDIT.LOGGING」への対応

TOE は、「監査ログ機能」で本方針を実現する。

TOE の「監査ログ機能」は、セキュリティに関連する事象を監査ログとして記録する。格納された監査ログは、識別認証された機器管理者だけが、読み出しと削除をすることができる。ただし、監査ログの改変はできない。

(4) 組織のセキュリティ方針「P.INTERFACE.MANAGEMENT」への対応

TOE は、「ユーザー管理機能」と「ネットワーク保護機能」で、本方針を実現する。

TOE の「ユーザー管理機能」は、識別認証の成功した利用者だけに TOE の利用を許可する。また、利用者が操作をしない状態が規定時間経過した場合には、セッションを切断する。

また、TOE の「ネットワーク保護機能」は、TOE の外部インタフェースから受信したデータを TOE が必ず介在して処理することで、電話回線を含む外部インタフェースから内部ネットワークへの不正な転送を防止する。

(5) 組織のセキュリティ方針「P.HDD. ENCRYPTION」への対応

TOE は、「HDD 暗号化機能」で本方針を実現する。

TOE の「HDD 暗号化機能」は、HDD に書き込むデータを暗号化する。暗号アルゴリズムは 256bit の AES である。

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。これらの前提条件は、PP に記述されているものと同じである。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.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

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。

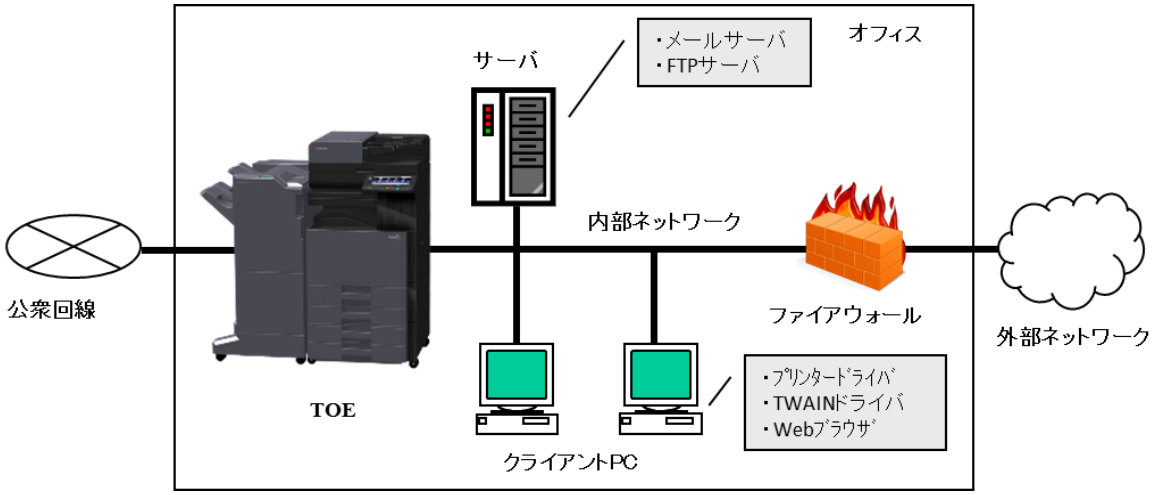

図 4-1　TOE の運用環境

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ドライバー
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ドライバー

(2) サーバ（メールサーバ）

機器管理者が TOE の監査ログを読み出すために使用する。また、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も必要である。以下のサーバが必要である。

・メールサーバ：IPsec(IKEv1)上のSMTPプロトコルに対応したもの

(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：IPsec(IKEv1)上のFTPプロトコルに対応したもの

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

本 TOE の評価されたセキュリティ機能には、以下の制約条件がある。

(1) USB メモリ

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。本評価では、USB メモリは共有設定されたフォルダと同じ扱いがされている。そのため、USB メモリに格納された文書データに対して、操作パネル以外のインタフェースの利用によって、他の利用者がアクセスできないという保証はない。USB メモリに共有できない文書データを格納している場合や、USB メモリの置き忘れの対策は、利用者の責任である。

(2) IPsec プロトコル

本評価では、IPsec プロトコルについて、IPv4 だけが評価されている。IPv6 用の IPsec は評価されておらず保証の対象外である。

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（サブシステム）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。

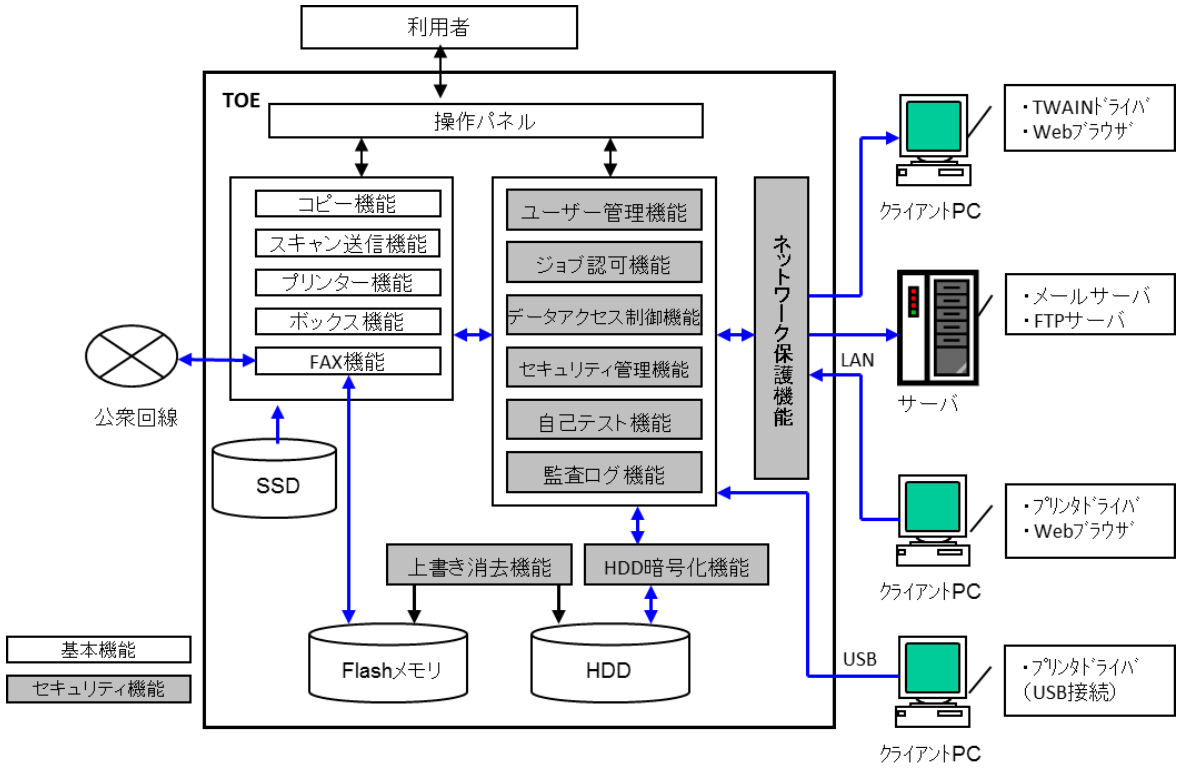

図 5-1　TOE の構成

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。なお、SSD はファームウェア格納用であり、SSD に文書データ等は保存されない。

(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) ジョブ認可機能

本機能は、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 の基本機能の利用を、許可された利用者のみに制限する機能である。

利用者が MFP の基本機能を使用する際には、利用者に設定された実行権限をチェックし、権限のある基本機能だけが実行を許可される。

(3) 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とジョブデータに対するアクセスを、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、文書データとジョブデータの所有者情報と、文書データが保存されているボックスの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データ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、すべてのデータの削除と、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。

(4) 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、参照、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参照と変更が可能である。

(5) 自己テスト機能

本機能は、以下の自己テストを行う機能である。

- TOE の起動時に、HDD 暗号化機能が正常に動作することを検証する。それにより暗号鍵の完全性も同時に検証される。
- 機器管理者の指示で、セキュリティ機能の実行モジュールのハッシュ値を検証する。

(6) 監査ログ機能

本機能は、セキュリティ機能に関する監査事象を監査ログとして記録する機能である。TOEに格納された監査ログは、識別認証された機器管理者だけが、E-mail送信による読出しと削除をすることができる。監査ログの改変はできない。

監査ログを格納する領域が満杯の場合には、最も古い監査ログが上書きされ、新しい監査ログが記録される。

(7) HDD 暗号化機能

本機能は、HDD に保存するデータを暗号化する機能である。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。

(8) 上書き消去機能

本機能は、文書データを削除する際に、文書データが格納されていた HDD と Flash メモリの領域を上書き消去する機能である。本機能は、以下のタイミングで実行される。

- MFP の基本機能が終了し文書データが不要になった時。TOE の処理の都合で TOE 内に一時的に作成されたデータも対象に含まれる。
- 利用者の指示で文書データを削除した時。
- 電源 ON にした時。電源 OFF 時に上書き消去処理が未完了の場合には、電源 ON 時に処理が再開される。

上書きするデータのパターンは、機器管理者の設定で 1 回または 3 回（DoD 方式）を選択することができる。なお、上書きデータは暗号化せずにそのまま HDD や Flash メモリに書き込まれる。

(9) ネットワーク保護機能

本機能は、IT 機器との通信において、以下の暗号化通信を行う機能である。

・クライアント PC：TLSv1.2
・メールサーバ：IPsec（IKEv1）
・FTP サーバ：IPsec（IKEv1）

また、公衆回線を含む外部インタフェースからの情報を、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も提供する。

5.2 IT環境

TOE の監査ログの読出しは、メールサーバを利用して E-mail 送信される。

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。本 TOE のドキュメントには日本向け（表 6-1）と海外向け（表 6-2）があり、販売地域によりいずれかが添付される。

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　日本向けガイダンス

名称	バージョン
TASKalfa 2552ci / TASKalfa 3252ci / TASKalfa 4052ci / TASKalfa 5052ci / TASKalfa 6052ci クイックガイド	初版 2016.1 302ND5603001
TASKalfa 2552ci / TASKalfa 3252ci / TASKalfa 3552ci / TASKalfa 4052ci / TASKalfa 5052ci / TASKalfa 6052ci セーフティーガイド / Safety Guide	2016.6 302ND5622101
TASKalfa 2552ci / TASKalfa 3252ci / TASKalfa 4052ci / TASKalfa 5052ci / TASKalfa 6052ci 使用説明書	Rev.3 2017.1 2NDKDJA003
FAX System 12 使用説明書	Rev.3 2016.7 3RKKDJA003
TASKalfa 6052ci / TASKalfa 5052ci / TASKalfa 4052ci / TASKalfa 3252ci / TASKalfa 2552ci / TASKalfa 6002i / TASKalfa 5002i / TASKalfa 4002i Data Security Kit (E) 使用説明書	2017.2 3MS2NDKDJA2
Command Center RX 操作手順書	Rev.7 2016.2 CCRXKDJA07
TASKalfa 2552ci / TASKalfa 3252ci / TASKalfa 4052ci / TASKalfa 5052ci / TASKalfa 6052ci プリンタードライバー操作手順書	2NDCLKDJA631.2 016.10
KYOCERA Net Direct Print 操作手順書	DirectPrintKDJA1. 2016.02
お知らせ / Notice	2017.2 303MS5638001
Data Security Kit (E) 設置手順書 / Installation Guide	2013.1 303MS56710-02
FAX System 12 設置手順書 / Installation Guide	2016.6 303RK56710-03

表6-2　海外向けガイダンス

名称	バージョン
TASKalfa 2552ci / TASKalfa 3252ci / TASKalfa 3552ci / TASKalfa 4052ci / TASKalfa 5052ci / TASKalfa 6052ci FIRST STEPS QUICK GUIDE	2016.6 302ND5602101
TASKalfa 2552ci / TASKalfa 3252ci / TASKalfa 3552ci / TASKalfa 4052ci / TASKalfa 5052ci / TASKalfa 6052ci セーフティーガイド / Safety Guide	2016.6 302ND5622101
TASKalfa 2552ci / TASKalfa 3252ci / TASKalfa 3552ci / TASKalfa 4052ci / TASKalfa 5052ci / TASKalfa 6052ci OPERATION GUIDE	Rev.3 2017.3 2NDKDEN003
FAX System 12 FAX OPERATION GUIDE	Rev.3 2016.07 3RKKDEN103
TASKalfa 6052ci / TASKalfa 5052ci / TASKalfa 4052ci / TASKalfa 3552ci / TASKalfa 3252ci / TASKalfa 2552ci / TASKalfa 6002i / TASKalfa 5002i / TASKalfa 4002i Data Security Kit (E) Operation Guide	2017.2 3MS2NDKDEN2
Command Center RX User Guide	Rev.7 2016.2 CCRXKDEN07
TASKalfa 2552ci / TASKalfa 3252ci / TASKalfa 3552ci / TASKalfa 4052ci / TASKalfa 5052ci / TASKalfa 6052ci Printer Driver User Guide	2NDCLKTEN630.2 016.10
KYOCERA Net Direct Print User Guide	DirectPrintKDEN1 .2016.02
お知らせ / Notice	2017.2 303MS5638001
Data Security Kit (E) 設置手順書 / Installation Guide	2013.1 303MS56710-02
FAX System 12 設置手順書 / Installation Guide	2016.6 303RK56710-03

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 10 月に始まり、平成 29 年 5 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 28 年 4 月、5 月、7 月、10 月、11 月、12 月及び平成 29 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。一部の開発・製造サイトについては、現地での調査は省略され、過去の認証案件での評価内容の再利用が可能であると、評価機関によって判断されている。また、平成 29 年 3 月及び 5 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。

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。

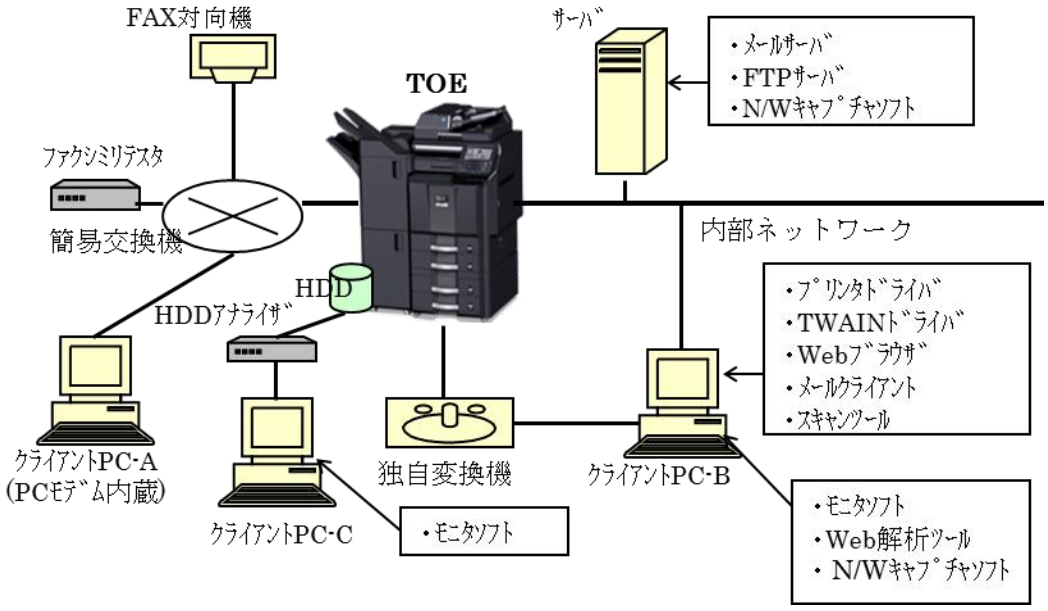

図7-1　開発者テストの構成図

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

名称	詳細
TOE	KYOCERA TASKalfa 6052ci, KYOCERA TASKalfa 5052ci, KYOCERA TASKalfa 4052ci, KYOCERA TASKalfa 3552ci ・Data Security Kit (E), FAX System 12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 2012 R2 Standard搭載PC ・メールサーバ：PMail Server 1.91 ・FTPサーバ：Microsoft Internet Information Services 8.5.9600.16384 ※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ドライバー v6.3.1625 ・TWAINドライバ：Kyocera TWAIN ドライバー v2.0.6525 ・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 ・モニタソフト：Tera Term Professional v4.78 ・Web解析ツール：Fiddler v4.5.1.5 ・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	HDDアナライザと接続し、TOE内のHDDの入出力データのモニタに使用 ・Windows 7 Professional SP1搭載PC ・モニタソフト：Tera Term Professional v4.78
HDDアナライザ	TOE内のHDD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 ・FS-3640MFP (京セラドキュメントソリューションズ社のMFP)
ファクシミリテスタ	ITU-T勧告に対応したスーパG3ファクシミリ対向試験器 ・スーパG3ファクシミリテスタ AFT-336N
簡易交換機	公衆回線を疑似的に実現する機器 ・X4008 Switch Simulator (AD SYSTEMS)

名称	詳細
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

開発者がテストしたTOEは、製品名称がKYOCERA TASKalfaで始まり末尾が「ci」のMFP全機種であり、2章のTOE識別と同一の識別を持つ。

表7-2に、開発者のテストしたMFP機種とTOEの他機種の関係を示す。表7-2で同じ行に記述されている製品は、名称が異なるだけで、同じ製品である。開発者テストの構成は、識別されたTOEをすべて含んでいるとみなすことができる。

表7-2　TOEのバリエーション

	テスト実施MFP	シリーズA	シリーズB	シリーズC	シリーズD
1	KYOCERA TASKalfa 6052ci	KYOCERA TASKalfa 6052ciG	Copystar CS 6052ci	TA Triumph-Adler 6006ci	UTAX 6006ci
2	KYOCERA TASKalfa 5052ci	KYOCERA TASKalfa 5052ciG	Copystar CS 5052ci	TA Triumph-Adler 5006ci	UTAX 5006ci
3	KYOCERA TASKalfa 4052ci	KYOCERA TASKalfa 4052ciG	Copystar CS 4052ci	TA Triumph-Adler 4006ci	UTAX 4006ci
4	KYOCERA TASKalfa 3552ci	－	Copystar CS 3552ci	－	－

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＞

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HDDアナライザを使用して、TOE内部の

動作を確認する。また、テスト用に TOE 内部にログを取得するように変更したファームウェアを使用し、そのログ情報やメモリ内容を、開発者用インタフェースを使用して確認する。

暗号アルゴリズム等については、上記の方法で取得したデータを別の方法で算出した既知解と比較することで、仕様どおりの暗号アルゴリズムが実装されていることを確認する。

＜開発者テストツール＞

開発者テストで利用したツールを表 7-3 に示す。

表 7-3　開発テストツール

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
Web解析ツール (Fiddler v4.5.1.5)	Webブラウザと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
HDDアナライザ＋モニタソフト(クライアントPC-C)	TOE内部のHDDのSATAインタフェースを流れるデータをキャプチャする。HDDの暗号化や上書き消去のデータの確認に使用
暗号機能テスト用ファームウェア	HDD暗号化機能の暗号鍵等の情報をログに出力するように変更した、テスト用ファームウェア。 暗号鍵生成や暗号アルゴリズムの実装部分はTOEと同一である
自己テスト機能テスト用ファームウェア	自己テストの検証対象を開発者が指定できるように変更した、テスト用ファームウェア。 自己テストの実装部分はTOEと同一である
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＋モニタソフト(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、テスト用ファームウェアのログの参照や、メモリダンプ等を行う

ツール名称	概要・利用目的
IPsecテスト用サーバ（表7-1の「サーバ」の代わりに使用）	TOEの設定で使用が禁止されているIPsec（IKEv1のaggressiveモードとIKEv2）が、実際に接続できないことの確認に使用。 ・Linux (Fedora Release 19)搭載PC ・IPsec: strongswan-5.1.3-1. fc19.i686 ・メールサーバ(SMTP):postfix-2.10. 3-1.fc19.i686 ・メールサーバ(POP) : dovecot-2.2. 15-1.fc19.i686 ・FTPサーバ : vsftpd-3.0.2-5.fc19.i686

＜開発者テストの実施内容＞

各種インタフェースより、MFP の基本機能とセキュリティ管理機能を操作し、様々な入力パラメタに対して、適用される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。

入力パラメタのバリエーションには、Web ブラウザと TOE の間の通信データの書き換えや、バッファオーバフローをはじめとする不正な処理を引き起こす可能性のあるデータも含まれている。

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117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環境は、以下を除き、図 7-1 に示した開発者テストの構成と同じである。

・TOE として、TASKalfa 6052ci 及び TASKalfa 3552ci だけを使用。

評価者は、TOE の機種の違いは印刷速度だけであり、セキュリティ機能は同一であるため、2 機種のテストで充分であると判断している。

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、開発者テストに用いら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、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 開発者とは異なる入力データや操作の組み合わせのバリエーションを確認する。

② 開発者がテストしていないふるまいを確認する。

③ 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を確認する。
・評価者考案テストと合わせて、すべてのインタフェース種別を確認する。
・評価者考案テストと合わせて、すべての利用者役割を確認する。
・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。
・通信データの書き換えなど脆弱性対策に寄与するものを確認する。

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＞

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である。

＜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、30 項目のサンプリングテストと、12 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7-4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	・パスワードの文字列、アカウントロックまでの閾値の変更、利用者の権限変更など、開発者と異なるパラメタを用いて、仕様どおりに動作することを確認する。 ・文書が格納された状態でのボックスの所有者変更とアクセス制御の確認など、開発者が確認していない組み合わせの操作を行い、仕様どおりに動作することを確認する。
観点②	・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た場合、通算されることを確認する。 ・自己テスト機能で、ハッシュ値自体の改ざんなど、開発者がテストしていない異常ケースを確認する。

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 各種インタフェースに、公知の脆弱性が存在する懸念がある。

② 印刷処理に、公知の脆弱性が存在する懸念がある。

③ 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。

④ 通信データを書き換えて、Web ブラウザでは入力できない文字列を TOE に入力することにより、セキュリティ機能が正常に動作しない懸念がある。

⑤ SSL/TLS プロトコルで弱い暗号方式が使われる懸念がある。

⑥ 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主なツールを表 7-5 に示す。

表7-5　侵入テストツール

ツール名称	概要・利用目的
Nmap v6.49 BETA4	利用可能なネットワークポートを検出するツール
netcat v1.11	ネットワークポートへのデータ送信に使用
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 v4.6.2	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-1.1.0c vm-486)	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

＜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した。 ・操作パネル、プリンタドライバ、Webブラウザから、不正なスクリプトやSQL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した。 ・Webブラウザの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した。
脆弱性②	・PDF、PostScript、印刷ジョブコマンド等による不正な印刷処理が実行される可能性のあるファイルをTOEに入力しても、不正な処理は実行されないことを確認した。
脆弱性③	・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した。 - アカウントロックまでの認証失敗回数の保持 - アカウントロックされた状態の維持 - 上書き消去処理（電源ON後に再開される）
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、TOEが誤動作しないことを確認した。
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した。
脆弱性⑥	・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した。

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

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。

・PP 適合：
2600.1, Protection Profile for Hardcopy Devices, Operational Environment A
（IEEE Std 2600.1-2009）

また、上記 PP で定義された以下の SFR パッケージに適合する。
- 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A
- 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A
- 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A
- 2600.1-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment A
- 2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment A
- 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A

・セキュリティ機能要件：　コモンクライテリア　パート２　拡張
・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
・追加の保証コンポーネント　ALC_FLR.2

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 EAL3 及び追加の保証コンポーネント ALC_FLR.2 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提供される。

TASKalfa 6052ci, TASKalfa 5052ci, TASKalfa 4052ci, TASKalfa 3552ci Series, Data Security Kit (E), FAX System 12 付きモデル セキュリティターゲット, 第 0.95 版, 2017 年 3 月 28 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送受信データはTOE内のFlashメモリに格納される
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、クライアントPC(TWAINドライバ)、TOEに接続されたUSBメモリに送信する機能。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TOEに蓄積され、操作パネルからの指示で出力される
ボックス	TOE内で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	TOE内に文書データを保存し、それを読み出して印刷や送信をする機能。送信手段は、FTPサーバ、メールサーバ、クライアントPC(TWAINドライバ)、TOEに接続されたUSBメモリ、及びFAX送信が可能である。ボックス機能は、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 6052ci, TASKalfa 5052ci, TASKalfa 4052ci, TASKalfa 3552ci Series, Data Security Kit (E), FAX System 12 付きモデル セキュリティターゲット, 第0.95版, 2017年3月28日, 京セラドキュメントソリューションズ株式会社

[13] TASKalfa 6052ci, TASKalfa 5052ci, TASKalfa 4052ci, TASKalfa 3552ci Series, Data Security Kit (E), FAX System 12 付きモデル評価報告書, 第1.2版, 2017年5月8日, 一般社団法人ITセキュリティセンター 評価部

[14] IEEE Std 2600.1-2009, IEEE Standard for a Protection Profile in Operational Environment A, Version 1.0, June 2009