認 証 報 告 書

東京都文京区本駒込2丁目28番8号
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

IT製品（TOE）

申請受付日（受付番号）	令和元年7月16日（IT認証9718）
認証識別	JISEC-C0670
製品名称	KONICA MINOLTA bizhub C4050i/bizhub C3350i with FK-517, DEVELOP ineo+ 4050i/ineo+ 3350i with FK-517
バージョン及びリリース番号	G00-45
製品製造者	コニカミノルタ株式会社
機能要件適合	プロテクションプロファイル適合、CCパート2拡張
プロテクションプロファイル	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (認証識別: JISEC-C0553)
ITセキュリティ評価機関の名称	みずほ情報総研株式会社 情報通信研究部 マルチメディア技術チーム情報セキュリティ評価課

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。
令和2年3月17日

セキュリティセンター セキュリティ技術評価部
技術管理者　矢野 達朗

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 5
② Common Methodology for Information Technology Security Evaluation Version 3.1 Release 5

評価結果：合格

「KONICA MINOLTA bizhub C4050i/bizhub C3350i with FK-517, DEVELOP ineo+ 4050i/ineo+ 3350i with FK-517 バージョン G00-45」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、コニカミノルタ株式会社が開発した「KONICA MINOLTA bizhub C4050i/bizhub C3350i with FK-517, DEVELOP ineo+ 4050i/ineo+ 3350i with FK-517 バージョン G00-45」（以下「本 TOE」という。）についてみずほ情報総研株式会社 情報通信研究部 マルチメディア技術チーム情報セキュリティ評価課（以下「評価機関」という。）が令和 2 年 3 月に完了した 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コニカミノルタ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、第 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。詳細は第 2 章以降を参照のこと。

1.1.1 プロテクションプロファイルまたは保証パッケージ

本 TOE は、次のプロテクションプロファイル[14][15]（以下「適合 PP」という。）に適合する。

Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015
(認証識別: JISEC-C0553)

1.1.2 TOEとセキュリティ機能性

本 TOE は IT 製品であり、コピー、スキャン、プリント、ファクス、文書の保存と取り出し機能等を備えたデジタル複合機（以下「MFP」という。）である。

本 TOE は、MFP が扱うデータの暴露や改ざんを防止するために、MFP 用のプロテクションプロファイルである適合 PP が要求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適合 PP の要求する保証要件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

本 TOE は、以下の脅威を想定している。

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機能に影響するデータは、TOE の操作や、TOE が接続されているネットワークへのアクセスにより、不正に暴露や改ざんされる脅威がある。

また、TOE 自身の故障や、不正なソフトウェアのインストールにより、TOE が持つセキュリティ機能が損なわれる脅威がある。

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。

TOE は､不正な物理的アクセスが制限され､インターネットから保護された LAN に接続される環境で運用されることを想定している。

運用中の TOE の維持管理は、調達者から信頼されている管理者がガイダンス文書に従って適切に行わなければならない。また、TOE の利用者は、安全に TOE を使用するよう訓練を受けていなければならない。

1.1.3 免責事項

本評価では、以下に示す運用は保証の対象外である。

- 「4.3 運用環境における TOE 範囲」で示す TOE の運用環境がセキュアではない状態での運用
- 「7.5 評価構成について」で示す条件以外での TOE の運用

本評価では、以下の保証はされない。

- 本 TOE に保存される利用者の文書データ等の暗号化

1.2 評価の実施

認証機関が運営する IT セキュリティ評価及び認証制度に基づき、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、令和 2 年 3 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。認証の過程において発見された問題については、認証レビューを作成した。認証機関が指

摘した問題点は、すべて解決され、かつ、TOE の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 TOE識別

本 TOE は、以下のとおり識別される。

TOE名称： KONICA MINOLTA bizhub C4050i/bizhub C3350i with FK-517, DEVELOP ineo+ 4050i/ineo+ 3350i with FK-517

バージョン： G00-45

TOE の構成品とその識別情報を表 2-1 に示す。

表 2-1 TOEの構成品

構成品	識別情報
MFP本体	・名称： KONICA MINOLTA bizhub C4050i、 KONICA MINOLTA bizhub C3350i、 DEVELOP ineo+ 4050i、 DEVELOP ineo+ 3350i ・バージョン G00-45
FAXキット(FK-517)	・AA1K

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 本体と FAX キットに表示された以下の情報を確認する。

・MFP 本体

- 名称

  筐体に貼られたラベルの型番が、表 2-1 の「MFP 本体」の識別情報の名称のうちのいずれかであること

- バージョン

  操作パネルに表示されるバージョンが、表 2-1 の「MFP 本体」の識別情報のバージョンと一致すること

・FAX キット

FAX キットの刻印が、表 2-1 の「FAX キット（FK-517)」の識別情報と一致すること

3 セキュリティ方針

本 TOE は、コピー、スキャン、プリント、ファクス、文書の保存と取り出し機能等といった 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ーとやりとりしたりする機能を持つ。

TOE は、適合 PP の要求を満足する以下のセキュリティ機能を提供する。

(1) 識別認証機能

(2) アクセス制御機能

(3) 暗号化機能

(4) 高信頼通信機能

(5) セキュリティ管理機能

(6) 監査機能

(7) 高信頼な運用機能

(8) FAX 分離機能

本 TOE のセキュリティ機能の詳細は、5.1 節に示す。

TOE が想定する利用者役割、保護資産、脅威、組織のセキュリティ方針の詳細を 3.1 節から 3.4 節に示す。

3.1 利用者の役割

TOE の使用において、表 3-1 に示す利用者を想定する。

表 3-1 利用者の役割

名称		定義
U.USER （許可利用者）		Any identified and authenticated User.
	U.NORMAL (Normal User)	識別され、認証された利用者で、管理者役割を持たない利用者 A User who has been identified and authenticated and does not have an administrative role
	U.ADMIN (Administrator)	識別され、認証された利用者で管理者役 割を持つ利用者 A User who has been identified and authenticated and has an administrative role

3.2 保護資産

TOE の保護資産は、以下の表 3-2 の 2 種類に分類できる。 2 種類の保護資産のうち、利用者データは表 3-3、TSF データは表 3-4 のように、それぞれさらに 2 種類の保護資産で構成される。

表 3-2 TOEの保護資産

名称	種別	定義
D.USER	User Data	TSFの操作に影響を及ぼさない、利用者のために利用者によって作成されたデータ Data created by and for Users that do not affect the operation of the TSF
D.TSF	TSF Data	TSFの操作に影響を与えるかもしれないTOEのためのTOEによって作成されたデータ Data created by and for the TOE that might affect the operation of the TSF

表 3-3 保護資産(利用者データ)

名称	種別	定義
D.USER.DOC	User Document Data	電子的またはハードコピーの形式で、利用者の文書に含まれる情報 Information contained in a User's Document, in electronic or hardcopy form
D.USER.JOB	User Job Data	利用者の文書または文書処理ジョブに関連する情報 Information related to a User's Document or Document Processing Job

表 3-4 保護資産(TSFデータ)

名称	種別	定義
D.TSF.PROT	Protected TSF Data	データの所有者でもなく、または管理者役割も持たない利用者によって、改ざんされた TSF データが TOE のセキュリティ影響を及ぼすかもしれないが、暴露については容認できるような TSF データ。 TSF Data for which alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable
D.TSF.CONF	Confidential TSF Data	データの所有者でもなく、管理者役割も持たない利用者によって、暴露または改ざんされた TSF データが、TOE のセキュリティに影響を及ぼすかもしれないような TSF データ。 TSF Data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE

3.3 脅威

本 TOE は、表 3-5 に示す脅威を想定する。

表 3-5 想定する脅威

名称	定義
T.UNAUTHORIZED_ACCESS	攻撃者は、TOEのインタフェースを通じて、TOE内の利用者文書データへアクセス（閲覧、改変、または削除）、または利用者ジョブデータを変更（改変または削除）するかもしれない。 An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	攻撃者は、TOEのインタフェースを通じて、TOE内のTSFデータへの不正なアクセスを得るかもしれない。 An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	TOEの操作が許可された場合、TSFの誤作動によって、セキュリティの損失を引き起こすかもしれない。 A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	攻撃者は、TOEに不正なソフトウェアをインストールするかもしれない。 An attacker may cause the installation of unauthorized software on the TOE.

名称	定義
T.NET_COMPROMISE	攻撃者は、ネットワーク通信をモニターしたり操作したりすることで、送信中のデータにアクセスしたり、TOEのセキュリティを危殆化したりするかもしれない。 An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

3.4 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 3-6 に示す。

表 3-6 組織のセキュリティ方針

名称	定義
P.AUTHORIZATION	利用者は、文書処理及び管理機能を実行する前に権限を付与されなければならない。 Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	セキュリティ関連アクティビティは監査されなければならず、またこのようなアクションのログは保護され、外部ITエンティティへ送信されなければならない。 Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	TOEは、LAN上の他のデバイスと自身を識別できなければならない。 The TOE must be able to identify itself to other devices on the LAN.
P.FAX_FLOW	TOEがPSTNファクス機能を提供する場合、PSTNファクス回線とLANの間に分離を保証する。 If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.

※本 TOE のストレージデバイスは、現地交換可能ではないため、適合 PP の P.STORAGE_ENCRYPTION は、該当しない。

4 前提条件と評価範囲の明確化

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

4.1 使用及び環境に関する前提条件

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

表 4-1 前提条件

名称	定義
A.PHYSICAL	TOE、及びTOEが保存または処理するデータの価値に見合った物理セキュリティが、その環境によって提供されることを想定する。 Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	運用環境は、LANインタフェースへの外部からの直接のアクセスからTOEを保護することを想定する。 The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ADMIN	TOE管理者は、サイトセキュリティ方針に従ってTOEを管理すると、信頼されている。 TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	許可された利用者は、サイトセキュリティ方針に従ってTOEを使用するよう教育訓練を受けている。 Authorized Users are trained to use the TOE according to site security policies.

4.2 運用環境と構成

本 TOE はオフィスに設置され、公衆電話回線網及び組織の内部ネットワークである LAN で接続され、同様に LAN に接続されたクライアント PC 及び各種サーバーと利用される。本 TOE の一般的な運用環境を図 4-1 に示す。

利用者は、TOE の操作パネル、LAN に接続された PC を操作して本 TOE を使用する。

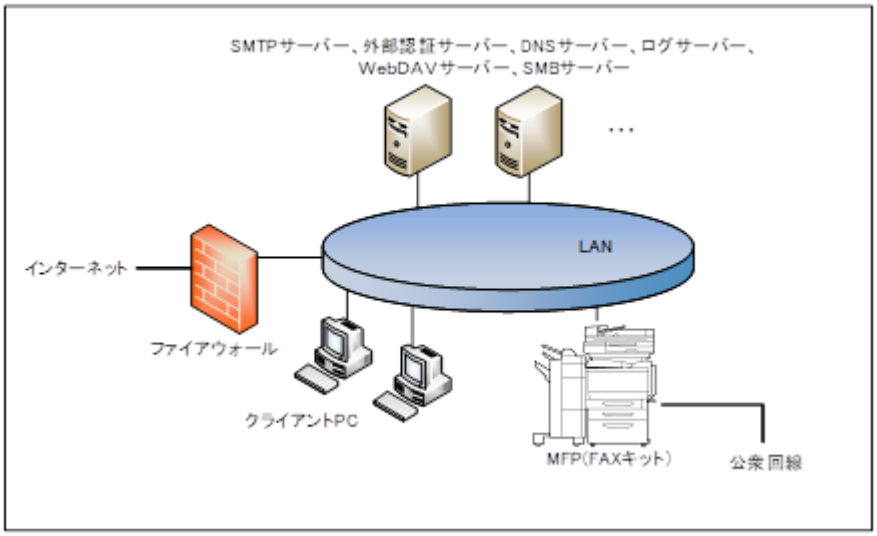

図 4-1 TOEの運用環境

TOE の使用環境の構成品について以下に示す。

(1) ログサーバー

本 TOE により生成された監査ログを保存するためのサーバーである。本サーバーの設置は、必須である。

WebDAV プロトコルに対応したソフトウェアが必要である。(本評価では、OS: Microsoft Windows Server 2012 R2 Standard 付属の IIS 8.0 を使用)

(2) 外部認証サーバー

TOE の利用者を識別・認証するサーバーである。外部サーバー認証方式で運用する場合に必要となる。

本評価では、以下を使用した。

Microsoft Windows Server 2012 R2 Standard に搭載される Active Directory

(3) DNSサーバー

ドメイン名を IP アドレスに変換するサーバーである。

Microsoft Windows Server 2012 R2 Standard に搭載される Active Directory

(4) SMTP サーバー、WebDAV サーバー、SMB サーバー

スキャンしたデータや TOE 内に保存されている電子文書を TOE から送信し、格納するサーバーである。

本評価では、以下を使用した。

・SMTP サーバー

Black Jumbo Dog Ver. 5.9.5

・WebDAV サーバー

Microsoft Windows Server 2012 R2 Standard 付属の IIS 8.0

・SMB サーバー

Microsoft Windows Server 2012 R2 Standard でのファイル共有

(5) クライアント PC

利用者が使用する汎用の PC である。

TOE の使用には、以下のソフトウェアが必要である。

・プリンタドライバ:

KONICA MINOLTA C4050i Series PCL / PS

・Web ブラウザ:

Microsoft Internet Explorer 11

なお、本構成に示されている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 では、設置が必須であるログサーバー以外にも、外部認証サーバー等のサーバーを設置する場合がある。 また、外部ネットワークであるインターネットとの接続にはファイアウォールの設置が必要である。 これらのサーバー及びファイアウォールがセキュアに運用されることは、運用者の責任となる。

本 TOE の暗号化機能は、通信データの暗号化に使用される。TOE に保存されるデータの暗号化は含まない。

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 の枠線で囲まれているベージュ色の部分が TOE であり、利用者(U.USER)、ログサーバー、外部認証サーバー、DNS サーバー、SMTP サーバー、WebDAV サーバー、SMB サーバー、クライアント PC、FAX は含まれない。

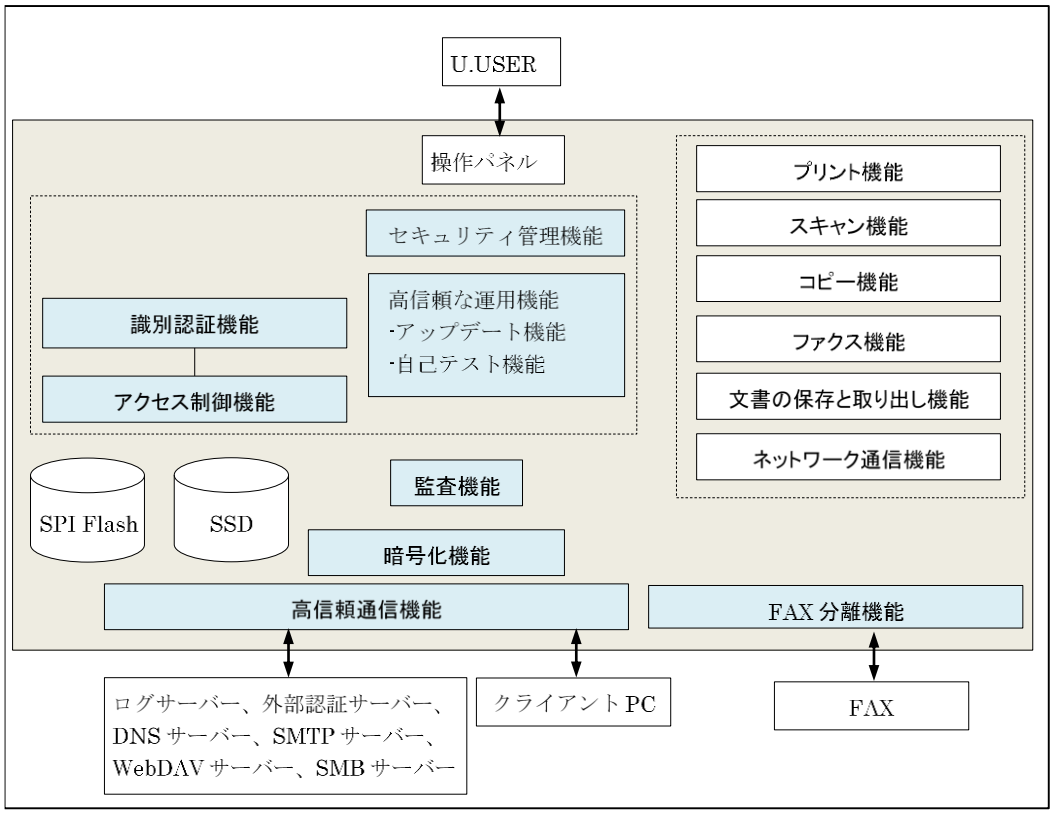

図 5-1 TOE境界

なお、SSD には利用者文書データ等が保存されるが、SSD 単独では取り外せない構造になっている。そのため、適合 PP の「現地交換可能な不揮発性ストレージデバイス」には該当しない。

TOE の機能は、セキュリティ機能（図 5-1 の色付きの四角で示されている機能）と基本機能（白地の四角で示されている機能）で構成される。

以下で、セキュリティ機能について説明する。基本機能については、第 11 章を参照のこと。

5.1.1 セキュリティ機能

(1) 識別認証機能

操作パネル、クライアントPCのWebブラウザ、プリンタドライバにおいて、TOE の利用者をログイン名とパスワードにより識別認証する機能である。

- 管理者の設定した文字数以上で、アルファベットの大文字、小文字、数字、及び特殊文字のパスワードを要求する。
- TOE 内に保存されている利用者情報を使用する「本体認証方式」と外部の認証サーバーを利用する「外部サーバー認証方式」をサポートする。
- パスワード入力時、入力された文字の代わりにダミー文字を表示する。
- 本体認証方式では、管理者が指定した回数、パスワードによる認証が失敗すると、その利用者はロックアウトされる。 ロックアウトは、ロックアウト状態でない管理者が解除することができる。
- 操作パネル、クライアント PC の Web ブラウザでは、識別認証後に管理者が設定した時間、利用者が操作を行わないとセションを終了する。

(2) アクセス制御機能

TOE の基本機能で利用者データを操作するときに利用者データのアクセス制御を行う機能である。

- アクセス制御は、利用者データの所有者情報と、利用者の識別情報及び役割に基づいて行われる。

(3) 暗号化機能

TOE がクライアント PC やログサーバー等と通信するときに LAN 上の保護資産を暗号化する機能である。

- 暗号鍵は RAM(揮発メモリ)及び SSD に保存される。

(4) 高信頼通信機能

通信が既知の終端との間で行われることを保証する機能である。

- ログサーバー、外部認証サーバー、DNS サーバー、SMTP サーバー、WebDAV サーバー、SMB サーバー、クライアント PC と通信する際、接続先の正当性を検証し、(3) 暗号化機能 によってネットワーク上を流れる保護資産を暗号化することで保護する。

(5) セキュリティ管理機能

セキュリティ機能の設定等をシステム管理者に制限する機能である。 ただし、一般利用者は、自分のパスワードの変更が可能である。

(6) 監査機能

TOE の使用およびセキュリティに関連する事象のログを事象発生時刻等とともにログファイルとして記録し、監査できる形式で提供する機能である。

- ログファイルは、(4) 高信頼通信機能を使用してログサーバーに送信され、ログサーバーから閲覧することができる。ログファイルは、ログサーバーへの送信が成功するまで TOE 内に保存される。

(7) 高信頼な運用機能

TOE のファームウェアアップデートを開始する前に、アップデート対象のファームウェアの真正性を検証し、それが正規のものであることを確認する機能、および、自己テストを実施する機能である。

(8) FAX 分離機能

TOE のファクス I/F が、TOE が接続している PSTN とネットワークとの間のネットワークブリッジを作成するために使用されるのを防止する機能である。

5.2 IT環境

TOE は、LAN を介して各種サーバーやクライアント PC と通信を行う。

TOE は、生成した監査データをログサーバーに送信する。管理者はログサーバーから監査データを読み出す。

外部認証方式の場合は、認証サーバーを使用して、利用者の識別認証を行う。

TOE は、スキャンして読込んだ利用者文書データを WebDAV サーバーと SMB サーバーに格納、及び SMTP サーバーを用いて E メール送信することができる。

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表 6-1 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 添付ドキュメント

種類	名称	バージョン	言語
FULL版	bizhub C4050i ユーザーズガイド	1.00	日本語
	bizhub C4050i/C3350i User's Guide	1.00	英語
	ineo+ 4050i/3350i User's Guide	1.00	英語
セキュリティ機能編	bizhub C4050iユーザーズガイド　セキュリティ機能編	1.02	日本語
	bizhub C4050i/C3350i User's Guide [Security Operations]	1.02	英語
	ineo+ 4050i/3350i User's Guide [Security Operations]	1.02	英語

7 評価機関による評価実施及び結果

7.1 評価機関

評価を実施したみずほ情報総研株式会社 情報通信研究部 マルチメディア技術チーム情報セキュリティ評価課は、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、適合 PP が要求する 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及び適合 PP の保証アクティビティを用いて行われた。

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 のワークユニット及び適合 PP の保証アクティビティ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、令和元年 7 月に始まり、令和 2 年 3 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、令和元年 7 月～令和 2 年 2 月に評価機関または開発者サイトで評価者テストを実施した。

認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。

これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.4 製品テスト

評価者は、評価の過程で示された証拠を検証した結果から、製品のセキュリティ機能が確実に実現されていることを保証するための評価者独立テスト及び脆弱性評定に基づく評価者侵入テストを実行した。

7.4.1 開発者テスト

本評価において、開発者テストは保証要件には含まれない。

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現されていることを保証するための評価者独立テスト（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

独立テストの構成は、図 4-1 で示した TOE の運用環境に準じ、その構成要素は表 7-1 のとおりである。以下の点で相違があるが、これらの構成でも、ST において識別されている構成と同等であり、本 TOE の機能の確認において問題がないことが評価者により評価されている。

- 外部ネットワークからの不正アクセスに対し TOE を保護するために設置するファイアウォールは、TOE の動作に影響を与えるものではないことからテスト環境には存在しない。
- 公衆電話回線の代わりに、公衆電話回線と同じファクス通信プロトコルをエミュレートすることができる電話回線擬似交換機を使用している。
- 暗号試験などの一部のテストでは、TOE 内の内部のふるまいを刺激・観察するための開発者用インタフェースを使用している。

表 7-1 独立テストの構成要素

要素	詳細
TOE	・KONICA MINOLTA bizhub C4050i/bizhub C3350i with FK-517, DEVELOP ineo+ 4050i/ineo+ 3350i with FK-517 バージョン G00-45
ログサーバー	・OS：Microsoft Windows Server 2012 R2 Standard ・ログサーバーソフトウェア：IIS（OS付属）
外部認証サーバー	・OS：Microsoft Windows Server 2012 R2 Standard ・Kerberosソフトウェア：Active Directory（OS付属。）
DNSサーバー	・OS：Microsoft Windows Server 2012 R2 Standard ・DNSサーバーソフトウェア：Microsoft DNS（OS付属）

SMTPサーバー	・OS：Microsoft Windows Server 2012 R2 Standard ・SMTPサーバーソフトウェア：Black Jumbo Dog 5.9.5
WebDAVサーバー	・OS：Microsoft Windows Server 2012 R2 Standard ・WebDAVサーバーソフトウェア：IIS（OS付属）
SMBサーバー	・OS：Microsoft Windows Server 2012 R2 Standard ・SMBサーバーソフトウェア：ファイル共有機能（OS付属）
クライアントPC	・OS：Microsoft Windows7 Professional Service Pack1 ・Webブラウザ： ・Internet Explorer 11 ・プリンタドライバ： ・KONICA MINOLTA C4050i Series - PCL Ver. 1.1.28.0 - PS Ver. 1.1.28.0

⑵ 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、適合PPの要求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 セキュリティ機能をSFRごとに確認する。

② 暗号実装が正しいことを確認する。

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 の外部インタフェースについて、TOE の操作パネル、クライアント PC、テストツールを使用して入力を行い、そのふるまいを以下の手法で確認した。

- ふるまいが、TOE の外部インタフェースから確認可能な場合は、TOE の外部インタフェースを利用する。
- ふるまいが、TOE の外部インタフェースから確認できない場合は、ログサーバー内のログの調査、ネットワークアナライザや、開発者用インタフェースを使用する。

＜独立テストの実施内容＞

独立テストは、評価者によって 39 項目実施された。

独立テストの観点とそれに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

観点	テスト概要
①	セキュリティ機能の確認 ・適合PPの保証アクティビティまたはSFRの仕様から作成したテスト項目により、すべてのセキュリティ機能が仕様どおりであることをSFRごとに確認する。
②	暗号実装の確認 ・TOEの開発者用インタフェースを使用して、テスト対象の以下の暗号アルゴリズムの実装を確認する。 - RSA(鍵生成、署名生成/検証) - AES-CBC-128、AES-CBC-256、AES-ECB-256 - SHA-1、SHA-256、SHA-384、SHA-512 - HMAC-SHA-1、HMAC-SHA-256、HMAC-SHA-384、HMAC-SHA-512 - CTR_DRBG

c) **結果**

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

7.4.3 評価者侵入テスト

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

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) **懸念される脆弱性**

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

① TOEの稼働しているネットワークサービスに公知の脆弱性が存在するこ

とにより悪用される懸念がある。

② TOEのWebインタフェースにおいて、URLの直接指定による識別認証機能等のバイパスやXSSなどの公知の脆弱性が存在することにより悪用される懸念がある。

③ TOEに入力される不正な印刷データにより、印刷ジョブの操作やバッファオーバーフローまたは任意のコードの実行が発生する懸念がある。

④ Webインタフェースからの不正な入力により、識別認証機能がバイパスされる懸念がある。

⑤ コニカミノルタ社の遠隔診断サービスがTOEで意図せず動作することにより、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＞

評価者独立テストの環境に、以下の表 7-3 に示すテストツールを追加して実施した。

表 7-3 侵入テストで使用したツール

ツール名称	概要・利用目的
脆弱性スキャンツール Nessus　8.5.1	公知の脆弱性を検出するために使用
Web脆弱性スキャンツール OWASP ZAP　2.8.0	Webの一般的な脆弱性を検出するために使用
Webアプリケーション解析ツール Fiddler　5.0. 20192.25091	Webアプリケーションがやり取りする通信データを捕捉、もしくは発行するために使用
プリンタセキュリティテストツール PRET　0.40	印刷デバイスに対しプリンタ言語を用いて脆弱性を検出するために使用
TCP/UDPデータ通信ツール nc　1.10	識別認証の脆弱性を検出するために使用
侵入テスト用ツール Metasploit Framework v5.0.2	不正な印刷用ファイルを作成するために使用

＜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 7-4 に示す。

表 7-4 侵入テスト概要

脆弱性	テスト概要
①	脆弱性スキャンツールを使用して、想定しないポートが開いていないこと及び使用可能なポートに公知の脆弱性が存在しないことを確認する。
②	Web脆弱性スキャンツールとWebアプリケーション解析ツールを使用して、Webインタフェースに公知の脆弱性が無いことを確認する。
③	不正なふるまいを発生させることを意図したPostscriptやPJL言語、PDF形式の印刷データを使用することにより、意図しないふるまいが発生しないことを確認する。
④	識別認証機能において入力される文字列により、不正なふるまいが発生しないことを確認する。
⑤	コニカミノルタ社の遠隔診断サービスに対し、意図しないふるまいが発生し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、第 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は、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。 ガイダンスと異なる設定にした場合は、本評価による保証の対象ではない。

7.6 評価結果

評価者は、評価報告書をもって本 TOE が CEM のワークユニット及び適合 PP の保証アクティビティの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：

Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015

Protection Profile for Hardcopy Devices - v1.0 Errata #1, June 2017

「ハードコピーデバイスのプロテクションプロファイル」適合の申請案件についてのガイドライン[16]

・FCS_RBG_EXT.1 のテストに関連する措置について

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、適合 PP が要求する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。

ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1

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、以下の観点で認証を実施した。

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CEMのワークユニット及び適合PPの保証アクティビティ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及び適合PPの保証アクティビティに適合していること。

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

8.1 認証結果

評価機関より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 の評価が適合 PP の要求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、「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。

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。

名称：	KONICA MINOLTA bizhub C4050i/bizhub C3350i with FK-517, DEVELOP ineo+ 4050i/ineo+ 3350i with FK-517 セキュリティターゲット
STバージョン：	2.00
発行日：	2020年2月27日
作成者：	コニカミノルタ株式会社

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）
PP	Protection Profile（プロテクションプロファイル）
SFR	Security Functional Requirement（セキュリティ機能要件）
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
CBC	Cipher Block Chaining
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
HMAC	Keyed-Hash Message Authentication Code
MFP	Multifunction Printer, Multifunction Peripheral
PSTN	Public Switched Telephone Network
SHA	Secure Hash Algorithm
SMB	Server Message Block
WebDAV	Web-based Distributed Authoring and Versioning
XSS	Cross Site Scripting

本報告書で使用された用語の定義を以下に示す。

Field Replaceable (Unit)	故障を修理するために現場で交換可能な最小サブアセンブリ。 The smallest subassembly that can be swapped in the field to repair a fault.
Hardcopy Device	電子的文書または画像の物理的媒体を生成または取り扱うシステム。このようなシステムはプリンター、スキャナー、ファクス装置、デジタルコピー機、デジタル複合機,「オールインワン」及びその他の同様な製品を含む。 A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, MFPs (multifunction peripherals), MFDs (multifunction devices), “all-in-ones” and other similar products.
コピー機能	利用者による操作パネルからの操作によって、紙文書を読み取って読み取った画像を複写印刷する機能
スキャン機能	利用者による操作パネルからの操作によって、紙文書を読み取って文書ファイルを生成し、送信（E-mail、WebDAV、SMB）する機能
ネットワーク通信機能	ローカルエリアネットワーク(LAN）上で文書を送受信する機能
文書の保存と取り出し機能	個人ボックス、強制メモリ受信ボックス、パスワード暗号化PDFボックスに電子文書を保存、もしくは保存した電子文書を取り出す機能
ファクス機能	標準ファクシミリプロトコルを用いて、公衆電話回線交換網(PSTN)を介して文書を送受信する機能
プリント機能	クライアントPCのプリンタドライバーもしくはWebブラウザを利用して、LAN経由で受信した印刷データを認証&プリントボックスもしくはパスワード暗号化PDFボックスに一時蓄積し、印刷する機能
保証アクティビティ	PP適合のために評価者が実施しなければならない評価作業。 CEMの補足であり、適合PP [14]では適合PPの中に記述されている。

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30年7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30年9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30年9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 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[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5版, 2017年4月, CCMB-2017-04-001 (平成29年7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5版, 2017年4月, CCMB-2017-04-002 (平成29年7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5版, 2017年4月, CCMB-2017-04-003 (平成29年7月翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[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5版, 2017年4月, CCMB-2017-04-004 (平成29年7月翻訳第1.0版)

[12] KONICA MINOLTA bizhub C4050i/bizhub C3350i with FK-517, DEVELOP ineo+ 4050i/ineo+ 3350i with FK-517 セキュリティターゲット, STバージョン 2.00, 2020年2月27日, コニカミノルタ株式会社

[13] KONICA MINOLTA bizhub C4050i/bizhub C3350i with FK-517, DEVELOP ineo+ 4050i/ineo+ 3350i with FK-517 評価報告書, 第7版, 2020年3月2日, みずほ情報総研株式会社 情報通信研究部マルチメディア技術チーム情報セキュリティ評価課

[14] Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (認証識別: JISEC-C0553)

[15] Protection Profile for Hardcopy Devices - v1.0 Errata #1, June 2017

[16] 「ハードコピーデバイスのプロテクションプロファイル」適合の申請案件についてのガイドライン 第1.6版, 2019年8月1日, 独立行政法人情報処理推進機構