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24年11月26日 (IT認証2434)
認証番号	C0442
認証申請者	コニカミノルタ株式会社
TOEの名称	bizhub C554e/bizhub C454e/bizhub C364e/bizhub C284e/bizhub C224e/ineo+ 554e/ineo+ 454e/ineo+ 364e/ineo+ 284e/ineo+ 224e
TOEのバージョン	G00-19
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	コニカミノルタ株式会社
評価機関の名称	みずほ情報総研株式会社 情報セキュリティ評価室

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26年10月23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 3

② Common Methodology for Information Technology Security Evaluation
Version 3.1 Release 3

評価結果：合格

「bizhub C554e/bizhub C454e/bizhub C364e/bizhub C284e/bizhub C224e/ineo+ 554e/ineo+

454e/ineo+ 364e/ineo+ 284e/ineo+ 224e」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「bizhub C554e/bizhub C454e/bizhub C364e/bizhub C284e/bizhub C224e/ineo+ 554e/ineo+ 454e/ineo+ 364e/ineo+ 284e/ineo+ 224e、バージョン G00-19」（以下「本 TOE」という。）についてみずほ情報総研株式会社 情報セキュリティ評価室（以下「評価機関」という。）が平成 26 年 10 月 14 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、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、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、スキャン機能、印刷機能、ファクス機能、文書の保存と取り出し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、以下に示す運用や機能は保証の対象外である。

本 TOE はファクス機能を含む PP 適合を主張しており、本評価の対象は、TOE である MFP に、オプションの FAX キットを搭載した構成である。FAX キットを搭載していない構成は本評価の対象ではない。

本評価では、「7.5 評価構成について」の設定条件が適用された構成だけが TOE として評価されている。それらの設定条件を変更した運用は、本評価による保証の対象外である。

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 26 年 10 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、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： bizhub C554e/bizhub C454e/bizhub C364e/bizhub C284e/bizhub C224e/ineo+ 554e/ineo+ 454e/ineo+ 364e/ ineo+ 284e/ ineo+ 224e

バージョン： G00-19

開発者： コニカミノルタ株式会社

TOE のバージョンは、MFP 基板、SSD 基板、ファームウェア及び BIOS のバージョンの総称である。表 2-1 に TOE の識別の詳細を示す。

表2-1 TOEの識別の詳細

名称 (MFP本体名称)	バージョン	
bizhub C554e, bizhub C454e, ineo+ 554e, ineo+ 454e	MFP基板	A5AYH020-07
	SSD基板	A5C1H02D-02
	ファームウェア	A5C10Y0-F000-G00-19
	BIOS	A5C10Y0-1E00-G00-04
bizhub C364e, bizhub C284e, bizhub C224e, ineo+ 364e, ineo+ 284e, ineo+ 224e	MFP基板	A5C1H020-07
	SSD基板	A5C1H02D-02
	ファームウェア	A5C10Y0-F000-G00-19
	BIOS	A5C10Y0-1E00-G00-04

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。

TOE の名称は、MFP 本体の表面に印字されている機種名を確認する。TOE のバージョンは、サービスエンジニアに依頼して、MFP 基板と SSD 基板のバージョンである部品番号、及び、操作パネルに表示されたファームウェアと BIOS のバージョンを確認する。

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、スキャン機能、印刷機能、ファクス機能、文書の保存と取り出し機能といった 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、デジタル複合機用の 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、スキャン機能、印刷機能、ファクス機能、文書の保存と取り出し機能といった MFP の基本機能の利用者である。

・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、印刷用の各種パラメタが該当する。

・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、ログインパスワード、文書データを保存するボッ

クスのパスワード、暗号鍵の生成に使用される暗号化ワード、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、利用者のユーザ ID と権限、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、「識別認証機能」、「利用者制限制御機能」、「蓄積文書アクセス制御機能」、「残存情報消去機能」及び「ネットワーク通信保護機能」で対抗する。

TOE の「識別認証機能」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「利用者制限制御機能」は、識別認証された利用者が、コピー機能、スキャン機能、印刷機能、ファクス機能、文書の保存と取り出し機能といった 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。その際、利用者データに対するアクセス制御も行なわれ、利用者データに対してアクセス権限のある利用者だけが、アクセスを許可される。ただし、ボックスに蓄積された文書データについては、次の「蓄積文書アクセス制御機能」が適用される。

TOE の「蓄積文書アクセス制御機能」は、利用者がボックスに蓄積された利用者データを操作する際に、ボックスの種別に応じたアクセス制御を行い、権限のある利用者だけに操作を許可する。

TOE の「残存情報消去機能」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 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「ネットワーク通信保護機能」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、「識別認証機能」、「セキュリティ管理機能」及び「ネットワーク通信保護機能」で対抗する。

TOE の「識別認証機能」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設定、参照、変更を、識別認証された管理者だけに許可する。ただし、一般利用者は、本人のログインパスワード等の変更は可能である。

TOE の「ネットワーク通信保護機能」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.CRYPTO 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.CRYPTO	The Data stored in an HDD must be encrypted to improve the secrecy.

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、「識別認証機能」及び「利用者制限制御機能」で本方針を実現する。

TOE の「識別認証機能」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「利用者制限制御機能」は、識別認証された利用者が、コピー機能、スキャン機能、印刷機能、ファクス機能、文書の保存と取り出し機能といった 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、HDD 暗号化機能、暗号化ワード及び TSF 実行コードが正常であることを、起動時に検証する。

(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、セキュリティ機能に関連する事象を監査ログとして記録する。TOE に格納された監査ログは、識別認証された管理者だけが、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、「識別認証機能」と「外部インタフェース分離機能」で、本方針を実現する。

TOE の「識別認証機能」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「外部インタフェース分離機能」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 LAN 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.CRYPTO」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 に保存する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、内部の LAN に接続し、同様に内部の LAN 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 である MFP と接続し、TOE の印刷機能を使用することもできる。

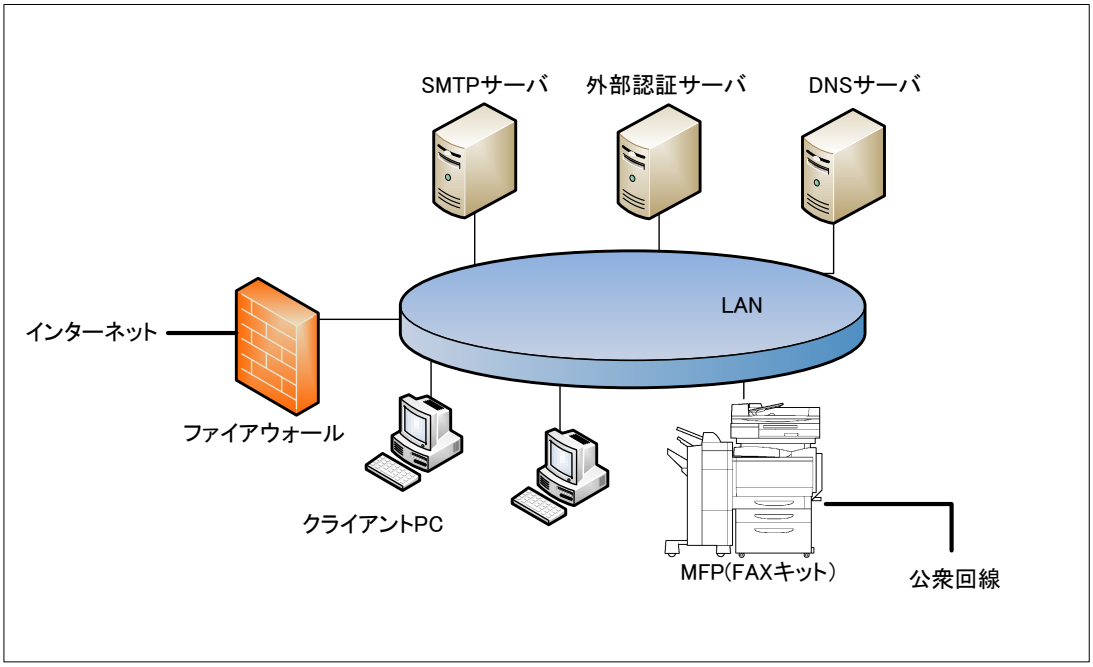

図 4-1　TOE の運用環境

図 4-1 において、MFP が TOE である。ただし、MFP に内蔵する FAX キットは TOE に含まない。TOE である MFP 以外の構成品を以下に示す。

(1) FAX キット

公衆回線を経由して、ファクスデータの送受信と遠隔診断機能の通信を行う。以下の MFP 用オプションが必要である。

・コニカミノルタ株式会社 FK-511

(2) クライアント PC

利用者が、LAN 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4-1　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 6 または 8
プリンタドライバ	・KONICA MINOLTA C554e Series PCL Ver. 2.1.2.0、PS Ver. 2.1.2.0、XPS Ver. 2.1.0.0 ・KONICA MINOLTA C364e Series PCL Ver. 2.1.2.0、PS Ver. 2.1.2.0、XPS Ver. 2.1.0.0

種別	名称とバージョン
スキャナドライバ	・HDD Twain Driver 4.0.07000 ・Real Time Mode Twain Driver 4.0.07000
ボックス支援ツール	・Box Operator Ver. 3.2.11000
管理者用ツール	・Data Administrator with Device Set-Up and Utilities Ver. 1.0.05000.09131 (プラグイン: Data Administrator 4.1.20000.11011) (プラグイン: HDD BackUp Utility Ver. 1.3.1000 00006)

(3) SMTP 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。

(4) 外部認証サーバ

TOE の利用者を Kerberos プロトコルで識別認証する。TOE の設定で、外部サーバ認証方式を選択した場合に必要である。本評価では、以下のソフトウェアを使用する。

・Microsoft Windows Server 2008 R2 Standard Service Pack1 に搭載される Active Directory

(5) DNS サーバ

ドメイン名を IP アドレスに変換するサーバである。本評価では、以下のソフトウェアを使用する。

・Microsoft Windows Server 2003R2 Standard Edition Service Pack2

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を印刷する機能を提供している。USB に格納された文書データは、操作パネルからの利用者は誰でもアクセスが可能である。USB メモリの置き忘れ等の対策は、利用者の責任となる。

TOE は、利用者がログインしたまま放置することを防止するために、無操作の状態が規定時間経過した場合にセッションを切断する機能を有している。しかし、セッション切断までの時間は、クライアント PC 上のツールによって違いがある。

特に、管理者が使用する Data Administrator の場合は 60 分の固定値であり、他のツールよりも時間が長いので、管理者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（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。FAX キットは TOE に含まれていない。

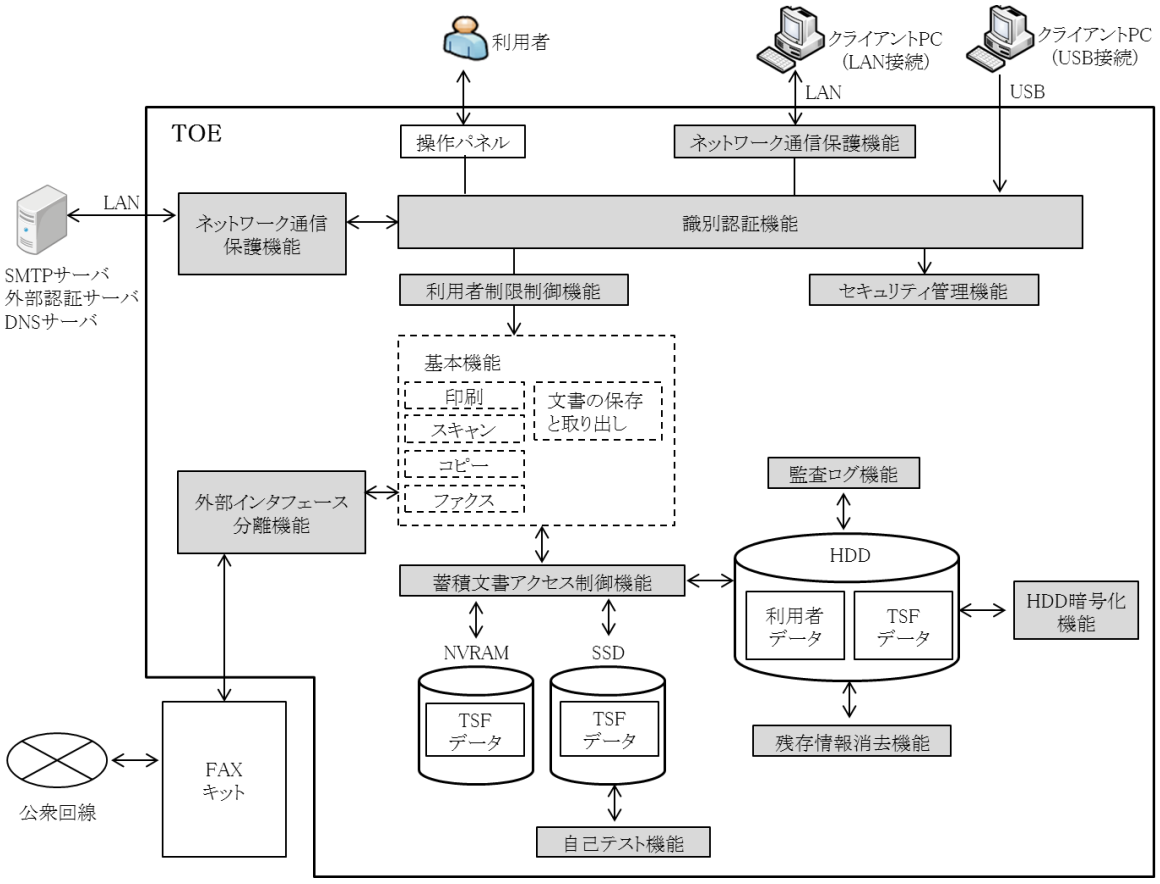

図5-1　TOEの構成

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) 識別認証機能

本機能は、TOE の利用者をユーザ ID とログイン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、各種ツール)

認証方式には、TOE に格納されたユーザ ID とログインパスワードを使用する「本体認証」と、TOE 外部の Kerberos サーバを使用する「外部サーバ認証」がある。

また、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。

- ログインパスワードは 8 桁以上の所定の品質が要求される。
- 連続した認証失敗回数が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。

ログインパスワードの品質チェックは、本体認証の場合にはログインパスワードの設定変更時に行われる。外部サーバ認証の場合にはログイン時に行われ、外部認証サーバに登録されたログインパスワードが TOE の品質を満足しない場合は、ログインは許可されない。

(2) 利用者制限制御機能

本機能は、識別認証された利用者の操作に対するアクセス制御と、TOE の利用に伴って生成される文書データに対するアクセス制御を行う機能である。ただし、蓄積された文書データに対するアクセス制御は「蓄積文書アクセス制御機能」で行う。

利用者が、印刷機能、コピー機能、スキャン機能、ファクス機能、文書の保存と取り出し機能といった MFP の基本機能を使用する際には、利用者に設定された権限をチェックし、権限のある基本機能だけが実行を許可される。

利用者が、文書データに対して印刷やプレビューなどの操作を行う際には、文書データの所有者だけが操作を許可される。文書データを削除する場合には、文書データの所有者と管理者だけが削除を許可される。

なお、TOE に USB メモリを接続した場合、USB メモリに格納された文書データについては、操作パネルからの利用者だけがアクセス可能であり、操作パネル以外の Web ブラウザ等のインタフェースからはアクセスすることができない。

(3) 蓄積文書アクセス制御機能

本機能は、TOE のボックスに蓄積された文書データを取り出す際にアクセス制御を行い、権限のある利用者だけに文書データの取り出しを許可する機能である。

アクセス制御の方式は、文書データを格納するボックスの種別によって異なり、文書データに付与されたユーザ ID やグループ ID、ボックスに設定されたパスワード、文書データに設定されたパスワードなどのいずれかが使用される。それにより、所有者、共有者、パスワードの一致する利用者のアクセスが許可される。

ボックスや文書データのパスワードは、ログインパスワードと同様に、設定時に 8 桁以上の所定の品質が要求される。

なお、管理者は、ボックスに蓄積されたすべての文書データのバックアップとリストア及び削除が可能である。

(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、本人のログインパスワードと、アクセスを許可されたボックスのパスワード等の情報は、変更可能である。なお、文書データに設定されたパスワードは、管理者を含めてどの利用者も変更することはできない。

(5) 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、識別認証された管理者だけが、クライアント PC へのダウンロードと削除をすることができる。監査ログの改変はできない。

(6) 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、導入時に管理者が設定する 20 桁の暗号化ワードを元に、コニカミノルタ社の独自アルゴリズムで生成する。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。

(7) 残存情報消去機能

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 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、管理者の設定で複数のパターンの中から選択することができる。また、上書きデータを暗号化して HDD に書き込む方式と、上書きデータを暗号化せずにそのまま HDD に書き込む方式があり、管理者の設定で選択することができる。

(8) 自己テスト機能

本機能は、TOE の起動時に以下の自己テストを行う機能である。

- TOE 内蔵の検証用データによる、暗号化ワードと暗号化機能の検証
- ファームウェアのハッシュ値の検証

(9) ネットワーク通信保護機能

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：IPsec、SSLv3、TLS（v1.0、v1.1、v1.2）
・外部認証サーバ：Kerberos v5
・SMTP サーバ：IPsec
・DNS サーバ：IPsec

(10) 外部インタフェース分離機能

本機能は、電話回線を含む外部インタフェースから LAN への不正な転送を防止する機能である。TOE の外部インタフェースから受信したデータは、TOE が必ず介在して処理する。

5.2 IT環境

TOE は、外部サーバ認証方式の場合には、外部の認証サーバ（Kerberos プロトコル）を使用して、利用者の識別認証を行う。

TOE のファクス機能は、TOE に含まれていない FAX キットを介して、ファクスデータの送受信を行う。ただし、ファクス機能に関するアクセス制御や不正アクセス防止などのセキュリティ機能は、TOE 内で実現している。

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語版と 2 種類の英語版があり、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。

（日本語版）

- bizhub C554e/C454e/C364e/C284e/C224e ユーザーズガイド Ver. 1.00
- bizhub C554e/C454e/C364e/C284e/C224e ユーザーズガイド セキュリティ機能編 Ver. 1.07

（英語版）

- bizhub C554e/C454e/C364e/C284e/C224e User's Guide Ver. 1.00
- bizhub C554e/C454e/C364e/C284e/C224e User's Guide [Security Operations] Ver. 1.07

（英語版）

- ineo+ 554e/454e/364e/284e/224e User's Guide Ver. 1.00
- ineo+ 554e/454e/364e/284e/224e User's Guide [Security Operations] Ver. 1.07

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 情報セキュリティ評価室は、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 24 年 11 月に始まり、平成 26 年 10 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 25 年 2 月、5 月、6 月、7 月、11 月及び 12 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 25 年 11 月及び平成 26 年 6 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。

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、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、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。

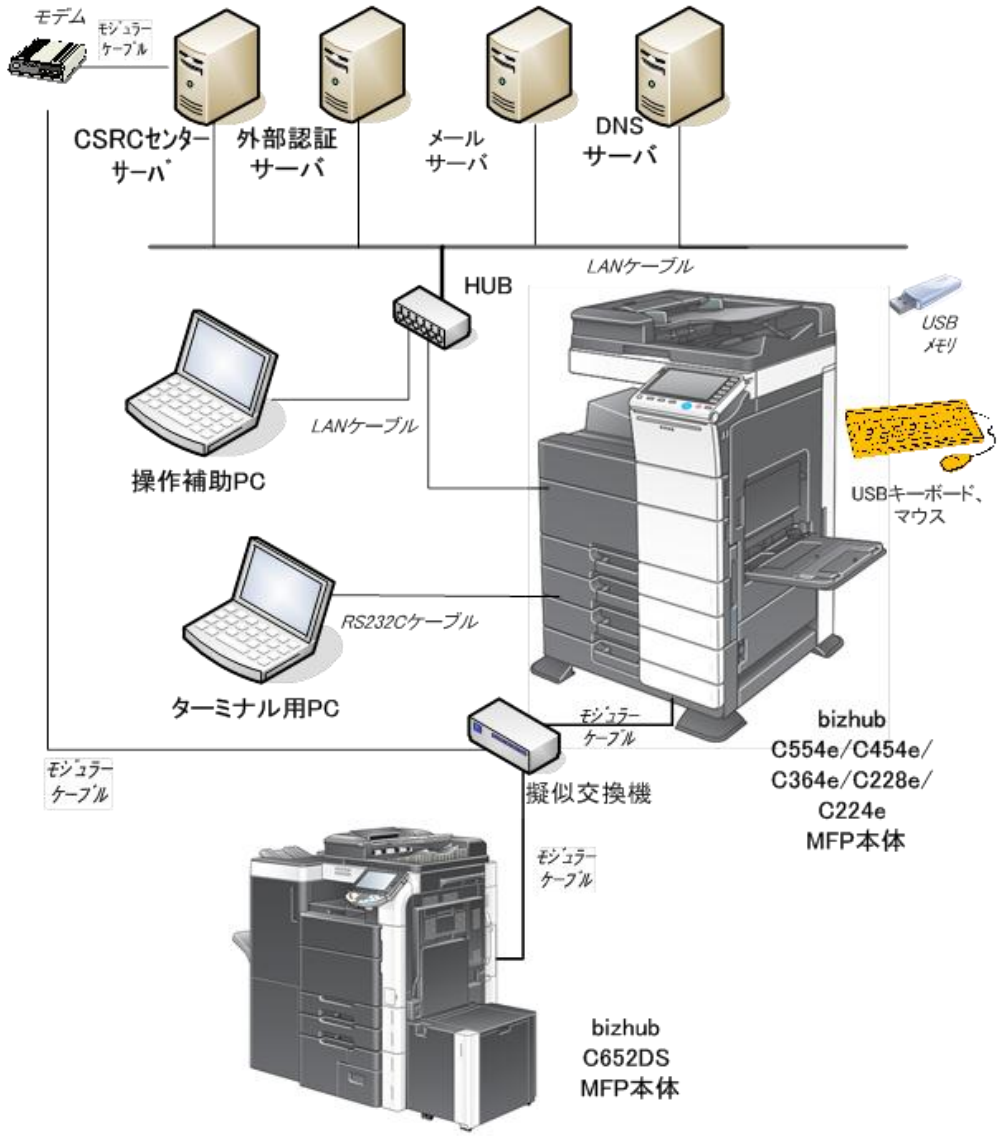

図7-1　開発者テストの構成図

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
MFP本体 (TOE)	bizhub C554e、bizhub C454e、bizhub C364e、bizhub C284e、bizhub C224e（バージョンG00-19）
MFP本体内蔵 FAXキット	コニカミノルタ社　FK-511
操作補助PC (クライアントPC)	以下の2機種を使用 ・Windows XP SP3搭載PC (Webブラウザ:　Internet Explorer Ver.6) ・Windows Vista SP2搭載PC (Webブラウザ: Internet Explorer Ver.8) ※上記に表4-1に示した各種ドライバやツールを搭載
外部認証サーバ	・Windows Server 2008 R2 Standard SP2搭載PC ・Kerberosソフトウェア: Active Directory (OS付属)
メールサーバ (SMTPサーバ)	・Windows Server 2003R2 Standard SP2搭載PC ・SMTPソフトウェア: Black Jumbo Dog
DNSサーバ	・Windows Server 2003R2 Standard SP2搭載PC ・DNSソフトウェア: OS付属
CSRCセンター サーバ	コニカミノルタ社の遠隔診断のサービスと同じ機能を提供するサーバ ・Windows Server 2003R2 Standard SP2搭載PC ・CSRCセンターソフトウェア Ver.2.7.0
bizhub C652DS MFP本体	TOEのFAX送受信の対向機として使用
疑似交換機 (公衆回線)	公衆回線を疑似的に実現する回線交換機 ・ネイクス社 CE-97
USBメモリ	TOEに文書データを登録するために使用 ・Sony USM1GJX, USM2GJ-3C
USBキーボード、 マウス	TOEの操作パネルは、オプションでUSBキーボードを使用することもできる。マウスは使用できない。その機能のテストに使用
ターミナル用PC	RS232Cを経由してTOEの開発者用インタフェースと接続 ・Windows XP SP3搭載PC ・ターミナルソフトウェア: Tera Term Pro Ver.4.29

開発者がテストしたTOEは、TOEの中でbizhubシリーズの全機種である。TOEのineo+シリーズは、名称が異なるだけでbizhubシリーズと同じ製品である。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。

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の外部インタフェースについて、TOEの操作パネル、PC、テストツールを使用して入力を行い、そのふるまいの確認を行った。ふるまいの確認には、以下のような手法が用いられている。

- TOEが提供しているインタフェースで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、監査ログ、通信データを確認する。

- TOEが提供しているインタフェースでは確認できないTOE内部のデータやHDD上のデータについては、開発者インタフェースを使用して確認する。

暗号アルゴリズムについては、上記の方法で取得したデータとOpenSSLで暗号化したデータを比較することで、仕様どおりに実装されていることを確認している。ただし、TOE内部の自己テストやWebのセッション情報生成のために使用されているハッシュアルゴリズムについては、ソースコードレビューを行うことで、仕様どおりに実装されていることを確認している。

＜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7-2に示す。

表7-2　開発テストツール

ツール名称	概要・利用目的
Fiddler Ver.2.2.2.0	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

ツール名称	概要・利用目的
Open APIテストツール Ver.7.2.0.5	コニカミノルタ社製のOpen API用テストツール。Open APIはクライアントPC上のツールData Administratorが使用しているTOEのネットワークインタフェースである
SocketDebugger Ver.1.12	TCP/IPのソケット通信のデバッグ支援ツール。クライアントPC上のData Administrator以外のツールやTWAIN Driverが使用しているTOEのネットワークインタフェースのテストに使用
OpenSSL Ver.1.0.0d	SSL、暗号アルゴリズム、ハッシュ関数のテストに使用
OpenSSL Ver.1.0.1e	TLS v1.2のテストに使用
ターミナル用PC	開発者インタフェースを使用して、暗号鍵等のTOE内部のメモリ内容や、HDDのデータを参照する
WireShark Ver. 1.2.2	LAN上の通信データのモニタと解析を行う

＜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、上書き消去途中の電源 OFF と ON も含まれている。

セキュリティ機能については、認証方式、IPv4 と IPv6 など、TOE の設定によってふるまいが異なる場合も確認されている。

なお、クライアント PC として開発者が使用した補助 PC の Windows と Web ブラウザの組合せでは TLS v1.2 プロトコルをサポートしていないが、開発者は OpenSSL を使用することで TLS v1.2 のテストを代替している。

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315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と同じ構成である。

・TOE として、bizhub C454e と bizhub C364e だけを使用。
・Windows7 及び Internet Explorer8 を搭載した検査用 PC を追加。

評価者は、TOE 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、印刷速度の異なる 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 開発者がテストしていない限界値のふるまいを確認する。

② 開発者がテストしてない複数のインタフェースや操作を組み合わせたふるまいを確認する。

③ 開発者テストを補足するために、入力データや操作環境のバリエーション

を確認する。

④　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と外部インタフェースを確認する。
・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。
・開発者の実施したソースコードレビューの内容を確認する。
・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、47 項目のサンプリングテストと、14 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 7-1 に示す。

表 7-1 実施した主な独立テスト

観点	テスト概要
観点①	・ログインパスワード、ボックスのパスワード、暗号化ワードなどについて、変更時に最大文字数より一桁多い文字列を入力した場合のふるまいを確認する。
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。 ・複数の利用者が共有ボックスにアクセスしている状態で、共有ボックスのパスワードを変更した場合のふるまいを確認する。 ・利用者の複数の権限を一度の操作で変更した場合、変更した複数の権限のとおりにアクセス制御されることを確認する。
観点③	・FAXデータを用いた遠隔診断機能について、開発者テストと異なるデータについても、不正なデータが拒否されることを確認する。 ・Windows7上のInternet Explorer8を用いて、TLS 1.2プロトコルで正常に使用できることを確認する。

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 ネットワークインタフェースに、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。

③ TOE に秘密のログインアカウント等の秘密情報が含まれている場合、悪用される懸念がある。

④ Web ブラウザ等から TOE を操作中に、TOE の電源を OFF にした場合、認証状態が維持されて悪用される懸念がある。

⑤ USB キーボードから TOE を操作すると、TOE の起動処理の中断等により、TOE が悪用される懸念がある。

⑥ 不正な通信データを TOE に送信することにより、識別認証とアクセス制御のバイパス、バッファオーバフローなどの攻撃が成功する懸念がある。

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、独立テスト環境と同じ環境で、検査用 PC に侵入テストツールを搭載して実施した。侵入テストで使用したツールの詳細を表 7-6 に示す。

表7-6　侵入テストツール

ツール名称	概要・利用目的
Nessus Version 5.2.4	各種通信プロトコルのセキュリティスキャナ（脆弱性データベースは2013年10月28日時点で最新のもの）
Nikto Version 2.1.5	Web用のセキュリティスキャナ（脆弱性データベースは2013年10月28日時点で最新のもの）
nmap Version 6.40	利用可能なネットワークポートを検出するツール
Fiddler Version 2.4.5.6	Webデバッガ。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。 ※評価者は、該当するテスト項目について、3種類のツールのいずれかを使用している。
TamperIE Version 1.0.1.13	
Burp Suite Version 1.5.0	
extrstr Version 0.2	評価機関が開発したバイナリ解析ツール。バイナリファイルに含まれている文字列を抽出するために使用
Metasploit Version 4.9.2	PDFの脆弱性を検査するための検査データの作成に使用

＜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 7-7 に示す。

表7-7　侵入テスト概要

脆弱性	テスト概要
脆弱性①	・nmap、Nessus、NiktoをTOEに実施し、オープンポートに公知の脆弱性がないことを確認した。
脆弱性②	・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した。
脆弱性③	・extrstrを用いて、TOEの更新媒体に格納されたバイナリを解析し、秘密のログインアカウントなど、悪用される可能性のある秘密の文字列が含まれていないことを確認した。

脆弱性④	TOEの操作パネルやPC上のWebブラウザや各種ツールでTOEを操作中に、TOEの電源をOFF・ONしても、認証状態は維持されず、再ログインしないと使用できないことを確認した。
脆弱性⑤	TOEの起動途中にUSBキーボードを操作しても、TOEの起動処理に影響がないことを確認した。
脆弱性⑥	・Webデバッガを使用して、WebブラウザからTOEへの通信データを書き換えても、識別認証やアクセス制御のバイパス、バッファオーバフロー等による想定外の動作が、できないことを確認した。 ・Web以外の独自インタフェースについても、開発者テストツールを用いて、Webの場合と同等の確認を行った。

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、セキュリティ機能の様々な設定を一括してセキュアな値に設定する「セキュリティ強化設定」の他に、個別に設定しなければならない設定値も存在する。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も含まれているので、注意が必要である。例えば、以下のような設定値も含まれている。

・インターネットファクス機能の無効化
・IPP以外の印刷プロトコルの無効化
・SNMPの無効化

なお、ガイダンスには、本評価で保証された評価構成に戻す方法も記述されている。

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 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。

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

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 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。

本 TOE の印刷機能では、クライアント PC からの印刷データは TOE 内に蓄積され、紙印刷出力をするためには操作パネルからの操作が必要である。しかし、TOE のボックスに保存された文書データは、クライアント PC からの操作で紙印刷出力が可能である。出力された紙のセキュリティを確保するために、紙印刷出力を操作パネルからの操作に制限することを期待する調達者にとっては、ニーズに合致しない可能性があるので、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本認証報告書とともに提供される。

bizhub C554e/bizhub C454e/bizhub C364e/bizhub C284e/bizhub C224e/ineo+ 554e/ineo+ 454e/ineo+ 364e/ineo+ 284e/ineo+ 224e セキュリティターゲット, バージョン 1.36, 2014 年 10 月 10 日, 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）
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。

暗号化ワード	HDD暗号化の暗号鍵の生成に使用される20桁の文字列
印刷機能	クライアントPCからLANまたはUSBインタフェースを経由して、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
遠隔診断機能	MFPの保守のために、公衆回線を経由してコニカミノルタ社のサポートセンターと接続し、MFPの動作状態や印刷数等の機器情報を通信する機能
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
スキャン機能	操作パネルの操作で、紙文書を読み取って文書データを生成する機能。生成した文書データは「文書の保存と取り出しの機能」で取り出す
ファクス機能	ファクス送信機能は、紙文書またはTOEに蓄積された文書データを、電話回線を介して外部のファクス装置に送信する機能。紙文書の送信は操作パネル、蓄積された文書データの送信は操作パネル及びクライアントPCのWebブラウザから操作する。 ファクス受信機能は、外部のファクス装置から電話回線を介して文書データを受信する機能。受信したデータは「文書の保存と取り出しの機能」で取り出す
文書の保存と取り出しの機能	TOE内に文書データを蓄積し、それを取り出す機能
ボックス	TOE内で文書データを蓄積するディレクトリ。ボックスには、個

人専用や共有可能なものなど、いくつかの種別がある

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26年3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26年4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25年4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 3, July 2009, CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003

[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3版, 2009年7月, CCMB-2009-07-001, (平成21年12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3版, 2009年7月, CCMB-2009-07-002, (平成21年12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3版, 2009年7月, CCMB-2009-07-003, (平成21年12月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

[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3版, 2009年7月, CCMB-2009-07-004, (平成21年12月, 翻訳第1.0版)

[12] bizhub C554e/bizhub C454e/bizhub C364e/bizhub C284e/bizhub C224e/ineo+ 554e/ineo+ 454e/ineo+ 364e/ineo+ 284e/ineo+ 224e セキュリティターゲット, バージョン 1.36, 2014年10月10日, コニカミノルタ株式会社

[13] bizhub C554e/bizhub C454e/bizhub C364e/bizhub C284e/bizhub C224e/ineo+ 554e/ineo+ 454e/ineo+ 364e/ineo+ 284e/ineo+ 224e 評価報告書, 第2版, 2014年10月14日, みずほ情報総研株式会社 情報セキュリティ評価室

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