認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙押印済

評価対象

申請受付日（受付番号）	**平成20年10月30日 （IT認証8239）**
認証番号	C0223
認証申請者	**コニカミノルタビジネステクノロジーズ株式会社**
TOE**の名称**	**日本語名：**bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 **全体制御ソフトウェア** **英語名：**bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 Control Software
TOE**のバージョン**	A0R50Y0-0100-G00-20 **（システム制御部）** A0R50Y0-1D00-G00-11 **（BIOS制御部）**
PP適合	**なし**
適合する保証パッケージ	EAL3
開発者	**コニカミノルタビジネステクノロジーズ株式会社**
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21年7月15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

「[日本語名] bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 全体制御ソフトウェア、[英語名] bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 Control Software、バージョン：A0R50Y0-0100-G00-20（システム制御部）、A0R50Y0-1D00-G00-11（BIOS制御部）」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

1.1 はじめに

この認証報告書は、「[日本語名] bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 全体制御ソフトウェア、[英語名] bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 Control Software、バージョン：A0R50Y0-0100-G00-20（システム制御部）、A0R50Y0-1D00-G00-11（BIOS制御部）」（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。）が行った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ビジネステクノロジーズ株式会社に報告するとともに、本TOEに関心を持つ利用者や運用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、本書と共に、対応するSTを併読されたい。本TOEの動作条件や運用のための前提についての詳細、本TOEが対抗する脅威へのセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件、及びセキュリティ仕様の概要と十分性の根拠は、STにおいて詳述されている。

本認証報告書は、市販される本TOEを購入する一般消費者を読者と想定している。本認証報告書は、本TOEに対して適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

1.1.1 評価保証レベル

本TOEが適合を主張する評価保証レベルは、EAL3である。

1.1.2 PP適合

適合するPPはない。

1.2 評価製品

1.2.1 製品名称

本TOEは、以下の製品のセキュリティ機能である。

製品名称：　[日本語名] bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622

[英語名] bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622

バージョン：　上記の内容により識別可能。

開発者：　コニカミノルタビジネステクノロジーズ株式会社

1.2.2 製品概要

本TOEが搭載される、bizhub 501、bizhub 421、bizhub 361、ineo 501、ineo 421、ineo 361、VarioLink 5022、VarioLink 4222、VarioLink 3622は、コピー、プリント、スキャン、FAXの各機能を選択、組み合わせて構成されるコニカミノルタビジネステクノロジーズ株式会社が提供するデジタル複合機（Multi Functional Peripheral。以下「MFP」という。）である。

本TOEは、MFP本体のパネルやネットワークから受け付ける操作制御処理、画像データの管理等、MFPの動作全体を制御する“ bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 全体制御ソフトウェア ”であり、MFPに保存される機密性の高いドキュメントの暴露に対する保護機能を提供する。また、MFP内の画像データを保存する媒体であるHDDが不正に持ち出される等の危険性に対して、HDDに搭載されるHDDロック機能を活用することにより、不正なアクセスを防止することが可能である。他に、TOEは各種上書き削除規格に則った削除方式を有し、HDDのすべてのデータを完全に削除する。

1.2.3 TOE範囲とセキュリティ機能

1.2.3.1 TOE に関係する役割

本TOEに関係する役割を以下に示す。

(1) ユーザ

MFPに登録されるMFPの利用者。一般には、オフィス内の従業員等が想定される。

(2) 管理者

MFPの運用管理を行うMFPの利用者。MFPの動作管理、ユーザの管理を行う。一般には、オフィス内の従業員の中から選出される者がこの役割を担うことが想定される。

(3) サービスエンジニア

MFPの保守管理を行う利用者。MFPの修理、調整の保守管理を行う。（一般的には、コニカミノルタビジネステクノロジーズ株式会社と提携し、MFPの保守

サービスを行う販売会社の担当者が想定される。）

(4) MFPを利用する組織の責任者

MFPが設置されるオフィスを運営する組織の責任者。MFPの運用管理を行う管理者を任命する。

(5) MFPを保守管理する組織の責任者

MFPを保守管理する組織（一般的には、MFPの保守サービスを行う販売会社）の責任者。MFPの保守管理を行うサービスエンジニアを任命する。

この他に、TOEの利用者ではないがTOEにアクセス可能な者として、オフィス内に出入りする者等が想定される。

1.2.3.2 TOE の範囲と動作概要

本TOEは、MFPの全体制御ソフトウェアであり、システム制御部とBIOS制御部から構成される。MFP本体内のMFP制御コントローラ上にあるコンパクトフラッシュメモリ（以下「CF」という。）上に本TOEの一部であるシステム制御部が、また、フラッシュメモリ上に本TOEの一部であるBIOS制御部が搭載され、主電源がONになるとRAMにロードされ動作する。本TOEとMFPの関係を図1-1に示す。

なお、図1-1中の「※」で示されたHDD、FAXユニット、暗号化プロテクションチップ、イメージコントローラはMFPのオプションパーツである。本TOEの動作環境としてはこれらのオプションが装備されていることを想定している。

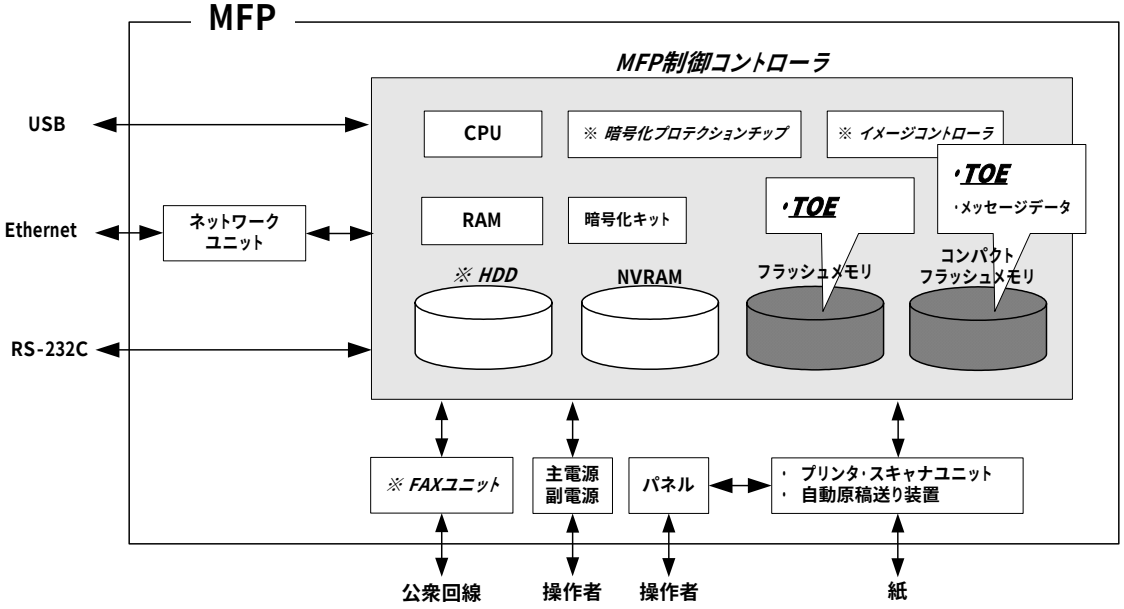

図1-1 TOEに関係するハードウェア構成

本TOEと関係する要素について以下に示す。

(1) コンパクトフラッシュメモリ（CF）
本TOEの一部であるシステム制御部のオブジェクトコードが保管される記憶媒体。TOEの他に、パネルやネットワークからのアクセスに対するレスポンス等で表示するための各国言語メッセージデータも保管される。また、TOEの処理に使われるMFPの動作において必要な様々な設定値が保管される。
CFにはパスワードを設定することが可能で、パスワードに一致しないと読み書きすることができないセキュリティ機能（CFロック機能）が搭載されている。なお、パスワード照合に一定回数不成功となるとパスワード照合機能をロックする機能も準備されている。

(2) フラッシュメモリ
本TOEの一部であるBIOS制御部のオブジェクトコードが保管される記憶媒体。

(3) HDD（※オプション）
容量60GBのハードディスクドライブ。画像データがファイルとして保管されるほか、伸張変換等の画像データや送信宛先データが一時的に保管される領域としても利用される。
HDDにはパスワードを設定することが可能で、パスワードに一致しないと読み書きすることができないセキュリティ機能（HDDロック機能）が搭載されている。なお、パスワード照合に一定回数不成功となるとパスワード照合機能をロックする機能も準備されている。
オプションパーツであるが、本評価では必須の構成部品である。

(4) NVRAM
不揮発性メモリ。TOEの処理に使われるMFPの動作において必要な様々な設定値等が保管される記憶媒体。

(5) 暗号化キット、暗号化プロテクションチップ（※オプション）
HDD、CFに書き込まれる画像データを暗号化するための暗号化機能がMFP制御コントローラ上のハードウェアである暗号化キットに実装されている。暗号化機能を動作させるためにはオプション購入の暗号化プロテクションチップが必要。

(6) イメージコントローラ（※オプション）
MFP制御コントローラとビデオバスで接続される画像変換処理のためのコントローラ
オプションパーツであるが、本評価では必須の構成部品である。

(7) パネル
タッチパネル液晶ディスプレイとテンキーやスタートキー、ストップキー画面

の切り替えキーを備えたMFPを操作するための専用コントロールデバイス。

(8) 主電源、副電源
MFPを動作させるための電源スイッチ。

(9) ネットワークユニット
Ethernet接続インタフェースデバイス。10BASE-T、100BASE-TX、Gigabit Ethernetをサポート。

(10) USB
ローカル接続でプリントするためのポート。プリント機能の他には、設定データ等のバックアップ、TOEのアップデートを本インタフェースから行うことも可能。

(11) FAXユニット（※オプションパーツ）
公衆回線を介してFAXの送受信や遠隔診断機能（後述）の通信に利用されるデバイス。販売上の都合によりMFPには標準搭載されず、オプションパーツとして販売される。

(12) スキャナユニット/自動原稿送り装置
紙から図形、写真を読み取り、電子データに変換するためのデバイス。

(13) プリンタユニット
MFP制御コントローラから印刷指示されると、印刷用に変換された画像データを実際に印刷するためのデバイス。

(14) RS-232C
シリアル接続することが可能。公衆回線と接続されるモデムと接続して、遠隔診断機能（後述）を利用することも可能である。

本TOEの利用者（ユーザ、管理者、サービスエンジニア）は、MFP本体のパネルやネットワーク接続されているクライアントPCからネットワークを介して本TOEの各種機能を使用する。本TOEの機能概要について以下に示す。

(1) 基本機能
MFPには、基本機能としてコピー、プリント、スキャン、FAXといった画像に関するオフィスワークのための一連の機能が存在し、TOEはこれら機能の動作における中核的な制御を行う。MFP制御コントローラ外部のデバイスから取得した生データを画像ファイルに変換し、RAMやHDDに登録する。（クライアントPCからのプリント画像ファイルは、複数の変換処理が行われる。）画像ファイルは、印刷用または送信用のデータとして変換され、目的のMFP制御コントローラ外部のデバイスに転送される。

コピー、プリント、スキャン、FAX等の動作は、ジョブという単位で管理され、パネルからの指示により動作順位の変更、印字されるジョブであれば仕上がり等の変更、動作の中止が行える。

(2) ボックス機能

画像ファイルを保管するための領域として、HDDにボックスと呼称されるディレクトリを作成できる。ボックスには、ユーザが占有する個人ボックス、登録されたユーザが一定数のグループを作って共同利用するための共有ボックス、所属部門のユーザ間で共有するグループボックスといった3つのタイプのボックスを設定することができる。個人ボックスは、所有するユーザだけに操作が制限され、共有ボックスは、そのボックスに設定されるパスワードを利用者間で共用することによって、アクセス制御を行っている。グループボックスは、その部門の利用を許可されたユーザだけに操作が制限される。TOEは、パネル、またはクライアントPCからネットワークを介したネットワークユニットから伝達される操作要求に対して、ボックス、ボックス内の画像ファイルに対する操作要求を処理する。

(3) ユーザ認証機能

TOEは、MFPを利用する利用者を制限することができる。パネル、またはネットワークを介したアクセスにおいてTOEはMFPの利用を許可されたユーザであることをユーザID、ユーザパスワードを使って識別認証する。識別認証が成功すると、TOEはユーザに対して基本機能及びボックス機能などの利用を許可する。

ユーザ認証方式には以下に示す方式がある。

【本体認証】

MFP制御コントローラ上のHDDにユーザID、ユーザパスワードを登録し、MFPにて認証する方式。

【外部サーバ認証】

MFP本体側でユーザID、及びユーザパスワードを管理せず、オフィス内LANで接続されるユーザ情報管理サーバ上に登録されるユーザID、及びユーザパスワードを用いて、MFPにて認証処理を行い、認証する方式。

本評価においては、本体認証方式、及びActive Directoryを利用した外部サーバ認証方式が評価対象となっている。

(4) 部門認証機能

TOEは、MFPを利用する利用者を部門単位でグルーピングして管理することができる。

部門認証には以下に示す方式がある。

【ユーザ認証連動方式】
ユーザに予め部門IDを設定し、ユーザの認証時に所属部門の部門IDと関連付ける方式。

【個別認証方式】
各部門IDに設定される部門パスワードによって認証された場合に当該部門IDと関連付ける方式。

(5) 管理者機能
TOEは、認証された管理者だけが操作することが可能な管理者モードにてボックスの管理、本体認証の場合におけるユーザの情報の管理、ネットワークや画質等の各種設定の管理等の機能を提供する。

(6) サービスエンジニア機能
TOEは、サービスエンジニアだけが操作することが可能なサービスモードにて、管理者の管理、スキャナ・プリント等のデバイスの微調整等のメンテナンス機能等を提供する。

(7) 暗号鍵生成機能
オプション製品である暗号化プロテクションチップがMFP制御コントローラに設置されている場合に、暗号化キットにてHDDの画像データ書き込み、読み込みにおいて暗号化・復号処理を実施する。(TOEは、暗復号処理そのものを行わない。)
管理者機能にて本機能の動作設定を行う。動作させる場合は、TOEはパネルにて入力された暗号化ワードより暗号鍵を生成する。

(8) 遠隔診断機能
FAX公衆回線口やRS-232Cを介したモデム接続、E-mail等いくつかの接続方式を利用して、コニカミノルタビジネステクノロジーズ株式会社が製造するMFPのサポートセンターと通信し、MFPの動作状態、印刷数等の機器情報を管理する。また必要に応じて適切なサービス（追加トナーの発送、課金請求、故障診断からサービスエンジニアの派遣等）を提供する。
セキュリティ強化機能（後述）を有効にした場合、本機能は無効に設定される。

(9) TOEの更新機能
TOEはTOE自身を更新するための機能を有する。更新手段は、遠隔診断機能の項目の1つとしても存在する他、Ethernetを介してFTPサーバよりダウンロードする方法（インターネット経由TOE更新機能)、USBメモリ等のメモリ媒体を接続して行う方法がある。
セキュリティ強化機能（後述）を有効にした場合、Ethernetを介したTOE更新機能は無効に設定される。

(10) 暗号通信機能

TOEはクライアントPCからMFPへ送信するデータ、MFPからダウンロードして受信するデータをSSL/TLSを利用して暗号化することができる。本機能は、管理者機能にて動作設定が行える。

(11) S/MIME証明書自動登録機能

S/MIME用に各宛先に設定可能な証明書（ITU-T X.509準拠）を自動登録する機能。メールに証明書が添付されている場合、当該メールのヘッダー情報にてユーザIDを判別し、証明書を当該ユーザの証明書として登録する。

(12) セキュリティ強化機能

管理者機能、サービスエンジニア機能におけるセキュリティ機能のふるまいに関係する各種設定機能は、管理者機能における「セキュリティ強化機能」による動作設定により、セキュアな値に一括設定が行える。設定された各設定値は、個別に設定を脆弱な値に変更することが禁止される。また個別には動作設定機能を持たない機能として、ネットワーク設定のリセット機能、ネットワーク介したTOEの更新機能が存在するが、これら機能の利用は禁止される。

1.2.3.3 TOE のセキュリティ機能

本TOEの保護資産は、MFPの利用において生成される、以下の画像ファイルである。

・セキュリティ文書プリントファイル
セキュリティ文書プリントによって登録される画像ファイル。

・認証&プリントファイル
認証＆プリント機能を利用してプリントデータが登録される場合に認証＆プリントファイルとして保管される画像ファイル。

・ボックスファイル
個人ボックス、共有ボックス、グループボックスに保管される画像ファイル。

また、MFPをリース返却、廃棄するなど利用が終了した場合やHDD、CFが盗難にあった場合等ユーザの管轄から保管されるデータが物理的に離れてしまった場合は、ユーザはHDD、CF、NVRAMに残存するあらゆるデータの漏洩可能性を懸念する。従ってこの場合は以下のデータファイルを保護対象とする。

・セキュリティ文書プリントファイル

・認証&プリントファイル

・ボックスファイル

・オンメモリ画像ファイル
メモリ上で待機状態にあるジョブの画像ファイル。

・保管画像ファイル
セキュリティ文書プリントファイル、認証&プリントファイル、ボックスファイル以外の保管される画像ファイル。

・HDD残存画像ファイル
一般的な削除操作（ファイル管理領域の削除）だけでは削除されない、HDDデータ領域に残存するファイル。

・CF残存画像ファイル
一般的な削除操作（ファイル管理領域の削除）だけでは削除されない、CFのデータ領域に残存するファイル。HDDを標準搭載している状態では発生しない。HDDを装着せず、利用していた場合に画像ファイルがCFに保存されることがある。

・画像関連ファイル
プリント画像ファイル処理において生成されたテンポラリデータファイル。

・送信宛先データファイル
画像を送信する宛先となるE-mailアドレス、電話番号等が含まれるファイル。

これらの保護資産を保護するために、本TOEは、以下のセキュリティ機能を保持する。

第一に、保護資産であるセキュリティ文書ファイルやボックスファイルの不正な操作を防ぐために、利用者が許可されたものであることの確認を行うための識別認証機能、各利用者の保護資産へのアクセスを制限するアクセス制御機能を提供する。

第二に、MFP上で保護資産が格納されることになるHDD、CF、NVRAMからの情報の漏洩を防ぐために、TOE範囲外のHDDやCFのロック機能、暗号化キットによる暗号化機能を利用し、本TOEは、MFP起動時に正当なHDDやCFであることを検証する機能、HDDやCFの全領域の上書き削除機能、NVRAMの設定値の初期化機能、HDDに書き込むデータの暗号化機能を提供する。

第三に、ユーザや管理者が利用するクライアントPCと本TOEの間で通信される画像ファイルを安全に保護するために、正しい相手先との通信に利用する高信頼チャネル機能、S/MIMEを利用してMFPからクライアントPCに送信される画像ファイルを暗号化して送信する機能を提供する。

第四に、MFP及びTOEの動作を決定する各種設定ファイルに対する不正な操作を防ぐために、利用者が管理者及びサービスエンジニアであることの確認を行う識別認証機能、各利用者に設定ファイルの変更等のアクセスを制限する管理機能を提供

する。

1.3 評価の実施

認証機関が運営するITセキュリティ評価･認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[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」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

① 本TOEのセキュリティ設計が適切であること。
② 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。
③ 本TOEがセキュリティ設計に基づいて開発されていること。
④ 上記①、②、③を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 全体制御ソフトウェア A0R50Y0-0100-G00-20 A0R50Y0-1D00-G00-11 セキュリティターゲット」（以下「本ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1 （[5][8]のいずれか） 附属書A、CCパート2（[6][9]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 全体制御ソフトウェア 評価報告書」（以下「評価報告書」という。）[13]に示されている。なお、評価方法は、CEM（[11][12]のいずれか）に準拠する。

1.4 評価の認証

認証機関は、評価機関が作成した、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、本TOE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。評価は、平成21年7月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEM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概要

2.1 セキュリティ課題と前提

TOEが解決すべき課題と、必要とする前提を以下に示す。

2.1.1 脅威

本TOEは、表2-1に示す脅威を想定し、これに対抗する機能を備える。

表2-1 想定する脅威

識別子	脅 威
T.DISCARD-MFP（MFPのリース返却、廃棄）	リース返却、または廃棄となったMFPが回収された場合、悪意を持った者が、MFP内のHDD、CF、NVRAMを解析することにより、セキュリティ文書プリントファイル、認証&プリントファイル、ボックスファイル、オンメモリ画像ファイル、保管画像ファイル、HDD残存画像ファイル、CF残存画像ファイル、画像関連ファイル、送信宛先データファイル、設定されていた各種パスワード等の秘匿情報が漏洩する。
T.BRING-OUT-STORAGE（HDDの不正な持ち出し）	・悪意を持った者や悪意を持ったユーザが、MFP内のHDDを不正に持ち出して解析することにより、セキュリティ文書プリントファイル、認証&プリントファイル、ボックスファイル、オンメモリ画像ファイル、保管画像ファイル、HDD残存画像ファイル、画像関連ファイル、送信宛先データファイル、設定されていた各種パスワード等が漏洩する。 ・悪意を持った者や悪意を持ったユーザが、MFP内のHDDを不正にすりかえる。すりかえられたHDDには新たにセキュリティ文書プリントファイル、認証&プリントファイル、ボックスファイル、オンメモリ画像ファイル、保管画像ファイル、HDD残存画像ファイル、画像関連ファイル、送信宛先データファイル、設定されていた各種パスワード等が蓄積され、悪意を持った者や悪意をもったユーザは、このすりかえたHDDを持ち出して解析することにより、これら画像ファイル等が漏洩する。
T.ACCESS-PRIVATE-BOX（ユーザ機能を利用した個人ボック	悪意を持った者や悪意を持ったユーザが、他のユーザが個人所有するボックスにアクセスし、ボックスファイルをダウンロード、印刷、送信（E-mail送信、FTP送信、FAX

スへの不正なアクセス）	送信、SMB 送信、WebDAV送信）することにより、ボックスファイルが暴露される。
T.ACCESS-PUBLIC-BOX（ユーザ機能を利用した共有ボックスへの不正なアクセス）	悪意を持った者や悪意を持ったユーザが、利用を許可されない共有ボックスにアクセスし、ボックスファイルをダウンロード、印刷、送信（E-mail送信、FTP送信、FAX送信、SMB送信、WebDAV送信）、他のボックスへ移動・コピーすることにより、ボックスファイルが暴露される。
T.ACCESS-GROUP-BOX（ユーザ機能を利用したグループボックスへの不正なアクセス）	悪意を持った者や悪意を持ったユーザが、そのユーザが所属していない部門が所有するグループボックスにアクセスし、ボックスファイルをダウンロード、印刷、送信（E-mail送信、FTP送信、FAX送信、SMB送信、WebDAV送信）することにより、ボックスファイルが暴露される。
T.ACCESS-SECURE-PRINT（ユーザ機能を利用したセキュリティ文書プリントファイル及び認証&プリントファイルへの不正なアクセス）	・悪意を持った者や悪意を持ったユーザが、利用を許可されないセキュリティ文書プリントファイルを印刷することにより、セキュリティ文書プリントファイルが暴露される。 ・悪意を持った者や悪意を持ったユーザが、他のユーザが登録した認証&プリントファイルを印刷することにより、認証&プリントファイルが暴露される。
T.UNEXPECTED-TRANSMISSION（想定外対象先への送受信）	・悪意を持った者や悪意を持ったユーザが、ボックスファイルの送信に関係するネットワーク設定を変更することにより、宛先が正確に設定されていてもボックスファイルがユーザの意図しないエンティティへ送信（E-mail送信、FTP送信）されてしまい、ボックスファイルが暴露される。 <ボックスファイル送信に関係するネットワーク設定> - SMTPサーバに関する設定 - DNSサーバに関する設定 ・悪意を持った者や悪意を持ったユーザが、TOEが導入されるMFPに設定されるMFPを識別するためのネットワーク設定を変更し、不正な別のMFP等のエンティティにおいて本来TOEが導入されるMFPの設定（NetBIOS名、AppleTalkプリンタ名、IPアドレス等）を設定することにより、セキュリティ文書プリントファイル、認証&プリントファイルが暴露される。 ・悪意を持った者や悪意を持ったユーザが、TSI受信設定を変更することにより、ボックスファイルが意図しない保管領域に保存されて暴露される。 ・悪意を持った者や悪意を持ったユーザが、PC-FAX動作

	設定を変更し、共有ボックス等のボックスへの保管設定状態から、全ユーザ共通領域に保管される設定に変更することにより、ボックスファイルが意図しない保管領域に保存されて暴露される。 ※ 本脅威は、PC-FAX動作設定が、ボックスへの保管設定状態を運用として意図している場合のみ発生する脅威である。
T.ACCESS-SETTING（セキュリティに関係する機能設定条件の不正変更）	悪意を持った者や悪意を持ったユーザが、セキュリティ強化機能に関係する設定を変更してしまうことにより、ボックスファイル、セキュリティ文書プリントファイル、認証&プリントファイルが漏洩する可能性が高まる。
T.BACKUP-RESTORE（バックアップ機能、リストア機能の不正な使用）	悪意を持った者や悪意を持ったユーザが、バックアップ機能、リストア機能を不正に使用することにより、ボックスファイル、セキュリティ文書プリントファイル、認証&プリントファイルが漏洩する。またパスワード等の秘匿性のあるデータが漏洩し、各種設定値が改ざんされる。
T.BRING-OUT-CF（CFの不正な持ち出し）	悪意を持った者や悪意を持ったユーザが、MFP内のCFを不正に持ち出して解析することによって以下の可能性が考えられる。 ・設定値（SNMPパスワード、WebDAVサーバパスワード）が漏洩する。 ・改ざんされた設定値（SNMPパスワード、その他各種機能の動作設定値）で動作させられる。 ・改ざんされたTOEで動作させられる。 ・CF残存画像ファイルより、CF内に存在した画像情報が漏洩する。

2.1.2 組織のセキュリティ方針

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2-2に示す。

表2-2 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.COMMUNICATION-DATA（画像ファイルのセキュアな通信）	IT機器間にて送受信される秘匿性の高い画像ファイル（セキュリティ文書プリントファイル、認証&プリントファイル、ボックスファイル）は、組織・利用者が希望する場合において、正しい相手先に対して信頼されるパスを介して通信する、または暗号化しなければならない。

ここでいう「IT機器間」とは、利用者が使用するクライアントPCとMFPの間を指している。

2.1.3 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表2-3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2-3 TOE使用の前提条件

識別子	前提条件
A.ADMIN（管理者の人的条件）	管理者は、課せられた役割として許可される一連の作業において、悪意を持った行為は行わない。
A.SERVICE（サービスエンジニアの人的条件）	サービスエンジニアは、課せられた役割として許可される一連の作業において、悪意を持った行為は行わない。
A.NETWORK（MFPのネットワーク接続条件）	・TOEが搭載されるMFPを設置するオフィス内LANは、盗聴されない。 ・TOEが搭載されるMFPを設置するオフィス内LANが外部ネットワークと接続される場合は、外部ネットワークからMFPへアクセスできない。
A.SECRET（秘密情報に関する運用条件）	TOEの利用において使用される各パスワードや暗号化ワードは、各利用者から漏洩しない。
A.SETTING（セキュリティ強化機能の動作設定条件）	セキュリティ強化機能が有効化した上で、TOEが搭載されたMFPを利用する。

2.1.4 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。

＜管理者・一般利用者向けドキュメント＞

・bizhub 501 / 421 / 361 ユーザーズガイド セキュリティ機能編 Ver.1.03
・bizhub 501 / 421 / 361 User's Guide [Security Operations] Ver.1.03
・ineo 501 / 421 / 361 User's Guide [Security Operations] Ver.1.03
・VarioLink 5022 / 4222 / 3622 User's Guide [Security Operations] Ver.1.03

＜サービスエンジニア向けドキュメント＞
・bizhub 501 / 421 / 361 サービスマニュアル セキュリティ機能編　Ver.1.01
・bizhub 501 / 421 / 361 ineo 501 / 421 / 361 VarioLink 5022 / 4222 / 3622
SERVICE MANUAL SECURITY FUNCTION　Ver.1.01

2.1.5 構成条件

本TOEは、ソフトウェアである。本評価は以下のハードウェア及びソフトウェア上での動作を対象とする。なお、本構成に示されるハードウェア及びソフトウェアの信頼性は本評価の範囲外である。

- コニカミノルタビジネステクノロジーズ株式会社が提供するデジタル複合機、bizhub 501、bizhub 421、bizhub 361、ineo 501、ineo 421、ineo 361、VarioLink 5022、VarioLink 4222、VarioLink 3622にオプションである、HDDロック機能付きのHDD、FAXユニット、暗号化プロテクションチップ、イメージコントローラを搭載した状態。
- ユーザの識別認証において外部サーバ認証方式を選択した場合、外部認証サーバとしてWindowsプラットフォームのネットワーク環境にてユーザ情報を一元管理するためにWindows Server 2000（それ以降）が提供するディレクトリサービスであるActive Directoryが必要。

2.2 セキュリティ対策

TOEは、具備したセキュリティ機能により以下のように2.1.1の脅威に対抗し、2.1.2の組織のセキュリティ方針を満たす。

（1）脅威「T.DISCARD-MFP（MFPのリース返却、廃棄）」に対抗するためのセキュリティ機能
本脅威は、ユーザから回収されたMFPより情報漏洩する可能性を想定している。

本TOEで、HDDのデータ領域およびCFのデータ領域に上書き削除を実行すると共にNVRAMやCFに設定されているパスワード等の設定値を初期化する機能（以上、「全領域上書き削除機能」）を保持することで、リース返却、または廃棄となったMFPに接続されたHDD、CF、NVRAMに格納された保護資産やセキュリティに関する設定値が漏洩することを防いでいる。

（2）脅威「T.BRING-OUT-STORAGE（HDDの不正な持ち出し）」に対抗するためのセキュリティ機能
本脅威は、MFPを利用している運用環境からHDDが盗み出される、または不正なHDDが取り付けられて、そこにデータが蓄積されたところで持ち出さ

れることにより、HDD内の画像データが漏洩する可能性を想定している。

本TOEの範囲外であるHDDでHDDロックパスワードによる認証が完了するまで書き込みを許可しないHDDロック機能を利用し、本TOEで、HDDロック機能を持つHDDと連動するための機能（以上、「HDDロック動作サポート機能」）を保持することで、HDDからの情報の読み出しにはHDDロックパスワードが要求されることとなり、MFPに接続されているHDDを不正に持ち出して解析することによりHDDに格納された保護資産やセキュリティに関する設定値が漏洩することを防いでいる。加えて、本TOEの範囲外である暗号キットで暗号化機能を利用し、本TOEで、HDDに書き込む画像データの暗号化を行う暗号鍵の生成機能（以上、「暗号鍵生成機能」）及び暗号キットと連動するための機能（以上、「暗号化キット動作サポート機能」）を保持することで、暗号化されたデータがHDDに格納され、HDDから情報を読み出した場合でも、解読が困難となる。

本TOEで、HDDがHDDロック機能を持つ正当なHDDであることを検証する機能（以上、「HDD検証機能」）を保持することで、HDDロック機能等を持つ正当なHDDのみに情報が格納されることとなり、MFPに接続されているHDDがHDDロック機能を持たないHDDにすりかえられ、そのHDDが持ち出されて、データが漏洩することを防いでいる。

（3）脅威「T.ACCESS-PRIVATE-BOX（ユーザ機能を利用した個人ボックスへの不正なアクセス）」に対抗するためのセキュリティ機能
本脅威は、ユーザ各位が画像ファイルの保管に利用する個人ボックスに対して、ユーザ機能を利用して不正な操作が行われる可能性を想定している。

本TOEで、MFPの諸機能を利用するにあたって、ユーザ及び管理者を識別認証する機能（以上、「ユーザ機能」、「管理者機能」）、個人ボックスに対するアクセス制御機能（以上、「ボックス機能」）、ユーザ及び個人ボックスに関する設定の変更を管理者及びユーザに制限する機能（以上、「管理者機能」、「ユーザ機能」、「ボックス機能」）を保持することで、ユーザ及び個人ボックスの設定の変更は管理者及び許可されたユーザのみに制限され、個人ボックスの操作は、正規のユーザのみに制限されることとなり、ユーザ機能を利用して不正な操作が行われることを防いでいる。

また、本TOEは、ユーザの識別認証機能において、本TOEの範囲外であるActive Directoryによるユーザ情報管理サーバから認証情報の取得を行うための機能（以上、「外部サーバ認証動作サポート機能」）も保持している。

（4）脅威「T.ACCESS-PUBLIC-BOX（ユーザ機能を利用した共有ボックスへの不正なアクセス）」に対抗するためのセキュリティ機能
本脅威は、ユーザが共有して利用する画像ファイルの保管場所である共有

ボックスに対して、ユーザ機能を利用して不正な操作が行われる可能性を想定している。

本TOEで、MFPの諸機能を利用するにあたって、ユーザ及び管理者を識別認証する機能（以上、「ユーザ機能」、「管理者機能」）、共有ボックスのアクセスにおける認証機能、共有ボックスに対するアクセス制御機能、共有ボックスに関する設定の変更を管理者及びユーザに制限する機能（以上、「ボックス機能」）、ユーザに関する設定の変更を管理者及び許可されたユーザに制限する機能（以上、「管理者機能」、「ユーザ機能」）を保持することで、共有ボックス及びユーザの設定の変更は管理者及び許可されたユーザのみに制限され、共有ボックスの操作は正規のユーザのみに制限されることとなり、ユーザ機能を利用して不正な操作が行われることを防いでいる。

また、本TOEは、ユーザの識別認証機能において、本TOEの範囲外であるActive Directoryによるユーザ情報管理サーバから認証情報の取得を行うための機能（以上、「外部サーバ認証動作サポート機能」）も保持している。

（５）脅威「T.ACCESS-GROUP-BOX（ユーザ機能を利用したグループボックスへの不正なアクセス）」に対抗するためのセキュリティ機能
本脅威は、その部門の利用が許可されたユーザが利用する画像ファイルの保管場所であるグループボックスやその中のボックスファイルに対して、ユーザ機能を利用して不正な操作が行われる可能性を想定している。

本TOEで、MFPの諸機能を利用するにあたって、ユーザ及び管理者を識別認証する機能（以上、「ユーザ機能」、「管理者機能」）、グループボックスに対するアクセス制御機能、グループボックスに関する設定の変更を管理者及びユーザに制限する機能（以上、「ボックス機能」）、ユーザに関する設定の変更を管理者及び許可されたユーザに制限する機能（以上、「管理者機能」、「ユーザ機能」）を保持することで、グループボックス及びユーザの設定の変更は管理者及び許可されたユーザのみに制限され、グループボックスの操作は正規のユーザのみに制限されることとなり、ユーザ機能を利用して不正な操作が行われることを防いでいる。

また、本TOEは、ユーザの識別認証機能において、本TOEの範囲外であるActive Directoryによるユーザ情報管理サーバから認証情報の取得を行うための機能（以上、「外部サーバ認証動作サポート機能」）も保持している。

（６）脅威「T.ACCESS-SECURE-PRINT（ユーザ機能を利用したセキュリティ文書プリントファイル及び認証&プリントファイルへの不正なアクセス）」に対抗するためのセキュリティ機能
本脅威は、ユーザ機能を利用したセキュリティ文書プリントファイル、認証&プリントファイルに対して不正な操作が行われてしまう可能性を想定して

いる。

本TOEで、MFPの諸機能を利用するにあたって、ユーザ及び管理者を識別認証する機能（以上、「ユーザ機能」、「管理者機能」）、セキュリティ文書パスワードによる認証機能、認証&プリントファイルを登録したユーザを識別認証する機能、セキュリティ文書プリントファイル及び認証&プリントファイルに対するアクセス制御機能、セキュリティ文書プリントファイル及び認証&プリントファイルに関する設定の変更を管理者に制限する機能（以上、「セキュリティ文書プリント機能」）、ユーザに関する設定の変更を管理者及び許可されたユーザに制限する機能（以上、「管理者機能」、「ユーザ機能」）を保持することで、セキュリティ文書プリントの設定の変更は管理者に、ユーザの設定の変更は管理者及び許可されたユーザのみに制限され、セキュリティ文書プリントファイル及び認証&プリントファイルの操作は正規のユーザのみに制限されることとなり、ユーザ機能を利用して不正な操作が行われることを防いでいる。

また、本TOEは、ユーザの識別認証機能において、本TOEの範囲外であるActive Directoryによるユーザ情報管理サーバから認証情報の取得を行うための機能（以上、「外部サーバ認証動作サポート機能」）も保持している。

（7）脅威「T.UNEXPECTED-TRANSMISSION（想定外対象先への送受信）」に対抗するためのセキュリティ機能

本脅威は、送信に関係するネットワーク設定、MFPのアドレスに関係するネットワーク設定、PC-FAX動作設定、TSI受信設定を不正に変更された場合に想定外対象先へ情報が送信されてしまう可能性を想定している。

本TOEで、管理者を識別認証する機能、ネットワーク設置、PC-FAX動作設定、TSI受信設定等の変更を管理者のみに制限する機能（以上、「管理者機能」）を保持することで、ネットワーク設置、PC-FAX動作設定、TSI受信設定等の変更は管理者に制限され、想定外対象先へ情報が送信されてしまうことを防いでいる。

（8）脅威「T.ACCESS-SETTING（セキュリティに関係する機能設定条件の不正変更）」に対抗するためのセキュリティ機能

本脅威はセキュリティに関係する特定の機能設定を変更されることにより、結果的にボックスファイル、セキュリティ文書プリントファイルや認証&プリントファイルの漏洩に発展する可能性を想定している。

本TOEで、管理者を識別認証する機能（以上、「管理者機能」、「SNMP管理者機能」）、サービスエンジニアを識別認証する機能（以上、「サービスモード機能」）、セキュリティに関係する特定の機能設定を管理者及びサービスエンジニアに制限する機能（以上、「管理者機能」、「SNMP管理者機能」、「サー

ビスモード機能」）を保持することで、セキュリティに関係する特定の機能設定の変更は管理者及びサービスエンジニアに制限され、結果的にボックスファイル、セキュリティ文書プリントファイルや認証&プリントファイルの漏洩に発展することを防いでいる。

（9）脅威「T.BACKUP-RESTORE（バックアップ機能、リストア機能の不正な使用）」に対抗するためのセキュリティ機能

本脅威は、バックアップ機能、リストア機能が不正に利用されることにより、ボックスファイル、セキュリティ文書プリントファイルや認証&プリントファイルが漏洩する可能性がある他、パスワード等秘匿性のあるデータが漏洩する、各種設定値等が改ざんされた結果、ボックスファイル、セキュリティ文書プリントファイルや認証&プリントファイルが漏洩する可能性を想定している。

本TOEで、管理者を識別認証する機能、バックアップ機能、リストア機能の使用を管理者のみに制限する機能（以上、「管理者機能」）を保持することで、バックアップ機能、リストア機能の使用は管理者に制限され、ボックスファイル、セキュリティ文書プリントファイル、認証&プリントファイル、パスワード等秘匿性のあるデータが漏洩することを防いでいる。

（10）脅威「T.BRING-OUT-CF（CFの不正な持ち出し）」に対抗するためのセキュリティ機能

本脅威は、CFを持ち出されることにより、CF内の情報が漏洩する可能性や、情報やTOEが改ざんされて設置されることによって不正な操作が行われる可能性を想定している。

本TOEの範囲外であるCFでCFロックパスワードによる認証が完了するまで書き込みを許可しないCFロック機能を利用し、本TOEで、CFロック機能等を持つCFと連動するための機能（以上、「CFロック動作サポート機能」）を保持することで、CFからの情報の読み出しにはCFロックパスワードが要求されることとなり、MFPに接続されているCFを不正に持ち出して解析することによりCFに格納された情報が漏洩することを防いでいる。

本TOEで、CFがCFロック機能を持つ正当なCFであることを検証する機能（以上、「CF検証機能」）を保持することで、CFロック機能を持つ正当なCFのみに情報が格納されること、正当なTOEで動作することとなり、MFPに接続されているCFがCFロック機能を持たないCFにすりかえられ、そのCFが持ち出されて情報が漏洩することや、情報やTOEが改ざんされて設置されることによって不正な操作が行われることを防いでいる。

（11）組織のセキュリティ方針「P.COMMUNICATION-DATA（画像ファイルのセキュアな通信）」を満たすためのセキュリティ機能

本組織のセキュリティ方針は、ネットワーク上に流れる画像ファイルについて、秘匿性を確保するために、組織・利用者が希望する場合において正しい相手先へ信頼されるパスを介した処理を行う、または暗号化すること規定している。希望に応じて対応できればよいため、すべての通信においてセキュアな通信機能を提供する必要はなく、セキュリティ文書プリント、認証&プリントファイル、ボックスファイルを扱うにあたり、MFPと利用者の使うクライアントPC間で最低限1つの手段が提供される必要がある。

本TOEにおいて、秘匿性のある画像データを含むセキュリティ文書プリントファイル、認証&プリントファイル、ボックスファイルに対して、MFPからクライアントPC、またはクライアントPCからMFPといった画像の送受信において正しい相手先に高信頼チャネルを提供する機能（以上、「高信頼チャネル機能」）、秘匿性のある画像データを含むボックスファイルに対してS/MIMEで送信するための暗号鍵生成機能、ボックスファイルの暗号化機能、S/MIMEで送信するための暗号鍵の暗号化機能（以上、「S/MIME暗号処理機能」）、管理者を識別認証する機能、高信頼チャネルやS/MIMEに関する設定の変更を管理者のみに制限する機能（以上、「管理者機能」）を保持することで、ネットワーク上に流れる画像ファイルを秘匿した形で送受信し、設定の変更を管理者に制限することで正しい相手先に送信可能となる。

3 評価機関による評価実施及び結果

3.1 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。

3.2 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20年11月に始まり、平成21年7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2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21年2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。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

3.3 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。

3.3.1 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3-1　開発者テストの構成図に示す。

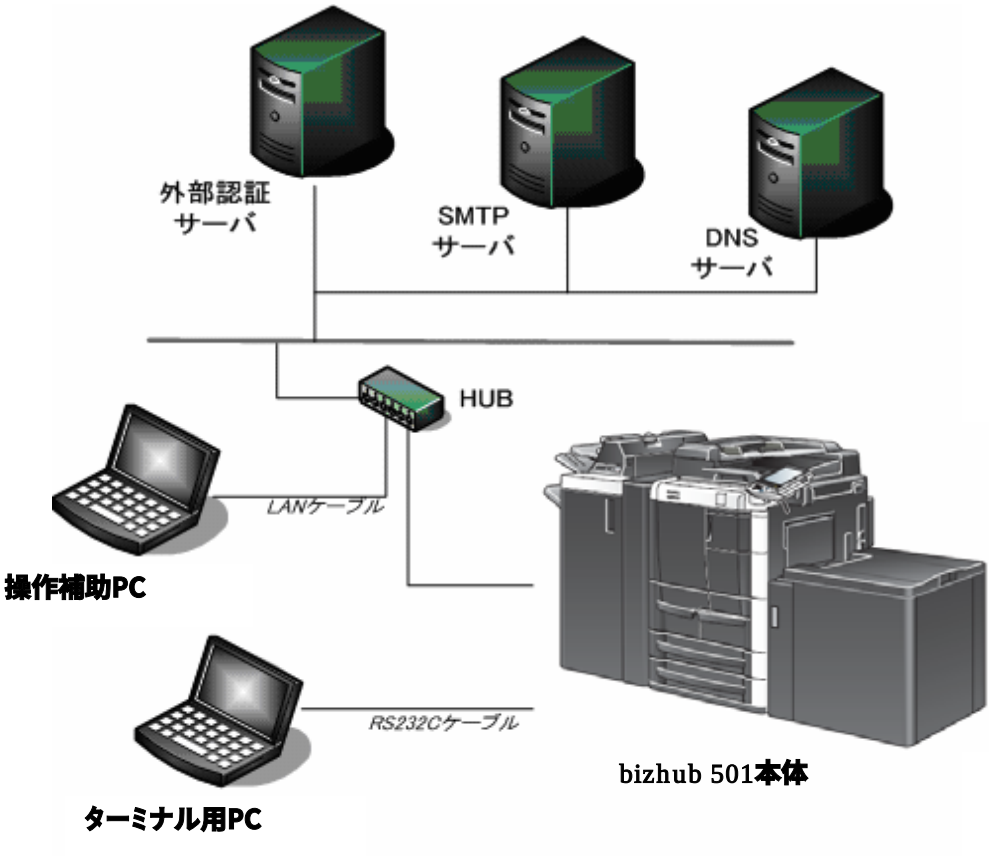

図3-1　開発者テストの構成図

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。

なお、TOEが搭載されるMFPとして、bizhub 501のみが選択されているが、評価者により以下の確認が行われた結果、問題ないと判断されている。

・bizhub 501、bizhub 421、bizhub 361の違いは、コピー/プリント速度及び耐久性保証値の違いだけであることを開発者から提供された資料により確認。
・bizhub 501に実施した開発者テストの一部を抽出したサンプリングテストをbizhub 361に実施し、得られたテスト結果が同一でありセキュリティ機能に影響を与えないことを確認。

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。

＜テスト手法＞
開発者が利用可能な外部インタフェースを持つ機能については、その外部インタフェースを使用してセキュリティ機能を実行することにより行い、開発者が利用可能な外部インタフェースを持たない機能については、セキュリティ機能の実行結果をダンプツールや通信データをキャプチャするツールにより取得し、解析するという方法で実施された。

＜テストで使用したツール等＞
テストで使用したツール等を表3-1に示す。

表3-1 開発者テストで使用したツール等

ハードウェア・ソフトウェア名称	概要・利用目的
疑似交換機	FAX通信を行う為の装置。疑似交換機を使用することにより、MFP本体と、通信対向機でFAXの通信が行える。
FAX対向機	FAX通信にて、MFP本体へFAX送信する為の対向機である。
KONICA MINOLTA 501 Series PCL Driver　Ver. 2.0.1.0	bizhub 501の同梱CDに内蔵されている専用プリンタドライバーソフトウェア
KONICA MINOLTA 501 Series XPS+ Driver　Ver. 2.0.1.0	bizhub 501の同梱CDに内蔵されている専用プリンタドライバーソフトウェア
Internet Explorer Ver.6.0.2900.2180	汎用のブラウザソフトウェア．操作補助PC上でPSWCを動作させるのに用いる、またSSL/TLS確認ツールとして使用する。
Fiddler Ver.1.2.0.0	http他のWebアクセスのモニター＆解析ツール．MFP本体と操作補助用PC間でHTTPSプロトコルのテストを行うために使用する
Open APIテストツール Ver.7.2.0.5	Open APIの評価用に作られた専用テストツール．Open APIの殆どのテストは、このツールにて通信レベルでの機能確認を行う
SocketDebugger Ver.1.12	TCP-Socketのテストツールとして使用する。
WireShark Ver0.99.5	LAN上の通信をモニター＆解析するツール．通信ログ取得に使用する
Mozilla Thunderbird Ver. 2.0.0.12	汎用メーラーソフト。操作補助PC上でS/MIMEメール確認用ツールとして使用する。
Open SSL Ver.0.9.8.g	SSLおよびハッシュ関数の暗号化ツールソフトウェア．

ハードウェア・ソフトウェア名称	概要・利用目的
MG-SOFT MIB Browser Professional SNMPv3 Edition（以後MIB Browserと省略） Ver.10.0.0.4044	MIB専用ブラウザソフトウェア．SNMP関連のテストに使用する
Tera Term Pro Ver.4.10	ターミナル用PCで動作させるターミナルソフトウェア. MFP本体と接続して、TOEの状態をモニターするためにMFP本体に内蔵されているターミナルソフトウェアを動作させるために使用する
ディスクダンプエディタ Ver.1.33	HDDの内容を表示させるツールソフトウェア
TamperIE Ver.1.0.1.13	Webブラウザを使ってパブリックユーザによるログインを行った際､TamperIEを使ってPOSTパラメタを変更する。
Stirling Ver.1.31	暗号鍵、デコードS/MIMEメッセージの内容確認、プリントファイルの編集用のバイナリエディタとして使用する。
FFFTP Ver.1.92a	FTPクライアントソフトとして使用する。
Microsoft Office Excel 2007 12.0.6123.1000	エクスポートファイルの内容確認用ソフトとして使用する。
MIME Base64 エンコード／デコード v1.0	S/MIMEメッセージのEncode/Decode確認ツールとして使用する。
PageScope Data Administrator（PSDA）with Device Set-Up and Utilities Ver. 1.0.2000.21092	複数台のMFPに対応する管理者用デバイス管理ツール（下記2つのプラグインソフトの起動が可能）
HDD Backup Utility Ver. 1.3.01000.1050	HDD Backup Utility は、ネットワーク上のMFP（複合機）に搭載されている記録メディアのバックアップ（保存）とリストア（復元）を行うユーティリティである。
PageScope Data Administrator（PSDA） Ver. 4.1.2000.12051	MFP本体に、EmailやFaxなどの宛先情報の登録や、ユーザへの使用制限の設定を行うためのツール。OpenAPIインタフェース確認ツールとして使用する。
PageScope Box Operator（PSBO）	ハードディスクに保存されたイメージ文書の取得、印刷などを行なうためのツール。

ハードウェア・ソフトウェア名称	概要・利用目的
Ver. 3.2.01000	TCP Socketインタフェース確認ツールとして使用する。
PageScope Web Connection（PSWC） Ver. 3.2.1	MFP本体に内蔵されており、ブラウザを利用して、本体の状態確認/設定を行うためのツール。 HTTPインタフェース確認ツールとして使用する。
sslproxy Ver.2.0	操作補助PC内にあり、本体装置と操作補助PCのブラウザソフトとの間に入っているプロキシソフト。本体装置とはSSLで通信して、ブラウザソフトとは非SSLでやり取りするので、sslproxy によりSSLによる暗号化を避けてFiddler、SocketDebuggerでのモニターが可能となる。
Black Jumbo Dog Ver4.1.3	イントラネット用の簡易サーバソフトウェア。 S/MIMEテスト時に、Web・メールサーバ機能として使用する。

b. 実施テストの範囲

テストは開発者によって199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。

3.3.2 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. 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、以下の観点での独立テストを考案した。

＜テストの観点＞

①開発者テストの状況を踏まえ、より多くのセキュリティ機能をテストする。

②すべての確率的・順列的メカニズムをテスト対象とする。

③確率的・順列的メカニズムのテストにおいて、TSFIへのパスワードの入力方式の違いによるふるまいをテストする。

④開発者テストの厳密さを踏まえ、必要と判断されるバリエーションをテストする。

⑤インタフェースの複雑性を踏まえ、必要と判断されるバリエーションをテストする。

⑥革新的または一般的でない特徴を持つインタフェースについて、必要と判断されるバリエーションをテストする。

b. 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。

＜テスト手法＞

評価者が利用可能な外部インタフェースを持つ機能についてはその外部インタフェースを使用してセキュリティ機能を実行することにより行い、評価者が利用可能な外部インタフェースを持たない機能については、セキュリティ機能の実行結果をダンプツールや通信データをキャプチャするツールにより取得し、解析するという方法で実施された。

＜テストで使用したツール等＞

テストで使用したツール等は、開発者テストと同様である。

＜テストの観点とテスト概要＞

独立テストの観点ごとのテスト概要を表3-2に示す。

表3-2 独立テストの観点とテスト概要

独立テストの観点	テスト概要
観点①	開発者が実施したテストに追加して確認する必要があると判断したテストを実施した。
観点②	ユーザの識別認証等の確率的・順列的メカニズムに着目し、文字桁数及び文字種類を変化されたテストを実施した。
観点③	パスワードの入力方式の違いによるふるまいを確認するために、動作させるインタフェースを考慮してテストを実施した。
観点④	開発者が実施したテストに追加して確認する必要があると判断した、HDD検証機能、CFロック検証機能、WebDAVサーバパスワード変更機能、暗号化の状況を確認するテストを実施した。
観点⑤	ボックスの種類の組み合わせによる複雑度に着目し、ボックスの種類を変更した場合の動作を確認するテストを実施した。
観点⑥	HDD検証機能、CFロック検証機能は革新的または一般的でない機能と判断し、動作を確認するテストを実施した。

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。

3.3.3 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。

＜侵入テストを必要とする脆弱性＞

①想定外のサービスが起動している可能性がある。

②脆弱性検査ツールにより公知の脆弱性が検出される可能性がある。

③入力データのバリエーションによって、TOEのふるまいに影響を与える

可能性がある。
④セッション情報の推測が容易である可能性がある。
⑤電源のON/OFFによりセキュリティ機能に影響する可能性がある。
⑥利用者の排他制御が適切に行われない可能性がある。
⑦CFロックパスワードの設定状況によりセキュリティ機能に影響する可能性がある。

b. 実施テストの範囲

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。

＜テスト環境＞

評価者が実施した侵入テストの構成を図3-2に示す。

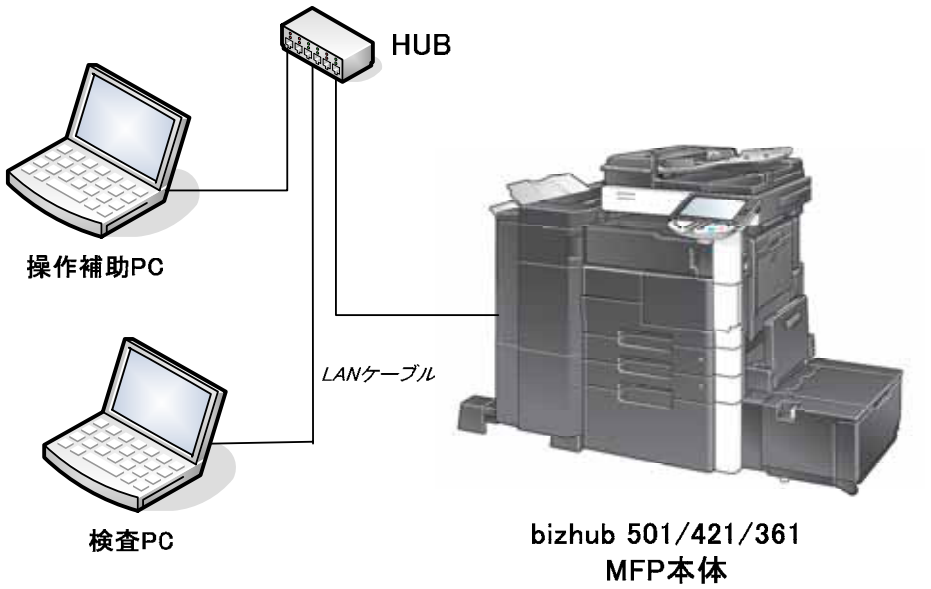

図3-2 侵入テストの構成図

＜テスト手法＞

パネルを操作してTOEに刺激を与え、そのふるまいを目視により検査する方法、操作補助PCを操作してネットワーク経由でTOEにアクセスすることにより、そのふるまいを目視で確認する方法やテストツールを使ってパラメタ等を改ざんし、そのふるまいをテストツールで確認する方法、検査PCを操作して脆弱性検査ツールによる公知の脆弱性をスキャンする方法で実施された。

＜テストで使用したツール等＞

テストで使用したツール等を表3-3に示す。

表3-3 侵入テストで使用したツール等

テスト構成環境	詳細
検査対象 （TOE）	・bizhub 501/421/361に搭載されたTOE （システム制御部：A0R50Y0-0100-G00-20、BIOS制御部：A0R50Y0-1D00-G00-11） ・ネットワーク構成 MFP毎にハブまたはクロスケーブルに接続し、侵入テストを実施した。
操作補助PC	・Windows XP SP2で動作するネットワーク端子付きのPC。 ・表3-1で示されているツールも利用。 （Fiddler、OpenAPIテストツール、SocketDebugger等） ・PSWC（PageScope Web Connectionの略）、Https、TCPSocket、OpenAPI、SNMP等を用いてMFPにアクセスし、ネットワーク設定等を実施することが可能。また、TamperIEの利用も可能。
検査PC	・検査PCは共にWindows XP SP2で動作するネットワーク端子付きのPCであり、本端末をクロスケーブルでMFPに接続し、脆弱性テストを実施している。 ・テストツールの説明 ① snmpwalk Version 3.6.1 ・MIB情報取得ツール。 ② openSSL Version 0.9.8d ・SSL及びハッシュ関数の暗号化ツール。 ③ Nesuss 3.2.1.1 ・システム上に存在する脆弱性を検査するセキュリティスキャナ。 ④ TamperIE 1.0.1.13 ・Internet Explorer等の一般的なWebブラウザから送信されるデータを任意のデータに改ざんするWebプロキシツール。 ⑤ sslproxy Version 2.0 ・SSL-プロキシサーバソフトウェア。 ⑥ Fiddler 2.2.0.7 ・HTTPのやり取りをモニターするWebデバッガー。 ⑦ Wireshark 1.06 ・パケットアナライザ。 ⑧ Nikto Version 2.03 ・CGIの公知の脆弱性検査ツール。

＜懸念される脆弱性とテストの概要＞

懸念される脆弱性ごとのテスト概要を表3-4に示す。

表3-4 懸念される脆弱性とテスト概要

懸念される脆弱性	テスト概要
脆弱性①	Nessus等のツール及び動作検証により、悪用可能でないか確認するテストを実施した。
脆弱性②	Nessus等のツール及び結果分析により、悪用可能でないか確認するテストを実施した。
脆弱性③	ネットワーク経由で入力するパラメタ等を編集して送信することにより、セキュリティ機能のふるまい（ドメイン分離、バイパス、干渉

懸念される脆弱性	テスト概要
	等）に影響を与えないことを確認するテストを実施した。
脆弱性④	セッション維持のためのメカニズムが一意性を保っていることを確認するテストを実施した。
脆弱性⑤	強制的な電源OFF/ONにより、初期化プロセス、画面表示等のセキュリティ機能に影響を与えないことを確認するテストを実施した。
脆弱性⑥	パネルとネットワーク経由で同時にアクセスし、排他制御が行われることを確認するテストを実施した。
脆弱性⑦	CFロックパスワードの設定状況によりセキュリティ機能のふるまいに影響を与えないことを確認するテストを実施した。

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。

3.4 評価結果

3.4.1 評価結果

評価報告書をもって、評価者は本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。

3.4.2 評価者コメント/勧告

・ガイダンスに従い、CFロック機能のCFロックパスワードは機器毎に一意となるように設定する必要がある。

・HDDやCFからの直接的なロックパスワードの読み出しのための解析については、専用機器を使用する必要性から残存脆弱性と判断しているが、専用機器や解読サービスが安価に提供されることにより、それらが悪用され、各種ロックパスワードが容易に解析される可能性が高まる。よって、当該事項を脅威と捉える消費者は、オプションとなっている暗号化機能による画像データの暗号化を検討することが望ましい。

4 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正しく反映されていること。
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。

5 結論

5.1 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。

5.2 注意事項

・ユーザ認証機能で外部サーバ認証方式を選択する場合、Active Directoryを利用した外部サーバ認証方式を利用することを前提としており、TOEは、TOEの範囲外であるActive Directoryで管理されている識別認証の情報を正当なものとして受け入れて動作する。

・オプションパーツであるFAXユニットが未装着の場合、FAXの送受信に関わるセキュリティ機能が利用できなくなるだけであり、その他のセキュリティ機能の動作には影響しない。

6 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。

API	Application Programming Interface（API）
BIOS	Basic Input/Output System（BIOS）
CF	CompactFlash（コンパクトフラッシュ）
DNS	Domain Name System（DNS）
FTP	File Transfer Protocol（FTP）
HDD	Hard Disk Drive（ハードディスクドライブ）
HTTPS	HyperText Transfer Protocol Security（HTTPS）
MFP	Multiple Function Peripheral（デジタル複合機）
MIB	Management Information Base（MIB）
NVRAM	Non-Volatile Random Access Memory（NVRAM）
RAM	Random Access memory（RAM）
SMB	Server Message Block（SMB）
SMTP	Simple Mail Transfer Protocol（SMTP）
SNMP	Simple Network Management Protocol（SNMP）
SSL/TLS	Secure Socket Layer/Transport Layer Security（SSL/TLS）
S/MIME	Secure Multipurpose Internet Mail Extensions（S/MIME）
TSI	Transmitting Subscriber Identification（TSI）
USB	Universal Serial Bus（USB）
WebDAV	Web-based Distributed Authoring and Versioning（WebDAV）

本報告書で使用された用語の定義を以下に示す。

BIOS	コンピュータに接続された周辺機器を制御するプログラム群のこと。
CFロック機能	CFにパスワードを設定し、パスワードに一致しないと読み書き

	することができなくなる機能のこと。
CFロックパスワード	CFの読み書きが禁止されている状態を解除するためのパスワードのこと。
DNS	インターネットでドメイン名とIPアドレスの関係を管理するプロトコルのこと。
FTP	TCP/IPネットワークで使うファイル転送プロトコルのこと。
HDDロック機能	HDDにパスワードを設定し、パスワードに一致しないと読み書きすることができなくなる機能のこと。
HDDロックパスワード	HDDの読み書きが禁止されている状態を解除するためのパスワードのこと。
HTTPS	WebサーバとクライアントのSSLによる暗号化機能を追加したプロトコルのこと。
MIB	SNMPを利用して管理される各種機器が公開している各種設定情報のこと。
NVRAM	電源を切っても記憶がなくならない不揮発性の性質を持つ、ランダムにアクセスできるメモリのこと。
PageScope Web Connection	MFP本体に内蔵されており、ブラウザを利用して、本体の状態確認/設定を行うためのツールのこと。
PC-FAX動作	FAX受信時に指定された情報に基づき、受信画像データの保存ボックス振り分け処理を行う動作のこと。
SMB	Windowsでファイル共有、プリンタ共有を実現するプロトコルのこと。
SMTP	TCP/IPでメールを転送する時のプロトコルのこと。
SNMP	ネットワーク経由で各種機器を管理するためのプロトコルのこと。
SNMPパスワード	TOEで使用されているSNMP v3を利用する場合に利用者を確認するためのパスワード（Privacyパスワード、Authenticationパスワード）の総称。
SSL/TLS	インターネット上で情報を暗号化してやり取りするプロトコルのこと。
S/MIME	電子メールの暗号化方式の標準のこと。RSAの公開鍵暗号方式を用いてメッセージを暗号化して送受信。認証機関が発行した電子証明書が必要。
TSI受信	送信者毎に、保管すべきボックスを指定することができる機能のこと。
WebDAV	HTTP1.1を拡張した仕様で、Webサーバ上のファイル管理を目的としたプロトコルのこと。
暗号化ワード	暗号化キットにおいて暗号化・復号処理を行う際の暗号鍵を生成

	する元となる情報のこと。
オフィスLAN	TOEが接続され、スイッチングハブ等の利用、盗聴の検知機器の設置等オフィスの運用によって、盗聴されず、外部とはファイアウォール等を介して接続されるネットワークのこと。
管理者モード	MFPに対して管理者に許可された操作を行うことが可能な状態のこと。
外部ネットワーク	TOEが接続されるオフィスLANとファイアウォール等によりアクセス制限されたネットワークのこと。
サービスモード	MFPに対してサービスエンジニアに許可された操作を行うことが可能な状態のこと。
セキュリティ文書パスワード	セキュリティ文書プリントファイルに対する操作を行う前に許可された利用者であるかどうかを確認するためのパスワードのこと。
セキュリティ文書プリントファイル	セキュリティ文書プリントによって登録される画像ファイルのこと。
セキュリティ文書プリント	プリンタドライバでセキュリティ文書パスワードを指定し、MFPからの印刷はそのパスワードで認証された場合に制限する印刷方法のこと。
フラッシュメモリ	EEPROM構造を高速・高集積化し、一括型の消去機構を搭載したメモリデバイスのこと。
ボックスファイル	個人ボックス、共有ボックス、グループボックスに保管される画像ファイルのこと。

7 参照

[1] bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 全体制御ソフトウェア A0R50Y0-0100-G00-20 A0R50Y0-1D00-G00-11 セキュリティターゲット バージョン1.07 2009年4月20日 コニカミノルタビジネステクノロジーズ株式会社

[2] 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

[3] 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

[4] 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

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 1 September 2006 CCMB-2006-09-001

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

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

[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）

[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）

[10] 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）

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

[12] 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）

[13] bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 全体制御ソフトウェア 評価報告書 第2版 2009年6月8日 みずほ情報総研株式会社 情報セキュリティ評価室