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23年3月24日 (IT認証1346)
認証番号	C0313
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 C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 全体制御ソフトウェア 英語名　：bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Control Software
TOEのバージョン	A0ED0Y0-0100-GM0-24
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23年8月31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 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 リリース3
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 リリース3

評価結果：合格

「日本語名：bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 全体制御ソフトウェア、英語名：bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Control Software バージョン：A0ED0Y0-0100-GM0-24」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

この認証報告書は、コニカミノルタビジネステクノロジーズ株式会社が開発した「日本語名：bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 全体制御ソフトウェア、英語名：bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Control Software バージョン：A0ED0Y0-0100-GM0-24」（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23年8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に関心を持つ消費者や調達者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書の付属書であるセキュリティターゲット（以下「ST」という。）を併読されたい。特に本TOEのセキュリティ機能要件、保証要件及びその十分性の根拠は、STにおいて詳述されている。

本認証報告書は、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が適合する保証要件に基づいた認証結果を示すものであり、個別のIT製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本TOEの機能、運用条件の概要を以下に示す。詳細は2章以降を参照のこと。

1.1.1 保証パッケージ

本TOEの保証パッケージは、EAL3である。

1.1.2 TOEとセキュリティ機能性

本TOEが搭載される、bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405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 C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 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内に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、ASICを利用し、HDDに書き込まれる画像データを含むすべてのデータを暗号化することにより、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により、HDDのすべてのデータを完全に削除する機能や、FAX機能を踏み台として内部ネットワークにアクセスする危険性に対して、FAX公衆回線網からのアクセスを制御する機能を提供する。

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。

1.1.2.1 脅威とセキュリティ対策方針

本TOEは、以下のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

- MFPを返却または廃棄した後にMFPから情報が漏洩することを脅威と想定する。この脅威に対抗するために、TOEは記憶媒体の情報を消去する機能を持つ。
- MFPからHDDを持ち出され、持ち出されたHDDから情報が漏洩することを脅威と想定する。この脅威に対抗するために、TOEは、TOEの範囲外であるASICの暗号化機能を利用して情報を暗号化してからHDDに記録する。
- 個人ボックス、共有ボックス、グループボックスに保存されるボックスファイルに対し、許可されないアクセスが行われることを脅威と想定する。この脅威に対抗するために、TOEはユーザを識別・認証し、TOEが保持しているユーザ及びボックスファイルの情報に基づいてアクセスの可否を判定する。
- セキュリティ文書ファイル、認証&プリントファイルに対し、許可されないアクセスが行われることを脅威と想定する。この脅威に対抗するために、TOEはユーザを識別・認証し、セキュリティ文書ファイル、認証&プリントファイルを保存した本人のみがこれらのファイルを操作できるようにする。
- 以下のような原因で情報が漏洩することを脅威と想定する。
  - TOEからボックスファイルを送信したときに、利用者が意図したのと

は異なる送信先に送付されること

- TOEになりすまして、セキュリティ文書ファイル、認証&プリントファイルを詐取すること
- TOEがボックスファイルを受信したときに、利用者が意図したのとは異なる場所に保存されること

この脅威に対抗するために、TOEは識別・認証により管理者かどうかを確認し、管理者にのみ、送信先に関する設定、TOEになりすますための設定、保存先に関する設定の操作を許可する。

- セキュリティ強化機能の設定が変更されてしまうことで、情報の漏洩が防げない状態となることを脅威と想定する。この脅威に対抗するために、TOEは識別・認証により管理者またはサービスエンジニアかどうかを確認し、管理者またはサービスエンジニアに対してのみセキュリティ強化機能の設定の変更を許可する。
- バックアップ機能、リストア機能が悪用され、その結果、情報の漏洩や設定値の変更が起こることを脅威と想定する。この脅威に対抗するために、TOEは識別・認証により管理者かどうかを確認し、管理者にのみ、バックアップ機能、リストア機能の使用を許可する。

（補足） TOEはユーザ認証の機能を持つが、TOEの範囲外であるActive Directoryを利用してユーザ認証を行うこともできる。

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

この利用環境において、LANが外部ネットワーク(インターネット等、組織外のもの)と接続する場合も外部ネットワークからMFPにアクセスできないように管理され、LANを通る通信は盗聴されないように管理される。

管理者とサービスエンジニアは信頼できることが想定され、それ以外のユーザも自らのパスワードの秘密は守ることができることが想定される。

本TOEは、セキュリティ強化機能の設定が有効である状態で利用されることが想定される。

1.1.3 免責事項

・ ユーザ認証機能で外部サーバ認証方式を選択する場合の Active Directory の機能は、本評価で保証されたものではない。

・MFPに搭載されているASICの暗号化機能は、本評価で保証されたものではない。

・ FAXユニット制御機能は、オプションパーツであるFAXユニットが装着されている場合のみ有効である。

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セキュリティ認証申請手続等に関する規程」[2]、「ITセキュリティ評価機関承認申請手続等に関する規程」[3]に規定された内容に従い、評価機関によって本TOEに関わる機能要件及び保証要件に基づいてITセキュリティ評価が実施され、平成23年8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。

本TOEの評価がCC（[4][5][6]または[7][8][9]）及びCEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は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： 日本語名：bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 全体制御ソフトウェア

英語名 ：bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Control Software

バージョン： A0ED0Y0-0100-GM0-24

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

製品が評価･認証を受けた本TOEであることを、TOEの設置の際等に、利用者は以下のようにサービスエンジニアに依頼して確認することができる。

サービスエンジニアのパネル操作により、TOEのバージョンとチェックサムを表示させることができる。TOEのバージョンを確認し、チェックサムがサービスマニュアルに記載されたものと同じであることを確認することにより、設置された製品が評価を受けた本TOEであることを確認できる。

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。

本TOEは、以下のデータを扱う。

- セキュリティ文書ファイル
- 認証&プリントファイル
- ボックスファイル

これらのデータを意図しない漏洩から保護するために、TOEはこれらのデータまたは関連するデータへアクセスしようとする者を識別・認証し、アクセス制御を行う。さらに、これらのデータまたは関連するデータを記録した媒体からの漏洩を防ぐために、TOEは、ASICを活用しての暗号化機能と、データ消去機能を提供する。

本TOEは、消費者の要求のため、以下も実現する。

- これらのデータの通信路からの漏洩を防ぐための機能
- MFPのFAX公衆回線口から内部ネットワークにアクセスを許さないための仕組み

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人物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、調整等の保守管理を行う。一般には、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にアクセス可能な人物として、オフィス内に出入りする人物等が想定される。

3.2 セキュリティ機能方針

TOEは、3.2.1に示す脅威に対抗し、3.2.2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。

3.2.1 脅威とセキュリティ機能方針

3.2.1.1 脅威

本TOEは、表3-1に示す脅威を想定し、これに対抗する機能を備える。

表3-1 想定する脅威

識別子	脅 威
T.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、NVRAMを解析することにより、セキュリティ文書ファイル、ボックスファイル、認証&プリントファイル、オンメモリ画像ファイル、保存画像ファイル、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の秘匿情報が漏洩する。

識別子	脅　威
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、セキュリティ文書ファイル、ボックスファイル、認証&プリントファイル、オンメモリ画像ファイル、保存画像ファイル、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ファイル、ボックスファイル、認証&プリントファイル、オンメモリ画像ファイル、保存画像ファイル、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、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操作（コピー、移動、ダウンロード、印刷、送信等）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操作（コピー、移動、ダウンロード、印刷、送信等）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操作（コピー、移動、ダウンロード、印刷、送信等）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ファイル、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ファイルを操作（印刷等）することにより、セキュリティ文書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、他のユーザが保存した認証&プリントファイルを操作（印刷等）することにより、認証&プリントファイルが暴露される。

識別子	脅　威
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存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受信設定を変更し、共有ボックス等のボックスへの保存設定状態から、全ユーザ共通領域に保存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存領域に保存されて暴露される。 ※ 本脅威は、PC-FAX受信設定が、ボックスへの保存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。

3.2.1.2 脅威に対するセキュリティ機能方針

本TOEは、表3-1に示す脅威に対し、以下のセキュリティ機能方針で対抗する。

(1) 脅威「T.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のデータ領域に上書き削除を実行すると共にNVRAM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、又は廃棄となったMFPに接続されたHDD、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、又は不正な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ASICの暗号化機能を利用し、本TOEで、HDDに書き込むデータの暗号化を行う暗号鍵の生成(以上、「暗号化鍵生成機能」)、及びASICと連動するための機能(以上、「ASIC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。

(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存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存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」)、共有ボックスへのアクセスにおける識別認証機能、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許可された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存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ファイル、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、ネットワーク設定、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、ネットワーク設定、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やセキュリティ文書ファイル、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やセキュリティ文書ファイル、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、セキュリティ文書ファイル及び認証&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、セキュリティ文書ファイル及び認証&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、セキュリティ文書ファイル、認証&プリントファイルや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。

3.2.2 組織のセキュリティ方針とセキュリティ機能方針

3.2.2.1 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。

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.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（セキュリティ文書ファイル、ボックスファイル、認証&プリントファイル）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。
P.REJECT-LINE (公衆回線からのアクセス禁止)	公衆回線網から、MFPのFAX公衆回線口を介しての内部ネットワークへのアクセスは禁止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。

3.2.2.2 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機能を具備する。

(1) 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、又は暗号化することを規定している。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、セキュリティ文書ファイル、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、セキュリティ文書ファイル、認証&プリントファイル、ボックスファイルに対して、MFPとクライアント間における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」)、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。

(2) 組織のセキュリティ方針「P.REJECT-LINE(公衆回線からのアクセス禁止)」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、MFPに搭載されたFAXユニットのFAX公衆回線ロを経由した内部ネットワークへのアクセスを禁止すること規定している。本機能はMFPにFAXユニットを装着した場合に提供される。

本TOEにおいて、内部ネットワークに存在するデータに対して、公衆回線からFAXユニットのFAX公衆回線ロを経由してのアクセスを禁止する機能(以上、「FAXユニット制御機能」)を保持することで、FAXユニットのFAX公衆回線ロを経由した内部ネットワークへのアクセスを禁止することが可能となる。

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.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)	ユーザがTOEを利用する際、セキュリティ強化機能の設定が有効である。 (補足)セキュリティ強化機能を有効にすることで、一部の機能が使えなくなる。本STの「1.4.3.8 セキュリティ強化機能」に記載されている各設定の説明を参照のこと。

4.2 運用環境と構成

本TOEは、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MFPである、bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo$^+$ 360 / ineo$^+$ 280 / ineo$^+$ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 のいずれかに搭載される。

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

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(またはそれ以降)が提供するディレクトリサービスであるActive Directoryが必要となる。

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

以下における、ASIC及びActive Directoryの信頼性は本評価の範囲ではない。

- 本TOEは情報を暗号化してからHDDに記録する機能を持つが、その際の暗号化の演算は、MFPの一部であるASICによって行われる機能のため、TOEの範囲外であり、本評価の対象外である。
- 本TOEはユーザを認証する機能を持つが、ユーザ認証機能で外部サーバ認証方式を選択した場合には、認証処理に外部サーバのディレクトリサービスであるActive Directoryが使われる。
  外部サーバ認証方式を選択した場合、本TOEは外部サーバに対して認証情報を問合せ、認証情報を取得することでユーザ識別認証機能を提供している。
  外部サーバのActive Directoryによって行われる認証機能はTOEの範囲外であり、本評価の対象外である。

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

本TOEは、MFPの全体制御ソフトウェアであり、MFP本体内のMFP制御コントローラ上にあるフラッシュメモリ上に搭載され、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5-1に示す。

なお、デバイス接続I/Fキット、FAXユニットはMFPのオプションパーツである。本TOEの動作環境としては、デバイス接続I/FキットはBluetooth端末を利用する場合に、FAXユニットはFAX機能を利用する場合に装着されていることを想定している。

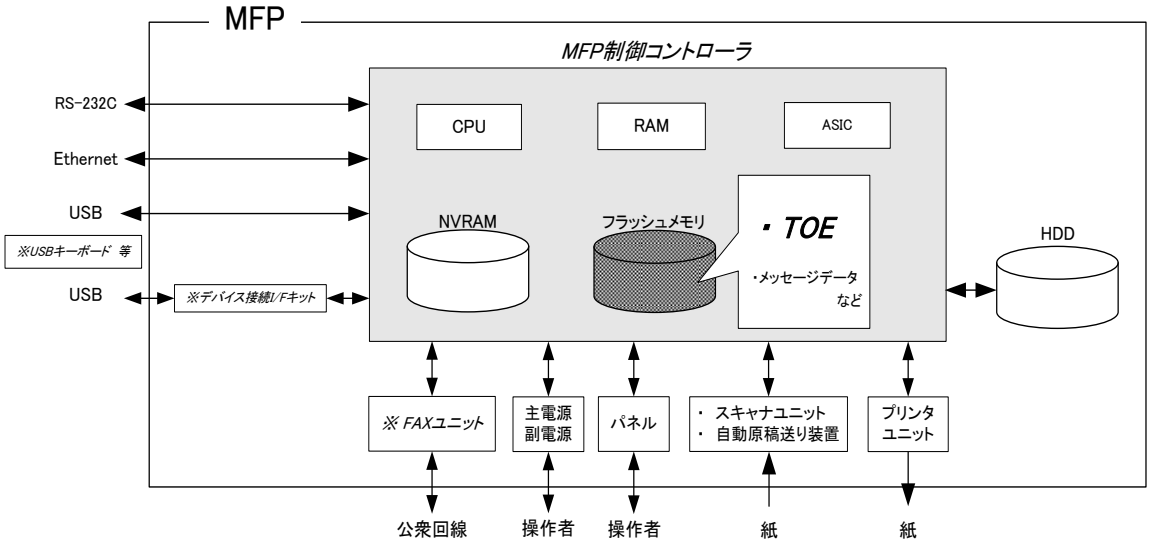

図5-1 TOEに関係するハードウェア構成

TOEは、OSの部分と、MFPの制御を行うアプリケーションの部分から構成される。MFPの制御を行うアプリケーションの部分は、さらに以下の部分から構成される。

- ネットワーク経由のインタフェースを提供する部分
  Ethernetの制御を行い、TCP/IPベースの通信機能を提供する。
  この部分で、通信の暗号化の機能も提供される。

- パネル経由のインタフェースを提供する部分
  パネルからの入力を受け付ける機能と、パネルの画面を描画する機能を持つ。

・ ジョブ管理を行う部分
ジョブとは、コピー、プリント、スキャン、FAX、ボックスファイル操作等の実行制御や動作順位を管理するための単位である。
ジョブは、「ネットワーク経由のインタフェースを提供する部分」または「パネル経由のインタフェースを提供する部分」からの操作や、FAXユニットからの受信を「各種デバイスを制御する部分」が受けた場合に発生し、登録される。
実際のジョブの実行は、以降の「共通の管理を行う部分」「HDDを扱う部分」「各種デバイスを制御する部分」を利用して実現する。

・ 共通の管理を行う部分
この部分で、各種の設定値が管理され、TOEの他の部分が設定値へアクセスするための手段が提供される。各種の設定値の中には認証情報等セキュリティ機能の実施に使われる情報も含まれる。
この部分では、識別・認証を実施する機能や、アクセス制御の機能も提供される。

・ HDDを扱う部分
この部分で、画像データの処理とHDDへの入出力の機能が提供される。
HDDへの入出力の機能では、書き込む際の暗号化と、読み込む際の復号が、ASICを利用して行われる。

・ 各種デバイスを制御する部分
スキャナユニット、プリンタユニット、FAXユニットを制御して、コピー、プリント、スキャン、FAXの実際の動作を実現する部分である。
また、FAXユニットから内部ネットワークをアクセスさせないような仕組みになっている。

・ サポートの機能を提供する部分
この部分で、MFPのサポートに使われる機能(MFPの診断のための機能、TOEの更新の機能)が提供される。

5.2 IT環境

図5-1に示した本TOEのIT環境を構成する要素について以下に示す。

(1) フラッシュメモリ

TOEであるMFP全体制御ソフトウェアのオブジェクトコードが保存される記憶媒体。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存される。

(2) 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存される記憶媒体。これらの設定値は「共通の管理を行う部分」で管理されるものである。

(3) ASIC

HDDに書き込まれるすべてのデータを暗号化するためのHDD暗号化機能を実装した特定利用目的集積回路。ASICは、「HDDを扱う部分」から利用される。

(4) HDD

容量250GB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存されるほか、伸張変換等で一時的に画像データ、送信宛先データが保存される領域としても利用される。「HDDを扱う部分」から読み書きされる。

(5) 主電源、副電源

MFPを動作させるための電源スイッチ。

(6) 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等を備えたMFPを操作するための専用コントロールデバイス。「パネル経由のインタフェースを提供する部分」により制御される。

(7) 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。「各種デバイスを制御する部分」により制御される。

(8) 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。「各種デバイスを制御する部分」により制御される。

(9) Ethernet

10BASE-T、100BASE-TX、Gigabit Ethernetをサポート。「ネットワーク経由のインタフェースを提供する部分」により制御される。

(10) USB

外部メモリへの画像のコピー、外部メモリからの画像のコピーやプリント、TOEのアップデート等を本インタフェースから実施できる。また、オプションパーツの接続インタフェースとして対応している。

オプションパーツには、Bluetooth端末から画像のコピーやプリントを行う場合に必要となるデバイス接続I/Fキット、パネル操作でのキー入力を補完するUSBキーボード等があり、外部メモリ等を含め使用できるようにする必要がある。

(11) RS-232C

D-sub9ピンを介して、シリアル接続することが可能。故障時等に本インタフェースを介してメンテナンス機能を使用することができる。また公衆回線と接続されるモデムと接続して、遠隔診断機能を利用することも可能。「サポートの機能を提供する部分」により制御される。

(12) FAXユニット

公衆回線を介してFAXの送受信や遠隔診断機能の通信に利用されるFAX公衆回線ロを持つデバイス。「各種デバイスを制御する部分」により制御される。

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。組織が希望する場合に購入するもので、FAXユニットの搭載は必須ではない。

6 製品添付ドキュメント

本TOEに添付されるドキュメントの識別を以下に示す。TOEの利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

＜管理者・一般利用者向けドキュメント＞

・bizhub C360 / C280 / C220 ユーザーズガイド　セキュリティ機能編　Ver.1.02
・bizhub C360 / C280 / C220 User's Guide [Security Operations]　Ver.1.02
・bizhub C7728 / C7722 User's Guide [Security Operations]　Ver.1.02
・ineo+ 360 / 280 / 220 User's Guide [Security Operations]　Ver.1.02
・VarioLink 3622c / 2822c / 2222c User's Guide [Security Operations]　Ver.1.02
・D407 / D406 / D405 User's Guide [Security Operations]　Ver.1.02

＜サービスエンジニア向けドキュメント＞

・bizhub C360 / C280 / C220 サービスマニュアル　セキュリティ機能編 Ver.1.03
・bizhub C360 / C280 / C220 / C7728 / C7722SERVICE MANUAL SECURITY FUNCTION　Ver.1.03
・ineo+ 360 / 280 / 220 SERVICE MANUAL　SECURITY FUNCTION Ver.1.03

・VarioLink 3622c / 2822c / 2222c SERVICE MANUAL SECURITY FUNCTION Ver.1.03

・D407 / D406 / D405 SERVICE MANUAL　SECURITY FUNCTION　Ver.1.03

7 評価機関による評価実施及び結果

7.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告された。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。

7.2 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23年3月に始まり、平成23年8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、サイト検査については、同シリーズの過去の実施状況を勘案し、構成管理システム、配付手続き、セキュリティ手段が異なる部分を中心に、平成23年5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施行状況の調査を行った。また、平成23年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。

7.3 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

7.3.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価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。

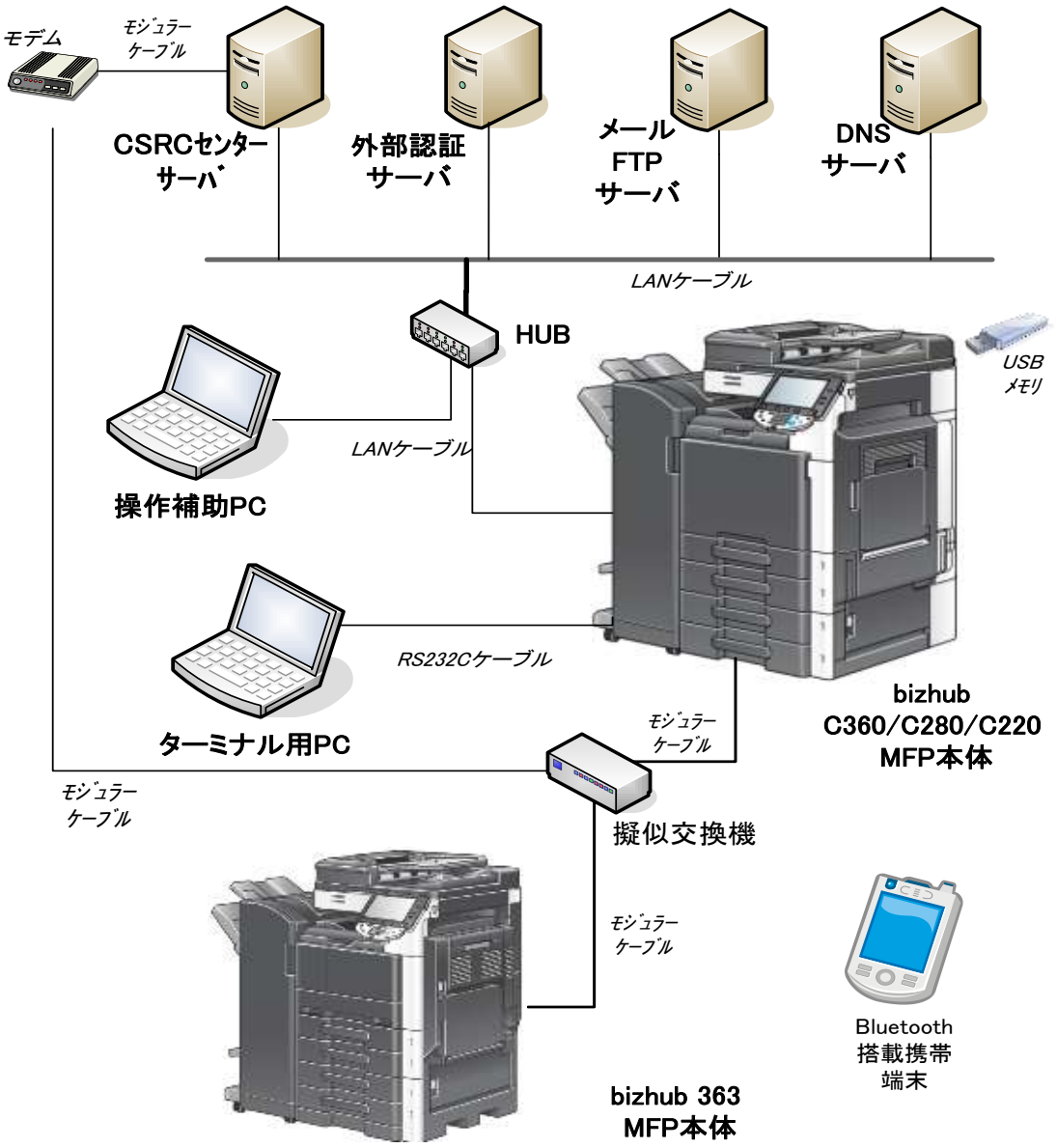

図7-1　開発者テストの構成図

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＞

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実施された。また、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。

＜開発者テストツール等＞

表7-1　開発テストツール

ツール名称	概要・利用目的
KONICA MINOLTA C360 Series PCL/XPS Ver.3.0.16.0	bizhub C360 / C280 / C220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. 6.0.2800.1106 (Win2000) Ver. 6.0.2900.2180 (WinXP)	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. 2.2.2.0	http他のWebアクセスのモニタ＆解析ソフトウェアツール。MFP本体と操作補助用PC間でHTTPプロトコルの確認、及びテストを行うために使用する。
Open APIテストソフトウェアツール Ver.7.2.0.5	Open APIの評価用に作られた専用テストソフトウェアツール。Open APIの殆どのテストは、このツールソフトウェアルを用いてメッセージレベルでの機能確認を行う。
SocketDebugger Ver. 1.12	TCP-Socketのテストソフトウェアツールとして使用する。
WireShark Ver. 1.2.2	LAN上の通信をモニタ＆解析するソフトウェアツール。通信ログ取得に使用する。

ツール名称	概要・利用目的
Mozilla Thunderbird Ver. 2.0.0.21	汎用メーラーソフトウェア。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. 0.9.8k(25-Mar-2009)	SSLおよびハッシュ関数の暗号化ソフトウェアツール。
MG-SOFT MIB Browser Professional SNMPv3 Edition 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. 4.29	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. 1.43	HDDの内容を表示させるソフトウェアツール。
Stirling Ver. 1.31	バイナリエディタソフトウェアツール。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として使用する。
FFFTP Ver. 1.92a	FTPクライアントソフトウェアとして使用する。
MIME Base64 エンコード/デコード Ver. 1.0	MIME Base64 のエンコード/デコードを行なうソフトウェアツール。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 with Device Set-Up and Utilities Ver. 1.003200.10051	複数台のMFPに対応する管理者用デバイス管理ソフトウェアツール。 (下記プラグインソフトウェアの起動が可能)
HDD Backup Utility (プラグイン) Ver. 1.3.03000 781	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 Box Operator (PSBO) Ver. 3.2.03000	ハードディスクに保存されたイメージ文書の取得、印刷等を行なうためのソフトウェアツール。 高信頼チャネル動作確認ツールとして使用する。

ツール名称	概要・利用目的
sslproxy Ver. 1.2	操作補助PC内にあり、本体装置と操作補助PCのブラウザソフトウェアとの間に入っているプロキシソフトウェア。 本体装置とはSSLで通信して、ブラウザソフトウェアとは非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でのモニタが可能となる。
Black Jumbo Dog Ver. 4.2.2	イントラネット用の簡易サーバソフトウェア。 メールサーバ、FTPサーバ機能として使用する。
CSRCセンターソフトウェア Ver. 2.6.1	CSRCのセンター用のサーバソフトウェア。 CSRCとは、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、MFPの機器の状態をリモートで管理する保守サービスである。

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348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。

7.3.2 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

評価者が実施したテストの構成は、開発者テストと同様の構成である。

独立テストは本STにおいて識別されているTOE構成と同一のTOEテスト環

境で実施されている。

なお、TOEが搭載されるMFPとして、bizhub C280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。

- C7728はC280に対応、C7722はC220に対応、仕向地により名称が異なるものである。
- ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405は、bizhub C360 / bizhub C280 / bizhub C220のOEM製品である。
- bizhub C360 / bizhub C280 / bizhub C220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した。

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。

＜テストの観点＞

① 開発者テストの状況を踏まえ、すべてのセキュリティ機能を対象とする。
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、又は一般的ではない特性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。
⑦ セキュリティ機能への影響が大きいと思われるパラメタを抽出し、入力データのバリエーション等を変更してテスト項目を設定した。

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＞
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実施された。また、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。

＜独立テストツール等＞
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。

＜独立テストの観点ごとの概要＞
独立テストの観点ごとのテスト概要を表7-2に示す。

表7-2 実施した独立テスト

独立テストの観点	テスト概要
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し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の厳密さを踏まえ、WebDAVサーバパスワード変更機能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	FAXユニット制御機能のふるまい、及びBluetooth端末の異常系のふるまいは革新的、又は一般的ではないと判断し、動作を確認するテストを実施した。
観点⑦	機能改良に関連し、セキュリティ機能への影響が大きいと思われるパラメタを抽出し、入力データのバリエーション等を変更してテスト項目を設定した。

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。

7.3.3 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。

＜侵入テストを必要とする脆弱性＞

① TOEに使われているコンポーネントに関連する想定外のサービスが起動している可能性がある。

② TOEに使われているコンポーネントに関連する公知の脆弱性の存在が懸念される。

③ ネットワーク経由で入力するパラメタ等は機能仕様で定められるが、入力の方法によっては機能仕様では想定されていないような入力が可能となり、TOEのふるまいに影響を与えることが懸念される。

④ Webインタフェースを持つことが機能仕様からわかるため、Webインタフェースに一般的に考えられる懸念としてセッションの乗っ取りが容易にできないかどうか開発証拠資料を探索したところ、懸念がないという確信には至らなかった。

⑤ セキュリティ機能をバイパスや改ざんされる懸念がないかどうかを開発証拠資料に対して探索したところ、電源のON/OFFのタイミングによってはそのような懸念があることが検出された。

⑥ 認証機能を提供する複数のタイプのインタフェースが存在することがSTからもわかる。開発証拠資料から異なるタイプのインタフェースからの認証が競合する場合を検討し、操作者が異なる権限で操作できてしまうことが懸念された。

⑦ セキュリティ強化機能の設定はHDD上にはないことが開発証拠資料からはわかるが、HDDの交換がセキュリティ強化機能に影響しないと確信できるようなテストは確認できない。

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＞

評価者が実施した侵入テストの構成を図7-2に示す。

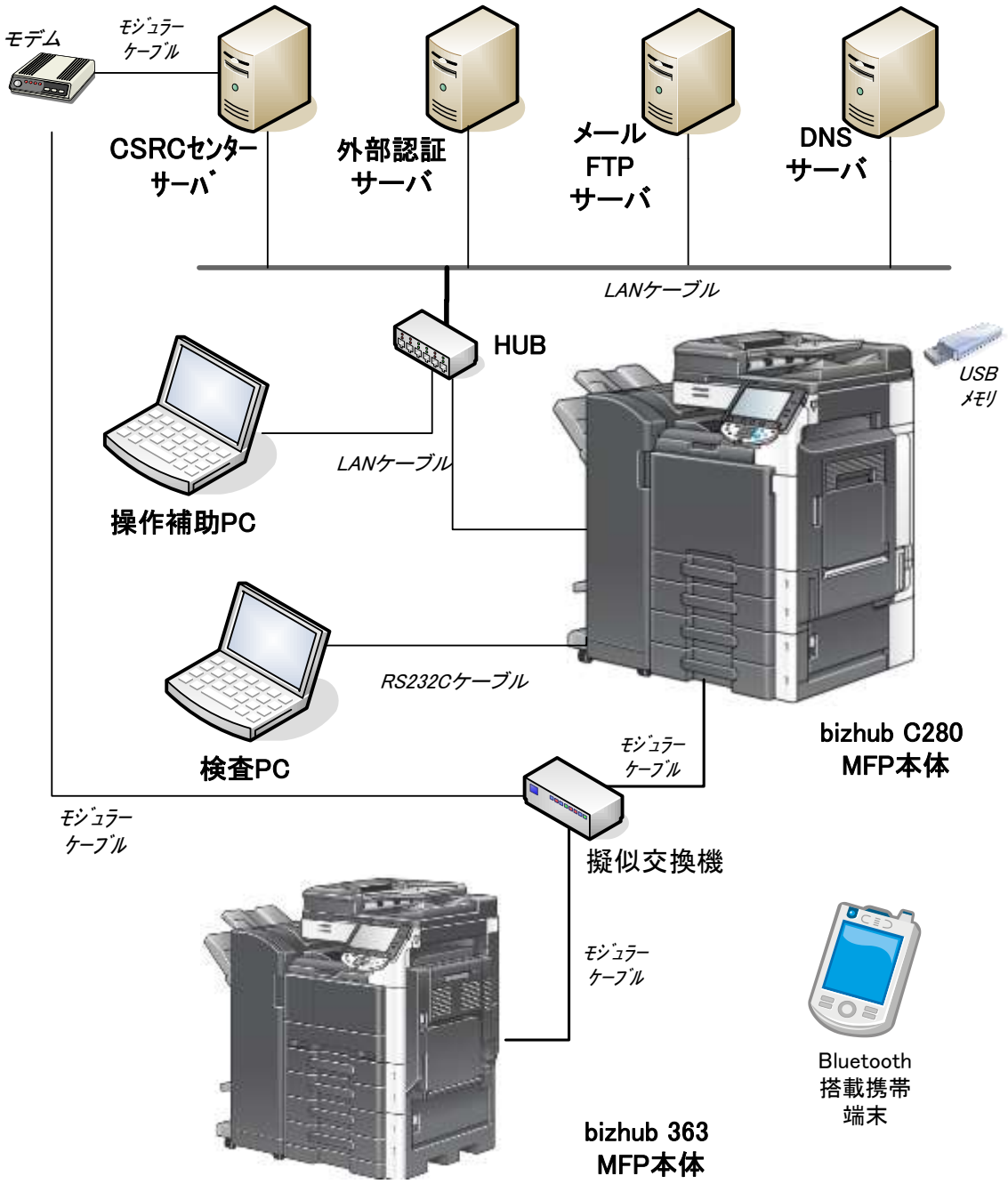

図7-2　侵入テストの構成図

＜侵入テスト手法＞

侵入テストは、以下の方法で実施された。

・ パネルを操作してTOEに刺激を与え、その振る舞いを目視により確認する方法。
・ 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。
・ 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。

＜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 C280 に搭載されたTOE (バージョン：A0ED0Y0-0100-GM0-24) ・ネットワーク構成 MFPごとにハブ、又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)またはWindows 2000(SP4)で動作するネットワーク端子付きのPC。 ・表7-1 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。

テスト構成環境	詳細
検査PC	・検査PCは共にWindows XP SP3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(プラグインや脆弱性データベースは2011年5月4日時点の最新版を適用している。) ① snmpwalk Version 3.6.1 ・MIB情報取得ツール。 ② openSSL Version 0.9.8r ・SSL、及びハッシュ関数の暗号化ツール。 ③ Nessus 4.4.1.(build 15078) ・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 v 1.2 2000/01/29 ・SSL-プロキシサーバソフトウェア。 ⑥ Fiddler 2.3.3.5 ・MS 社で提供する HTTP のやりとりをモニタする Web デバッガー。 ⑦ WireShark 1.4.6 ・800 以上のプロトコルを解析できるパケットアナライザソフト。 ⑧ Nikto Version 2.1.4 ・CGIの公知の脆弱性検査ツール。

＜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7-3に示す。

表7-3　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

懸念される脆弱性	テスト概要
	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	HDDの交換がセキュリティ強化機能の設定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

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。

7.4 評価構成について

(1) 動作機種について

本TOEは、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MFPである、bizhub C360、bizhub C280、bizhub C220、bizhub C7728、bizhub C7722、ineo+ 360、ineo+ 280、ineo+ 220、VarioLink 3622c、VarioLink 2822c、VarioLink 2222c、D407、D406、D405 のいずれかに搭載されることが想定されている。

これらの全ての機種において評価されたというわけではないが、7.3.2で示した理由により、これらの全ての機種において評価されたとみなすことができる。

(2) TOEの設定について

評価は、以下の設定で実施された。

- セキュリティ強化機能は「有効」
- ユーザ認証の方式は、以下のいずれか

「本体認証」

「外部認証」でActive Directoryを使用

これらの設定は、STで示されている設定の通りである。

7.5 評価結果

評価者は、評価報告書をもって本TOEがCEMのワークユニットすべてを満たしていると判断した。

評価では以下について確認された。

- PP適合：なし
- セキュリティ機能要件：　コモンクライテリア　パート2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

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。

7.6 評価者コメント/勧告

消費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。

認証機関は、本ST及び評価報告書において、問題点がないことを確認し、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、及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL3に対する保証要件を満たすものと判断する。

8.2 注意事項

・ 本TOEは、脅威に対抗するために、以下の機能に依存する(4.3参照)。
  - MFPに搭載されているASIC
  - Active Directory (ユーザ認証機能で外部サーバ認証方式を選択する場合)

  これらの機能の信頼性については、本評価で保証されたものではなく、運用者の判断となる。

・ オプションパーツであるFAXユニットが未装着の場合、セキュリティ機能であるFAXユニット制御機能は無効になる。(そのことは、その他のセキュリティ機能の動作には影響しない。)

・ セキュリティ強化機能を有効にすることで、一部の機能が使えなくなる。本STの「1.4.3.8 セキュリティ強化機能」に記載されている各設定の説明を注意深く確認することを推奨する。

・ S/MIME証明書の有効性(証明書失効リストへの照合)については、管理者が有効な証明書を登録するように管理すること。

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 C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 全体制御ソフトウェア A0ED0Y0-0100-GM0-24 セキュリティターゲット バージョン1.01　2011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

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。

API	Application Programming Interface (API)
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)
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。

Bluetooth	携帯端末等で数m程度の機器間接続に使われる短距離無線通信技術の一つこと。
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。
HTTPS	Webサーバとクライアントの間で安全な通信を行うために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。
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、保存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	ASIC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。
オフィス内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内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。
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存される画像ファイルのこと。

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23年2月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証申請手続等に関する規程, 平成23年2月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認申請手続等に関する規程, 平成23年2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 3, July 2009, CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: 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 C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo$^+$ 360 / ineo$^+$ 280 / ineo$^+$ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405　全体制御ソフトウェア A0ED0Y0-0100-GM0-24 セキュリティターゲット バージョン1.01　2011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

[13] bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo$^+$ 360 / ineo$^+$ 280 / ineo$^+$ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 全体制御ソフトウェア 評価報告書 初版 2011年8月11日 みずほ情報総研株式会社 情報セキュリティ評価室