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22年1月29日** (IT**認証**0285)
認証番号	C0276
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**	bizhub C360 / bizhub C280 / bizhub C220 PKI Card System Control Software
TOE**のバージョン**	A0ED0Y0-0100-GM0-31
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22年10月22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 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

「bizhub C360 / bizhub C280 / bizhub C220 PKI Card System Control Software バージョン A0ED0Y0-0100-GM0-31」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「bizhub C360 / bizhub C280 / bizhub C220 PKI Card System Control Software バージョン A0ED0Y0-0100-GM0-31」（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22年9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 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 PKI Card System Control Software"であり、MFPとクライアントPC間でやりとりされる機密性の高いドキュメントのうち、クライアントPCからMFPへ送信するプリントデータに対して、専用のプリンタドライバ、及びICカードを利用して実現される暗号化プリントを、専用ドライバ(ローダブルドライバ)、及び生成する際に利用したICカードを使い印刷する機能を提供する。またMFPからメール送信す

るスキャン画像データに対してローダブルドライバ及びICカードを利用したS/MIMEによる保護機能を提供する。いずれもICカードとTOEが連携し、これらセキュリティ機能を実現する。

さらにMFP内で処理する画像データを一時的に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を利用して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を有し、HDDのすべてのデータを完全に削除する機能や、ファクス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有し、MFPを利用する組織の情報漏洩の防止に貢献する。

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。

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している。

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。

MFP及びクライアントPCでICカードリーダが利用でき、LANではSMTPサーバが利用でき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る。例えば、パスワー

ドや暗号化ワードの秘密は守ることができることが想定される。

TOEの利用において使用されるICカードは、その正当なユーザによってのみ使用され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

・ 画像ファイルの通信の暗号化、電子署名、認証に使われるICカード、ICカードリーダ、専用ドライバ、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22年9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。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 C360 / bizhub C280 / bizhub C220 PKI Card System Control Software
バージョン：	A0ED0Y0-0100-GM0-31
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がセキュリティサービスとしてどのような方針あるいは規則のもと、機能を実現しているかを述べる。

本TOEは、MFPの返却や廃棄時、またはHDDが不正に持ち出された時に情報の漏洩が起こることを防止するため、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。

- 秘匿性の高い画像ファイルに対する、送受信の際の暗号化、TOEから送信する際のデジタル署名、TOEが受信した場合に送信した本人のみが印刷できる仕組み
- 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
ICカードを所有しているMFPの利用者。(一般的には、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。

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、暗号化プリントファイル、スキャン画像ファイル、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、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、暗号化プリントファイル、スキャン画像ファイル、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、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には新たに暗号化プリントファイル、スキャン画像ファイル、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、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。

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って、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による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機能(以上、「暗号鍵生成機能」)、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。

3.2.2 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-CRYPTO (画像ファイルの暗号化通信)	IT機器間にて送受信される秘匿性の高い画像ファイル（暗号化プリントファイル、スキャン画像ファイル）は、暗号化されなければならない。
P.COMMUNICATION-SIGN (画像ファイルの署名)	秘匿性の高い画像ファイル（スキャン画像ファイル）を含むメールには、デジタル署名が付加されなければならない。
P.DECRYPT-PRINT (画像ファイルの復号)	MFPで受信した秘匿性の高い画像ファイル（暗号化プリントファイル）は、そのファイルを生成した利用者だけに印刷することが許可される。

識別子	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)	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-CRYPTO(画像ファイルの暗号化通信)」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機密性を確保するために、画像ファイルを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、すべての画像ファイルにおいて暗号化する必要はなく、暗号化プリントファイル、スキャン画像ファイルを扱うにあたって、MFPと利用者の使うクライアントPC間で暗号化されている必要がある。

本TOEにおいて、MFPからユーザ自身のクライアントPCへメールで送信されるスキャン画像ファイルを暗号化する機能(以上、「S/MIME暗号化機能」)を保持し、クライアントPCからMFPへ送信される暗号化プリントファイルに対して、本TOEの範囲外であるICカードと専用ドライバを利用して暗号化することで、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することができる。

(2) 組織のセキュリティ方針「P.COMMUNICATION-SIGN(画像ファイルの署名)」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、メールを用いて流れる画像ファイルの完全性を確保するために、署名を付加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、すべての画像ファイルにおいて署名を付加する必要はなく、スキャン画像ファイルを扱うにあたって、署名が付加されている必要がある。

本TOEにおいて、MFPからユーザ自身のクライアントPCへメールにて送信されるスキャン画像ファイルに対して、本TOEの範囲外であるICカードと連動するための機能(以上、「ICカード動作サポート機能」)を保持し、ICカードを利用し、本TOEで署名を付加する機能(以上、「S/MIME署名機能」)を保持することで、メールを用いて流れる画像ファイルに対して、完全性を確保した形で送信することができる。

(3) 組織のセキュリティ方針「P.DECRYPT-PRINT(画像ファイルの復号)」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、暗号化プリントファイルを生成したユーザのみが当該暗号化プリントファイルに対して、復号、印刷が行えることを規定している。

本TOEにおいて、暗号化プリントファイルに対して、本TOEの範囲外であるICカードと連動するための機能(以上、「ICカード動作サポート機能」)を保持し、その暗号化プリントファイルを生成したICカードを使用した場合のみに、本TOEで暗号化プリントファイルを復号し、印刷を許可する機能(以上、「暗号化プリントファイル復号機能」)を保持することで、暗号化プリントファイルを生成したユーザのみが、当該暗号化プリントファイルの復号、印刷を行うことができる。

(4) 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公衆回線口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公衆回線口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公衆回線口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 前提条件と使用環境

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使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.IC-CARD (ICカードに関する運用条件)	TOEの利用において使用されるICカードは、正当なユーザに所有されている。
A.SETTING (セキュリティに関する動作設定条件)	ユーザがTOEを利用する際、セキュリティに関する以下の動作設定がTOEに対し行われている。 ・ パスワードを連続で一定回数間違った場合に認証操作を禁止する。 ・ インターネット経由TOE更新機能を利用不可とする。 ・ メンテナンス機能を利用不可とする。 ・ サービスエンジニアのログイン認証を有効とする。 ・ HDD暗号化機能を有効とする。 ・ パネル以外からの管理者機能による設定を不可とする。

4.2 使用環境と構成

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 のいずれかに搭載される。MFPには、ICカードリーダが接続されることを想定する。FAXユニットを搭載するかど

うかは任意である。

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ICカードを認証するために、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をオフィス内LANに接続した状態を想定する。

専用のプリンタドライバがインストールされ、ICカードリーダが接続されたクライアントPCが、オフィス内LANに接続されることを想定する。

SMTPサーバがオフィス内LANに接続されることを想定する。オフィス内LANでDNSサーバを利用するかどうかは任意である。

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 使用環境におけるTOE範囲

以下における、ASIC、ICカード、ICカードリーダ、専用ドライバ、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。
- 組織のセキュリティ方針の実現のために、画像ファイルの通信の暗号化、電子署名、認証が必要である。これらの機能を実現するために、本TOEは、ICカード、ICカードリーダ、専用ドライバ、Active Directoryと連携するが、これらは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）について、目的と関連を説明する。

5.1 TOE境界とコンポーネント構成

本TOEは、MFP全体の動作を統括制御するソフトウェアである。MFP本体内のMFP制御コントローラ上の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、図5-1中の「※」で示されたFAXユニットはMFPのオプションパーツである。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。

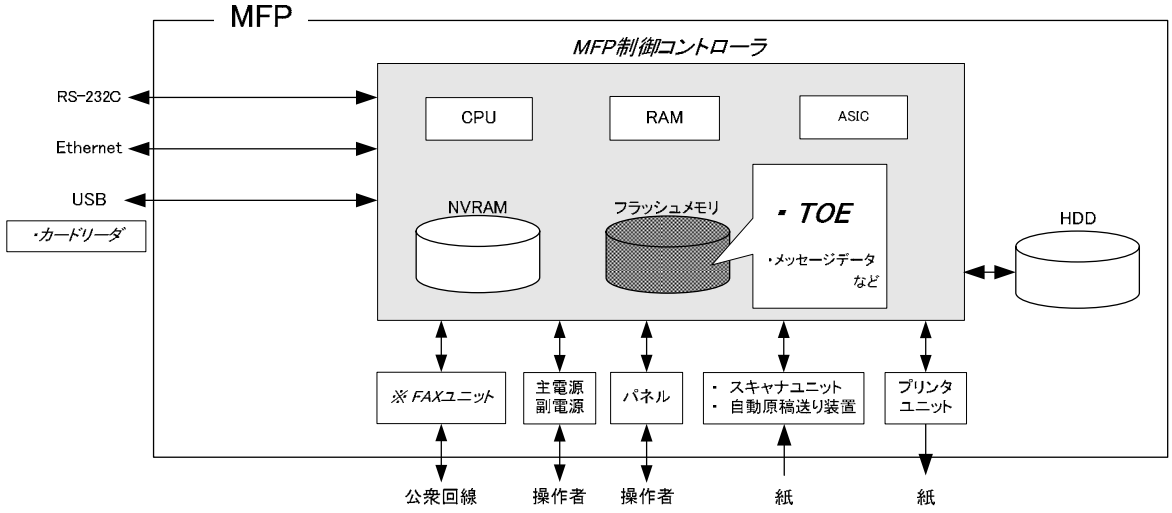

図5-1　TOE境界

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。
- 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。
  この部分は、カードリーダを介してICカードの機能を利用して、以下の機能も実現する。
  - S/MIMEの暗号化/復号/署名
  - 暗号化プリントファイルの復号

- 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。
  管理者から指示があった場合には、HDDのすべてのデータに対し、指定された方式で上書きをする。

- 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 PKI Card System Control Software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等も保存される。

(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が保存される領域としても利用される。また、ICカードにアクセスするためのローダブルドライバもここに保存される。「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

ICカードに対応したカードリーダが接続できる。カードリーダは販売上の都合によりMFPには標準搭載されず、オプションパーツであるが、本STの想定

では必須の構成部品である。

(11) ICカード

Common Access Card(CAC)、及びPersonal ID Verification(PIV)の標準仕様をサポートするICカード。
共通鍵の復号、メッセージダイジェストに対する署名の演算、公開鍵の提供の機能により、「共通の管理を行う部分」をサポートする。

(12) 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。

(13) FAXユニット(※オプションパーツ)

公衆回線を介してFAXの送受信に利用されるFAX公衆回線口をもつデバイス。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。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・ユーザ向けドキュメント＞

- bizhub C360 / C280 / C220 for PKI Card System User's Guide [Security Operations] Ver.1.00

＜サービスエンジニア向けドキュメント＞

- bizhub C360 / C280 / C220 for PKI Card System SERVICE MANUAL SECURITY FUNCTION Ver.1.02

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。

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22年1月に始まり、平成22年9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22年6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22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。

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。

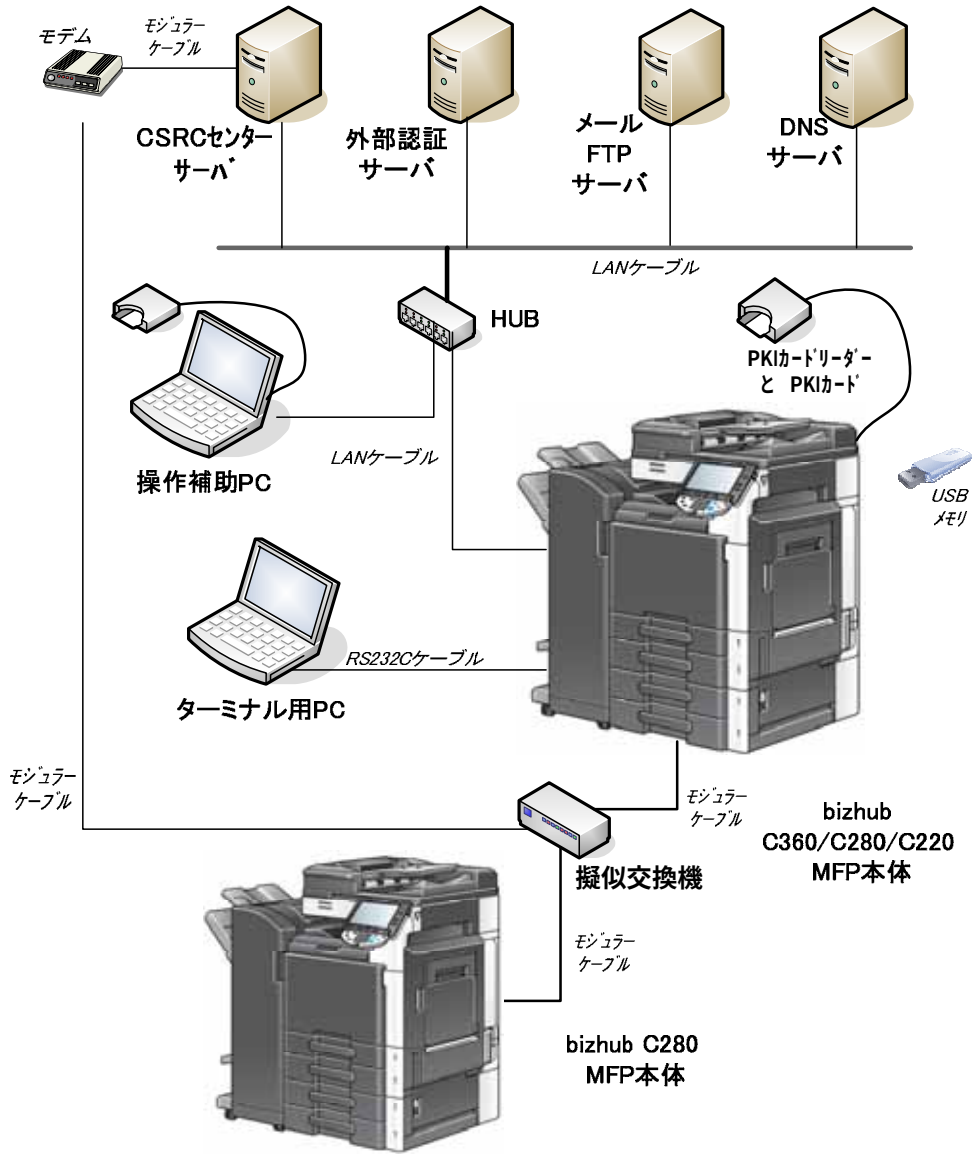

図7-1　開発者テストの構成図

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7-1に示す。

表7-1　開発者テストで使用したツール等

デバイス・ソフトウェア名称	概要・利用目的
KONICA MINOLTA C360 Series PCL Driver Ver.3.0.16.BT12_01	bizhub C360 Series PKIカードシステム専用のプリンタドライバーソフトウェア。暗号化プリントに使用する。
ActiveClient 6.1	スマートカード用ドライバーソフトウェア。補助操作PCにおいてPKIカード用のドライバとして使用する。
SCR3310 USB Smart Card Reader Driver V4.41	PKIカードリーダ用ドライバーソフトウェア。操作補助PCにインストールして使用する。
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、データ確認に使用する。
Mozilla Thunderbird Ver. 2.0.0.21	汎用の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-May-2009)	ハッシュ関数や暗号・復号化ソフトウェアツール。S/MIMEの署名検証に使用する。
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。

デバイス・ソフトウェア名称	概要・利用目的
ディスクダンプエディタ Ver. 1.4.3	HDDの内容を表示させるソフトウェアツール。 HDDの内容確認に使用する。
Stirling Ver. 1.31	バイナリエディタソフトウェアツール。デコードS/MIMEメッセージの内容確認に使用する。
MIME Base64 エンコード／デコード v1.0	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メッセージのデコードに使用する。
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. 2.4.0	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. 実施テストの範囲

テストは開発者によって38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。

7.3.2 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。

評価者が実施したテストの構成を図7-1に示す。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。

なお、TOEが搭載されるMFPとして、bizhub C360 / 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。

・ bizhub C360 / bizhub C280 / bizhub C220 の違いは、コピー/プリント速度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) 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へのパスワード入力方式の違いによるふるまいをテストする。
④ 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。
⑤ 革新的、又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. 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。

＜テストの手法＞

評価者が利用可能な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。

＜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7-2に示す。

表7-2 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	管理者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	S/MIME暗号化機能による複雑度に着目し、スキャン画像データを暗号化してメールで送信する場合の動作を確認するテストを実施した。
観点⑤	FAXユニット制御機能、HDD暗号化の暗号鍵生成機能、暗号化プリント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。

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 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。
④ カードリーダ、MFP、外部認証サーバ間で転送されるデータが盗聴される可能性がある。
⑤ 異なるインタフェースからの認証が競合すると、操作者が異なる権限で操作できてしまう可能性がある。
⑥ HDDが持ち出された場合、特定の条件において脅威を軽減するメカニズムの動作に確信がない。

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7-2に示す。

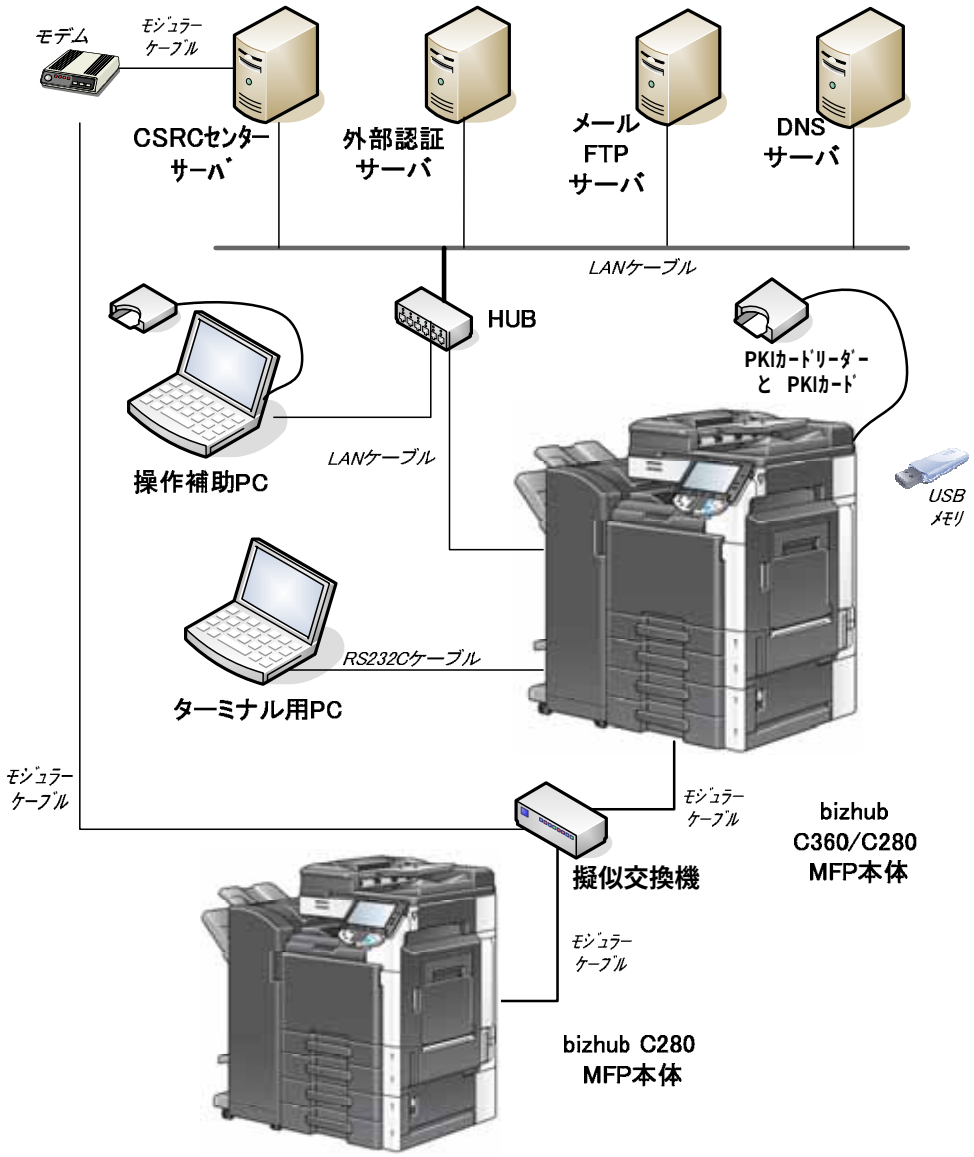

図7-2　侵入テスト環境

＜テスト手法＞

操作パネルを操作して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、そのふるまいをテストツールで確認する方法、ICカードを利用し認証動作を確認する方法、認証の過程においてICカードとTOE間で転送されるデータを確認する方法、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7-3に示す。

表7-3　侵入テスト構成

テスト構成環境	詳細
検査対象(TOE)	・bizhub C360 / bizhub C280 / bizhub C220 に搭載されたTOE(バージョン：A0ED0Y0-0100-GM0-31) ・ネットワーク構成 MFP毎にハブ、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(Thunderbird、ディスクダンプエディタ等)、USBアナライザ(CATC社製)用ソフトも利用。 ・プリンタドライバ、ICカード等を用いてMFPに接続し、暗号化プリント機能を使用することが可能。
検査PC	・検査PCは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(下記ツールの動作確認は、みずほ情報総研内のネットワーク環境にて実施済み。プラグインや脆弱性データベースは2010年6月11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 0.9.8n ・SSL及びハッシュ関数の暗号化ツール。 ③ Nessus 4.2.2.(build 9129) ・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 WireShark 1.2.4 ・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。

＜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7-4に示す。

表7-4　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。

懸念される脆弱性	テスト概要
脆弱性③	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④	カードリーダ、MFP、外部認証サーバ間で転送されるデータから、セキュリティ機能に影響を与える情報が漏洩しないことを確認するテストを実施した。
脆弱性⑤	操作パネルから認証されている状態で、ICカードによる認証を試みた場合や、その逆の場合において、操作者とは異なる権限での操作が可能となるような状況とはならないことを確認するテストを実施した。
脆弱性⑥	特定の条件の下で、脅威を軽減するメカニズムが動作するかどうか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。

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。

- パスワードを連続で一定回数間違った場合に認証操作を禁止する。
- インターネット経由TOE更新機能を利用不可とする。
- メンテナンス機能を利用不可とする。
- サービスエンジニアのログイン認証を有効とする。
- HDD暗号化機能を有効とする。
- パネル以外からの管理者機能による設定を不可とする。

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

評価の結果は、第2章で識別されたTOEについて、本章の評価された構成のみに適用される。

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 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。

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、及び組織のセキュリティ方針を満たすために、ASIC(MFPに搭載されている)、ICカード、ICカードリーダ、専用ドライバ、及びActive Directoryの機能に依存する(4.3参照)。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、運用者判断となる。

・ Active DirectoryサーバによってICカードを認証するための情報は、ICカードを発行する際にICカードを発行する事業者によってActive Directoryに登録される。

・ 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。)

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、公表のため、本報告書とは別文書として、以下のとおり提供される。

bizhub C360 / bizhub C280 / bizhub C220 PKI Card System Control Software セキュリティターゲット バージョン1.02　2010年6月24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。

CAC	Common Access Card (CAC)
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)
MFP	Multiple Function Peripheral (デジタル複合機)
MIB	Management Information Base (MIB)
NVRAM	Non-Volatile Random Access Memory (NVRAM)
PIV	Personal ID Verification (PIV)
RAM	Random Access Memory (RAM)
SMTP	Simple Mail Transfer Protocol (SMTP)
SNMP	Simple Network Management Protocol (SNMP)
SSL	Secure Socket Layer (SSL)
S/MIME	Secure Multipurpose Internet Mail Extensions (S/MIME)
USB	Universal Serial Bus (USB)

本報告書で使用された用語の定義を以下に示す。

CAC	米国国防総省内の認証機関により発行されるICカードのこと。
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。
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。
PIV	連邦政府機関によって発行された証明書や関連情報を用いて実施する本人確認方式のこと。

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。
SSL	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。
オフィス内LAN	TOEが接続され、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。
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。

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19年5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19年5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19年5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 PKI Card System Control Software セキュリティターゲット バージョン1.02　2010年6月24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 PKI Card System Control Software 評価報告書 初版 2010年9月13日 みずほ情報総研株式会社 情報セキュリティ評価室