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21年1月6日** (IT**認証**9242)
認証番号	C0231
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 C353 PKI Card System Control Software
TOE**のバージョン**	A02E0Y0-0100-GM0-U4
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8月17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

「bizhub C353 PKI Card System Control Software、バージョン：A02E0Y0-0100-GM0-U4」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、「bizhub C353 PKI Card System Control Software、バージョン：A02E0Y0-0100-GM0-U4」（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適合である。

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： bizhub C353 PKI Card System Control Software
バージョン： A02E0Y0-0100-GM0-U4
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 C353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 C353 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、その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、HDDに搭載されるHDDロック機能の活用、又は暗号化基板を利用し、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
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。

1.2.3.2 TOE の範囲と動作概要

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1-1に示す。

なお、図1-1中の「※」で示されたFAXユニット、暗号化基板、カードリーダはMFPのオプションパーツである。本TOEの動作環境として、カードリーダと暗号化基板(HDDに書き込むデータを暗号化する機能を選択する場合)は装着されていることを想定している。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。

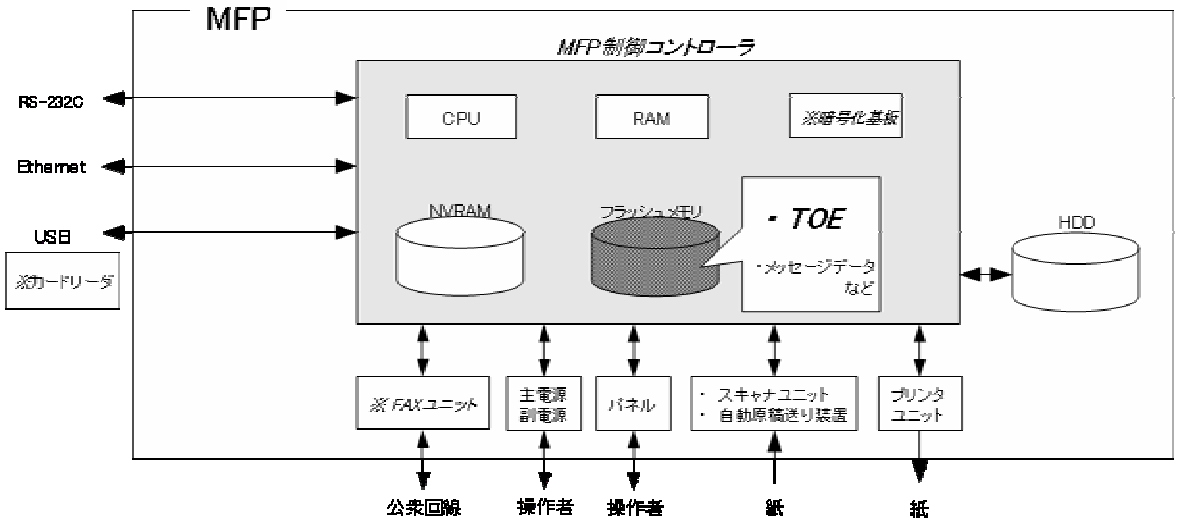

図1-1 TOEに関係するハードウェア構成

本TOEと関係する要素について以下に示す。

(1) フラッシュメモリ

TOEであるPKI Card System Control Software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等も保管される。

(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

定値等が保管される記憶媒体。

(3) 暗号化基板(※オプションパーツ)

HDDに書き込まれるすべてのデータを暗号化するための暗号化機能を実装した特定利用目的集積回路。

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基板が必要。

(4) HDD

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、伸張変換などで一時的に画像データが保管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専用ドライバもここに保存される。

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。

(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。

(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。

(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。

(9) Ethernet

10BASE-T、100BASE-TX、Gigabit Ethernetをサポート。

(10) USB/カードリーダ(※オプションパーツ)

USBメモリからのプリントの他、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。

(12) RS-232C

D-sub9ピンを介して、シリアル接続することが可能。故障時など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(後述)を利用することも可能である。

(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。

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がこれらの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、又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。また、ICカードと連携して各種機能を実現する。

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) 暗号化プリント機能

クライアントPCより専用のプリンタドライバから生成された暗号化プリントファイルを受信した場合、暗号化されたまま印刷待機状態で保管する。

パネルからの印刷指示により、ICカードを利用したPKI処理を経て、暗号化プリントファイルを復号して印刷を実行する。

(3) Scan To Me機能

ICカード所有者が、MFPからICカードを利用したPKI処理を経て自身のメールアドレスへスキャン画像を送信する機能であり、以下の2つの機能を利用する。

【S/MIME暗号化機能】

ユーザがスキャンした画像ファイルをメールアドレスへ送信する際、ス

キャン画像をS/MIMEメールデータファイルとして暗号化する。

【デジタル署名機能】

ユーザがスキャンした画像ファイルをメールアドレスへ送信する際、S/MIMEメールデータファイルとして、メールの送信者を証明し、メールデータを保証する署名データを付加する。

(4) 管理者機能

TOEは、認証された管理者だけがパネルから操作することが可能な管理者モードにて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。

(5) 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。

(6) 暗号鍵生成機能

オプション製品である暗号化基板がMFP制御コントローラに設置されている場合、暗号化基板にてHDDへのデータ書き込み、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。

(7) 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といった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。

本機能は、前提条件により使用が禁止されている。

(8) 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ほか、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)、コンパクトフラッシュメモリ媒体を接続して行う方法がある。

インターネット経由TOE更新機能は、前提条件により使用が禁止されている。

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。

・暗号化プリントファイル
クライアントPCから専用のプリンタドライバ、及びICカードを使って生成され、MFPに蓄積される暗号化された画像ファイル。

・スキャン画像ファイル
MFPでその場でスキャンした画像ファイル。

また、MFPをリース返却、廃棄する等利用が終了した場合やHDD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。

・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
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
暗号化プリント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。

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

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

第二に、MFPからクライアントPCへ送信される画像ファイル(スキャン画像ファイル)を安全に保護するために、本TOEは、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。さらに、TOE範囲外のICカードを利用し、本TOEは、MFPからクライアントPCに送信される画像ファイルに署名を付加して送信する機能を提供する。

第三に、クライアントPCからMFPに送信される画像ファイル(暗号化プリント

ファイル)が不正な利用者に印刷されることを防ぐために、TOE範囲外のICカードを利用し、本TOEは、画像ファイルを生成したユーザのみが画像ファイルの復号、印刷を行える機能を提供する。

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 C353 PKI Card System Control Software 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 C353 PKI Card System Control Software 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。評価は、平成21年8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、又は廃棄となった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、保管画像ファイル、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、保管画像ファイル、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、保管画像ファイル、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。

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-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。

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。

識別子	前提条件
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)	・管理者のパスワードを連続で一定回数間違った場合に管理者認証操作を禁止する。 ・遠隔診断機能を利用不可とする。 ・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。 ・暗号化機能、もしくはHDDロック機能を有効とする。 ・パネル以外からの管理者機能による設定を不可とする。

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・ユーザ向けドキュメント＞

・bizhub C353 for PKI Card System User's Guide [Security Operations] Ver.1.01

＜サービスエンジニア向けドキュメント＞

・bizhub C353 for PKI Card System 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であるbizhub C353にオプション製品である、FAXユニット、暗号化基板、カードリーダを搭載した状態。
- 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。
- 専用のプリンタドライバをインストールしたクライアントPCにカードリーダを接続し、SMTPサーバ・DNSサーバを利用できる状態。

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は、以下の①、②のいずれか、又は両方の機能を選択して使用することによって、HDD内のデータが漏洩する可能性を防いでいる。

① 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。

② 本TOEの範囲外である暗号化基板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」)、及び暗号化基板と連動するための機能(以上、「暗号化基板動作サポート機能」)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) 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。

(4) 組織のセキュリティ方針「P.COMMUNICATION-CRYPTO(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。

(5) 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。

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21年1月に始まり、平成21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、平成21年3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3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。

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。

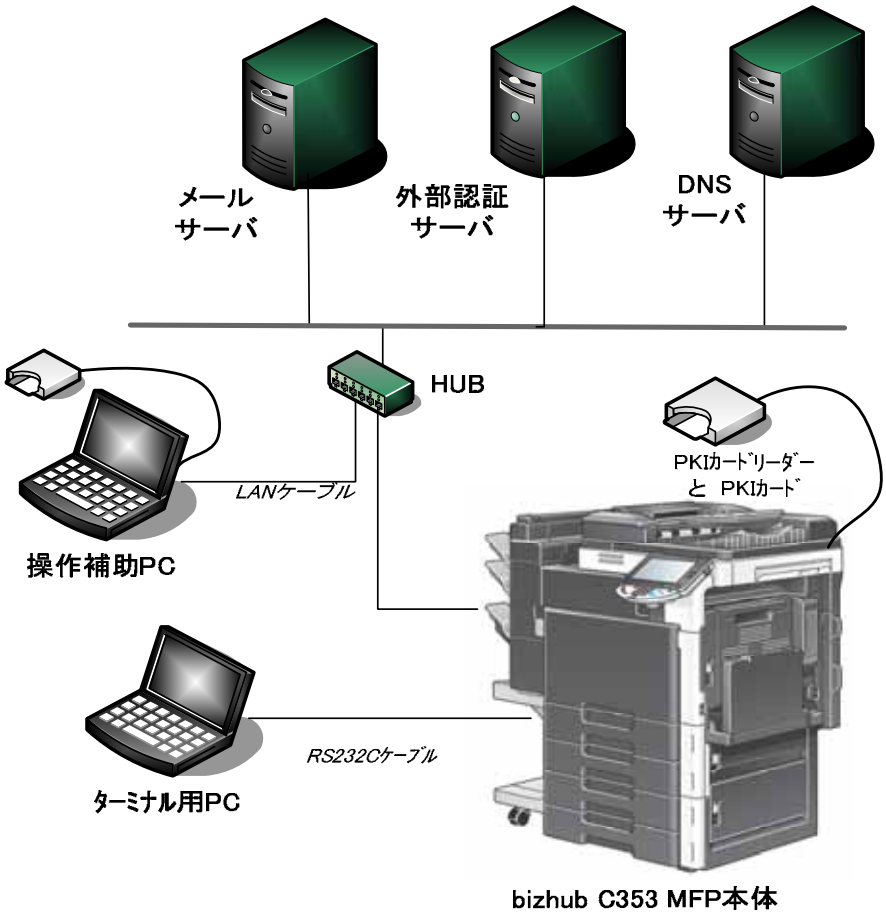

図3-1　開発者テストの構成図

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。

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

デバイス・ソフトウェア名称	概要・利用目的
KONICA MINOLTA C353 Series PCL Driver Ver.6.3.0.BT21_00	bizhub C353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。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 Ver0.99.5	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. 2.0.0.17	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.0.98i 15 Sep 2008	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。
ディスクダンプエディタ Ver.1.33	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.1.3.1.0	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。S/MIMEテスト時に、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40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。

評価者が実施したテストの構成を図3-1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。

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. 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	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⑤	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⑥	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。

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 ネットワーク経由からのアクセスによって、セキュリティ機能がバイパスされる可能性がある。
④ 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。
⑤ 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。

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。

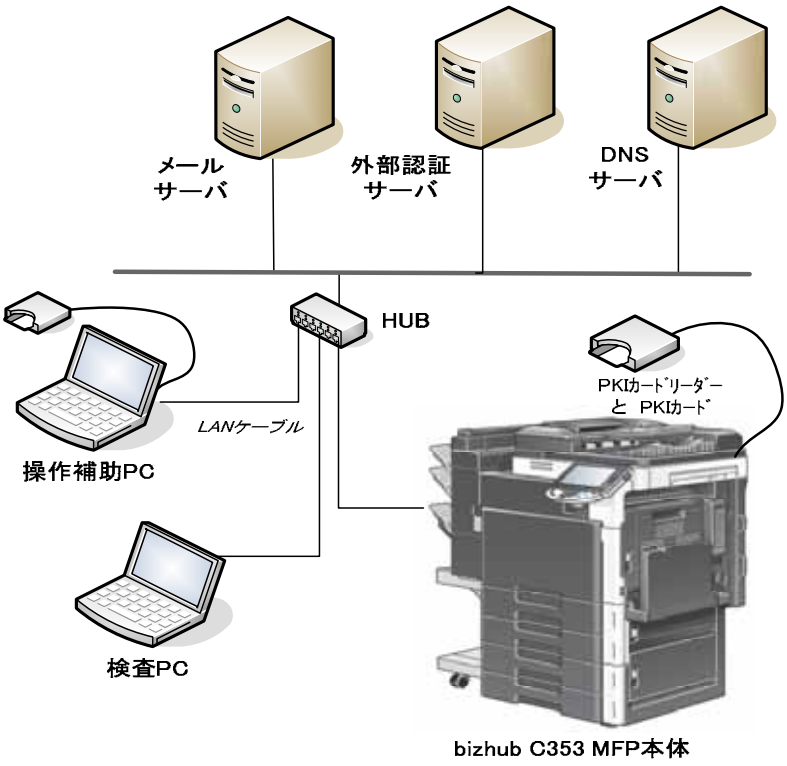

図3-2 侵入テストの構成図

＜テスト手法＞
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 C353に搭載されたTOE(バージョン：A02E0Y0-0100-GM0-U4) ・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(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カードなどを用いて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(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2009年3月20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 0.9.8d ・SSL及びハッシュ関数の暗号化ツール。 ③ Nessus 3.2.1.1　build 2G299_Q(2009 年 3 月 20 日時点のプラグインを使用) ・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

テスト構成環境	詳細
	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 ・MS社で提供するHTTPのやりとりをモニタするWebデバッカー。 ⑦ WIRESHARK 1.06 ・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 2.03(2009 年 3 月 20 日時点のプラグインを使用) ・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コマンド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	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⑤	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。

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

脅威「T.BRING-OUT-STORAGE(HDDの不正な持ち出し)」に対抗するために、HDDのロック機能のセット、又はHDDの暗号化機能のセット、もしくはその両方を消費者は選択することができるが、HDDロック機能のセットのみを選択した場合、以下の点に留意すること。

・HDD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。

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

- 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ユニットが未装着であっても、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。

CAC	Common Access Card (CAC)
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)
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。
HDDロック機能	HDDにパスワードを設定し、パスワードが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。
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/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。
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。
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。
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。

7 参照

[1] bizhub C353 PKI Card System Control Software セキュリティターゲット バージョン 1.07 2009年8月5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 C353 PKI Card System Control Software 評価報告書 第4版 2009年8月10日 みずほ情報総研株式会社 情報セキュリティ評価室