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26年5月21日 (IT認証4506)
認証番号	C0478
認証申請者	コニカミノルタ株式会社
TOEの名称	bizhub C3850 / bizhub C3350 PKI Card System Control Software
TOEのバージョン	A3GN30G0213999P
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27年8月26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4
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4

評価結果：合格

「bizhub C3850 / bizhub C3350 PKI Card System Control Software」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

この認証報告書は、コニカミノルタ株式会社が開発した「bizhub C3850 / bizhub C3350 PKI Card System Control Software バージョン A3GN30G0213999P」(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 27 年 7 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株式会社に報告するとともに、本 TOE に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

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

本認証報告書は、市販される本 TOE を購入する調達者を読者と想定している。本認証報告書は、本 TOE が適合する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本 TOE の機能、運用条件の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 保証パッケージ

本 TOE の保証パッケージは、EAL3 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 C3850、bizhub C3350 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 C3850 / bizhub C3350 PKI Card System Control Software"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。なお、本 TOE は監査ログ機能を有さない。

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、HDD に書き込まれる画像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 に保存される画像データを含むデータ領域を完全に削除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である。

1.1.2.1 脅威とセキュリティ対策方針

本TOEは､以下の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 から不正に HDD を持ち出してアクセスすることにより、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、暗号化機能により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。

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 Active Directory 及び 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。

・ セキュリティ強化機能の設定を有効にする必要がある。有効にした場合、MFP の一部の機能は使えなくなる。STの「1.4.3.5. 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。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価・認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって本 TOE に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 27 年 7 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、所見報告書、及び関連する評価証拠資料を検証し、本 TOE の評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。認証機関が指摘した問題点は、すべて解決され、かつ、TOE の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 TOE識別

本 TOE は、以下のとおり識別される。

TOE名称： bizhub C3850 / bizhub C3350 PKI Card System Control Software
バージョン： A3GN30G0213999P
開発者： コニカミノルタ株式会社

製品が評価･認証を受けた本 TOE であることを、管理者及びユーザ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 識別情報も含んだ）TOE のバージョンを表示させることができる。表示された TOE バージョンが、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 MFP に評価を受けた TOE が搭載されていることを確認することができる。

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、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、暗号化機能と、上書き削除機能を提供する。

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

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、保存画像ファイルが漏洩する。また、悪意を持った者が、MFP内のNVRAMを解析することにより、管理者パスワード、暗号化ワードが漏洩する。
T.ACCESS-HDD (HDD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、MFPに搭載されているHDDに対して、(MFPを使用せず)不正に(HDDを取り出してPCに接続して解析する等)アクセスして、HDDに保管されているすべての画像ファイルやパスワードなどのデータが暴露される。

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のHDDやNVRAMより情報漏洩する可能性を想定している。

本TOEで、HDDの画像データを含むデータ領域に上書き削除を実行する機能と、NVRAMに格納された情報を初期化する機能を保持することで、ユーザから回収されたMFPのHDDやNVRAMに格納された保護資産が漏洩することを防いでいる。

HDDの上書き削除の方式としては、以下の方式を選択できる。(例えば一番上の項目は0x00で1回上書きすることを表し、2番目の項目は乱数, 乱数, 0x00の順で上書きをすることを表す。「検証」とは、最後の上書きが正しく行われたこ

とを、実際にHDDの内容を読み込んで確認することを表す。)

- 0x00
- 乱数 ⇒ 乱数 ⇒ 0x00
- 0x00 ⇒ 0xFF ⇒ 乱数 ⇒ 検証
- 乱数 ⇒ 0x00 ⇒ 0xFF
- 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF
- 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 乱数
- 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0xAA
- 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0xAA ⇒ 検証

(2) 脅威「T.ACCESS-HDD(HDD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、MFPを使用せずにHDDにアクセスされることにより、HDDに保管されている保護資産が暴露される可能性を想定している。

本TOEでは、HDDに保管される画像データ、TSFデータを暗号化することにより、対抗する。

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。

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 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。

4.2 運用環境と構成

本TOEは、コニカミノルタ株式会社が提供するMFPである、bizhub C3850 / bizhub C3350 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。

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、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 運用環境におけるTOE範囲

以下における、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。

- 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）を説明する。

5.1 TOE境界とコンポーネント構成

TOEの物理的範囲は、以下のソフトウェアである。

・コントローラーファームウェア（SSDに存在）

コントローラーファームウェアはOSを含めた、MFPの全体制御を行うソフトウェアである。これらのソフトウェアにより、コピー、プリント、スキャン、FAX等のオフィスワークのための一連の機能（基本機能）と、セキュリティ機能とを提供する。

5.2 TOEの動作環境

TOEが動作するために必要なMFP上のハードウェア環境の構成を**図5-1**に示す。MFP制御コントローラーはMFP本体内に据え付けられ、TOEはそのMFP制御コントローラー上のSSDにコントローラーファームウェアが存在し、電源がONになると揮発性RAM（**図5-1**においては、「RAM」と表記）にロードされ動作する。以下には**図5-1**にて示されるMFP制御コントローラー上の特徴的なハードウェア、MFP制御コントローラーとインタフェースを持つハードウェアについて説明する。

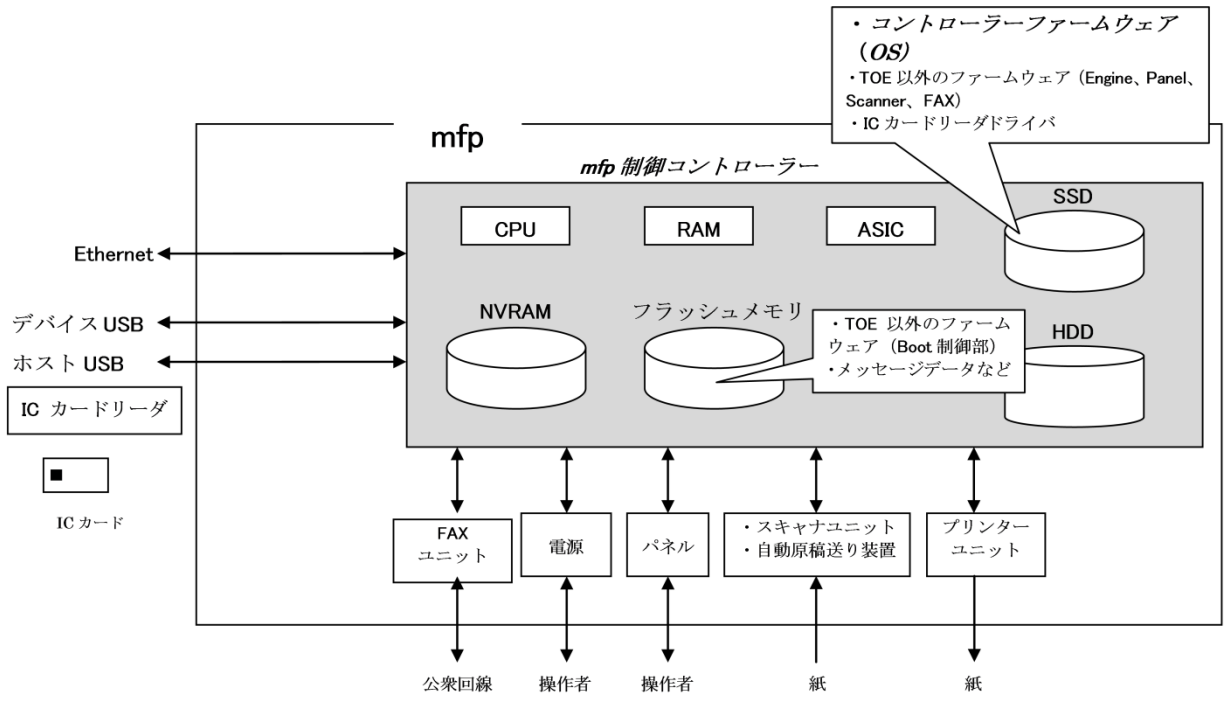

図5-1　TOEに関連するハードウェア構成

・フラッシュメモリ
電源起動直後の制御を行うBoot制御部のオブジェクトコードが保管される記憶媒体。
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、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も保存される。

・HDD（ハードディスクドライブ）
画像データ、ICカードのID等が保管される。

・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。NVRAMには、管理者パスワード、CE パスワード、暗号化ワードが保管される。

・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。

・電源
MFPを動作させるための電源スイッチ。

・Ethernet
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。

・デバイスUSB
MFP本体の後ろ側にあるローカル接続で印刷するためのポート。

・ホストUSB
MFPのパネル側にあるUSBポートで、ICカードリーダを接続する。ユーザはICカードを利用してMFPにアクセスすることが可能となる。
TOEのアップデート、USBインタフェースに接続したUSBメモリからの印刷あるいはスキャンしたデータを保存することも可能。なお、この印刷及びスキャンには暗号化プリント、及びS/MIME暗号処理機能は含まれていない。

・FAXユニット
公衆回線を介してFAXの送受信に利用されるデバイス。

・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。

・プリンターユニット
MFP制御コントローラー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。

・SSD（Solid State Drive）
Flash Memory Driveである。TOEである全体制御ソフトウェアにおけるコントローラーファームウェアのオブジェクトコード、TOE以外のファームウェアであるEngine、Panel、Scanner、FAXのファームウェアのオブジェクトコード、ICカードリーダドライバ等が保管される記憶媒体。

・ASIC（Application Specific Integrated Circuit）
画像処理全般を行うために設計された集積回路。また、画像を印刷するときに画像の展開と色合いの調整等の処理も行う。

・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。

・ICカードリーダ
ICカードを読み取るための機器。

・ICカードリーダドライバ
ICカードリーダにアクセスするためのドライバ。

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(海外版)＞

・ bizhub C3850/C3350 for PKI Card System User's Guide [Security Operations] Ver. 1.04

＜管理者・ユーザ向けドキュメント(日本版)＞

・ bizhub C3850/C3350 PKIカードシステム ユーザーズガイド　セキュリティ機能編 Ver. 1.04

＜サービスエンジニア向けドキュメント(海外版)＞

・ bizhub C3850/C3350 for PKI Card System SERVICE MANUAL [SECURITY FUNCTION] Ver. 1.03

＜サービスエンジニア向けドキュメント(日本版)＞

・ bizhub C3850/C3350 for PKI Card System サービスマニュアル　セキュリティ機能編 Ver. 1.03

7 評価機関による評価実施及び結果

7.1 評価機関

評価を実施したみずほ情報総研株式会社 情報セキュリティ評価室は、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）と相互承認している認定機関（独立行政法人評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

7.2 評価方法

評価は、CC パート 3 の保証要件について、CEM に規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告された。評価報告書では、本TOEの概要と、CEMのワークユニットごとの評価内容及び判断結果を説明する。

7.3 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成 26 年 5 月に始まり、平成 27 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、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 26 年 10 月、平成 27 年 1 月、及び 4 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 27 年 4 月に開発者サイトで開発者のテスト環境を使用し、開発者テストのサンプリングチェック及び評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。

これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.4 製品テスト

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

7.4.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価者が評価した開発者テストの内容を以下に説明する。

(1) 開発者テスト環境

開発者が実施したテストの構成を図7-1に、主な構成機器のリストを表7-1に示す。

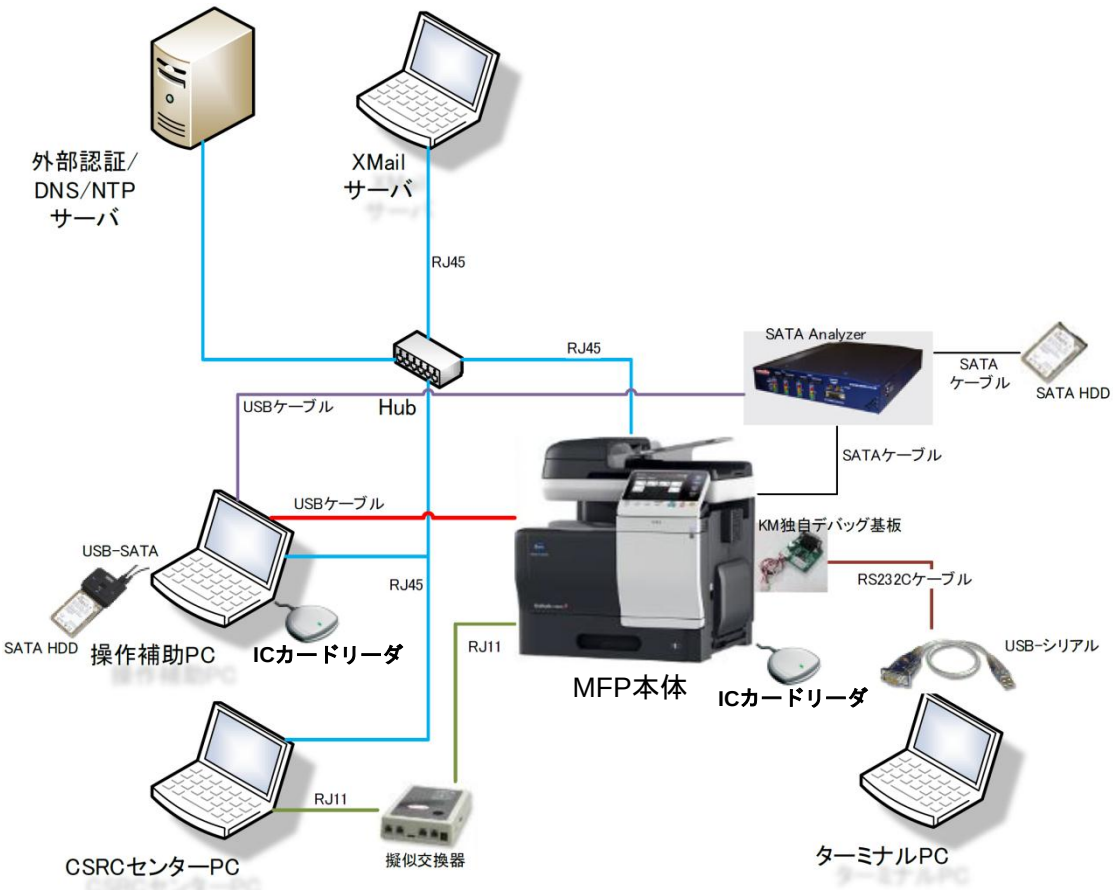

図7-1　開発者テストの構成図

開発者テストはSTにおいて識別されているTOE構成と同一の環境において実施されていると見なせることが評価者により確認されている。

具体的な根拠は以下のとおりである。

・TOE は STで識別されたものと同一のMFP（bizhub C3850 / bizhub C3350）に搭載される

・CSRCセンターPC(CSRCは、MFPの機器の状態をリモートで管理する保守サービス)、デバッグのためのデバイス、MFPがHDDに書き込むデータをキャプチャーするためのデバイスが接続されるが、これらはTOEのセキュリティ機能の動作、テスト結果に影響を与えるものではない

表7-1　主なテスト構成機器

No.	構成機器名称	概要・利用目的
1	bizhub C3850/bizhub C3350 MFP本体	テスト対象となるMFP実機である。ファームウェアには、TOEであるセキュリティ機能搭載バージョンを用いる。 ・搭載されるTOE 名称：bizhub C3850 / bizhub C3350 PKI Card System Control Software 識別（ソフトウェア識別、バージョン）：A3GN30G0213999P
2	ICカードリーダ (AU-211P / Identive SCR-3310 / SCR-3310v2)	ICカードからICカード情報を読み取る。 MFP本体、及び操作補助PCに接続する。
3	ICカード(PIV/CAC)	PKI機能を実現するICカード。カード認証、暗号化プリント、S/MIME送受信などに使用する。
4	操作補助PC	Windows 7 Professional SP1で動作するネットワーク端子付きのPC。各テストのうち、SNMP、暗号化プリント、S/MIMEメール受信等、ネットワークアクセスが必要なテストに使用する。
5	外部認証/DNS/NTP サーバ	WindowsServer2003R2 SP2, WindowsServer2003 SP2が動作するサーバ機で、以下のサーバ機能を提供する。 ・ 外部認証サーバ（Active Directoryにより、(所有者)のアクセス権管理を行う） ・ DNSサーバ（ドメイン名をIPアドレスに翻訳する） ・ NTPサーバ（操作補助PCの時刻を合わせる）

No.	構成機器名称	概要・利用目的
6	XMailサーバ	インターネット上で電子メールの送受信に利用されるサーバ。MFP本体のネットワーク設定に基づく動作テストを行う。
7	HUB	LANを構築するための接続機器。TCP/IP接続可能な100BASE-T仕様のHUBを使用する。
8	RJ45(LANケーブル)	MFP本体とHUB、さらに操作補助PCや外部認証サーバ、XMailサーバ等が接続された基幹ネットワーク線とHUBを接続する10BASE/100BASE-T準拠の通信ケーブル。
9	USBケーブル	MFP本体と操作補助PCを接続する。
10	SATAProtocolAnalyzer	HDD書き込み処理のキャプチャーが可能なツール。
11	USB-SATA	SATA HDDをUSBでPCに接続する変換機。
12	CSRC センター PC	CSRCの使用が制限されることの確認に使用する。
13	ターミナルPC	KM独自デバッグ基板を介して、デバッグ操作をするために使用する。
14	USB-シリアルケーブル	USB-シリアル変換ケーブル。操作補助PCにシリアルポートを追加する。
15	RS232Cケーブル	シリアルポートとKM独自デバッグ基板の接続するための通信ケーブル。
16	KM独自デバッグ基板	コニカミノルタ独自のデバッグ専用の基板。RS232CケーブルとMFP本体との間に接続し、ターミナルPCよりデバッグ操作を可能にする。
17	疑似交換機	モデム付きPCとMFP本体をモジュラーケーブルで接続し、疑似的にFAX回線を形成する。
18	RJ11(モジュラーケーブル)	RJ11形式の電話回線用ケーブル。

(補足) 図 7-1 の「SATA HDD」は、MFP 本体に内蔵されている HDD を表す。

⑵ 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＞

セキュリティ機能を刺激するためのインタフェースとして、MFP のパネル操作、ネットワーク及び USB で MFP に接続された操作補助 PC からの操作が使用された。セキュリティ機能の動作結果は、パネル表示、ネットワーク接続された操作補助 PC 上への表示、デバッグ基板からの出力のターミナル PC 上への表示を目視により確認する方法、MFP に接続された解析ツールのキャプチャー結果を確認する方法が採られた。HDD 暗号化機能については、同等の機能が搭載された PC 環境を用いて HDD のマウントに関するテスト、暗号化ファイルに関する復号テストを行った。またネットワーク上の通信データについては操作補助 PC 上で通信パケットをキャプチャーし、内容を確認している。

＜開発者テストツール＞

テストで使用した主なソフトウェア、ツールを表 7-2 に示す。

表7-2　開発テストツール

No.	ツール・ソフトウェア名称	概要・利用目的
1	KONICA MINOLTA C3850 Series PCL v1.3.6.0	PKIカードシステム専用プリンタドライバソフトウェア。
2	ActivClinet v7.0.2.25	ICカード用ドライバソフトウェア。補助操作PCにおいてICカード用のドライバとして使用する。
3	WireShark Ver.1.12.0	LAN上の通信をモニター&解析するソフトウェア。通信ログ取得に使用する。
4	Mozilla ThunderBird Ver. 31.0	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。
5	Open SSL　Ver.1.0.1h	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。
6	Tera Term Pro Ver.4.82	ターミナル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。
7	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。
8	Base64 エンコーダ V4.41	Base64エンコーダ 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。

No.	ツール・ソフトウェア名称	概要・利用目的
9	XMail Ver.1.27 XMailCFG241b.zip	メールサーバ機能として使用する。
10	Apache 2.2.25	Webサーバのソフトウェア。Xmail（メールサーバ）の管理用に使用する。
11	ActivePerl 5.16.3.1603	perlインタプリタソフトウェア。メールサーバの稼働のために使用する。
12	Internet Explorer Ver. 11	汎用のブラウザソフトウェア。MFP本体の設定に使用する。
13	LeCroy STX SATA Protocol Suite ver4.20 Build10	HDD上書き消去実行時のHDD書き込み処理をキャプチャーするために使用する。
14	Knoppix7.0.2LiveCD	MFPと同等の暗号環境を整えるために、操作補助PCのOSを一時的にLinuxに変更して操作するためのソフトウェア。
15	CSRC Ver.2.8.1 Rev.03	CSRCのアプリケーション。CSRCの使用が制限されることの確認に使用する。
16	Fiddler.exe Ver.2.4.6.2	http他のWebアクセスのモニター＆解析ソフトウェア。MFP本体と操作補助PC間でIPPプロトコルのテストを行うために使用する。
17	ICカードリーダドライバ(デバイス/ICカードリーダ用) Ver.A3GN0Y0-A401-G00-00	MFP本体において、ICカードリーダよりICカードを読み取る際に使用する。
18	MG-SOFT MIB Browser Professional SNMPv3 Edition Ver.12.20.0.5040	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。

＜開発者テストの実施＞

TOE のセキュリティ機能の実行は、MFP 上のパネルの手動操作、操作補助 PC 上でプリンタドライバ等を使用した手動操作により行う。

HDD 暗号化機能については、同等の機能が実装された Linux OS 環境を使用して行う。

セキュリティ機能のふるまい、応答の確認は、パネル表示結果の目視確認、印刷出力結果の目視確認、解析ツールで収集した HDD の入出力経路上のデータ解析、操作補助 PC 上に表示された結果の目視確認、デバッグ基板からの出力をターミナル PC で観察、キャプチャーした通信パケット内容のデータ解析の手段を用いて行い、観察されたテスト結果が期待される結果と一貫していることを確認している。

b) **開発者テストの実施範囲**

開発者テストは開発者によって55項目実施された。カバレージ分析によって、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証された。深さ分析によって、TOE設計に記述されたすべてのサブシステムとサブシステムインタフェースが十分にテストされたことが検証された。

c) **結果**

評価者は、開発者テストの実施方法、実施項目の正当性を確認し、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

7.4.2 評価者独立テスト

評価者は、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実行されることを再確認するサンプルテストを実施するとともに、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることをより確信するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

評価者が実施したテストの構成は、図 7-1 に示した開発者テストと同様の構成である。

また、「7.4.1 開発者テスト」に記載の根拠と同様の理由で、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と見なすことができる。

(2) 独立テスト概説

評価者の実施した独立テストは以下のとおりである。

a) **独立テストの観点**

評価者は、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。

＜独立テストの観点＞

① 操作ケースや入力パラメタの網羅性の観点から開発者テストが不足していると判断されるTSFに関して、操作ケースや入力パラメタの種類、組み合わせを追加したテストを実施する。
② パラメタを入力するインタフェース種別に関して、開発者テストとは異なる組み合わせを追加し、TSFのふるまい、相互作用をより厳密に確認するためのテストを実施する。
③ 独立テスト、サンプリングテストの実施により、TOEが提供する全てのセキュリティ機能性を網羅できるように考慮する。

b) 独立テスト概要

評価者が実施した独立テストの概要は以下のとおりである。

＜独立テスト手法＞

開発者テストと同様のテスト手法が用いられた。

＜独立テストツール＞

開発者テストにおいて利用した表 7-2 のツールが用いられた。これらの仕様確認及び動作試験と校正は評価者によって実施されている。

＜独立テストの実施内容＞

独立テストの観点に基づき、独自テスト 7 件、サンプリングテスト 20 件のテストが実施された。実施された主なテスト内容と対応する独立テストの観点を表 7-3 に示す。

表7-3 実施した主な独立テスト

独立テストの観点	テスト概要
①	異常系入力値を追加した暗号化ワード設定、各種パスワード設定に関するテスト。
①	開発者テストでは暗号化プリントファイルが1つ登録された状態で実施されたテスト(正常な動作や電源断時の動作)に対し、暗号化プリントファイルが複数登録された状態についてのテストを追加した。
①②	開発者テストではCACカードを使用して実施されたテスト(S/MIME暗号化)に対し、PIVカードを使用する場合のテストを追加した。
①	パスワードの規約のパラメタに対し、セキュリティ強化機能有効時に許容されない値を入力するテスト。

c) 結果

評価者が実施したすべての独立テストは正しく完了し、評価者は TOE のふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが一致していることを確認した。

7.4.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

① 意図しないネットワークポートインタフェースが存在し、そこからTOEにアクセスできる可能性がある、もしくはオープンポートへの不正なデータ送信により保護資産が暴露される可能性がある。
② TOE自身の解析や改ざんを行うことにより、機密情報の漏えいやセキュリティ機能のバイパスの可能性がある。
③ 想定外のユーザ操作により、セキュリティ機能をバイパスされる可能性がある。
④ インタフェースに想定外の値が入力され、セキュリティ機能をバイパスされる可能性がある。
⑤ TOE資源の枯渇した状態で運用することにより、セキュリティ機能をバイパスされる可能性がある。
⑥ ICカードによる認証の際に、通信路の盗聴がTSFデータや資産の漏洩につながる可能性がある。

b) 侵入テストの概要

評価者は、潜在的な脆弱性が悪用される可能性を検出するために、以下の侵入テストを実施した。

＜侵入テスト環境＞

侵入テストは評価者独立テストと同一のテスト構成で実施された(侵入テストで使用されるツールがインストールされた検査用の PC が追加されたのみである)。

侵入テストでは、表 7-2 に示した開発者テストで使用されたツールに加え、表 7-4 に示したツールが使用された。

表7-4　侵入テストで使用されたツール

No.	ツール・ソフトウェア名称	概要・使用目的
1	nmap Version 6.47	ポートスキャンツール。
2	snmpwalk Version 3.6.1	MIB情報取得ツール。
3	Nessus Version 6.3.3	セキュリティスキャナ。
4	Nikto Version 2.1.5	セキュリティスキャナ。
5	extrstr Version 0.2	バイナリ解析ツール
6	USB Explorer Model 200	USBアナライザ
7	USB Analysis Software Version 3.3.4015.1	USBアナライザソフト

＜侵入テストの実施＞

潜在的な脆弱性の探索において識別された懸念される脆弱性について、これと対応する侵入テストの概要を表 7-5 に示す。評価者は潜在的な脆弱性が悪用される可能性の有無を決定するため、以下に示す侵入テスト（項目数 9 件）を実施した。

表 7-5　侵入テスト概要

脆弱性	テスト概要
①	ポートスキャンツールを使用し、意図しないネットワークポートが開いていないことを確認する。また、使用中のポートについても不正入力に対する脆弱性が存在しないことをセキュリティスキャナ等を使用して確認する。
②	TOEのバイナリを解析し機密情報の取得や改ざんができないこと

	を確認する。
③	通常運用と異なるタイミングで電源操作を行い、想定外の動作をしないことを確認する。
④	クライアントPCからの不正な受信データやUSBデバイスからの入力データによって想定外の動作をしないことを確認する。
⑤	HDD容量等のTOE資源が枯渇した状態で運用した場合に、TOEが想定外の動作をしないことを確認する。
⑥	ICカードによる認証中に、ICカードとTOEの間のUSBケーブル、TOEと外部認証サーバの間のLANケーブルの通信の内容を観察し、容易にTSFデータや資産の漏洩につながる内容はないことを確認する。

c) **結果**

評価者が実施した侵入テストでは､想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

7.5 評価構成について

(1) 動作機種について

本TOEは、コニカミノルタ株式会社が提供するMFPである、bizhub C3850 / bizhub C3350 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2機種において評価された。

(2) TOEの設定について

評価は、「セキュリティ強化機能」が有効の設定で実施された。

この設定は、STで示されている設定の通りである。

7.6 評価結果

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

評価では以下について確認された。

- PP 適合：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。

7.7 評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

8 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。認証機関は、本 ST 及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

8.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本 TOE が CC パート 3 の EAL3 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、以下の機能に依存する(4.3 参照)。
  - ICカード、ICカードリーダ、専用ドライバ
  - Active Directory

  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、調達者判断となる。

・ 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。

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 C3850 / bizhub C3350 PKI Card System Control Software セキュリティターゲット バージョン 1.09
2015 年 7 月 24 日　コニカミノルタ株式会社

11 用語

本報告書で使用された CC に関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用された TOE に関する略語を以下に示す。

CAC	Common Access Card (CAC)
DNS	Domain Name System (DNS)
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)
SSD	Solid State Drive (SSD)
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。
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27年6月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 平成27年6月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 平成27年6月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[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4版, 2012年9月, CCMB-2012-09-001, (平成24年11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4版, 2012年9月, CCMB-2012-09-002, (平成24年11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4版, 2012年9月, CCMB-2012-09-003, (平成24年11月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[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4版, 2012年9月, CCMB-2012-09-004, (平成24年11月, 翻訳第1.0版)

[12] bizhub C3850 / bizhub C3350 PKI Card System Control Software セキュリティターゲット バージョン 1.09 2015年7月24日 コニカミノルタ株式会社

[13] bizhub C3850 / bizhub C3350 PKI Card System Control Software 評価報告書 第5版(130785-01-R003-05) 2015年7月27日 みずほ情報総研株式会社 情報セキュリティ評価室