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26日** (IT**認証**9245)
認証番号	C0233
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 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 **全体制御ソフトウェア** **英語名：** bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Control Software
TOE**のバージョン**	A11U-0100-G10-06
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21日

セキュリティセンター 情報セキュリティ認証室
技術管理者　山里　拓己

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① 情報技術セキュリティ評価のためのコモンクライテリア バージョン3.1 改訂第2版 (翻訳第2.0版)
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 改訂第2版　(翻訳第2.0版)

評価結果：合格

「[日本語名] bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 全体制御ソフトウェア、[英語名] bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Control Software、バージョン：A11U-0100-G10-06」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「[日本語名] bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 全体制御ソフトウェア、[英語名] bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Control Software、バージョン：A11U-0100-G10-06」（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： [日本語名] bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink

2221
[英語名] bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221
バージョン： A11U-0100-G10-06
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 350、bizhub 250、bizhub 200、bizhub 362、bizhub 282、bizhub 222、ineo 362、ineo 282、ineo 222、VarioLink 3621、VarioLink 2821、VarioLink 2221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 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 全体制御ソフトウェア ”であり、MFPに保存される機密性の高いドキュメントの暴露に対する保護機能を提供する。また、MFP内の画像データを保存する媒体であるHDDが不正に持ち出される等の危険性に対して、不要となったデータを即時に上書き削除する保護機能、及びHDDに搭載されるHDDロック機能、暗号化基板を利用した暗号化機能を活用することにより、不正なアクセスを防止することが可能である。他に、TOEは各種上書き削除規格に則った削除方式を有し、HDDのすべてのデータを完全に削除する。

1.2.3 TOE範囲とセキュリティ機能

1.2.3.1 TOE に関係する役割

本TOEに関係する役割を以下に示す。

(1) ユーザ
MFPを使ってコピー、スキャン等を行う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の動作管理やボックスの管理を行う。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1-1に示す。

なお、図1-1中の「※」で示されたHDD、FAXユニット、暗号化基板、ローカル接続ユニット、遠隔診断通信中継ユニットはMFPのオプションパーツである。本TOEの動作環境としては、前提条件により接続しても利用できない遠隔診断通信中継ユニットを除く、オプションパーツが装備されている状態で動作する。

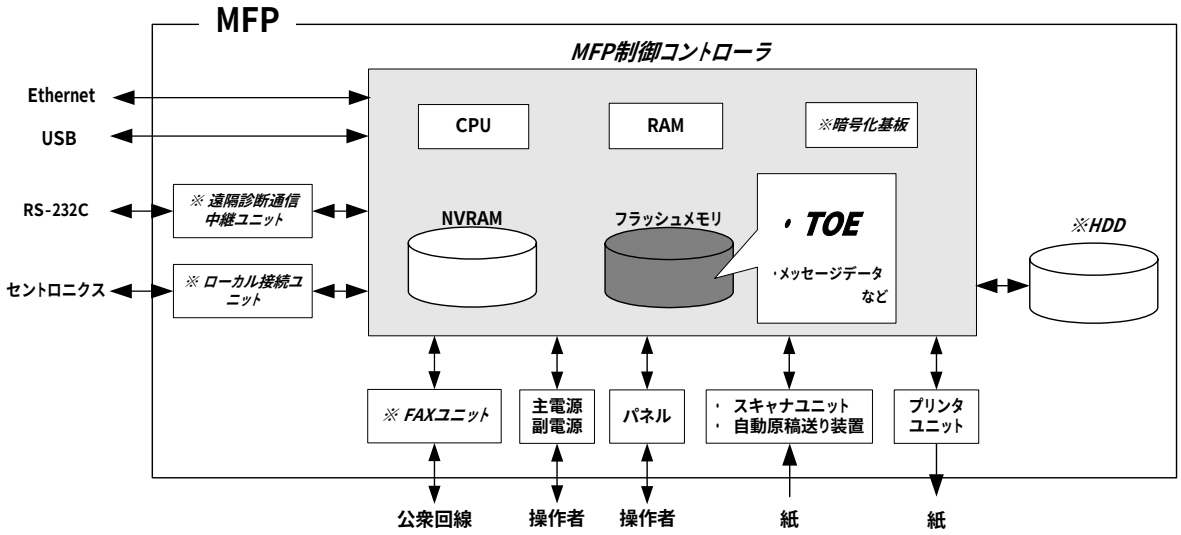

図1-1 TOEに関係するハードウェア構成

本TOE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が保管される。

(2) RAM
揮発性メモリ。画像データが保管される記憶媒体。

(3) NVRAM
不揮発性メモリ。MFPの動作において必要な様々な設定値(管理者パスワード、送信宛先データ)等が保管される記憶媒体。

(4) 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機能がハード的に実装されている。暗号化のための集積回路。
HDDに書き込まれる画像データを暗号化するセキュリティ機能(暗号化機能)を利用するためにはオプション購入の暗号化基板が必要。

(5) HDD(※オプションパーツ)
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他、RAMの処理容量を超える画像データがスワップされる領域として利用される。
HDDにはパスワードを設定することが可能で、パスワードに一致しないと読み書きすることができないセキュリティ機能(HDDロック機能)が搭載されている。なお、パスワード照合に一定回数不成功となるとパスワード照合機能をロックする機能も準備されている。
HDDロック機能、ボックス機能(後述)を利用するためにはオプション購入のHDDが必要。

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

(8) USB
ローカル接続によるプリントを行うポート。

(9) 主電源、副電源
MFPを動作させるための電源スイッチ。

(10) 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。

(11) プリンタユニット

MFP制御コントローラから印刷が指示された際に、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。

(12) 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。ただし、同オプションパーツが未装着でもセキュリティ機能には影響しない。

(13) ローカル接続ユニット(※オプションパーツ)

クライアントPCとMFPを、セントロニクスインタフェース(パラレルポート)を使って接続し、ローカル接続でプリント機能を使うためのユニット。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。ただし、同オプションパーツが未装着でもセキュリティ機能には影響しない。

(14) 遠隔診断通信中継ユニット(※オプションパーツ)

RS-232Cを介してシリアル接続することが可能。公衆回線と接続されるモデムと接続すれば、故障時等に本インタフェースを介して遠隔診断機能(後述)を使用することができる。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。ただし、前提条件により同オプションパーツを装着しても利用できない。

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

(1) 基本機能

MFPには、基本機能としてコピー、プリント、スキャン、FAXといった画像に関するオフィスワークのための一連の機能が存在し、TOEはこれら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。

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の中止が行える。

(2) 機密文書プリント機能

プリントデータと共に機密文書パスワードを受信した場合、画像ファイルを印刷待機状態でRAMに保管し、パネルからの印刷指示と機密文書パスワード入力により印刷を実行する。

(3) ユーザチョイス機能

基本機能において必要となる画質調整(倍率、印刷濃度等)を始めとして、標準レイアウト、省エネ移行時間、オートリセット(一定時間操作を行わないと、操作パネルの表示が基本画面に戻る機能)時間をユーザが自由に設定することができる。

(4) ボックス機能

画像ファイルを保管するための領域として、HDDにボックスと呼称されるディレクトリを作成できる。ボックスにはすべてのユーザが利用することが可能なpublicボックスと、パスワードを設定して個別、又は利用者間でパスワードを共有することによって利用するボックスの2つのタイプが存在する。TOEは、パネル、又はクライアントPCからネットワークを介して伝達される操作要求に対して、ボックス、ボックス内の画像ファイルに対する操作要求を処理する。

(5) 管理者機能

TOEは、認証された管理者だけが操作することが可能な管理者モードにてボックスの管理、ネットワークや画質等の各種設定の管理等の機能を提供する。

(6) サービスエンジニア機能

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

(7) 残存情報の上書き削除機能

ジョブの終了、ジョブ管理機能からの削除操作、ボックスに保管される画像ファイルの削除、画像ファイルの保管期間経過による削除等によって、不要になった画像ファイルの上書き削除を行う。

(8) 遠隔診断機能

RS-232Cを介したモデム接続経由、FAXユニット経由、E-mail等いくつかの接続方式を利用して、コニカミノルタホールディングス関連会社によって運営されるMFPのサポートセンターと通信し、MFPの動作状態、管理者パスワード等の設定情報、印刷枚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。

(9) TOEの更新機能

TOEはTOE自身を更新するための機能を有する。遠隔診断機能よりコマンドを受け付けるとEthernetを介してFTPサーバよりダウンロードし更新することが可能。また、コンパクトフラッシュメモリ媒体を接続して行う方法もある。
セキュリティ強化機能(後述)を有効にした場合、Ethernetを介したTOE更新機能が利用できなくなる。

(10) 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に、暗号化基板にてHDD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鍵ワードにより暗号鍵を生成する。

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。

- 機密文書プリントファイル
  機密文書プリントによって登録される画像ファイル。
- ボックスファイル
  publicボックス以外のボックスに保管される画像ファイル。

また、MFPをリース返却、廃棄する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。

- 全ボックスファイル
  publicボックスを含めたボックス内に保管される画像ファイル。
- スワップデータファイル
  RAM領域に収まらないサイズの大きいコピー、PCプリント(機密文書プリントファイルを含む)にて発生する、画像を構成するためのファイル。
- オーバーレイ画像ファイル
  背景画像ファイル。
- HDD蓄積画像ファイル
  PCプリントからHDDに保管し、パネルからの操作で印刷を行うためのファイル。

・ 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。本ファイルは、セキュリティ強化機能が有効である状態においては存在しない。
・ 送信宛先データファイル
E-mailアドレス、電話番号等が含まれるファイル。

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

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

第二に、MFP上で保護資産が格納されることになるHDDやNVRAMからの情報の漏洩を防ぐために、本TOEは、MFP起動時に正当なHDDであることを検証し、HDDに書き込まれた画像データが不要になった時点で上書き削除する機能、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し、さらに、TOE範囲外のHDDのロック機能や暗号化基板による暗号化機能を利用してHDDに書き込むデータの暗号化機能を提供する。

第三に、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 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 全体制御ソフトウェア 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 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 全体制御ソフトウェア 評価報告書」（以下「評価報告書」という。）[13]に示されている。なお、評価方法は、CEM（[11][12]のいずれか）に準拠する。

1.4 評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。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、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 TOE概要

2.1 セキュリティ課題と前提

TOEが解決すべき課題と、必要とする前提を以下に示す。

2.1.1 脅威

本TOEは、表2-1に示す脅威を想定し、これに対抗する機能を備える。

表2-1 想定する脅威

識別子	脅　威
T.DISCARD-MFP (MFPのリース返却、廃棄)	リース返却、または廃棄となったMFPが回収された場合、悪意を持った者が、MFP内のHDD 、NVRAMを解析することにより、機密文書プリントファイル、ボックスファイル、オンメモリ画像ファイル、スワップデータファイル、オーバーレイ画像ファイル、HDD残存画像ファイル、送信宛先データファイル、設定されていた各種パスワード等の秘匿情報が漏洩する。
T.BRING-OUT-STORAGE (HDDの不正な持ち出し)	・悪意を持った者や悪意を持ったユーザが、MFP内のHDDを不正に持ち出して解析することにより、全ボックスファイル、スワップデータファイル、オーバーレイ画像ファイル、HDD蓄積画像ファイル、残存画像ファイルが漏洩する。 ・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には新たにボックスファイル、スワップデータファイル、オーバーレイ画像ファイル、HDD蓄積画像ファイル、残存画像ファイルが蓄積され、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-BOX (ユーザ機能を利用した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ボックスにアクセスし、ボックスファイルをダウンロード、印刷、送信（E-mail送信、FTP送信、SMB送信）することにより、ボックスファイルが暴露される。
T.ACCESS-SECURE-PRINT (ユーザ機能を利用した	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機密文書プリントファイルを印刷することにより、機密文書プリントファイルが暴露される。

機密文書プリントファイルへの不正なアクセス)	
T.UNEXPECTED-TRANSMISSION (ネットワーク設定の不正変更)	・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など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アドレスなど）を設定することにより、不正なMFPに機密文書プリントファイルが送付され暴露される。
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、機密文書プリントファイルが漏洩する可能性が高まる。

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はない。

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2-2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2-2 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は、課せられた役割として許可される

(サービスエンジニアの人的条件)	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鍵ワードは、各利用者から漏洩しない。
A.SETTING (セキュリティ強化機能の動作設定条件)	セキュリティ強化機能を有効化した上で、TOEが搭載されたMFPを利用する。

2.1.4 製品添付ドキュメント

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

＜管理者・一般利用者向けドキュメント＞
・bizhub 350 / 250 / 200 ユーザーズガイド セキュリティ機能編 Ver.1.01
・bizhub 362 / 282 / 222 User's Guide [Security Operations] Ver.1.01
・ineo 362 / 282 / 222 User's Guide [Security Operations] Ver.1.01
・VarioLink 3621 / 2821 / 2221 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 350 / 250 / 200 サービスマニュアル セキュリティ機能編 Ver.1.01
・bizhub 362 / 282 / 222 / ineo 362 / 282 / 222 / VarioLink 3621 / 2821 / 2221 SERVICE MANUAL SECURITY FUNCTION Ver.1.01

2.1.5 構成条件

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

- コニカミノルタビジネステクノロジーズ株式会社が提供するデジタル複合機、bizhub 350、bizhub 250、bizhub 200、bizhub 362、bizhub 282、bizhub 222、ineo 362、ineo 282、ineo 222、VarioLink 3621、VarioLink 2821、VarioLink 2221にオプションであるHDD、暗号化基板、FAXユニット、ローカル接続ユニットを搭載した状態。

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で、HDDに書き込まれる画像データが不要になった時点で上書き削除を実行する機能(以上、「残存情報上書き削除機能」)を保持することで、HDD上には利用中である必要最小限のデータが存在することになり、HDD内のデータが漏洩する可能性を防いでいる。
また、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利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。また、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。

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ための暗号鍵の生成機能(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、解読が困難と成る。

(3) 脅威「T.ACCESS-BOX(ユーザ機能を利用した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、許可されたユーザのみ、又は許可されたユーザ間で共有して利用する画像ファイルの保管場所であるボックスに対して、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、ボックスのアクセスにおける認証機能、ボックスに対するアクセス制御機能、ボックスに関する設定の変更機能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」)を保持することで、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、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。

(4) 脅威「T.ACCESS-SECUIRE-PRINT(ユーザ機能を利用した機密文書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機密文書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、機密文書パスワードによる識別認証機能、機密文書プリントファイルに対するアクセス制御機能(以上、「機密文書プリント機能」)を保持することで、機密文書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。

(5) 脅威「T.UNEXPECTED-TRANSMISSION(ネットワーク設定の不正変更)」に対抗するためのセキュリティ機能
本脅威は、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。

(6) 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、機密文書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、セキュリティに関係する特定の機能設定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、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に制限され、結果的にボックスファイル、機密文書プリントファイルの漏洩に発展することを防いでいる。

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、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。

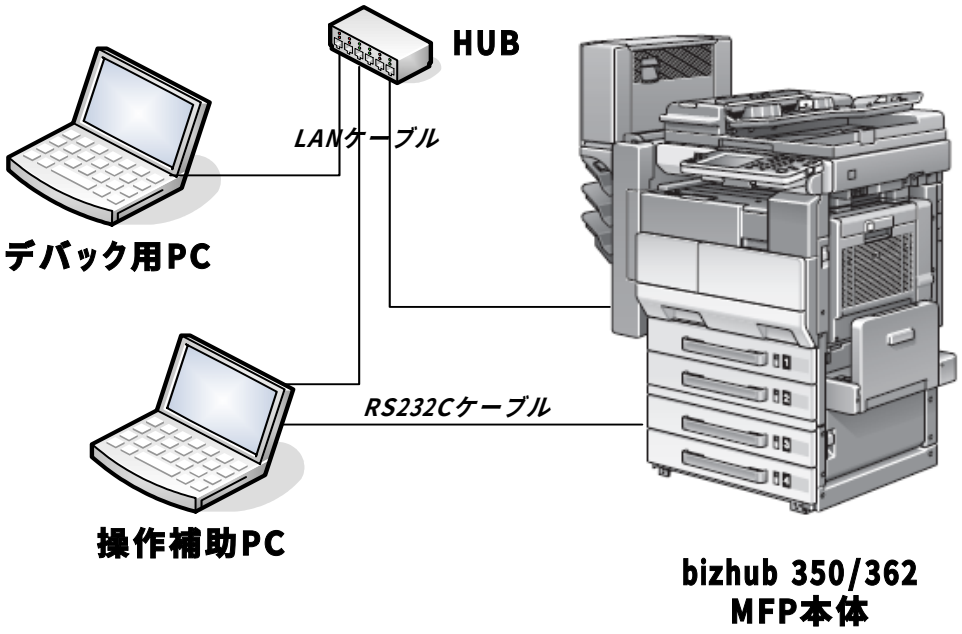

図3-1　開発者テストの構成図

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。

なお、TOEが搭載されるMFPとして、bizhub 350、bizhub 362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 350、bizhub 250、bizhub 200の違いは、コピー/プリント速度、及び耐久性保証値の違いだけであることを開発者から提供された資料により確認。

・bizhub 362、bizhub 282、bizhub 222の違いは、コピー/プリント速度、及び耐久性保証値の違いだけであることを開発者から提供された資料により確認。

・「bizhub 350、bizhub 250、bizhub 200」と「bizhub 362、bizhub 282、bizhub 222」の違いは、表示言語の違いだけであることを開発者から提供された資料により確認。

・bizhub 362に実施した開発者テストの一部を抽出したサンプリングテストをbizhub 350に実施し、表示言語の違いは除いて、得られたテスト結果が同一でありセキュリティ機能に影響を与えないことを確認。

2) 開発者テスト概説

開発者の実施したテストは以下のとおり。

a. テスト概要

開発者テストで実施されたテストの概要は以下のとおり。

＜テスト手法＞

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

＜テストで使用したツール等＞

テストで使用したツール等を表3-1に示す。

表3-1 開発者テストで使用したツール等

ハードウェア・ソフトウェア名称	概要・利用目的
Internet Explorer Ver.6.0.2800.1106	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。
TORNADO Ver2.1.2	VxWorks5.x用開発環境を構築するためのソフトウェアツール。デバッグ用PC上で起動し、実機で動作するデバッグ用オブジェクトの実行制御、デバッグを可能とする。MFP本体の動作ログを収集するために使用する。
Tiny FTP Daemon Ver. 0.52d	デバッグ用PC上で動作させるFTPサーバソフトウェア。操作補助PCから実行オブジェクトをダウンロードするために使用する。
Fiddler Ver.1.2.2	HTTP他のWebアクセスのモニター＆解析ツール．MFP本体と操作補助PC間の通信を解析して、イレギュラーテストを行うために使用する。
sslproxy Ver.1.2	操作補助PC上で動作させるSSL-Proxyサーバソフトウェア。PSWCを用いたテストで使用する。本体装置とはSSLで通信し、ブラウザソフトとは非SSLで通信するので、SSLによる暗号化を避けてFiddlerでのモニターが可能となる。
ディスクダンプエディタ Ver.1.33	操作補助PC上で起動し、HDDの内容のダンプ表示が可能なソフトウェア。ダンプしたデータをバ

ハードウェア・ソフトウェア名称	概要・利用目的
	イナリ形式で保存し、解析するために使用する。
Stirling Ver.1.31	操作補助PC上で、バイナリ形式ファイルを閲覧するためのビューアソフト。ダンプしたバイナリデータを検証するために使用する。
メモ帳	Windows2000に付属されるテキストエディタ。TORNADOのコンソールに表示されたログデータを、テキスト保存するために、デバッグ用PCで使用する。
MSG SOFT MIB Browser Professional SNMPv3Edition (以後MIB Browserと省略) Ver. 10.0.0.4044	操作補助PC上で動作させるMIBブラウザ専用ソフトウェア。 SNMP v1/v2/v3 の書き込み禁止確認テストに使用する。
BlackJumboDog Ver4.1.3	イントラネット用の簡易サーバソフトウェア。 E-Mail、FTPサーバ機能として、ボックス内ファイルのネット配信テストに使用する。
OPENSSL-0.9.8-Win32	補助操作PC上で動作させるSSLおよびハッシュ関数の暗号化ツールソフトウェア。HDD暗号鍵生成確認に使用する。
TeraTerm Pro Ver. 4.29	補助操作PC上で動作させるターミナルソフトウェア。 MFP本体の動作ログを収集するために使用する。
NMAP 4.01	補助操作PC上で動作させるPort Scanソフトウェア。 セキュリティ強化設定後の機能制限テストで使用する。
Wireshark 0.99.5	補助操作PC上で動作させるネットワークパケットアナライザソフトウェア。セキュリティ強化設定後の機能制限テストのログを記録するのに使用する。
PageScope Web Connection (PSWC) Ver A11U-0100-G10-06	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。
KONICAMINOLTA 362/282/222 Driver ver1.01	PCからのボックス保存、機密文書保存のテストに使用する。 尚、bizhub 350/250/200の場合は、それに対応するプリンタドライバを利用する。

b. 実施テストの範囲

テストは開発者によって33項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。深さ分析が実施され、TOE設計に記述されたすべてのサブシステムとサブシステムインタフェースが十分にテストされたことが検証されている。

c. 結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

3.3.2 評価者独立テスト

評価者は、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることの再確認のための独立テストを実施した。評価者が実施した独立テストの概要を以下に示す。

1) 評価者独立テスト環境

評価者が実施したテストの構成は、開発者テストと同様の構成である。

評価者テストは本STにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

2) 評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

a. 独立テストの観点

評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点での独立テストを考案した。

＜テストの観点＞

① 開発者テストの状況を踏まえ､すべてのセキュリティ機能をテストする。
② すべての確率的・順列的メカニズムをテスト対象とする。
③ 確率的・順列的メカニズムのテストにおいて、TSFIへのパスワードの入力方式の違いによるふるまいをテストする。
④ オプションパーツの有無に関係なく利用可能なセキュリティ機能をテストする。

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という方法で実施された。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	ユーザの識別認証等の確率的・順列的メカニズムに着目し、文字桁数及び文字種類を変化されたテストを実施した。
観点③	パスワードの入力方式の違いによるふるまいを確認するために、動作させるインタフェースを考慮してテストを実施した。
観点④	HDDの有無が異なる条件で、機密文書プリント機能の動作を確認するテストを実施した。
観点⑤	暗号鍵生成機能、暗号化基板動作サポー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 想定外のサービスを起動している可能性がある。
② 脆弱性検査ツールにより公知の脆弱性が検出される可能性がある。
③ 入力データのバリエーションによって、TOEのふるまいに影響を与える可能性がある。
④ 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 利用者の排他制御が適切に行われない可能性がある。
⑥ 暗号鍵ワードの設定状況によりセキュリティ機能に影響する可能性がある。

b. 実施テストの範囲

評価者は、潜在的な脆弱性が悪用される可能性があるかを決定するため、以下の侵入テストを実施した。

＜テスト環境＞

評価者が実施した侵入テストの構成を図3-2に示す。

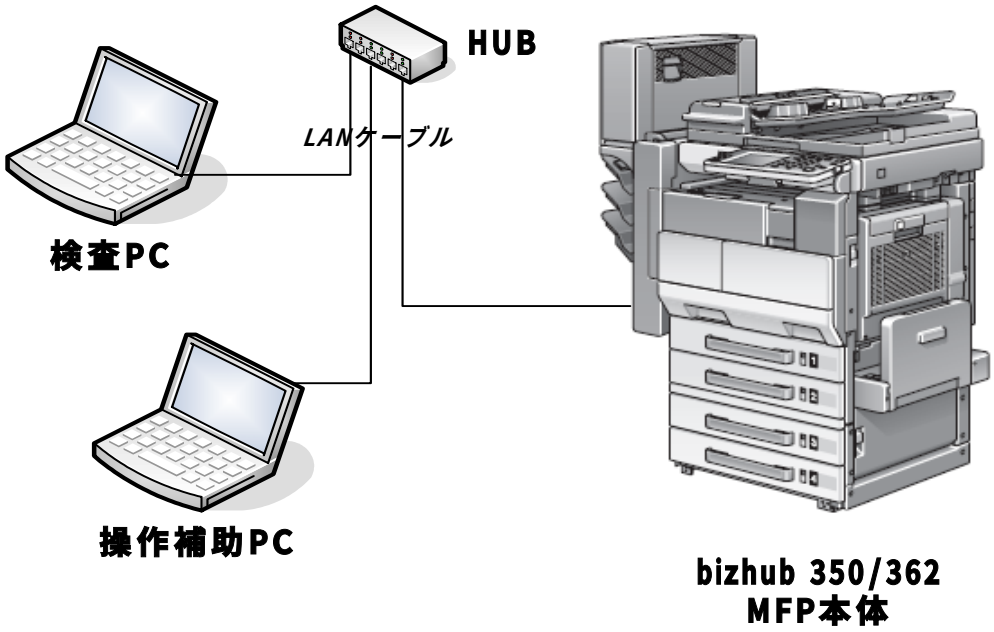

図3-2 侵入テストの構成図

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

＜テストで使用したツール等＞
テストで使用したツール等を表3-3に示す。

表3-3 侵入テストで使用したツール等

テスト構成環境	詳細
検査対象(TOE)	・bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221に搭載されたTOE(バージョン：A11U-0100-G10-06) ・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 2000(SP4)で動作するネットワーク端子付きのPC。 ・表3-1で示されているツールも利用(Fiddler、TamperIE等) ・PSWC(PageScope Web Connection の略)、HTTPS などを用いて 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 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(プラグインや脆弱性データベースは2009年5月25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 ・システム上に存在する脆弱性を検査するセキュリティスキャナ。 ④ TamperIE 1.0.1.13 ・Internet Explorer等の一般的なWebブラウザから送信されるデータを任意のデータに改ざんするWebプロキシツール。 ⑤ sslproxy Version 2.0 ・SSL-プロキシサーバソフトウェア ⑥ Fiddler 2.2.0.7 ・MS社で提供するHTTPのやりとりをモニターするWebデバッガー。 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 ・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概要＞

懸念される脆弱生ごとのテスト概要を表3-4に示す。

表3-4 懸念される脆弱性とテスト概要

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

懸念される脆弱性	テスト概要
	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	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⑥	暗号鍵ワードの設定状況によりセキュリティ機能のふるまいに影響を与えないことを確認するテストを実施した。

c. 結果

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

3.4 評価結果

3.4.1 評価結果

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

3.4.2 評価者コメント/勧告

脅威「T.BRING-OUT-STORAGE(HDDの不正な持ち出し)」に対抗するために、HDDロック動作サポート機能+HDD検証機能、又は暗号化基板動作サポート機能+暗号鍵生成機能、もしくはその両者を消費者は選択することができるが、HDDロック動作サポート機能+HDD検証機能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、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

・オプションパーツである、FAXユニット、ローカル接続ユニットが未装着でも、本TOEのセキュリティ機能には影響しない。

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。

DNS	Domain Name System (DNS)
FTP	File Transfer Protocol (FTP)
HDD	Hard Disk Drive (ハードディスクドライブ)
HTTPS	HyperText Transfer Protocol Security (HTTPS)
MFP	Multiple Function Peripheral (デジタル複合機)
MIB	Management Information Base (MIB)
NVRAM	Non-Volatile Random Access Memory (NVRAM)
RAM	Random Access Memory (RAM)
SMB	Server Message Block (SMB)
SMTP	Simple Mail Transfer Protocol (SMTP)
SNMP	Simple Network Management Protocol (SNMP)
SSL	Secure Socket Layer (SSL)

本報告書で使用された用語の定義を以下に示す。

DNS	インターネットでドメイン名とIPアドレスの関係を管理するプロトコルのこと。
FTP	TCP/IPネットワークで使うファイル転送プロトコルのこと。
HDDロック機能	HDDにパスワードを設定し、パスワードに一致しないと読み書きすることができなくなる機能のこと。
HDDロックパスワード	HDDの読み書きが禁止されている状態を解除するためのパスワードのこと。
HTTPS	Webサーバとクライアントの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。
publicボックス	すべてのユーザが利用することが可能なボックスに格納された画像ファイルのこと。
SMB	Windowsでファイル共有、プリンタ共有を実現するプロトコルのこと。
SMTP	TCP/IPでメールを転送する時のプロトコルのこと。
SNMP	ネットワーク経由で各種機器を管理するためのプロトコルのこと。
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。
暗号鍵ワード	暗号化基板において暗号化・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。
機密文書パスワード	機密文書プリントファイルに対する操作を行う前に許可された利用者あるかどうかを確認するためのパスワードのこと。
機密文書プリントファイル	機密文書プリントによって登録される画像ファイルのこと。
機密文書プリント	プリンタドライバで機密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。
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。
ボックスファイル	「public」以外のボックスに保管される画像ファイルのこと。

7 参照

[1] bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 全体制御ソフトウェア セキュリティターゲット バージョン 1.03 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 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 全体制御ソフトウェア 評価報告書 第2版 2009年8月12日 みずほ情報総研株式会社 情報セキュリティ評価室