



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3月23日 (IT認証9252)
認証番号	C0241
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 C652 / bizhub C552 / bizhub C452 / ineo ⁺ 652 / ineo ⁺ 552 / ineo ⁺ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c 全体制御ソフトウェア 英語名： bizhub C652 / bizhub C552 / bizhub C452 / ineo ⁺ 652 / ineo ⁺ 552 / ineo ⁺ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c Control Software
TOEのバージョン	A0P00Y0-0100-GM0-12
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11月30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。

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)

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 C652 / bizhub C552 / bizhub C452 / ineo+ 652 / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c 全体制御ソフトウェア、英語名：bizhub C652 / bizhub C552 / bizhub C452 / ineo+ 652 / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c Control Software、バージョン：A0P00Y0-0100-GM0-12」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
1.1	はじめに	1
1.1.1	評価保証レベル	1
1.1.2	PP適合	1
1.2	評価製品	1
1.2.1	製品名称	1
1.2.2	製品概要	2
1.2.3	TOE範囲とセキュリティ機能	2
1.3	評価の実施	9
1.4	評価の認証	10
2	TOE概要	11
2.1	セキュリティ課題と前提	11
2.1.1	脅威	11
2.1.2	組織のセキュリティ方針	13
2.1.3	操作環境の前提条件	14
2.1.4	製品添付ドキュメント	14
2.1.5	構成条件	15
2.2	セキュリティ対策	15
3	評価機関による評価実施及び結果	20
3.1	評価方法	20
3.2	評価実施概要	20
3.3	製品テスト	20
3.3.1	開発者テスト	20
3.3.2	評価者独立テスト	24
3.3.3	評価者侵入テスト	26
3.4	評価結果	29
3.4.1	評価結果	29
3.4.2	評価者コメント/勧告	29
4	認証実施	30
5	結論	31
5.1	認証結果	31
5.2	注意事項	31
6	用語	32
7	参照	35

1 全体要約

1.1 はじめに

この認証報告書は、「日本語名：bizhub C652 / bizhub C552 / bizhub C452 / ineo+ 652 / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c 全体制御ソフトウェア、英語名：bizhub C652 / bizhub C552 / bizhub C452 / ineo+ 652 / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c Control Software、バージョン：A0P00Y0-0100-GM0-12」（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充分性の根拠は、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 C652 / bizhub C552 / bizhub C452 / ineo+ 652 / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c 全体制御ソフトウェア

英語名： bizhub C652 / bizhub C552 / bizhub C452 / ineo+ 652 / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c Control Software

バージョン： A0P00Y0-0100-GM0-12

開発者： コニカミノルタビジネステクノロジー株式会社

1.2.2 製品概要

本TOEが搭載される、bizhub C652、bizhub C552、bizhub C452、ineo+ 652、ineo+ 552、ineo+ 452、VarioLink 6522c、VarioLink 5522c、VarioLink 4522c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 C652 / bizhub C552 / bizhub C452 / ineo+ 652 / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c 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、ASICを利用し、HDDに書き込まれる画像データを含むすべてのデータを暗号化することにより、不正なアクセスを防止することが可能である。他に、TOEは各種上書き削除規格に則った削除方式を有し、HDDのすべてのデータを完全に削除する機能や、FAXを踏み台として内部ネットワークにアクセスする危険性に対して、FAX公衆回線網からのアクセスを制御する機能を提供する。

1.2.3 TOE範囲とセキュリティ機能

1.2.3.1 TOE に関する役割

本TOEに関する役割を以下に示す。

(1) ユーザ

MFPに登録されるMFPの利用者。一般には、オフィス内の従業員等が想定される。

(2) 管理者

MFPの運用管理を行うMFPの利用者。MFPの動作管理や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、オフィス内に入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、FAXユニットはMFPのオプションパーツである。本TOEの動作環境としては、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。

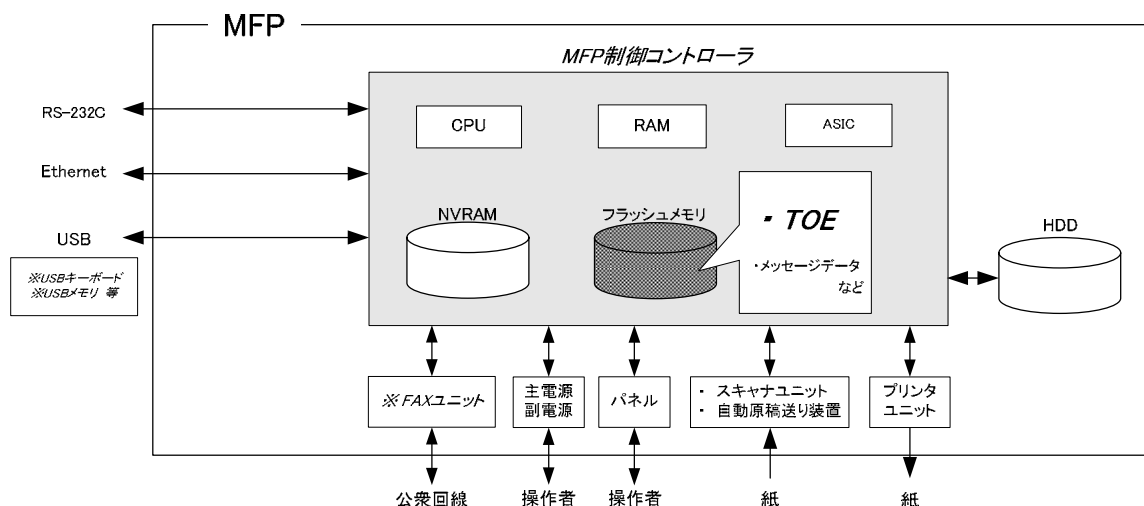


図1-1 TOEに関するハードウェア構成

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) 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) 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暗号化機能を実装した特定利用目的集積回路。
- (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管されるほか、伸張変換等で一時的に画像データ、送信宛先データが保管される領域としても利用される。
- (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。
- (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
USBメモリへの画像のコピー、USBメモリからの画像のコピーやプリント、TOEのアップデート等を本インターフェースから実施できる。
- (11) RS-232C
D-sub9ピンを介して、シリアル接続することが可能。故障時等に本インタ

フェースを介してメンテナンス機能を使用することができる。また公衆回線と接続されるモデムを接続して、遠隔診断機能(後述)を利用することも可能。

(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。

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) セキュリティ文書プリント機能(セキュリティ文書機能)

プリントデータと共にセキュリティ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保管し、パネルからの印刷指示とセキュリティ文書パスワード入力により印刷を実行する。

(3) 認証&プリント機能

本機能を利用者が利用設定すると、通常のプリントデータを印刷待機状態で保管し、パネルからのユーザ認証処理で印刷を行う機能。利用設定がなくとも、プリントデータに本機能の動作指定がある場合は、利用者による利用設定がある場合と同様に動作する。

(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、ユーザが占有する個人ボックス、登録されたユーザが一定数のグループを作って共同利用するための共有ボックス、所属部門のユーザ間で共有するグループボックスといった3つのタイプのボッ

クスを設定することができる。個人ボックスは、所有するユーザだけに操作が制限され、共有ボックスは、そのボックスに設定されるパスワードを利用者間で共用することによって、アクセス制御を行っている。グループボックスは、その部門の利用を許可されたユーザだけに操作が制限される。TOEは、パネル、またはクライアントPCからネットワークを介したネットワークユニットから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) ユーザ認証機能

TOEは、MFPを利用する利用者を制限することができる。パネル、またはネットワークを介したアクセスにおいてTOEはMFPの利用を許可されたユーザであることをユーザID、ユーザパスワードを使って識別認証する。識別認証が成功すると、TOEはユーザに対して基本機能及びボックス機能などの利用を許可する。

ユーザ認証方式には以下に示す方式がある。

【本体認証】

MFP制御コントローラ上のHDDにユーザID、ユーザパスワードを登録し、MFPにて認証する方式。

【外部サーバ認証】

MFP本体側でユーザID及びユーザパスワードを管理せず、オフィス内LANで接続されるユーザ情報管理サーバ上に登録されるユーザID及びユーザパスワードを用いて、MFPにて認証処理を行い、認証する方式。

本評価においては、本体認証方式及びActive Directoryを利用した外部サーバ認証方式が評価対象となっている。

(6) 部門認証機能

TOEは、MFPを利用する利用者を部門単位でグルーピングして管理することができる。

部門認証には以下に示す方式がある。

【ユーザ認証連動方式】

ユーザに予め部門IDを設定し、ユーザの認証時に所属部門の部門IDと関連付ける方式。

【個別認証方式】

各部門IDに設定される部門パスワードによって認証された場合に当該部門IDと関連付ける方式。

(7) 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、本体認証の場合におけるユーザの情報の管理、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。

(8) 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。

(9) 暗号鍵生成機能

ASIC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により暗号鍵を生成する。

(10) 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、WebDAV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。

(11) 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他、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)、USBメモリ等のメモリ媒体を接続して行う方法がある。

(12) 暗号通信機能

TOEはクライアントPCからMFPへ送信するデータ、MFPからダウンロードして受信するデータをSSL/TLSを利用して暗号化することができる。本機能は、管理者機能にて動作設定が行える。

(13) S/MIME証明書自動登録機能

S/MIME用に各宛先に設定可能な証明書(ITU-T X.509準拠)を自動登録する機能。メールに証明書が添付されている場合、当該メールのヘッダー情報にてユーザIDを判別し、証明書を当該ユーザの証明書として登録する。

(14) FAXユニット制御機能

MFPにFAXユニットを装着した場合、FAX公衆回線口からFAXユニットを通し

て、MFPに接続された内部ネットワークへのアクセスを禁止する。

(15) セキュリティ強化機能

管理者機能、サービスエンジニア機能におけるセキュリティ機能のふるまいに関係する各種設定機能は、管理者機能における「セキュリティ強化機能」による動作設定により、セキュアな値に一括設定が行える。設定された各設定値は、個別に設定を脆弱な値に変更することが禁止される。また、個別には動作設定機能を持たない機能として、ネットワーク設定のリセット機能、ネットワークを介したTOEの更新機能が存在するが、これらの機能の利用は禁止される。

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。

- ・ セキュリティ文書プリントファイル
セキュリティ文書プリントによって登録される画像ファイル。
- ・ 認証&プリントファイル
認証&プリント機能を利用してプリントデータが登録される場合に認証&プリントファイルとして保管される画像ファイル。
- ・ ボックスファイル
個人ボックス、共有ボックス、グループボックスに保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。

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

- プリント画像ファイル処理において生成されたテンポラリデータファイル
- ・ 送信宛先データファイル
- 画像を送信する宛先となる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、保護資産であるセキュリティ文書ファイル、認証&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、設定値が格納されるNVRAMからの情報の漏洩を防ぐために、本TOEは、HDDの全領域の上書き削除機能、NVRAMの設定値の初期化機能、また、TOE範囲外のASIC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、ユーザや管理者が利用するクライアントPCと本TOEの間で通信される画像ファイルを安全に保護するために、正しい相手先との通信に利用する高信頼チャンネル機能、S/MIMEを利用して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。

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。

本TOEのセキュリティ設計が適切であること。

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。

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。

上記 、 、 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 C652 / bizhub C552 / bizhub C452 / ineo+ 652 / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c 全体制御ソフトウェア A0P00Y0-0100-GM0-12 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 C652 / bizhub C552 / bizhub C452 / ineo+ 652 / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c 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11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、セキュリティ文書プリントファイル、ボックスファイル、認証&プリントファイル、オンメモリ画像ファイル、保管画像ファイル、HDD残存画像ファイル、画像関連ファイル、送信宛先データファイル、設定されていた各種パスワード等の秘匿情報が漏洩する。
T.BRING-OUT-STORAGE (HDDの不正な持ち出し)	<ul style="list-style-type: none"> ・悪意を持った者や悪意を持ったユーザが、MFP内のHDDを不正に持ち出して解析することにより、セキュリティ文書プリントファイル、ボックスファイル、認証&プリントファイル、オンメモリ画像ファイル、保管画像ファイル、HDD残存画像ファイル、画像関連ファイル、送信宛先データファイル、設定されていた各種パスワード等が漏洩する。 ・悪意を持った者や悪意を持ったユーザが、MFP内のHDDを不正にすりかえる。すりかえられたHDDには新たにセキュリティ文書プリントファイル、ボックスファイル、認証&プリントファイル、オンメモリ画像ファイル、保管画像ファイル、HDD残存画像ファイル、画像関連ファイル、送信宛先データファイル、設定されていた各種パスワード等が蓄積され、悪意を持った者や悪意をもったユーザは、このすりかえたHDDを持ち出して解析することにより、これら画像ファイル等が漏洩する。
T.ACCESS-PRIVATE-BOX (ユーザ機能を利用した個人ボックスへの)	悪意を持った者や悪意を持ったユーザが、他のユーザが個人所有するボックスにアクセスし、ボックスファイルを移動、コピー、ダウンロード、印刷、送信（E-mail送信、FTP送信、FAX送信、SMB送信、WebDAV送信）するこ

不正なアクセス)	とにより、ボックスファイルが暴露される。
T.ACCESS-PUBLIC-BOX (ユーザ機能を利用した共有ボックスへの不正なアクセス)	悪意を持った者や悪意を持ったユーザが、利用を許可されない共有ボックスにアクセスし、ボックスファイルを移動、コピー、ダウンロード、印刷、送信 (E-mail送信、FTP送信、FAX送信、SMB送信、WebDAV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-GROUP-BOX (ユーザ機能を利用したグループボックスへの不正なアクセス)	悪意を持った者や悪意を持ったユーザが、そのユーザが所属していない部門が所有するグループボックスにアクセスし、ボックスファイルを移動、コピー、ダウンロード、印刷、送信 (E-mail送信、FTP送信、FAX送信、SMB送信、WebDAV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セキュリティ文書プリントファイル、認証&プリントファイルへの不正なアクセス)	<ul style="list-style-type: none"> ・悪意を持った者や悪意を持ったユーザが、利用を許可されないセキュリティ文書プリントファイルを印刷することにより、セキュリティ文書プリントファイルが暴露される。 ・悪意を持った者や悪意を持ったユーザが、他のユーザが登録した認証&プリントファイルを印刷することにより、認証&プリントファイルが暴露される。
T.UNEXPECTED-TRANSMISSION (想定外対象先への送信)	<ul style="list-style-type: none"> ・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。 <p><ボックスファイル送信に関するネットワーク設定></p> <ul style="list-style-type: none"> ➢ SMTP サーバに関する設定 ➢ DNS サーバに関する設定 <ul style="list-style-type: none"> ・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、セキュリティ文書プリントファイル、認証&プリントファイルが暴露される。 ・悪意を持った者や悪意を持ったユーザが、TSI受信設定を変更することにより、ボックスファイルが意図しない保管領域に保存されて暴露される。 ・悪意を持った者や悪意を持ったユーザが、PC-FAX動作

	<p>設定を変更し、共有ボックス等のボックスへの保管設定状態から、全ユーザ共通領域に保管される設定に変更することにより、ボックスファイルが意図しない保管領域に保存されて暴露される。</p> <p>本脅威は、PC-FAX動作設定が、ボックスへの保管設定状態を運用として意図している場合のみ発生する脅威である。</p>
T.ACCESS-SETTING (セキュリティに関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する設定を変更してしまうことにより、ボックスファイル、セキュリティ文書プリントファイル、認証&プリントファイルが漏洩する可能性が高まる。
T.BACKUP-RESTORE (バックアップ機能、リストア機能の不正な使用)	悪意を持った者や悪意を持ったユーザが、バックアップ機能、リストア機能を不正に使用することにより、ボックスファイル、セキュリティ文書プリントファイル、認証&プリントファイルが漏洩する。またパスワード等の秘匿性のあるデータが漏洩し、各種設定値が改ざんされる。

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-DATA (画像ファイルのセキュアな通信)	IT機器間にて送受信される秘匿性の高い画像ファイル(セキュリティ文書プリントファイル、ボックスファイル、認証&プリントファイル)は、組織・利用者が希望する場合において、正しい相手先に対して信頼されるパスを介して通信する、または暗号化しなければならない。
P.REJECT-LINE (公衆回線からのアクセス禁止)	公衆回線網から、MFPのFAX公衆回線口を介しての内部ネットワークへのアクセスは禁止しなければならない。

ここでいう「IT機器間」とは、利用者が使用するクライアントPCとMFPの間を指している。

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)	<ul style="list-style-type: none"> ・TOEが搭載されるMFPを設置するオフィス内LANは、盗聴されない。 ・TOEが搭載されるMFPを設置するオフィス内LANが外部ネットワークと接続される場合は、外部ネットワークからMFPへアクセスできない。
A.SECRET (秘密情報に関する運用条件)	TOEの利用において使用される各パスワードや暗号化ワードは、各利用者から漏洩しない。
A.SETTING (セキュリティ強化機能の動作設定条件)	セキュリティ強化機能が有効化した上で、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 C652 / C552 / C452 ユーザーズガイド セキュリティ機能編
Ver.1.02
- ・ bizhub C652 / C552 / C452 User's Guide [Security Operations] Ver.1.02
- ・ ineo+ 652 / 552 / 452 User's Guide [Security Operations] Ver.1.02
- ・ VarioLink 6522c / 5522c / 4522c User's Guide [Security Operations]
Ver.1.02

< サービスエンジニア向けドキュメント >

- ・ bizhub C652 / C552 / C452 サービスマニュアル セキュリティ機能編
Ver.1.02

- ・ bizhub C652 / C552 / C452 SERVICE MANUAL SECURITY FUNCTION
Ver.1.02
- ・ ineo+ 652 / 552 / 452 SERVICE MANUAL SECURITY FUNCTION
Ver.1.02
- ・ VarioLink 6522c / 5522c / 4522c SERVICE MANUAL SECURITY FUNCTION
Ver.1.02

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。

- ・ ユーザの識別認証において外部サーバ認証方式を選択した場合、外部認証サーバとしてWindowsプラットフォームのネットワーク環境にてユーザ情報を一元管理するためにWindows Server 2000(それ以降)が提供するディレクトリサービスであるActive Directoryが必要。

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り、HDD内のデータが漏洩する可能性を想定している。

本TOEの範囲外であるASICの暗号化機能を利用し、本TOEで、HDDに書き込むデータの暗号化を行う暗号鍵の生成(以上、「暗号鍵生成機能」)、及びASICと連動するための機能(以上、「ASIC動作サポート機能」)を保持することで、暗号

化されたデータがHDDに格納され、HDDから情報を読み出した場合でも、解読が困難となる。

(3) 脅威「T.ACCESS-PRIVATE-BOX(ユーザ機能を利用した個人ボックスへの不正なアクセス)」に対抗するためのセキュリティ機能

本脅威は、ユーザ各位が画像ファイルの保管に利用する個人ボックスに対して、ユーザ機能を利用して不正な操作が行われる可能性を想定している。

本TOEで、MFPの諸機能を利用するにあたって、ユーザ及び管理者を識別認証する機能(以上、「ユーザ機能」、「管理者機能」)、個人ボックスに対するアクセス制御機能(以上、「ボックス機能」)、ユーザ及び個人ボックスに関する設定の変更を管理者及びユーザに制限する機能(以上、「管理者機能」、「ユーザ機能」、「ボックス機能」)を保持することで、ユーザ及び個人ボックスの設定の変更は管理者及び許可されたユーザのみに制限され、個人ボックスの操作は、正規のユーザのみに制限されることとなり、ユーザ機能を利用して不正な操作が行われることを防いでいる。

また、本TOEは、ユーザの識別認証機能において、本TOEの範囲外であるActive Directoryによるユーザ情報管理サーバから認証情報の取得を行うための機能(以上、「外部サーバ認証動作サポート機能」)も保持している。

(4) 脅威「T.ACCESS-PUBLIC-BOX(ユーザ機能を利用した共有ボックスへの不正なアクセス)」に対抗するためのセキュリティ機能

本脅威は、ユーザが共有して利用する画像ファイルの保管場所である共有ボックスに対して、ユーザ機能を利用して不正な操作が行われる可能性を想定している。

本TOEで、MFPの諸機能を利用するにあたって、ユーザ及び管理者を識別認証する機能(以上、「ユーザ機能」、「管理者機能」)、共有ボックスへのアクセスにおける識別認証機能、共有ボックスに対するアクセス制御機能、共有ボックスに関する設定の変更を管理者及び許可されたユーザに制限する機能(以上、「ボックス機能」)、ユーザに関する設定の変更を管理者及び許可されたユーザに制限する機能(以上、「管理者機能」、「ユーザ機能」)を保持することで、共有ボックス及びユーザの設定の変更は管理者及び許可されたユーザのみに制限され共有ボックスの操作は正規のユーザのみに制限されることとなり、ユーザ機能を利用して不正な操作が行われることを防いでいる。

また、本TOEは、ユーザの識別認証機能において、本TOEの範囲外であるActive Directoryによるユーザ情報管理サーバから認証情報の取得を行うための機能(以上、「外部サーバ認証動作サポート機能」)も保持している。

- (5) 脅威「T.ACCESS-GROUP-BOX(ユーザ機能を利用したグループボックスへの不正なアクセス)」に対抗するためのセキュリティ機能

本脅威は、その部門の利用が許可されたユーザが利用する画像ファイルの保管場所であるグループボックスや、その中のボックスファイルに対してユーザ機能を利用して不正な操作が行われる可能性を想定している。

本TOEで、MFPの諸機能を利用するにあたって、ユーザ及び管理者を識別認証する機能(以上、「ユーザ機能」、「管理者機能」)、グループボックスに対するアクセス制御機能、グループボックスに関する設定の変更を管理者及びユーザに制限する機能(以上、「ボックス機能」)、ユーザに関する設定の変更を管理者及び許可されたユーザに制限する機能(以上、「管理者機能」、「ユーザ機能」)を保持することで、グループボックス及びユーザの設定の変更は管理者及び許可されたユーザのみに制限され、グループボックスの操作は正規のユーザのみに制限されることとなり、ユーザ機能を利用して不正な操作が行われることを防いでいる。

また、本TOEは、ユーザの識別認証機能において、本TOEの範囲外であるActive Directoryによるユーザ情報管理サーバから認証情報の取得を行うための機能(以上、「外部サーバ認証動作サポート機能」)も保持している。

- (6) 脅威「T.ACCESS-SECURE-PRINT(ユーザ機能を利用したセキュリティ文書プリントファイル、認証&プリントファイルへの不正なアクセス)」に対抗するためのセキュリティ機能

本脅威は、ユーザ機能を利用したセキュリティ文書プリントファイル、認証&プリントファイルに対して不正な操作が行われてしまう可能性を想定している。

本TOEで、MFPの諸機能を利用するにあたって、ユーザ及び管理者を識別認証する機能(以上、「ユーザ機能」、「管理者機能」)、セキュリティ文書パスワードによる認証機能、認証&プリントファイルを登録したユーザを識別認証する機能、セキュリティ文書プリントファイル及び認証&プリントファイルに対するアクセス制御機能、セキュリティ文書プリントファイル及び認証&プリントファイルに関する設定の変更を管理者に制限する機能(以上、「セキュリティ文書プリント機能」)、ユーザに関する設定の変更を管理者及び許可されたユーザに制限する機能(以上、「管理者機能」、「ユーザ機能」)を保持することで、セキュリティ文書プリントの設定の変更は管理者に、ユーザの設定の変更は管理者及び許可されたユーザのみに制限され、セキュリティ文書プリントファイル及び認証&プリントファイルの操作は正規のユーザのみに制限されることとなり、ユーザ機能を利用して不正な操作が行われることを防いでいる。

また、本TOEは、ユーザの識別認証機能において、本TOEの範囲外であるActive Directoryによるユーザ情報管理サーバから認証情報の取得を行うための機能

(以上、「外部サーバ認証動作サポート機能」)も保持している。

- (7) 脅威「T.UNEXPECTED-TRANSMISSION(想定外対象先への送受信)」に対抗するためのセキュリティ機能

本脅威は、送信に関するネットワーク設定、MFPのアドレスに関するネットワーク設定、PC-FAX動作設定、TSI受信設定を不正に変更された場合に想定外対象先へ情報が送信されてしまう可能性を想定している。

本TOEで、管理者を識別認証する機能、ネットワーク設定、PC-FAX動作設定、TSI受信設定等の変更を管理者のみに制限する機能(以上、「管理者機能」)を保持することで、ネットワーク設定、PC-FAX動作設定、TSI受信設定等の変更は管理者に制限され、想定外対象先へ情報が送信されてしまうことを防いでいる。

- (8) 脅威「T.ACCESS-SETTING(セキュリティに関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する特定の機能設定を変更されることにより、結果的にボックスファイルやセキュリティ文書プリントファイル、認証&プリントファイルの漏洩に発展する可能性を想定している。

本TOEで、管理者を識別認証する機能(以上、「管理者機能」、「SNMP管理者機能」)、サービスエンジニアを識別認証する機能(以上、「サービスモード機能」)、セキュリティに関する特定の機能設定を管理者及びサービスエンジニアに制限する機能(以上、「管理者機能」、「SNMP管理者機能」、「サービスモード機能」)を保持することで、セキュリティに関する特定の機能設定の変更は管理者及びサービスエンジニアに制限され、結果的にボックスファイルやセキュリティ文書プリントファイル、認証&プリントファイルの漏洩に発展することを防いでいる。

- (9) 脅威「T.BACKUP-RESTORE(バックアップ機能、リストア機能の不正な使用)」に対抗するためのセキュリティ機能

本脅威は、バックアップ機能、リストア機能が不正に利用されることにより、ボックスファイル、セキュリティ文書プリントファイル及び認証&プリントファイルが漏洩する可能性がある他、パスワード等秘匿性のあるデータが漏洩する、各種設定値等が改ざんされた結果、ボックスファイル、セキュリティ文書プリントファイル及び認証&プリントファイルが漏洩する可能性を想定している。

本TOEで、管理者を識別認証する機能、バックアップ機能、リストア機能の使用を管理者のみに制限する機能(以上、「管理者機能」)を保持することで、バックアップ機能、リストア機能の使用は管理者に制限され、ボックスファイル、セキュリティ文書プリントファイル、認証&プリントファイルやパスワード等秘匿性のあるデータが漏洩することを防いでいる。

(10) 組織のセキュリティ方針「P.COMMUNICATION-DATA(画像ファイルのセキュアな通信)」を満たすためのセキュリティ機能

本組織のセキュリティ方針は、ネットワーク上に流れる画像ファイルについて、秘匿性を確保するために、組織・利用者が希望する場合において正しい相手先へ信頼されるパスを介した処理を行う、又は暗号化することを規定している。希望に応じて対応できればよいため、すべての通信においてセキュアな通信機能を提供する必要はなく、セキュリティ文書プリントファイル、認証&プリントファイル、ボックスファイルを扱うにあたり、MFPと利用者の使うクライアントPC間で最低限1つの手段が提供される必要がある。

本TOEにおいて、セキュリティ文書プリントファイル、認証&プリントファイル、ボックスファイルに対して、MFPとクライアント間における画像の送受信において正しい相手先に高信頼チャネルを提供する機能(以上、「高信頼チャネル機能」)、ボックスファイルに対してS/MIMEで送信するための暗号鍵生成機能、ボックスファイルの暗号化機能、S/MIMEで送信するための暗号鍵の暗号化機能(以上、「S/MIME暗号処理機能」)、管理者を識別認証する機能、高信頼チャネルやS/MIMEに関する設定の変更を管理者のみに制限する機能(以上、「管理者機能」)を保持することで、ネットワーク上に流れる画像ファイルを秘匿した形で送受信し、設定の変更を管理者に制限することで正しい相手先に送信可能となる。

(11) 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。

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3月に始まり、平成21年11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9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9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価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。

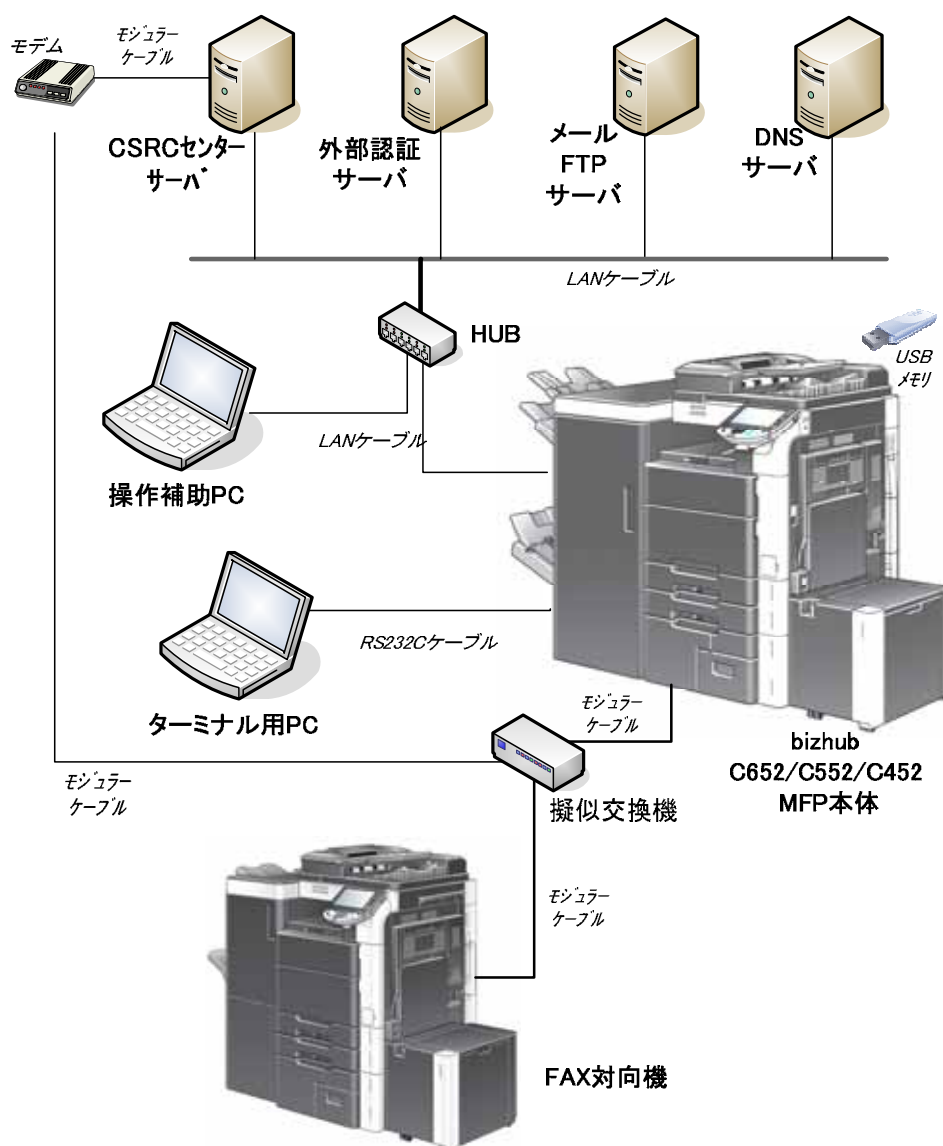


図3-1 開発者テストの構成図

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ーフェースを持つ機能については、その外部

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

<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

ツール名称	概要・利用目的
KONICA MINOLTA C652 Series PCL/XPS Ver. 2.1.4.0	bizhub C652 / C552 / C452の同梱CDに内蔵されている専用プリンタドライバソフトウェア。
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、またSSL/TLS確認ツールとして使用する。
Fiddler Ver. 2.2.2.0	http他のWebアクセスのモニター＆解析ソフトウェアツール。MFP本体と操作補助用PC間でHTTPプロトコルの確認、及びテストを行うために使用する。
Open APIテストソフトウェアツール Ver. 7.2.0.5	Open APIの評価用に作られた専用テストソフトウェアツール。Open APIの殆どのテストは、このツールソフトウェアを用いてメッセージレベルでの機能確認を行う。
SocketDebugger Ver. 1.12	TCP-Socketのテストソフトウェアツールとして使用する。
Wireshark Ver. 1.2.0	LAN上の通信をモニター＆解析するソフトウェアツール。通信ログ取得に使用する
Mozilla Thunderbird Ver. 2.0.0.21	汎用メーラーソフトウェア。操作補助PC上でS/MIMEメール確認用ツールとして使用する。
Open SSL Ver. 0.9.8k(25-May-2009)	SSLおよびハッシュ関数の暗号化ソフトウェアツール。
MG-SOFT MIB Browser Professional SNMPv3 Edition (以後MIB Browserと省略) Ver. 10.0.0.4044	MIB専用ブラウザソフトウェア。SNMP関連のテストに使用する。
Tera Term Pro Ver. 4.29	ターミナル用PCで動作させるターミナルソフトウェア。MFP本体と接続して、TOEの状態をモニターするために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。

ツール名称	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。
Stirling Ver.1.31	バイナリエディタソフトウェアツール。暗号鍵、デコードS/MIMEメッセージの内容確認、プリントファイルの編集用として使用する。
FFFTP Ver. 1.92a	FTPクライアントソフトウェアとして使用する。
MIME Base64 エンコード / デコード Ver. 1.0	MIME Base64 のエンコード/デコードを行なうソフトウェアツール。S/MIMEメッセージのEncode/Decode確認ツールとして使用する。
PageScope Data Administrator (PSDA) with Device Set-Up and Utilities Ver. 1.0.3000.4201	複数台のMFPに対応する管理者用デバイス管理ソフトウェアツール。 (下記プラグインソフトウェアの起動が可能)
HDD Backup Utility(プラグイン) Ver. 1.3.02000 600	HDD Backup Utility は、ネットワーク上のMFP(複合機)に搭載されている記録メディアのバックアップ(保存)とリストア(復元)を行うユーティリティ。
PageScope Box Operator (PSBO) Ver. 3.2.02000	ハードディスクに保存されたイメージ文書の取得、印刷などを行なうためのソフトウェアツール。 高信頼チャネル動作確認ツールとして使用する。
sslproxy Ver. 1.2	操作補助PC内にあり、本体装置と操作補助PCのブラウザソフトウェアとの間に入っているプロキシソフトウェア。 本体装置とはSSLで通信して、ブラウザソフトウェアとは非SSLでやり取りするので、sslproxyによりSSLによる暗号化を避けてFiddler、SocketDebuggerでのモニターが可能となる。
Black Jumbo Dog Ver. 4.2.2	イントラネット用の簡易サーバソフトウェア。 メールサーバ、FTPサーバ機能として使用する。
CSRCセンターソフトウェア Ver. 2.3.0	CSRCのセンター用のサーバソフトウェア

b. 実施テストの範囲

テストは開発者によって224項目実施されている。

カバレッジ分析が実施され、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。

なお、TOEが搭載されるMFPとして、bizhub C652、bizhub C552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 C652 / bizhub C552 / bizhub C452の違いは、コピー/プリント速度、及び耐久性保証値の違いだけであることを開発者から提供された資料により確認した。
- bizhub C652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 C552に実施し、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した。
- ineo+ 652 / ineo+ 552 / ineo+ 452、及びVarioLink 6522c / VarioLink 5522c / VarioLink 4522cは、それぞれbizhub C652 / bizhub C552 / bizhub C452をOEMしたものである。

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>

開発者テストの状況を踏まえ、すべてのセキュリティ機能を対象とする。
すべての確率的・順列的メカニズムをテスト対象とする。

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。

開発者テストの厳密さを踏まえ、必要と判断されるバリエーションをテストする。

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。

革新的、又は一般的ではない特性を持つインタフェースについて、必要と判断されるバリエーションをテストする。

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	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。

独立テスト の観点	テスト概要
観点	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	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	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、WebDAVサーバパスワード変更機能を確認するテストを実施した。
観点	ボックスの種類の組み合わせによる複雑度に着目し、ボックスの種類を変更した場合の動作を確認するテストを実施した。
観点	FAXユニット制御機能は革新的、又は一般的ではないと判断し、動作を確認するテストを実施した。

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 >

想定外のサービスが起動している可能性がある。

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。

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。

セッション情報の推測が容易である可能性がある。

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。

利用者の排他制御が適切に行われない可能性がある。

暗号化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。

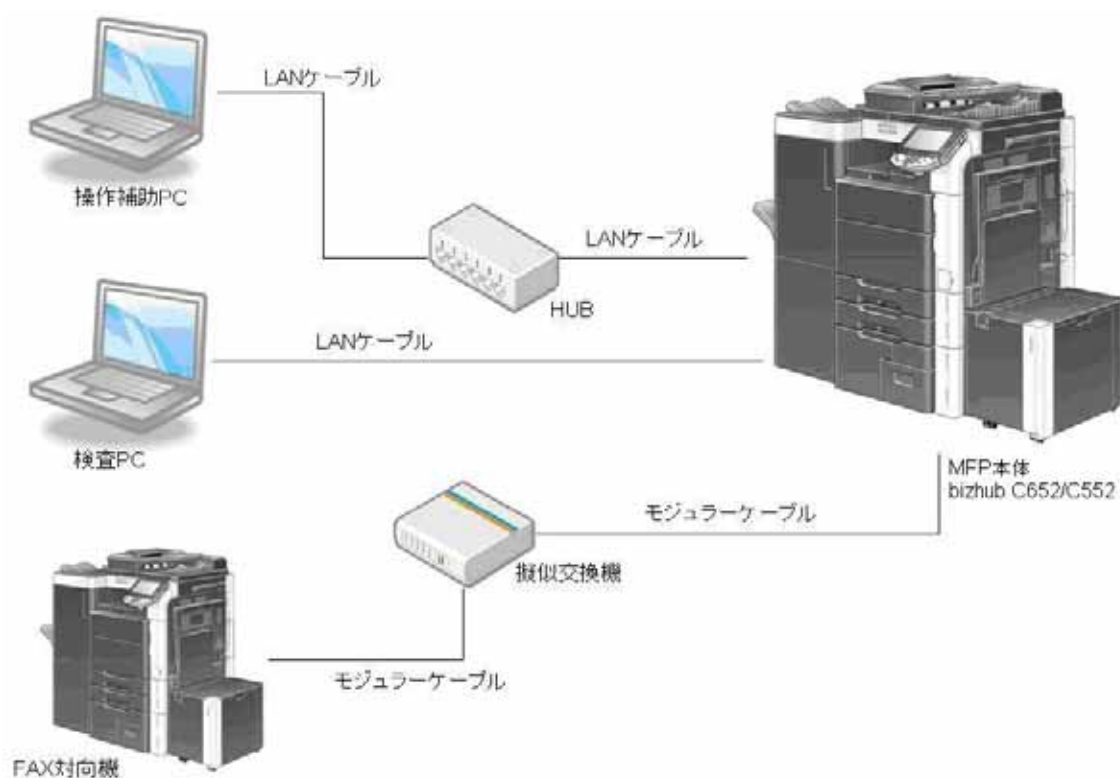


図3-2 侵入テストの構成図

< テスト手法 >

侵入テストは、以下の方法で実施された。

- ・ パネルを操作してTOEに刺激を与え、その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。
- ・ 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。

<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)	<ul style="list-style-type: none"> ・ bizhub C652 / C552に搭載されたTOE (バージョン : A0P00Y0-0100-GM0-12) ・ 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	<ul style="list-style-type: none"> ・ 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も利用(Fiddler、OpenAPIテストツール、SocketDebugger等)。 ・ PSWC(PageScope Web Connectionの略)、HTTPS、TCPSocket、OpenAPI、SNMP等を用いてMFPにアクセスし、ネットワーク設定等を実施することが可能。また、TamperIEの利用も可能。
検査PC	<ul style="list-style-type: none"> ・ 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8月31日時点の最新版を適用している。) <ul style="list-style-type: none"> snmpwalk Version 3.6.1 <ul style="list-style-type: none"> ・ MIB情報取得ツール。 openssl Version 0.9.8k (25-May-2009) <ul style="list-style-type: none"> ・ SSL及びハッシュ関数の暗号化ツール。 Nessus 4.0.0 build 4G1002_Q <ul style="list-style-type: none"> ・ 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。 TamperIE 1.0.1.13 <ul style="list-style-type: none"> ・ 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。 sslproxy v 1.2 <ul style="list-style-type: none"> ・ SSL-プロキシサーバソフトウェア。 Fiddler 2.2.2.0 <ul style="list-style-type: none"> ・ HTTPのやりとりをモニターするWebデバッガ。 WireShark 1.2.0 <ul style="list-style-type: none"> ・ 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。 Nikto Version 2.03 <ul style="list-style-type: none"> ・ 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 >

懸念される脆弱性毎のテスト概要を表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	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	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	ネットワーク経由で入力するパラメタ等を編集して送信することにより、セキュリティ機能のふるまい(ドメイン分離、バイパス、干渉等)に影響を与えないことを確認するテストを実施した。
脆弱性	セッション維持のためのメカニズムが一意性を保っていることを確認するテストを実施した。
脆弱性	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	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	暗号化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

特になし。

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。

所見報告書でなされた指摘内容が妥当であること。

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。

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。

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。

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

- ・ ユーザ認証機能で外部サーバ認証方式を選択する場合、Active Directoryを利用した外部サーバ認証方式を利用することを前提としており、TOEは、TOE範囲外であるActive Directoryで管理されている識別認証の情報を正当なものとして受け入れて動作する。
- ・ 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用になるが、その他の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。

API	Application Programming Interface (API)
DNS	Domain Name System (DNS)
FTP	File Transfer Protocol (FTP)
HDD	Hard Disk Drive (ハードディスクドライブ)
HTTPS	HyperText Transfer Protocol Security (HTTPS)
MFP	Multiple Function Peripheral (デジタル複合機)
MIB	Management Information Base (MIB)
NVRAM	Non-Volatile Random Access Memory (NVRAM)
RAM	Random Access memory (RAM)
SMB	Server Message Block (SMB)
SMTP	Simple Mail Transfer Protocol (SMTP)
SNMP	Simple Network Management Protocol (SNMP)
SSL/TLS	Secure Socket Layer/Transport Layer Security (SSL/TLS)
S/MIME	Secure Multipurpose Internet Mail Extensions (S/MIME)
TSI	Transmitting Subscriber Identification (TSI)
USB	Universal Serial Bus (USB)
WebDAV	Web-based Distributed Authoring and Versioning (WebDAV)

本報告書で使用された用語の定義を以下に示す。

DNS	インターネットでドメイン名とIPアドレスの関係を管理するプロトコルのこと。
FTP	TCP/IPネットワークで使うファイル転送プロトコルのこと。
HTTPS	Webサーバとクライアントの間で安全な通信を行うためにSSLによる暗号化機能を追加したプロトコルのこと。

MIB	SNMPを利用して管理される各種機器が公開している各種設定情報のこと。
NVRAM	電源を切っても記憶がなくなる不揮発性の性質を持つ、ランダムにアクセスできるメモリのこと。
PageScope Web Connection	MFP本体に内蔵されており、ブラウザを利用して、本体の状態確認/設定を行うためのツールのこと。
PC-FAX動作	FAX受信時に指定された情報に基づき、受信画像データの保存ボックス振り分け処理を行う動作のこと。
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。
SNMPパスワード	TOEで使用されているSNMP v3を利用する場合に利用者を確認するためのパスワード (Privacyパスワード、Authenticationパスワード) の総称。
SSL/TLS	インターネット上で情報を暗号化してやり取りするプロトコルのこと。
S/MIME	電子メールの暗号化方式の標準のこと。RSAの公開鍵暗号方式を用いてメッセージを暗号化して送受信。認証機関が発行した電子証明書が必要。
TSI受信	送信者毎に、保管すべきボックスを指定することができる機能のこと。
WebDAV	HTTP1.1を拡張した仕様で、Webサーバ上のファイル管理を目的としたプロトコルのこと。
暗号化ワード	ASICにおいて暗号化・復号処理を行う際の暗号鍵を生成する元となる情報のこと。
オフィス内LAN	TOEが接続され、スイッチングハブ等の利用、盗聴の検知機器の設置等オフィスの運用によって、盗聴されず、外部とはファイアウォール等を介して接続されるネットワークのこと。
管理者モード	MFPに対して管理者に許可された操作を行うことが可能な状態のこと。
外部ネットワーク	TOEが接続されるオフィス内LANとファイアウォール等によりアクセス制限されたネットワークのこと。
サービスモード	MFPに対してサービスエンジニアに許可された操作を行うことが可能な状態のこと。
セキュリティ文書パスワード	セキュリティ文書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であるかどうかを確認するためのパスワードのこと。

- こと。
- セキュリティ文書プリントファ
イル
- セキュリティ文書プリント
- フラッシュメモリ
- ボックスファイル
- セキュリティ文書プリントによって登録される画像ファイルのこと。
- こと。
- プリンタドライバでセキュリティ文書パスワードを指定し、MFPからの印刷はそのパスワードで認証された場合に制限する印刷方法のこと。
- 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。
- 個人ボックス、共有ボックス、グループボックスに保管される画像ファイルのこと。

7 参照

- [1] bizhub C652 / bizhub C552 / bizhub C452 / ineo+ 652 / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c 全体制御ソフトウェア A0P00Y0-0100-GM0-12 セキュリティターゲット バージョン 1.05
2009年11月10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 C652 / bizhub C552 / bizhub C452 / ineo+ 652 / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c 全体制御ソフトウェア 評価報告書 第2版 2009年11月16日
みずほ情報総研株式会社 情報セキュリティ評価室