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25年8月6日 (IT認証3471)
認証番号	C0458
認証申請者	コニカミノルタ株式会社
TOEの名称	日本語名：bizhub C3850 / bizhub C3350 / ineo+ 3850 / ineo+ 3350　全体制御ソフトウェア 英語名：bizhub C3850 / bizhub C3350 / ineo+ 3850 / ineo+ 3350 Control Software
TOEのバージョン	A3GN30G0142-999
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26年12月24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

「日本語名：bizhub C3850 / bizhub C3350 / ineo+ 3850 / ineo+ 3350　全体制御ソフトウェア 英語名：bizhub C3850 / bizhub C3350 / ineo+ 3850 / ineo+ 3350 Control Software バージョン：A3GN30G0142-999」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

この認証報告書は、コニカミノルタ株式会社が開発した「日本語名：bizhub C3850 / bizhub C3350 / ineo+ 3850 / ineo+ 3350 全体制御ソフトウェア　英語名　：bizhub C3850 / bizhub C3350 / ineo+ 3850 / ineo+ 3350 Control Software、 バージョン　A3GN30G0142-999」（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26年12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に関心を持つ消費者や調達者に対しセキュリティ情報を提供するものである。

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

本認証報告書は、市販される本TOEを購入する一般消費者を読者と想定している。本認証報告書は、本TOEが適合する保証要件に基づいた認証結果を示すものであり、個別のIT製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本TOEの機能、運用条件の概要を以下に示す。詳細は2章以降を参照のこと。

1.1.1 保証パッケージ

本TOEの保証パッケージは、EAL3である。

1.1.2 TOEとセキュリティ機能性

本TOEは、コピー、プリント、スキャン、FAXの各機能により構成されるデジタル複合機（以下「MFP」という。）に搭載され、MFP全体の動作を統括制御するソフトウェアである。

本TOEは、MFPに保存される機密性の高い保護対象資産の暴露に対する保護機能を提供する。他に、各種上書き消去規格に則り、HDDを始めとした記録媒体のデータを完全に消去する上書き消去機能を提供する。この機能をMFPの廃棄、リース返却時に使用することにより、MFPを利用する組織の情報漏洩を防止する。また、MFPのHDD内に保管されるすべての画像ファイル、パスワード等はTOEによってHDDに書き込むときに暗号化され、不正なアクセスから保護される。

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が提供する主なセキュリティ機能性、及びTOEの構成要件については次項のとおり。

1.1.2.1 脅威とセキュリティ対策方針

本TOEは、以下のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

MFP廃棄、リース返却の際にMFPに搭載されたHDD等の記録媒体から保護資産、設定情報等の機密情報が漏洩することを防ぐため、上書き消去等の手段によりMFP内のHDD等の記録媒体に記録されたデータを完全に消去し、再現を不可能とする機能を提供する。

MFPのHDDに蓄積された画像ファイルに対する、所有者の意図に反した不正アクセスによる暴露から保護するため、TOEの利用者に対して識別と認証を実施し、更に画像ファイルへのアクセスを、予め許可された利用者だけに限定する。

MFPに搭載されたHDDを持ち去り、データ読み出しを試みる等の不正なアクセスから保護するため、HDDに保管されているすべての画像ファイル、パスワード等の機密データを暗号化し情報の暴露を防ぐ。

上記のセキュリティ機能に関連する各種設定を管理者のみが行えるよう制限することで、セキュリティ機能の無効化や不正使用を防止する。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定している。

- 本TOE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 / ineo+ 3850 / ineo+ 3350 に搭載され使用される。
- 本TOEを含むMFPはオフィス内のLANに接続されることを想定しており、LANがインターネット等の外部ネットワークに接続される場合は、外部ネットワークから直接MFPにアクセスできないように管理される。

1.1.3 免責事項

本TOEが接続されるネットワークの通信経路における、盗聴からの通信データ保護は本評価対象の範囲外である。

1.2 評価の実施

認証機関が運営するITセキュリティ評価・認証制度に基づき、公表文書「ITセキュ

リティ評価及び認証制度の基本規程」[1]、「ITセキュリティ認証申請手続等に関する規程」[2]、「ITセキュリティ評価機関承認申請手続等に関する規程」[3]に規定された内容に従い、評価機関によって本TOEに関わる機能要件及び保証要件に基づいてITセキュリティ評価が実施され、平成26年12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、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、本TOEの評価がCC（[5][6]または[8][9]）及びCEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は本認証報告書を作成し、認証作業を終了した。

2 TOE識別

本TOEは、以下のとおり識別される。

TOE名称： 日本語名：bizhub C3850 / bizhub C3350 / ineo+ 3850 / ineo+ 3350 全体制御ソフトウェア
英語名：bizhub C3850 / bizhub C3350 / ineo+ 3850 / ineo+ 3350 Control Software

バージョン： A3GN30G0142-999

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、管理者及びユーザー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がセキュリティサービスとしてどのような方針あるいは規則のもと、機能を実現しているかを述べる。

TOEは、MFP廃棄、リース返却の際にMFPに搭載されたHDD等の記録媒体から保護資産、設定情報等の機密情報が漏洩することを防ぐためのセキュリティ機能、また、MFPのHDDに蓄積された画像ファイルに対する、所有者の意図に反した不正アクセスによる暴露から保護するためのセキュリティ機能を提供する。

さらに上記のセキュリティ機能に関連する各種設定を管理者のみが行えるよう制限することで、セキュリティ機能の無効化や不正使用を防止する。

3.1 セキュリティ機能方針

TOEは、3.1.1に示す脅威に対抗し、3.1.2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。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

本TOEは、表3-1に示す脅威を想定し、これに対抗する機能を備える。

表3-1 想定する脅威

識別子	脅 威
T.DISCARD-MFP（MFPのリース返却、廃棄）	リース返却、または廃棄となったMFPが回収された場合、悪意を持った者が、MFP内のHDD、NVRAMを解析することにより、Secure Print Data、Scan to HDD Data、ID&Print Data、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、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、S/MIME証明書データファイル、HDDやNVRAM上に設定されていた管理者パスワード、SNMPパスワード、ユーザー識別情報、ユーザーパスワード、暗号化ワード、ICカード情報、Secure Printパスワード、MFPの設定データ、高信頼チャネルの設定データ、外部サーバー識別設定データ、残存TSFデータが漏洩する。
T.ACCESS-DATA（ユーザー機能を利用したScan to HDD Data	悪意を持った者や悪意を持ったユーザーが、クライアントPCを介して他のユーザーが個人所有するScan to HDD Dataにアクセスし、HDDに保管されたScan to

への不正なアクセス）	HDD Dataをダウンロードすることにより、Scan to HDD Dataが暴露される。
T.ACCESS-SECURE-PRINT （ユーザー機能を利用したSecure Print Data、ID&Print Data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ーが、パネル、ICカードリーダーを介して利用を許可されないSecure Print Data、ID&Print Dataを印刷することにより、Secure Print Data、ID&Print Dataが暴露される。
T.UNEXPECTED-TRANSMISSION （想定外対象先への送信）	悪意を持った者や悪意を持ったユーザーが、パネル及びクライアントPCを介して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の設定データ（AppleTalkプリンター名（クライアントPCのみ）、IPアドレス（パネル、クライアントPC）など）を設定する。 また、悪意を持った者や悪意を持ったユーザーが、不正な送信宛先を設定する。
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ーが、パネルを介して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、セキュリティ機能が無効化される。
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ーが、クライアントPCを介してバックアップ機能、リストア機能を不正に使用することにより、Scan to HDD Data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、MFPの設定（IPアドレスなど）が改ざんされる。
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ーが、MFPに搭載されているHDDを持ち去る等不正にアクセスして、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。

3.1.1.2 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」への対抗

本脅威は、利用者から回収されたMFPから秘匿情報が漏洩する可能性を想定している。

本TOEでは、この脅威に対抗するために、MFP内のHDD、SSDのデータ領域を上書き消去すると共に、NVRAMに格納されたパスワード等の各種設定データを初期化する機能を提供する。この機能をMFP廃棄時やリース返却時

に、管理者がパネル操作により実行することにより、各秘匿情報が再現不可能な状態になりMFPからの情報漏洩を防ぐ。

(2) 脅威「T.ACCESS-DATA」への対抗

本脅威は、ユーザー各位が他のユーザーから保護することを意図して蓄積したScan to HDD Dataに対して、不正な操作が行われ情報が暴露される可能性を想定している。

本TOEでは、この脅威に対して利用者の識別認証、及びScan to HDD Dataに対するアクセス制御により対抗する。以下に各機能の詳細を述べる。

・利用者の識別認証

MFPを利用しようとする者に対して、ユーザーID、ユーザーパスワードの入力要求を行い、利用が許可された利用者であることを識別認証する。入力手段としてはMFPの操作パネルからの入力、クライアントPCからのネットワーク経由の入力がある。識別認証が成功すると、利用者の役割を関連付け、MFPの利用を許可する。

ユーザー認証方式として以下に示す方式があり、管理者が選択する。

【本体認証】

MFP制御コントローラー上のHDDにユーザーID、ユーザーパスワードを登録し、入力された情報と照合することによりTOEにて認証する方式。また管理者の設定により、MFPに接続されたICカードリーダーと利用者が保持するICカードを使用して認証する手段も使用できる。

【外部サーバー認証】

オフィス内LANで接続されるユーザー情報管理サーバー上に登録されるユーザーID及びユーザーパスワードを用いて、TOEにて認証する方式。外部サーバー認証ではActive Directory、NTLM等の複数の方式をサポートするが、本評価においてはActive Directoryを利用する場合のみが評価対象となる。

・Scan to HDD Dataに対するアクセス制御

Scan to HDD Dataに対する各種操作（一覧表示、ダウンロード、削除）を、Scan to HDD Dataの登録操作を行ったユーザーに限定する。これにより、MFPに蓄積されたScan to HDD Dataに対する不正なアクセスを防ぐ。

(3) 脅威「T.ACCESS-SECURE-PRINT」への対抗

本脅威は、ユーザー各位が機密性を確保することを意図して、クライアントPCからMFPに送信したプリントデータ（Secure Print Data、ID&Print Data）に対して、不正な操作が行われ情報が暴露される可能性を想定している。

本TOEでは、この脅威に対して利用者の識別認証、Secure Print機能、及び

ID&Print機能により対抗する。以下に各機能の詳細を述べる。Secure Print機能、及びID&Print機能の選択は、ユーザーがクライアントPCから印刷を行う際に行う。

・利用者の識別認証
脅威「T.ACCESS-DATA」への対抗手段と同様の識別認証機能により、MFPの利用を許可された利用者に限定する。

・Secure Print機能
パスワードと共に受信したプリントデータ（Secure Print Data）を印刷待機状態で保管する。
利用者の識別認証に成功したユーザーに対して、保管しているSecure Print Dataの一覧をパネル上に表示する。
ユーザーにより印刷､削除要求があった場合､パスワードの入力を要求し、Secure Print Dataに予め設定されたパスワードと一致した場合に要求された処理を実行する。
これにより、Secure Print Dataに対する不正な操作を防ぐ。

・ID&Print機能
クライアントPC上で設定されたユーザーIDと共に受信したプリントデータ（ID&Print Data）を印刷待機状態で保管する。
利用者の識別認証に成功したユーザーに対して、同じユーザーIDが設定されたプリントデータ（ID&Print Data）の一覧を表示し、印刷、削除処理を実行可能とする。
これにより、ID&Print Dataに対する不正な操作を防ぐ。

(4) 脅威「T.UNEXPECTED-TRANSMISSION」への対抗

本脅威は､TOEが搭載されるMFPのネットワーク設定等が不正に変更され、本来受信すべき情報が他のMFP等に不正に送信されてしまう可能性を想定している。

本TOEでは、この脅威に対して、MFPの設定データ（ネットワーク設定等）にアクセスする際には管理者の識別認証を行い､認証に成功した管理者のみに設定データに対する操作を許可することにより対抗する｡ネットワーク設定を行う際の管理者の識別認証手段としては､パネル上及びネットワーク経由での管理者パスワードによる認証と、SNMPを利用したネットワーク経由での（SNMPパスワードによる）認証があり、どちらも評価対象となる。

(5) 脅威「T.ACCESS-SETTING」への対抗

本脅威は、TOEのセキュリティ機能に関する設定が不正に変更され、TOEのセキュリティ機能が無効化される可能性を想定している。

本TOEでは、この脅威に対して、セキュリティ機能に関する設定データに

アクセスする際には管理者パスワードを用いて管理者の識別認証を行い、認証に成功した管理者のみに設定データに対する操作を許可することにより対抗する。

(6) 脅威「T.BACKUP-RESTORE」への対抗

本脅威は、バックアップ機能、リストア機能を不正に使用され、MFPに蓄積されたScan to HDD Data等の保護資産の漏洩、パスワード等秘匿性のある情報の漏洩、また不正に変更された設定データのリストアによるセキュリティ侵害の可能性を想定している。

本TOEでは、この脅威に対して、バックアップ機能、リストア機能を使用する際には管理者の識別認証機能を行い、認証に成功した管理者のみにバックアップ機能、リストア機能の使用を許可することにより対抗する。

(7) 脅威「T.ACCESS-HDD」への対抗

本脅威は、MFPに搭載されるHDDが持ち去られ、直接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。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 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-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（Secure Print Data、Scan to HDD Data、Scan to E-mail Data、ID&Print Data）は、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。 （補足） 本TOEにおいては、オフィス内LAN上での盗聴行為等の脅威は想定していないが、機密性の高い画像ファイルに関してはMFPの利用組織においてセキュアな通信が要求されることを想定している。 また、「IT機器間」とはクライアントPCとMFPの間を指している。

3.1.2.2 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

本TOEは、表3-2に示す組織のセキュリティ方針を、以下のセキュリティ機能方針により満たす。

(1) 組織のセキュリティ方針「P.COMMUNICATION-DATA」への対応

本組織のセキュリティ方針は､ネットワーク上を流れる画像ファイルに関して機密性を確保するためのものであり、特に秘匿性の高いデータとしてScan to HDD Data、Scan to E-mail Data、Secure Print Data、ID&Print DataについてMFPとクライアントPC間のセキュアな通信を求めている。

本TOEでは、TOEからクライアントPCにScan to HDD Dataを送信する際に、SSLを使用した暗号化通信を行う。また、TOEからScan to E-mail Dataを送信する際に、暗号化を行いS/MIMEを使用して相手に送信する。

クライアントPCからTOEに送信されるSecure Print Data、及びID&Print Dataの保護に関しては、MFPを利用する組織の責任者に対して、暗号通信機器の設置等を要求することにより組織のセキュリティ方針を満たすことができる。

4 前提条件と範囲の明確化

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は、管理者、ユーザー、及びサービスエンジニアから漏洩しない。また、暗号化ワードは管理者から漏洩しない。
A.SERVER-MNG（各サーバーに関する運用条件）	TOEの利用において使用されるSMTPサーバー、WebDAVサーバー、DNSサーバー、及びユーザー情報管理サーバーは、管理者により脆弱性対策が施され適切に管理される。

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 / ineo+ 3850 / ineo+ 3350 に搭載される。

本TOEを含むMFPは、一般的なオフィスに設置され、社内ネットワークであるオフィス内LANにクライアントPC、各種サーバーと共に接続され利用されることを想定している。またFAX通信に使用するため、公衆回線に接続される。

本TOEの一般的な運用環境を図4-1に示す。

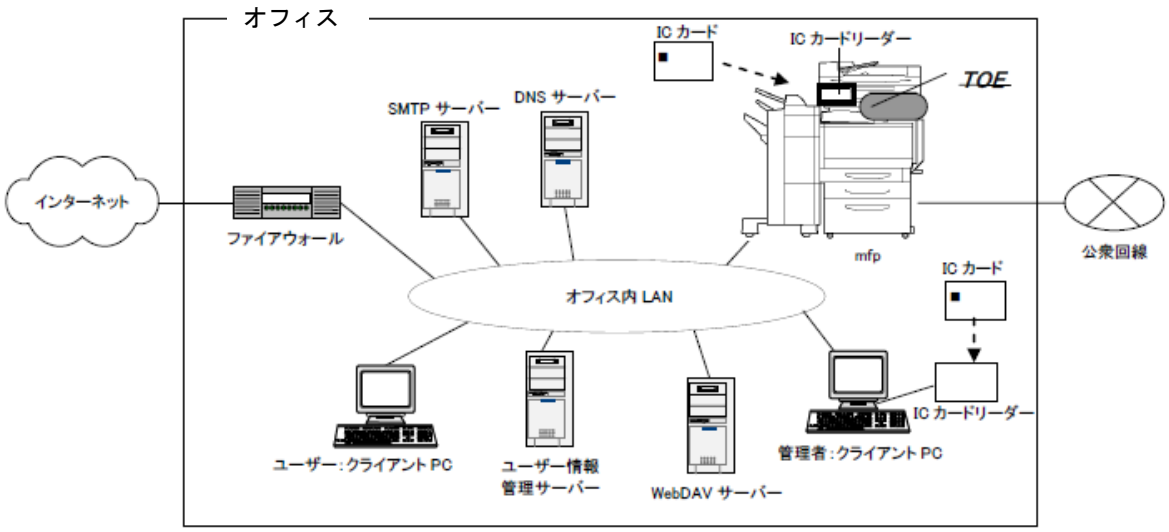

図4-1　TOEの運用環境

オフィス内LANには必要に応じてSMTPサーバー、WebDAVサーバーが接続され、相互にデータ通信を行うことができる（SMTPサーバー、WebDAVサーバーのドメイン名を設定する場合はDNSサーバーが必要になる）。また、オフィス内LANにはクライアントPCが接続され、Webやプリンタードライバー等を介して相互にデータ通信を行う。

ユーザーID、ユーザーパスワードを外部サーバーにて一元管理する場合は、ユーザー情報管理サーバーをオフィス内LANに接続する。TOEはこのサーバーで管理されるユーザー登録情報を使用して識別認証を行う。

オフィス内LANが外部ネットワークと接続する場合は、ファイアウォールを介して接続する等の措置が取られ、外部ネットワークからMFPに対するアクセスを遮断するための適切な設定が行われる。

オフィス内LANは、オフィスの運用によって、盗聴されないネットワーク環境が整備されている。

TOEが搭載されるMFPの利用に関連する人物の役割を以下に示す。

・管理者

MFP の運用管理を行う MFP の利用者。MFP の動作管理、ユーザーの管理を行う（一般には、オフィス内の従業員の中から選出される人物がこの役割を担うことが想定される）。

・サービスエンジニア

MFP の保守管理を行う利用者。保守契約が結ばれた場合、MFP の修理、調整等の保守管理を行う（一般には、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）。

・ユーザー

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）。管理者、及びサービスエンジニアは、ユーザーには含まれない。

・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。

この他に、TOEの利用者ではないがTOEにアクセス可能な人物として、オフィス内に出入りする人物等が想定される。

4.3 運用環境におけるTOE範囲

本TOEは、セキュア通信を行うための機能として、SSLを使用した暗号化通信を提供する。この機能によりTOEからクライアントPCに送信されるScan to HDD Dataの保護は実現されるが、クライアントPCからTOEに送信されるSecure Print Data、及びID&Print Dataの保護も要求される組織のセキュリティ方針（P.COMMUNICATION-DATA）は完全には実現されない。クライアントPCからTOEへのSecure Print Data、及びID&Print Dataの送信を保護するためには、暗号通信機器の設置等が前提となり、それらは運用者の責任となる。

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について、関連を説明する。

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。

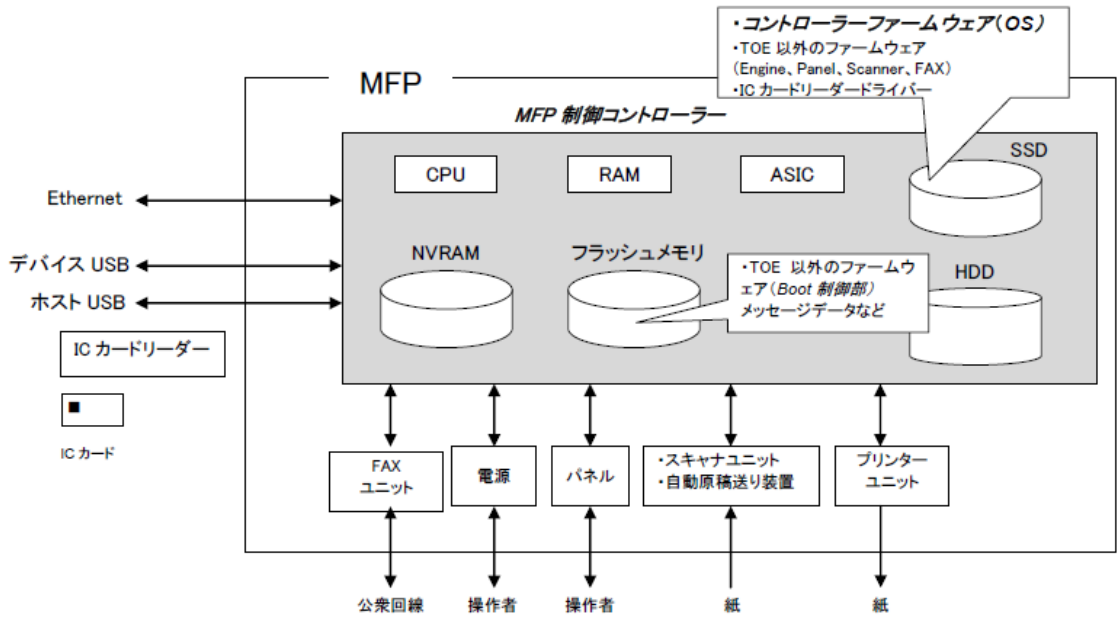

図5-1　TOEに関連するハードウェア構成

・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。

・HDD（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。また、ユーザーID、ユーザーパスワード、Secure Printパスワード等が保管される。

・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、SNMPパス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。TOEのアップデートを本インタフェースから行うことも可能。

・ホストUSB
MFPのパネル側にあるUSBポート。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が可能。なお、この印刷及びスキャンにはSecure Print及びScan to HDD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、画像データ、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カードリーダードライバー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
プラスチック製カードに半導体集積回路（ICチップ）を埋め込み、情報を記録できるカード。設定により利用者の識別認証時に使用される。
本TOEの運用環境では、組織の責任者が正しいユーザーへICカードを配布し、ICカードの所有者自身が適切にICカードを管理することが求められる。

・ICカードリーダー
ICカードを読み取るための機器。

・ICカードリーダードライバー
ICカードリーダーにアクセスするためのドライバー。

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。

目的	ガイダンス名称	バージョン
操作マニュアル	[海外版] bizhub C3850 / bizhub C3350 User's Guide [Security Operations] ineo+ 3850 / ineo+ 3350 User's Guide [Security Operations] [日本版] ユーザーズガイド セキュリティ機能編 bizhub C3850	 Ver.1.05 Ver.1.05 Ver.1.05
準備手続き	[海外版] bizhub C3850 / bizhub C3350 SERVICE MANUAL SECURITY FUNCTION ineo+ 3850 / ineo+ 3350 SERVICE MANUAL SECURITY FUNCTION [日本版] サービスマニュアル セキュリティ機能編 bizhub C3850	 Ver.1.03 Ver.1.03 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ている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

7.3 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25年8月に始まり、平成26年12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26年1月、2月、4月、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26年7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。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

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。評価した開発者テストの概要を以下に示す。

1) 開発者テスト環境

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

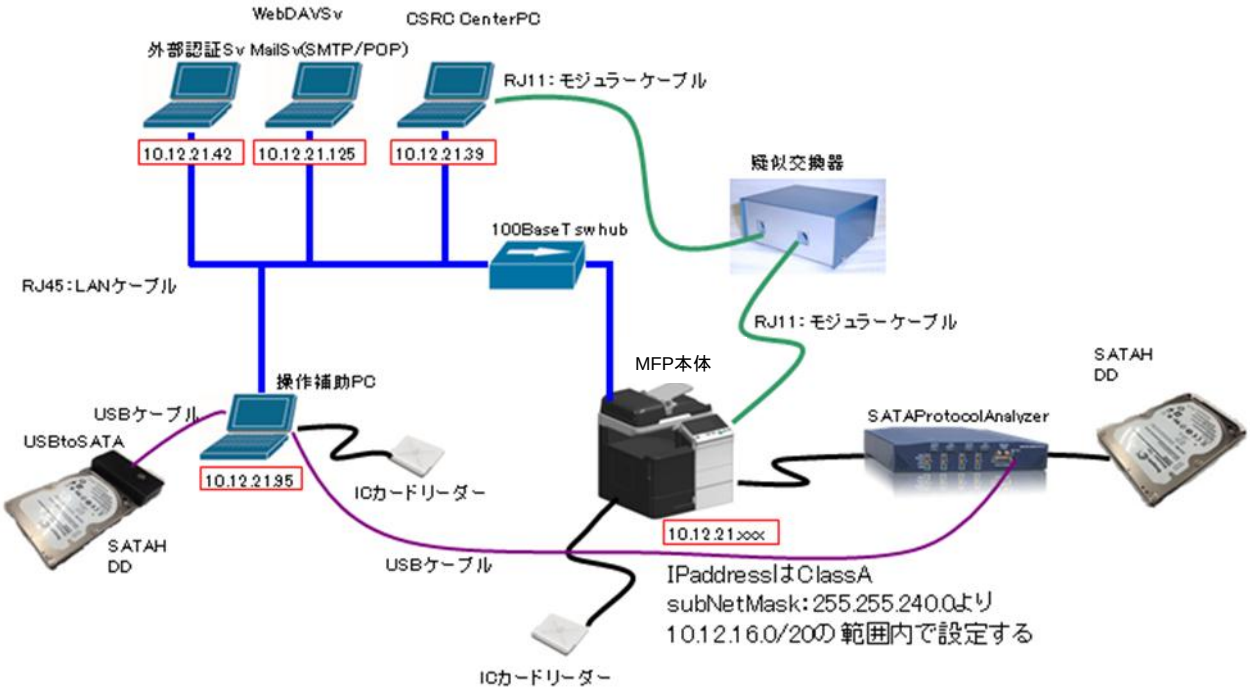

図7-1　開発者テストの構成図

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

（ineo+ 3850/ineo+ 3350については、それぞれbizhub C3850/bizhub C3350のOEM製品であり、セキュリティ機能への影響はないことが評価者により確認されており、これらのMFPは使用しなくても問題ないと判断されている。）

・MFPがHDD、及びSDD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 / ineo+ 3850 / ineo+ 3350 全体制御ソフトウェア 識別（ソフトウェア識別、バージョン）: A3GN30G0142-999
2	ICカードリーダー （AU-201、AU-201H）	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	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、PageScope Web Connection(以下「PSWC」という。)、HTTPS、TCP Socket、Open API、SNMP等、ネットワークアクセスが必要なテストに使用する。
4	外部認証Sv	Windows上でサービスされるActive Directoryを使ったユーザーのアクセス権管理を行うサーバー。外部ユーザー認証を使ったテストに使用する。
5	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。
6	LANケーブル	MFP本体とHUB、さらに操作補助PCや外部認証サーバー、SMTPサーバー、DNSサーバー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。
7	SATAProtocolAnalyzer	HDD書き込み処理のキャプチャーが可能なツール。
8	WebDAV Sv	CSRC（遠隔診断機能）が必要なテストに使用する。

No.	構成機器名称	概要・利用目的
9	Mail Sv	Scan To E-mail、CSRCのテストで使用する、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ー。
10	CSRC Center PC	CSRCのテストで使用する。
11	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。

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。

＜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、ネットワーク接続されたクライアント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クライアント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クライアント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　開発者テストツール

No.	ツール・ソフトウェア名称	概要・利用目的
1	Windows Printer Driver KONICA MINOLTA C3850 Series PCL6 v1.1.1.0 / XPS v1.1.1.0	MFPの同梱CDに内蔵されている専用プリンタードライバーソフトウェア
2	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。

No.	ツール・ソフトウェア名称	概要・利用目的
3	Internet Explorer Ver. 10	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確認ソフトウェアとして使用する。
4	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本体と操作補助用PC間でHTTPSプロトコルのテストを行うために使用する。
5	Open APIテストツール 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。Open APIの殆どのテストは、このソフトウェアにて通信レベルでの機能確認を行う。
6	WireShark Ver.1.10.5	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。
7	Win32OpenSSL Ver.1.0.1f	SSL及びハッシュ関数の暗号化ソフトウェア。
8	MG-SOFT MIB Browser Professional SNMPv3 Edition （以下「MIB Browser」という。） 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。
9	Stirling Ver.1.31	プリントファイルの編集用のバイナリエディタとして使用する。
10	Base64 エンコーダ V4.41	S/MIMEのOID確認前処理に使用する。
11	PageScope Data Administrator (PSDA) with Device Set-Up and Utilities Ver. 1.0.06000.03221	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。(下記(PSDA)のプラグインソフトの起動が可能)
	PageScope Data Administrator (PSDA) Ver 4.1.25000.07251	MFP本体に、E-mailやFAX等の宛先情報を登録する等、ユーザーへの使用制限の設定を行うためのプラグインソフトウェア。 OpenAPIインタフェース確認ソフトウェアとして使用する。
12	PageScope Web Connection(PSWC)	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/設定を行うためのソフトウェア。 HTTPインタフェース確認ソフトウェアとして使用する。

No.	ツール・ソフトウェア名称	概要・利用目的
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	assess.exe	NISTの乱数検定セット。
15	Mozilla Firefox Ver.27.0.1	汎用のブラウザソフトウェア。操作補助PC上でInternet Explorerではサポートしておらず、対応できないテスト項目の評価に用いる。
16	Apache for windows 2.2.25-win32-x86-openssl-0.9.8y.msi	WebDAVサーバー。
17	CSRC V2.8.1R1Rev15	CSRCアプリケーション。
18	ICカードリーダードライバー(本体・AU-201用)	ICカードよりICカードIDを読み取る際に使用する。 本ソフトはMFP本体で使用する。
19	ICカードリーダードライバー（操作補助PC・AU-201用） V2.1.02000	ICカードよりICカードIDを読み取る際に使用する。本ソフトは操作補助PCで使用する。
20	IC カードリーダードライバー(本体・AU-201H 用)	ICカードよりICカードIDを読み取る際に使用する。本ソフトはMFP本体で使用する。
21	ICカードリーダードライバー（操作補助PC・AU-201H用） V2.1.00000	ICカードよりICカードIDを読み取る際に使用する。本ソフトは操作補助PCで使用する。
22	Windows Scanner Driver KONICA MINOLTA bizhub C3850/C3350 (TWAIN drv v1.0.0.0)	TWAINドライバーを使用しての評価に用いる。

＜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、クライアントPC上で、プリンタードライバー、Webブラウザでの PSWC、PSDA、その他Fiddler2等のテストツール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SSDやHDDの入出力経路上のデータ解析、クライアントPC上に表示された結果の目視確認、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. 実施テストの範囲

テストは開発者によって115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TSFI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TSFサブシステムのふるまいと相互作用が十分にテストされたことが検証されている。

c. 結果

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

7.4.2 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、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) 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。

＜独立テストの観点＞

① 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、入力パラメタの種類、組み合わせを追加し、TSF毎にテストを実施する。

② パラメタを入力するインタフェース種別、クライアントPCとの接続方法に関して、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。

＜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。

＜独立テストの実施＞

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39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	異常系入力値を追加したID&Print機能に関するテスト
②	開発者テストとは異なるインタフェースを使用したセキュリティ管理機能に関するテスト

c. 結果

実施したすべての評価者独立テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

7.4.3　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。

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 想定外のユーザー操作により、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。

b. 侵入テストの概要

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

＜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クライアント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 Ver.6.46	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 5.2.7	セキュリティスキャナ。
4	Nikto	セキュリティスキャナ。

	Version 2.1.5	
5	extrstr Version 0.2	バイナリ解析ツール

＜脆弱性テストの実施＞

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 11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。

c.　結果

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

7.5　評価構成について

テスト構成ではオフィス内LANに接続されるサーバーとして、実施されたテスト内容に関連するWebDAVサーバー、外部認証サーバー、SMTPサーバーが使用されているが、TOEの実際の運用環境では、必要に応じて他のサーバー（DNSサーバー等）が接続される。

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。

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

- EAL3パッケージのすべての保証コンポーネント

評価では以下について確認された。

- PP適合：なし
- セキュリティ機能要件：　コモンクライテリア　パート２拡張
- セキュリティ保証要件：　コモンクライテリア　パート３適合

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

7.7 評価者コメント/勧告

消費者に喚起すべき評価者勧告は、特にない。

8 認証実施

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

① 所見報告書でなされた指摘内容が妥当であること。
② 所見報告書でなされた指摘内容が解決されていること。
③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。
④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。
⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

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の利用者は、1.1.3 免責事項、及び5.2 TOEの動作環境の記載内容を参照し、本評価において保証の対象となっているセキュリティ機能の範囲について注意する必要がある。

また、本TOEの管理者は、4.3 運用環境におけるTOE範囲の記載内容を参照し、オフィス内LANの運用上の要求事項が、実際のTOE運用環境において対応可能であるかどうかについて注意する必要がある。

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、公表のため、本報告書とは別文書として、以下のとおり提供される。

bizhub C3850 / bizhub C3350 / ineo+ 3850 / ineo+ 3350 全体制御ソフトウェア
A3GN30G0142-999　セキュリティターゲット
バージョン 1.16　2014年9月12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）
TSFI	TSF Interface（TSFインタフェース）

本報告書で使用されたTOEに関する略語を以下に示す。

CE	Customer Service Engineer サービスエンジニアの略称。
DNS	Domain Name System 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。
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 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。
NVRAM	Non-Volatile Random Access Memory 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。

RAM	Random Access memory 揮発性メモリ。
SMTP	Simple Mail Transfer Protocol TCP/IPでメールを転送する時のプロトコル。
SNMP	Simple Network Management Protocol 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。
SSL	Secure Socket Layer 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。
USB	Universal Serial Bus
WebDAV	Web-based Distributed Authoring and Versioning HTTP1.1を拡張した仕様で、Webサーバー上のファイル管理を目的としたプロトコル。

本報告書で使用された用語の定義を以下に示す。

Active Directory	Windowsプラットフォームのネットワーク環境にてユーザー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の方式。
AppleTalkプリンター	Apple社のMAC OSで利用されるネットワークプロトコルであるAppleTalkにおいて共有されるプリンター。
CEパスワード	サービスエンジニアの認証に使用するパスワード。
CSRC	コニカミノルタ株式会社が管理、運営する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遠隔診断機能。本TOEの運用環境ではセキュリティ強化機能が有効化されることにより、CSRCの一部機能（遠隔からのMFP設定変更）の使用が制限される。
ID&Print Data	クライアントPCからユーザーがID&Print機能を利用して送信した、ユーザー属性が付加されたプリントデータ。
ID&Print 機能	ユーザー識別認証を行い、同じユーザーの属性を持つプリントデータを印刷する機能。
Scan to E-mail Data	スキャナ機能を使用して生成された画像データを、暗号化した上でE-mailとして送信する機能（Scan to E-mail機

	能）で使用される画像ファイル。
Scan to HDD Data	Scan to HDD機能の中で、ユーザーがPrivate属性を選択してHDDに蓄積したデータ。
Scan to HDD 機能	スキャナ機能を使用して生成された画像データをユーザー情報とともにMFP内のHDDに格納する機能。格納する際にユーザーにより属性値（PrivateまたはPublic）が選択される。Privateが選択された画像データはScan to HDD Dataとして管理され、アクセスする際にユーザーIDとユーザーパスワードの入力が必要となる。
Secure Print Data	クライアントPCからユーザーが印刷機能を利用して、パスワードを付けてTOEに送信したデータ。
Secure Print機能	クライアントPCからパスワードと共に受信したプリントデータ（Secure Print Data）を印刷待機状態で保管し、パネルからの印刷指示とパスワード入力により印刷を実行する機能。
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の総称。
管理者パスワード	管理者の認証に使用するパスワード。
セキュリティ強化機能	TOEのセキュリティ機能の振る舞いに関係する各種設定を一括して管理する機能。セキュリティ強化機能が有効にされると、個別の設定値を脆弱な値に変更することが禁止される。TOEはこのセキュリティ強化機能を有効な状態で運用されることが前提となる。
ユーザーパスワード	ユーザー認証に使用するパスワード。

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26年4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26年4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25年4月
独立行政法人情報処理推進機構　CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part3: 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 / ineo+ 3850 / ineo+ 3350 全体制御ソフトウェア A3GN30G0142-999 セキュリティターゲット バージョン 1.16　2014年9月12日 コニカミノルタ株式会社

[13] コニカミノルタ株式会社 bizhub C3850 / bizhub C3350 / ineo+ 3850 / ineo+ 3350 全体制御ソフトウェア A3GN30G0142-999 評価報告書 初版 2014年12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