認　証　報　告　書

独立行政法人 情報処理推進機構
理事長　藤原　武平太　原紙押印済

評価対象

申請受付年月日（受付番号）	**平成17年9月13日（IT認証5051）**
認証番号	C0062
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 C250 / ineo+ 250 **全体制御ソフトウェア** **英語名　：**bizhub C250 / ineo+ 250 Control Software
TOE**のバージョン**	4038-0100-GM0-05-000
PP**適合**	**なし**
適合する保証要件	EAL3
TOE**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18年11月22日

独立行政法人 情報処理推進機構
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　田渕　治樹

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 Common Criteria for Information Technology Security Evaluation Version 2.1
② Common Methodology for Information Technology Security Evaluation Version 1.0
③ CCIMB Interpretations-0407

評価結果：合格

「日本語名：bizhub C250 / ineo+ 250 全体制御ソフトウェア、英語名：bizhub C250 / ineo+ 250 Control Software」は、独立行政法人 情報処理推進機構が定める ITセキュリティ認証手続規程に従い、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
1.2 評価製品 1
1.2.1 製品名称 1
1.2.2 製品概要 1
1.2.3 TOEの範囲と動作概要 2
1.2.4 TOEの機能 4
1.3 評価の実施 6
1.4 評価の認証 6
1.5 報告概要 7
1.5.1 PP適合 7
1.5.2 EAL 7
1.5.3 セキュリティ機能強度 7
1.5.4 セキュリティ機能 7
1.5.5 脅威 18
1.5.6 組織のセキュリティ方針 19
1.5.7 構成条件 19
1.5.8 操作環境の前提条件 19
1.5.9 製品添付ドキュメント 20
2 評価機関による評価実施及び結果 21
2.1 評価方法 21
2.2 評価実施概要 21
2.3 製品テスト 21
2.3.1 開発者テスト 21
2.3.2 評価者テスト 24
2.4 評価結果 26
3 認証実施 27
4 結論 28
4.1 認証結果 28
4.2 注意事項 33
5 用語 34
6 参照 36

1 全体要約

1.1 はじめに

この認証報告書は、「日本語名：bizhub C250 / ineo+ 250 全体制御ソフトウェア、英語名：bizhub C250 / ineo+ 250 Control Software」（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や本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応する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、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

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。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称:　日本語名：bizhub C250 / ineo+ 250 全体制御ソフトウェア
　　英語名：bizhub C250 / ineo+ 250 Control Software
バージョン:　4038-0100-GM0-05-000
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は、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 C250 / ineo^{+} 250）（以下、「MFP」という。）に搭載される組み込み型のソフトウェアである。本TOEは、MFPに搭載されるMFP制御コントローラ上のフラッシュメモリ上にあり、MFP本体のパネル（以下、「パネル」という。）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。

本TOEは、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し、ユーザの意図に反して暴露される可能性のあるデータを保護することを目的

としている。そのための機能として、特定のドキュメントへの操作を許可された利用者のみが可能とする機能、不要となったデータ領域を上書き削除する機能、設定値を含む機密情報を削除する機能、MFP内に画像データを保存するための媒体であるHDDが、不正に持ち出される等の危険性に対して、HDDが備える不正アクセス防止機能（HDDロック機能）を利用する仕組みを有する。また、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は、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鍵生成機能を提供する。

1.2.3 TOEの範囲と動作概要

本TOEは、MFP制御コントローラ上に据え付けられるMFP制御コントローラ上のフラッシュメモリ上に存在し、ロードされる。本TOEとMFPの関係を図1-1に示す。なお、図1-1において本TOEは網掛けで示されており、図中の「※」はMFPのオプションパーツであることを示す。

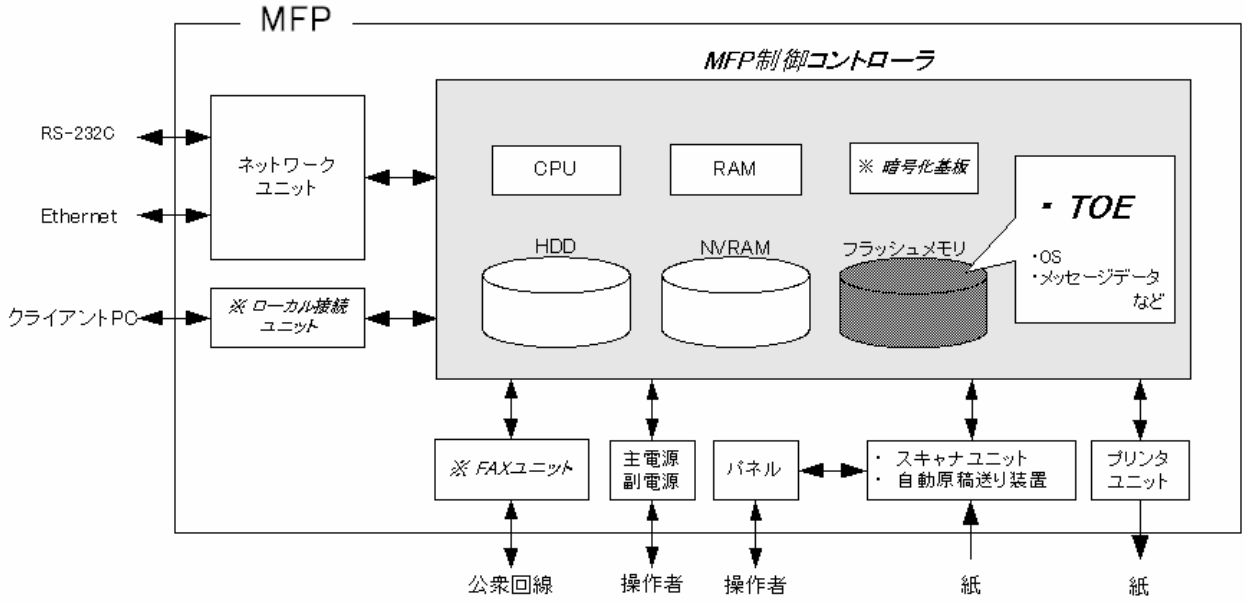


図1-1：TOEに関係するハードウェア構成

フラッシュメモリは、本TOEのオブジェクトコードが保管される記憶媒体であり、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などで表示するための各国言語メッセージデータやOSなども保管される。

NVRAMは不揮発性のメモリであり、様々な設定値（管理者パスワード、送信宛先データなど）等が保管される。

HDDは、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。また、本TOEにはHDDロック機能が搭載され、HDDにパスワードを設定することによって、不正なHDDへの読み書きを禁止することが可能となる。

暗号化基板はオプション製品として提供される。暗号化基板は、HDDに書き込まれ

るすべてのデータを暗号化するために、暗号鍵生成機能がハード的に実装される。

次に、本TOEの論理的な構成について示す。MFPには、「1.2.4 TOEの機能」に示す機能の他に、直接セキュリティとは関係の無い、基本機能、ユーザチョイス機能、遠隔診断機能が存在する。

基本機能は、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であり、TOEはこれら機能の動作における中核的な制御を行う。

遠隔診断機能は、RS-232Cを介したモデム接続経由、E-mailといった接続方式を利用して、コニカミノルタホールディングズ関連会社によって運営されるMFPサポートセンターと通信し、MFPの動作状態、設定情報、印刷数等の機器情報を管理するために用いられる。

これらの機能を使用することができるMFPの利用者は、パネルやネットワークを介してTOEが提供する各種機能を使用する。

MFPの利用に関連する人物に対し、その役割を以下に示す。

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などが想定される。)

2)管理者

MFPの運用管理行う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人物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、調整等の保守管理を行う。(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にアクセス可能な人物として、オフィス内に出入りする人物などが想定される。

1.2.4 TOEの機能

本TOEは、以下に示す機能を提供する。

1)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。

2)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の、2つのタイプが存在する。

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より、ボックス、ボックス内の画像ファイルに対し、クライアントPCからのダウンロード、削除、保管期間設定（期間経過後は自動的に削除)、及びボックスの名称変更、パスワードの変更、ボックスの削除、ボックスの属性設定（個人ボックス、共有ボックスの種別変更）といった機能を提供する。

3)ユーザ認証機能

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。ユーザ認証には、MFP制御コントローラ上のHDDにユーザID、ユーザパスワード登録する「本体認証」と、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、ユーザパスワードを用いてユーザを認証する「外部サーバ認証」の2つの方式が存在する。

4)管理者機能

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、本体認証の場合におけるユーザ情報の管理などの機能を提供する。また、その他の機能のふるまいに関係する動作設定機能を提供する。

5)サービスエンジニア機能

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・プリントなどのデバイスの微調整等のメンテナンス機能などを提供する。

6)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。

7)HDDロック機能

HDDは、不正な持ち出し等への対処機能として、パスワードを設定した場合にHDDロック機能が動作する。管理者機能にて本機能の動作設定を行い、MFPの起動動作において、MFP側に設定されたHDDロックパスワードとHDD側に設定されるHDDのパスワードロックを照合し、一致した場合にHDDへのアクセスを許可する。（HDDを持ち出されても、当該HDDが設置されていたMFP以外で利用することができない。）

8)暗号鍵生成機能

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。ただし、TOE自身は、暗号化・復号処理そのものは行わず、暗号鍵を生成する機能のみ提供する。

なお、本TOEの保護資産は、機密文書プリントによって登録される画像ファイル（機密文書ファイル)と、個人ボックス、または共有ボックスに保管される画像ファイル(ボックスファイル)となる。

また、MFPをリース返却、廃棄するなど利用が終了した場合や、HDDが盗難にあった場合など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も保護対象となる。

1)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。

2)保管画像ファイル

機密文書プリントファイル、ボックスファイル以外の保管される画像ファイル。

3)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。

4)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。

6)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、電話番号などが含まれるファイル。

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セキュリティ認証手続規程」[3]、「評価機関承認手続規程」[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 C250 / ineo^{+} 250 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：1.04」（以下「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][11][14]のいずれか) 附属書C、CCパート2（[6][9][12][15]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][13][16]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 C250 / ineo^{+} 250 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。）[22]に示されている。なお、評価方法は、CEMパート2（[17][18][19]のいずれか）に準拠する。また、CC及びCEMの各パートは補足（[20][21] のいずれか）の内容を含む。

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。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。評価は、平成18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、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL3適合である。

1.5.3 セキュリティ機能強度

STは、最小機能強度として、”SOF-基本”を主張する。

本TOEは、外部ネットワークからの攻撃から保護された、一般のオフィス環境での利用を想定している。TOEへのパネルを経由したアクセス、あるいは内部ネットワークを経由したアクセスは、管理者による管理下にあり、複雑な攻撃は想定されない。このため、攻撃者の攻撃力を「低レベル」と想定することは妥当である。

よってSOF-基本で十分である。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。

1)管理者機能（F.ADMIN）

パネルやネットワークからアクセスする管理者モードにおける管理者識別認証機能、管理者パスワードの変更やロックされたボックスのロック解除などのセキュリティ管理機能といった、管理者が操作する一連のセキュリティ機能である。

a. 管理者識別認証機能

管理者モードへのアクセス要求に対して、アクセスする利用者が管理者であることを識別及び認証する。

b. 管理者モードにて提供される機能

管理者モードへのアクセス要求において、管理者識別認証機能により管理者として識別認証されると、利用者を代行するタスクに管理者権限が関連づけられ、以下の操作、機能の利用が許可される。

①管理者パスワードの変更

管理者であることを再認証され、且つ新規設定されるパスワードが品質を満たしている場合、変更する。

管理者パスワードは、ASCIIコード（0x21 ～ 0x7E、ただし0x22と0x2B

を除く）（合計92文字が選択可能）を用いた8桁で設定される。

ネットワークからのアクセスでは、10^{10}以上のセッション情報を利用する。

パネルからのアクセスの場合、管理者パスワード入力のフィードバックに1文字毎“＊”を返す。

また、1つのキャラクタで構成されることはない。

認証に成功すると、認証失敗回数をリセットする。

管理者パスワードを利用する各認証機能において通算1～3回目となる認証失敗を検知すると、管理者パスワードを利用するすべての認証機能をロックする。（管理者モードへのアクセスを拒否する。）

認証機能のロックは、F.RESET機能が動作して解除する。

②ユーザの設定

ユーザIDを設定し、ユーザパスワードを登録してユーザを登録する。その際には、ユーザパスワードが品質を満たしていることを検証する。また、ユーザID、ユーザパスワードを変更、削除する。

ユーザパスワードは、ASCIIコード（0x21 ～ 0x7E、ただし0x22と0x2Bを除く）（合計92文字が選択可能）を用いた8桁以上で設定される。

また、1つのキャラクタで構成されることはない。

③ボックスパスワードの設定

未登録ボックスIDに対して、ユーザ属性を設定することで、共有ボックスとして登録する。ボックスパスワードの設定、変更、ボックスのユーザ属性の変更を行う。

ボックスパスワードは、ASCIIコード（0x20 ～ 0x7E、ただし0x22と0x2Bを除く）（合計93文字が選択可能）を用いた8桁で設定される。

個人ボックスのユーザ属性に登録されたユーザを指定し、別のユーザの個人ボックス、または共有ボックスに変更することができる。

また、1つのキャラクタで構成されることはない。

④ロックの解除

すべてのユーザの認証失敗回数、機密文書プリント、及びボックスの認証失敗回数、SNMPパスワードによる認証失敗回数を0クリアする。

アクセスがロックされているユーザ、機密文書プリント、ボックス、MIBオブジェクトが存在すれば、ロックが解除される。

⑤ユーザ認証機能の設定

ユーザ認証機能における認証方式を、本体認証、または外部サーバ認証に設定する。

⑥不正アクセス検出閾値の設定

認証操作禁止機能における不正アクセス検出閾値を1～3回で設定する。

⑦全領域上書き削除機能の設定と実行

消去方式を選択し、全領域の上書き削除を実行する。

（F.OVERWRITE-ALLを実行する。）消去方式は以下のとおり。

方式	上書きされるデータタイプとその順序
Mode:1	0x00
Mode:2	乱数 ⇒ 乱数 ⇒ 0x00
Mode:3	0x00 ⇒ 0xFF ⇒ 乱数 ⇒ 検証
Mode:4	乱数 ⇒ 0x00 ⇒ 0xFF
Mode:5	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF
Mode:6	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 乱数
Mode:7	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0xAA
Mode:8	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0xAA ⇒ 検証

⑧オートログオフ機能の設定

パネルオートログオフ時間を、1～9分の範囲で設定する。

⑨ネットワークの設定

以下の設定データの設定操作を行う。

・SMTPサーバに関係する一連の設定データ（IPアドレス、ポート番号等）

・DNSサーバに関係する一連の設定データ（IPアドレス、ポート番号等）

・MFPアドレスに関係する一連の設定データ（IPアドレス、NetBIOS名、AppleTalkプリンタ名等）

⑩バックアップ、リストア機能の実行

NVRAM、HDDに保管される設定データ（管理者パスワード、CEパスワードを除く）をバックアップ（参照）、リストア（変更）する。

⑪HDDロック機能の動作設定機能

HDDロック機能をOFFからONにする場合、設定されるHDDロックパスワードが品質を満たしていることを検証する。

HDDロックパスワードを変更する。現在設定されるHDDロックパスワードを使い、管理者であることを再認証され、且つ新規設定されるパスワードが品質を満たしている場合、変更する。

HDDロックパスワードは、ASCIIコード（0x21 ～ 0x7E、ただし0x22、0x28、0x29、0x2C、0x3A、0x3B、0x3C、0x3E、0x5B、0x5C、0x5Dを除く）（合計83文字が選択可能）を用いた20桁で設定される。

照合では、HDDロックパスワード入力のフィードバックに1文字毎“＊”を返す。

また、1つのキャラクタで構成されることはない。

⑫暗号化機能の動作設定

暗号化機能をOFFからONにする場合、設定される暗号鍵ワードが品質を満たしていることを検証し、F.CRYPTが実行される。

暗号鍵ワードを変更する。現在設定される暗号鍵ワードを使い、管理者であることを再認証され、且つ新規設定される管理者ワードが品質を満たしている場合、変更しF.CRYPTが実行される。

暗号鍵ワードは、ASCIIコード（0x21 ～ 0x7E、ただし0x22、0x28、0x29、0x2C、0x3A、0x3B、0x3C、0x3E、0x5B、0x5C、0x5Dを除く）（合計83文字が選択可能）を用いた20桁で設定される。

照合では、暗号鍵ワード入力のフィードバックに1文字毎“＊”を返す。また、1つのキャラクタで構成されることはない。

⑬セキュリティ強化機能に関連する機能

管理者が操作するセキュリティ強化機能の設定に影響する機能は以下の通り。

・セキュリティ強化機能の動作設定

セキュリティ強化機能の有効、無効を設定する機能。

・HDD論理フォーマット機能

HDDにOSのシステムファイルを再書き込みする機能、この論理フォーマットの実行に伴い、セキュリティ機能の設定が無効になる。

・全領域上書き削除機能

全領域上書き削除の実行により、セキュリティ強化機能の設定が無効になる。

⑭SNMPパスワードの変更

SNMPパスワードを変更する。新しく設定されるSNMPパスワードが、品質を満たしていることを検証する。

SNMPパスワードは、合計95文字が選択可能ASCIIコード（0x20 ～ 0x7E）を用いた8桁以上で設定される。

⑮SNMPパスワード認証機能の設定

SNMPパスワード認証機能における認証方式を「Authenticationパスワードのみ」または「Authenticationパスワード且つPrivacyパスワード」に設定する。

2)SNMP管理者機能（F.ADMIN-SNMP）

PCからSNMPを利用してネットワークを介したアクセスにおいて管理者を識別認証し、識別認証された管理者だけにネットワークの設定機能の操作を許可するセキュリティ機能である。

a. SNMPパスワードによる識別認証機能

SNMPを用いてネットワークを介してMIBオブジェクトにアクセスする利用

者が、管理者であることをSNMPパスワードによって識別認証する。

SNMPパスワードは、ASCIIコード（0x20 ～ 0x7E）（合計95文字が選択可能）を用いた8桁以上で設定される。

SNMPパスワードは、「Authenticationパスワード」と「Privacyパスワード」が存在し、これらを利用する認証機能において、通算1～3回となる認証失敗を検知すると、SNMPパスワードを利用するすべての認証機能をロックする。（MIBオブジェクトへのアクセスを拒否する。）

認証機能のロックは、F.ADMINのMIBオブジェクトに対するロック解除機能、またはF.RESET機能が動作して解除する。

認証成功時に、認証失敗回数をリセットするが、Privacyパスワード、Authenticationパスワードの双方を利用している場合は、双方共に認証に成功した場合に認証失敗回数をリセットする。

b. SNMPを利用した管理機能

SNMPパスワードにより管理者であることが識別認証されると、MIBオブジェクトへのアクセスが許可され、以下に示す設定データの設定操作を行うことが許可される。

①ネットワークの設定

以下の設定データの設定操作を行う。

・SMTPサーバに関係する設定データ（IPアドレス、ポート番号等）

・DNSサーバに関係する設定データ（IPアドレス、ポート番号等）

・MFPアドレスに関係する一連の設定データ（IPアドレス、NetBIOS名、AppleTalkプリンタ名等）

②SNMPパスワードの変更

SNMPパスワード（Privacyパスワード、Authenticationパスワード）を変更する。新しく設定されるSNMPパスワードは、ASCIIコード（0x20 ～ 0x7E）（合計95文字が選択可能）を用いた8桁以上で設定される。

③SNMPパスワード認証機能の設定

SNMPパスワード認証機能における認証方式を「Authenticationパスワードのみ」または「Authenticationパスワード且つPrivacyパスワード」に設定する。

3)サービスモード機能（F.SERVICE）

パネルからアクセスするサービスモードにおける、サービスエンジニア識別認証機能、CEパスワードの変更や管理者パスワードの変更などのセキュリティ管理機能といった、サービスエンジニアが操作する一連のセキュリティ機能である。

a. サービスエンジニア識別認証機能

パネルからサービスモードへのアクセス要求に対して、アクセスする利用者がサービスエンジニアであることを識別及び認証する。

b. サービスモードにて提供される機能

サービスモードへのアクセス要求においてサービスエンジニア識別認証機能により、サービスエンジニアとして識別認証されると、以下の機能の利用が許可される。

①CEパスワードの変更

サービスエンジニアであることを再認証され、且つ新規設定されるパスワードが品質を満たしている場合、変更する。

CEパスワードは、ASCIIコード（0x21 ～ 0x7E、ただし0x22と0x2Bを除く）（合計92文字が選択可能）を用いた8桁で設定される。

CEパスワード入力のフィードバックに1文字毎“＊”を返す。

認証に成功すると、認証失敗回数をリセットする。

CEパスワードを利用する各認証機能において通算1～3回目となる認証失敗を検知すると、CEパスワードを利用するすべての認証機能をロックする。（サービスモードへのアクセスを拒否する。）

認証機能のロックは、F.RESET機能が動作して解除する。

また、1つのキャラクタで構成されることはない。

②管理者パスワードの変更

管理者パスワードを変更する。設定される管理者パスワードは、ASCIIコード（0x21 ～ 0x7E、ただし0x22と0x2Bを除く）（合計92文字が選択可能）を用いた8桁で設定される。

③セキュリティ強化機能に関する機能

サービスエンジニアが操作するセキュリティ強化機能の設定に影響する機能は以下のとおり。

・HDD論理フォーマット機能

HDDにOSのシステムファイルを再書き込みする機能。この論理フォーマットの実行に伴い、セキュリティ強化機能の設定を無効にする。

・HDD物理フォーマット機能

HDDにトラック、セクター情報などの信号列を含めてディスク全体を規定パターンに書き直す機能。この物理フォーマットの実行に伴い、セキュリティ強化機能の設定を無効にする。

・HDD装着設定機能

搭載されたHDDを有効化するための機能。このHDD装着設定を無効化することにより、セキュリティ強化機能の設定を無効にする。

・イニシャライズ機能

NVRAMに書き込まれる各種設定値を工場出荷状態に戻すための機能。このイニシャライズ機能を実行することにより、セキュリティ強化機能の設定を無効にする。

④パスワード初期化機能に関する機能

サービスエンジニアが操作するパスワードの初期化に関係する機能は以下のとおり。

・イニシャライズ機能

NVRAMに書き込まれる各種設定値を工場出荷状態に戻すための機能。このイニシャライズ機能を実行することにより、管理者パスワード、SNMPパスワードを工場出荷の初期値に設定する。HDDロック機能、暗号化機能の動作設定をいずれもOFFにする。(動作設定がOFFされることにより、設定されていたHDDロックパスワード、暗号鍵ワードを再度利用することができなくなる。)

・HDD物理フォーマット機能

HDDにトラック、セクター情報などの信号列を含めてディスク全体を規定パターンに書き直す機能。この物理フォーマットの実行に伴い、HDDロック機能をOFFにする。(動作設定がOFFされることにより、設定されていたHDDロックパスワードを再度利用することができなくなる。)

4)ユーザ機能(F.USER)

MFPの諸機能を利用するにあたって、ユーザを識別認証する。また識別認証されたユーザには、F.BOXやF.PRINTなどの機能の利用を許可する他、本体認証時にMFP本体にて管理されるユーザパスワードの管理機能を提供する。

a. ユーザ識別認証機能

ボックスへのアクセス要求、機密文書プリントファイルの登録要求において、ユーザであることを識別認証する。識別認証されたユーザには、F.BOX及びF.PRINTの利用を許可する。

ユーザパスワードは、ASCIIコード(0x21 ～ 0x7E、ただし0x22と0x2Bを除く)(合計92文字が選択可能)を用いた8桁以上で設定される。

ネットワークからのアクセスでは、10^{10}以上のセッション情報を利用する。

ユーザパスワード入力のフィードバックに1文字毎“＊”を返す。

また、1つのキャラクタで構成されることはない。

認証に成功すると、認証失敗回数をリセットする。

当該ユーザに対して、通算1～3回目となる認証失敗を検知すると、当該ユーザに対する認証機能をロックする。

認証機能のロックは、F.ADMINのユーザ認証に対するロック解除機能、またはF.RESET機能が動作して解除する。

ユーザ認証方式に「外部サーバ認証」が選択されている場合で、上記の機能によって識別認証されたユーザがMFP本体に登録されていない場合 、そのユーザIDを登録する。

b.ユーザ識別認証ドメインにおけるオートログオフ機能

識別認証されたユーザがパネルからアクセス中、パネルオートログオフ時間以上何らかの操作を受け付けなかった場合、自動的にユーザ識別認証ドメインからログオフする。

c.ユーザパスワードの変更機能

識別認証され、ユーザ識別認証ドメインへのアクセスが許可されると、本人のユーザパスワードを変更することが許可される。なお、外部サーバ認証が有効の場合には、本機能は利用できない。

5)ボックス機能（F.BOX）

登録ユーザであると識別認証されたユーザに対して、そのユーザの個人ボックスの操作、管理を許可し、共有ボックスへのアクセスに対してボックスの利用を許可されたユーザであることを認証し、認証後に当該ボックス、ボックスファイルの各種操作を許可するアクセス制御機能などボックスに関係する一連のセキュリティ機能である。

a. ボックスの登録

選択した未登録ボックスIDに対して、ユーザ属性を選定し、個人ボックス、または共有ボックスを登録する。

個人ボックスの場合は、登録される任意のユーザIDを指定する。

共有ボックスの場合は、登録される共有ボックスのパスワードが品質を満たしていることを検証する。

共有ボックスのパスワードは、ASCIIコード（0x20 ～ 0x7E、ただし0x22と0x2Bを除く）（合計93文字が選択可能）を用いた8桁で設定される。

また、1つのキャラクタで構成されることはない。

b. 個人ボックス機能

識別認証されたユーザを代行するタスクは、ユーザ属性に識別認証されたユーザの「ユーザID」を持つ。このタスクは、このユーザ属性と一致するユーザ属性を持つ個人ボックスの一覧表示操作が許可される。

操作するボックスを選択すると、ユーザ属性に加えてそのボックスの「ボックスID」がボックスル属性としてタスクに関連付けられる。このタスクは、このユーザ属性及びボックス属性と一致するユーザ属性、ボックス属性を持つボックスファイルに対して、印刷、E-mail送信、FTP送信、FAX送信、SMB送信、ダウンロード、他のボックスへの移動、他のボックスへのコピー操作を行うことを許可される。

個人ボックスのユーザ属性を変更することができる。他の登録ユーザを指定すると、他のユーザが管理する個人ボックスになる。共有を指定すると、共有ボックスになり、その際には共有ボックスのパスワード登録が必要となる。

c. 共有ボックス機能

識別認証されたユーザを代行するタスクは、ユーザ属性に識別認証されたユー

ザの「ユーザID」を持つ。このタスクは、ユーザ属性に共有が設定される共有ボックスの一覧表示操作が許可される。

個々の共有ボックスへのアクセス要求に対しては、それぞれ当該ボックスの利用を許可されたユーザであることを認証する。

ネットワークからのアクセスでは、10^{10}以上のセッション情報を利用する。

パスワード入力のフィードバックに1文字毎“＊”を返す。

認証に成功すると、認証失敗回数をリセットする。

パネルからのアクセスの場合、認証に失敗するとパネルからの入力を5秒間受け付けない。

当該共有ボックスにおいて通算1～3回目となる認証失敗を検知すると、当該共有ボックスに対する認証機能をロックする。

認証機能のロックは、F.ADMINの共有ボックスに対するロック解除機能、またはF.RESET機能が動作して解除する。

ユーザを代行するタスクは、ユーザ属性に加えてそのボックスの「ボックスID」がボックス属性としてタスクに関連づけられる。このタスクは、ユーザ属性に共有が設定され、且つサブジェクト属性のボックス属性と一致するボックス属性を持つボックスファイルに対して印刷、E-mail送信、FTP送信、FAX送信、SMB送信、ダウンロード、他のボックスへの移動、他のボックスへのコピー操作を行うことを許可される。

共有ボックスのユーザ属性を変更することができる。登録ユーザを指定し、登録ユーザの個人ボックスに変更する。

共有ボックスのパスワードを変更する。

6)機密文書プリント機能（F.PRINT）

登録ユーザであると識別認証されたユーザの、パネルからの機密文書プリントファイルへのアクセスに対して、機密文書プリントファイルの利用を許可されたユーザであることを認証し、認証後に当該機密文書プリントファイルの印刷を許可するアクセス制御機能など、機密文書プリントに関係する一連のセキュリティ機能である。

a. 機密文書パスワードによる認証機能

登録ユーザであることが識別認証されると、機密文書プリントファイルへのアクセス要求に対して、アクセスする利用者が当該機密文書プリントファイルの利用を許可されたユーザであることを認証する。

機密文書パスワードは、ASCIIコード（0x20 ～ 0x7E、ただし0x22と0x2Bを除く）（合計93文字が選択可能）を用いた8桁で設定される。

パネルからのアクセスの場合、認証に失敗するとパネルからの入力を5秒間受け付けない。

機密文書パスワード入力のフィードバックに1文字毎“＊”を返す。

当該機密文書プリントファイルに対して、通算1～3回目となる認証失敗を検

知すると、当該機密文書プリントファイルに対する認証機能をロックする。

ロック状態は、F.ADMINの機密文書プリントファイルに対するロック解除機能、またはF.RESET機能が動作して解除する。

b. 機密文書プリントファイルに対するアクセス制御機能

認証されると、機密文書プリントファイルアクセス制御が動作する。

識別認証されたユーザを代行するタスクは、ファイル属性に、認証された機密文書プリントファイルの機密文書内部制御IDを持つ。

このタスクは、このファイル属性と一致するファイル属性を持つ機密文書プリントファイルに対して印刷を許可される。

c. 機密文書プリントファイルの登録機能

①機密文書パスワードの登録

機密文書プリントファイルの登録要求において、登録される機密文書パスワードが以下の条件を満たすことを検証する。

・ボックスパスワードは、ASCIIコード（0x20 ～ 0x7E、ただし0x22と0x2Bを除く）（合計93文字が選択可能）を用いた8桁で設定される。
・また、1つのキャラクタで構成されることはない。

②機密文書内部制御IDの付与

機密文書プリントファイルの登録要求において、機密文書パスワードの検証が完了すると、一意に識別される機密文書内部制御IDを当該機密文書プリントファイルに設定する。

7)全領域上書き削除機能（F.OVERWRITE-ALL）

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。削除、または初期化される対象は以下の通りである。

＜削除される対象：HDD＞
・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
・保管画像ファイル
・送信宛先データファイル
・ユーザID
・ユーザパスワード
・ボックスパスワード
・機密文書パスワード

＜初期化される対象：NVRAM＞
・管理者パスワード

・SNMPパスワード
・HDDロック機能の動作設定（OFF）
・暗号化機能の動作設定（OFF）
HDDに書き込むデータ、書き込む回数など削除方式は、F.ADMINにおける全領域上書き削除機能の消去方式に応じて実行される。HDDロック機能、及び暗号化機能は動作設定がOFFされることによって、設定されていたHDDロックパスワード、暗号鍵ワードが利用できなくなる。
なお、本機能の実行においてセキュリティ強化機能の設定は、無効になる。

8)暗号鍵生成機能（F.CRYPT）

コニカミノルタ暗号仕様標準によって規定されるコニカミノルタHDD暗号鍵生成アルゴリズム（SHA-1）を利用し、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鍵を生成する。コニカミノルタHDD暗号鍵生成アルゴリズム（SHA-1）とは、FIPS 180-1が規定するSHA-1を利用して暗号鍵を生成するアルゴリズムである。
暗号鍵ワードが決定されると、コニカミノルタHDD暗号鍵生成アルゴリズム（SHA-1）を用いて、暗号鍵ワードから160bitのハッシュ値を取得し、上位128bitを暗号鍵として生成する。

9)HDD検証機能（F.HDD）

HDDに対してHDDロックパスワードを設定している場合、不正なHDDが設置されていないことを検証し、正当性が確認された場合だけHDDへの読み込み、書き込みを許可するチェック機能である。
HDDにHDDロックパスワードが設定されている場合、TOE起動時のHDD動作確認において、HDDのステータス確認を行う。ステータス確認の結果、HDDロックパスワードが確かに設定されていることが返された場合は、HDDへのアクセスを許可し、HDDロックパスワードが設定されていないことが返された場合は、不正な可能性があるためHDDへのアクセスを拒否する。

8)認証失敗回数リセット機能（F.RESET）
管理者認証を始めとした各認証機能においてカウントされる認証失敗回数をリセットする機能である。（ロックの有無と関係しない。）
MFPの主電源がONされる、または停電などから復帰した場合など、TOEの起動により本機能は動作する。起動すると、以下の認証失敗回数をリセットする。アカウントロックされていた対象は、ロックが解除される。）
・管理者の認証に対する失敗回数
・SNMPパスワードを利用した認証に対する失敗回数
・サービスエンジニアの認証に対する失敗回数
・各ユーザの認証に対する失敗回数

・各共有ボックスの認証に対する失敗回数
・各機密文書プリントの認証に対する失敗回数

1.5.5 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

表1-1 想定する脅威

識別子	脅 威
T.DISCARD-MFP	・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を取り出して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、保管画像ファイル、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	・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、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、保管画像ファイル、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、保管画像ファイル、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	・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ダウンロード、印刷、送信（E-mail送信、FTP送信、FAX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-PUBLIC-BOX	・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ダウンロード、印刷、送信（E-mail送信、FTP送信、FAX送信、SMB送信）、他のボックスへ移動・コピーすることにより、ボックスファイルが暴露される。
T.ACCESS-SECURE-PRINT	・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。
T.ACCESS-NET-SETTING	・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＞

識別子	脅　威
	・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、機密文書プリントファイルが暴露される。
T.ACCESS -SETTING	・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。
T.BACKUP -RESTORE	・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、機密文書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。

1.5.6　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。

1.5.7　構成条件

TOEは、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 C250 / ineo+ 250において動作する。なお、暗号化基板についてはオプションパーツであるため、MFPには標準搭載されない。暗号化基板が装着されない場合は、暗号化に関する機能を利用することはできない。

1.5.8　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1-2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1-2　TOE使用の前提条件

識別子	前提条件
A.ADMIN	・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一連の作業において、悪意を持った行為は行わない。
A.NETWORK	・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	・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が有効化した上で、TOEが搭載されたMFPを利用する。
A.SERVER	・ユーザ認証方式に外部サーバ認証を利用する場合、TOEが搭載されるMFPを設置するオフィス内LANに接続されるユーザ情報管理サーバは、アカウントの管理、アクセス制御、パッチ適用などが適切に実施されている。

1.5.9 製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

＜管理者・一般利用者向けドキュメント＞

1) bizhub C250　ユーザーズガイド　セキュリティ機能編　（バージョン：1.02）

2) bizhub C250 / ineo^{+} 250　User's Guide [Security Operations]　（Ver.1.02）

3) ineo^{+}250　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＞

1)bizhub C250 サービスマニュアル　セキュリティ機能編 (Ver. 1.02)

2)bizhub C250 ineo^{+} 250 Service Manual Security Function (Ver. 1.02)

2 評価機関による評価実施及び結果

2.1 評価方法

評価は、CCパート3の保証要件について、CEMパート2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パート2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。

2.2 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17年10月に始まり、平成18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18年6月、7月、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・配付と運用・ライフサイクル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18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。

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。

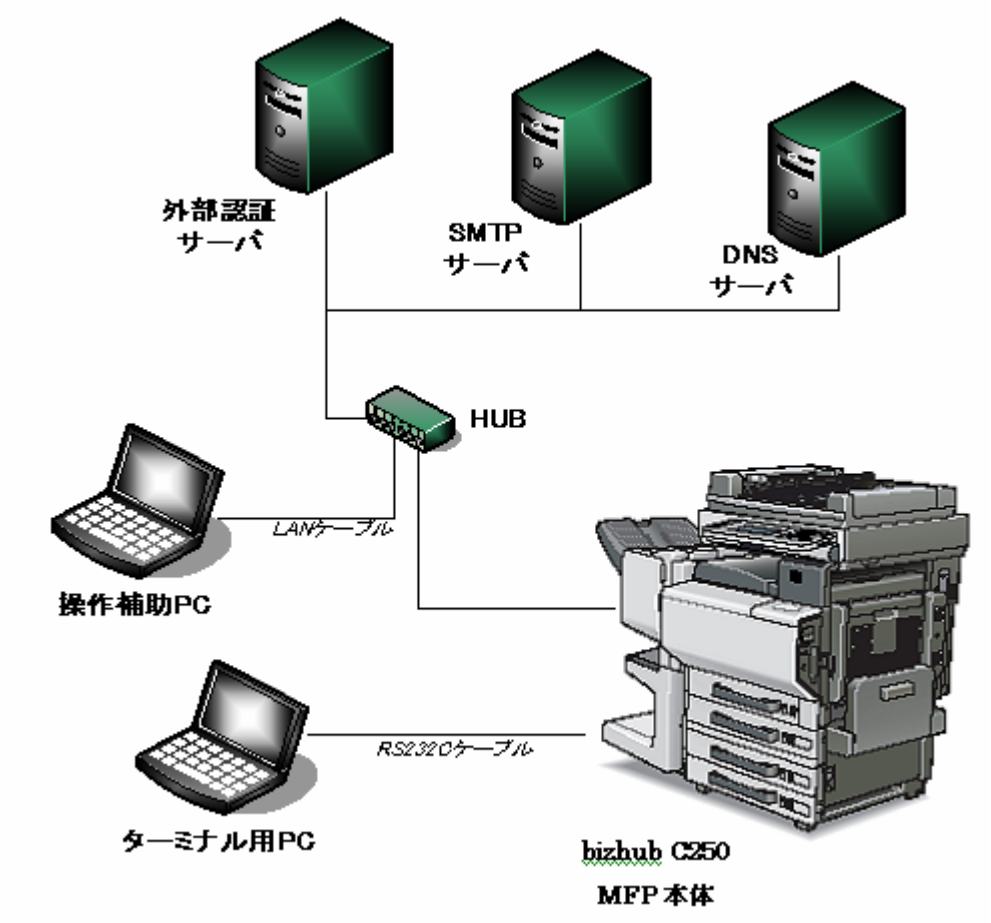
2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

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2-1に示す。



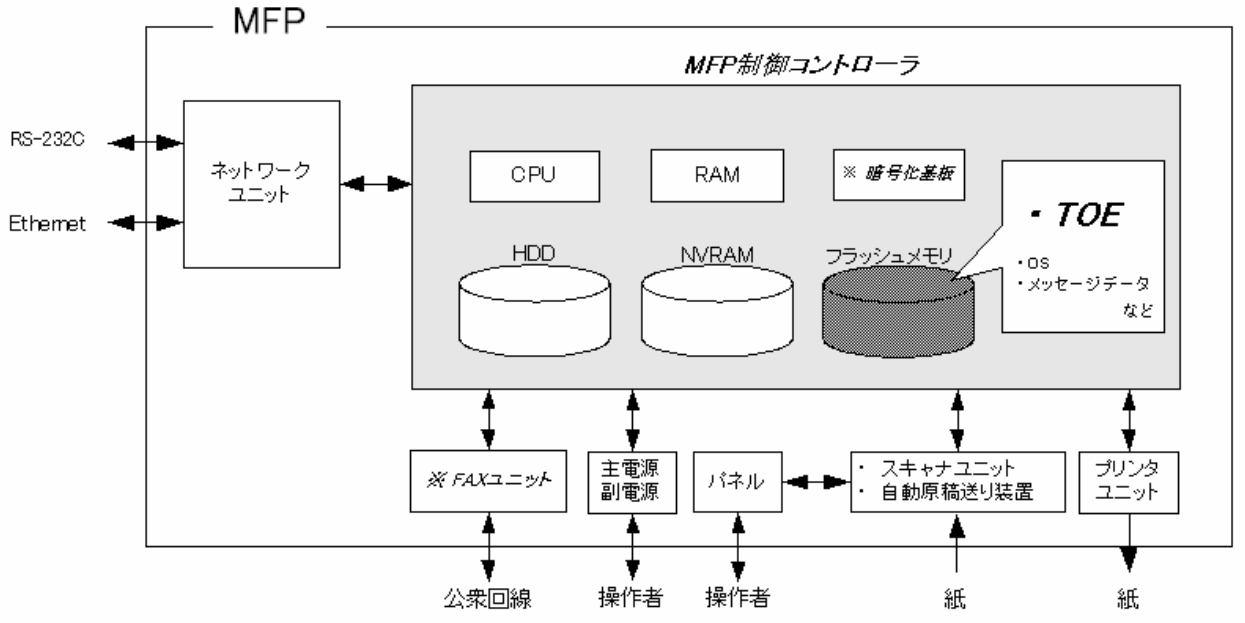


図2-1　開発者テストの構成図

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a.テスト構成

開発者が実施したテストの構成を図2-1に示す。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TOEテスト環境で実施されている。ただし、MFPからは、ローカル接続ユニット(オプションパーツ)が除かれた構成である。

b.テスト手法

テストには、以下の手法が使用された。

①設定値の変更、認証方法、アクセス制御の確認等に外部インタフェース（パネル、ネットワーク、及び電源OFF/ON）を利用し、出力メッセージや動作の変化、そのふるまいを確認する。ネットワークでは、PageScope Web Connection（PSWC）で利用するHTTPSプロトコル、TCP Socket（アプリケーションからのアクセスに使用するTCPベースのAPI)、OpenAPI（アプリケーションからのアクセスに利用するXMLベースのAPI)、SNMP（MIBを操作する)を利用してアクセスが可能であり､各プロトコルは､テストツールを利用してそれぞれのプロトコルのテストデータを送受することでセキュリティ機能のふるまいを観察することができる。また、HTTPSプロトコルを使用する際や、OpenAPIを使用する際のセッション情報が正しく生成されたことは、テストツールを用いることで確認することができる。

②①のインタフェースを利用して検証できないセキュリティ機能については、それぞれ個別のテスト手順を実施し、ふるまいの妥当性を確認する。該当するテストの概要は、以下のとおり。

・全領域上書き削除機能が正しく動作すること（“ 0x00⇒0xFF⇒0x00⇒0xFF⇒0x00⇒0xFF⇒0xAA⇒検証 ”にてHDDが削除されていること、管理者使用領域を初期化していること）を確認するため、HDDの内容をダンプ表示及び編集可能なツールを利用して確認する方法を採用している。

・暗号鍵が適切に生成されていることを確認するため、本体に直接接続したターミナル画面にて、メモリ上にあるデータを直接参照する方法を採用している。

・HDDロックパスワードが有効に機能することを確認するため､HDDロックパスワードが設定されていない他のHDDと交換して､エラーの発生状況を確認する方法を採用している。

・セキュリティ強化機能に関連する機能（HDD論理フォーマット、HDD物理フォーマット、HDD装着設定機能、イニシャライズ機能）のふるまいは、HDDがIT環境であることからMFPから参照できるこれらの機能の効果の観点から観察する方法を採用している。

c.実施テストの範囲

テストは開発者によっておよそ129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、上位レベル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。

d.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。

2.3.2 評価者テスト

1) 評価者テスト環境

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。

なお、侵入テストに関しては、ターミナル用PCを用いず、2台の検査PCを追加し、テストを効率的に行うため、同じMFP（bizhubC250）を３台用いて実施した。その概略図を図2-2に示す。

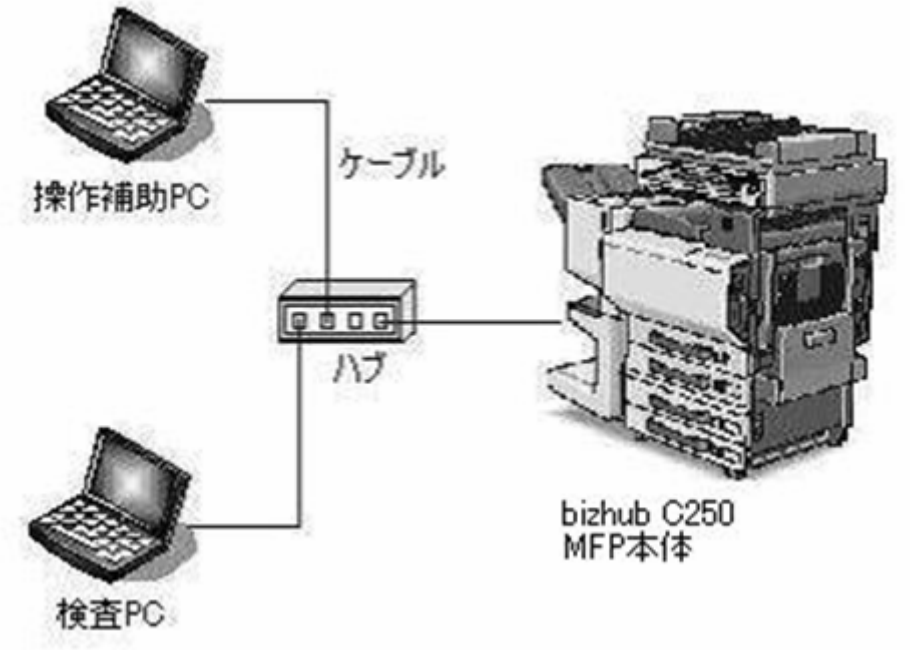


図2-2　開発者テスト（侵入テスト）の構成図

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテストの構成を図2-1、及び図2-2に示す。評価者テストは

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。

b.テスト手法

テストには、以下の手法が使用された。

設定値の変更、認証方法、アクセス制御の確認等に外部インタフェース（パネル、ネットワーク、及び電源OFF/ON）を利用し、出力メッセージや動作の変化、そのふるまいを確認する。ネットワークでは、PageScope Web Connection（PSWC）で利用するHTTPSプロトコル、TCP Socket（アプリケーションからのアクセスに使用するTCPベースのAPI)、OpenAPI（アプリケーションからのアクセスに利用するXMLベースのAPI)、SNMP（MIBを操作する）を利用してアクセスが可能であり、各プロトコルは、テストツールを利用してでそれぞれのプロトコルのテストデータを送受することでセキュリティ機能のふるまいを観察することができる。

また、HTTPSプロトコルを使用する際や、OpenAPIを使用する際のセッション情報が正しく生成されたことは、テストツールを用いることで確認することができる。

c.実施テストの範囲

評価者が独自に考案したテストを30項目、開発者テストのサンプリングによるテストを30項目、計60項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

① 開発者テストからは仕様通りに動作することが疑われるセキュリティ機能
② 他のセキュリティ機能よりも重要なセキュリティ機能
③ 機能強度の対象となるセキュリティ機能
④ 異なるインタフェースから利用される機能

また、評価者が実施した侵入テストについては、以下のように実施された。

TOEは大別して操作パネルからの操作、HTTPSプロトコル、TCP Socket、OpenAPI、SNMPによるネットワークを経由した操作、MFP本体の電源OFF/ONによる操作の3種類の操作が行える。操作パネル、MFP本体の電源OFF/ONによる操作は、操作パネル及びMFP本体の物理的な制約上から、想定される利用方法以外の操作、すなわち不正操作を行うことはまず不可能と判断される。これに対してネットワークを経由した操作は、非常に幅が広く、期待される入力以外の操作を容易に実施することができる。

そこで、ネットワークに関連した項目を中心に、以下3つの観点を考慮して7項目の侵入テストを考案した。

①開発者の脆弱性分析に基づく主張の真偽を検証する。
②評価者が考える明白な脆弱性への対処を検証する。
③開発者の機能強度主張の真偽を検証する。

表2-2に侵入テスト項目一覧を示す。

表2-2　侵入テスト項目一覧

テスト番号	[VLA]に基づく脆弱性検査のための侵入テスト名	侵入テスト考案の観点
VLA-T1	ネットワークI/Fのセキュリティ対策状況確認テスト（１）	観点①
VLA-T2	ネットワークI/Fのセキュリティ対策状況確認テスト（２）	観点①
VLA-T3	公知の脆弱性確認テスト	観点①
VLA-T4	HTTP要求に対するセキュリティ機能確認テスト	観点②
VLA-T5	Webサーバ機能の確認テスト	観点②
VLA-T6	機能強度に関する確認テスト	観点③
VLA-T7	cookieのランダム性確認テスト	観点③

d.結果

実施したすべての評価者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。

2.4　評価結果

評価報告書をもって、評価者は本TOEがCEMパート2のワークユニットすべてを満たしていると判断した。

3 認証実施

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 当該所見報告書でなされた指摘内容が妥当であること。

② 当該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。

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、ST及び評価報告書において、所見報告書及び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た。

4 結論

4.1 認証結果

提出された評価報告書、当該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保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1　評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE種別、境界の記述が明瞭であることを確認している。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫していることを確認している。
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST概説がST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。

ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件へ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、CCを参照しない要件の明示が必要である根拠が示されていること、それらの要件はCCの要件と同様のスタイルと詳細度で記述されていること、それらの要件は明確に曖昧さなく表現されていること、それらの要件は評価可能であること、それらの要件に対して保証要件が適切にサポートする根拠が示されていることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件の依存性の識別が不要であることを確認している。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。

ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
構成管理	**適切な評価が実施された**
ACM_CAP.3.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。
ACM_SCP.1.1E	評価はワークユニットに沿って行われ、構成要素リストがCCによって要求される一連の要素を含んでいることを確認している。
配付と運用	**適切な評価が実施された**
ADO_DEL.1.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
ADO_DEL.1.2D	評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、実地検査により確認している。
ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。
開発	**適切な評価が実施された**
ADV_FSP.1.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。
ADV_FSP.1.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。

ADV_HLD.2.1E	評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSF実現に必要なIT環境としてのハードウェア、ソフトウェア、ファームウェアを説明していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。
ADV_HLD.2.2E	評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_RCR.1.1E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であり、上位レベル設計が機能仕様の正しく完全な表現であることを、それらの対応分析により確認している。
ガイダンス文書	**適切な評価が実施された**
AGD_ADM.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
AGD_USR.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
ライフサイクルサポート	**適切な評価が実施された**
ALC_DVS.1.1E	評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。

ALC_DVS.1.2E	評価はワークユニットに沿って行われ、ALC_DVS.1.1Eで確認したセキュリティ手段が実施されていることを確認している。
テスト	**適切な評価が実施された**
ATE_COV.2.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_DPT.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。
ATE_IND.2.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。
ATE_IND.2.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。
ATE_IND.2.3E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。
脆弱性評定	**適切な評価が実施された**

AVA_MSU.1.1E	評価はワークユニットに沿って行われ、提供されたガイダンスがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていること、ガイダンスの完全性を保証する手段を開発者が講じていることを確認している。
AVA_MSU.1.2E	評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEのセキュアな運用に関わる設定が行えることを確認している。
AVA_MSU.1.3E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法を記述していることを確認している。
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。
AVA_SOF.1.2E	評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しいことを確認している。
AVA_VLA.1.1E	評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。
AVA_VLA.1.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
MFP	Multiple Function Peripheral
HDD	Hard Disk Drive
LAN	Local Area Network
IP	Internet Protocol
FTP	File Transfer Protocol
SNMP	Simple Network Management Protocol
NVRAM	Non-Volatile Random Access Memory

本報告書で使用された用語を以下に示す。

MFP 制御コントローラ	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ためのコントローラ。TOE はそのコントローラ上で動作するソフトウェアである。
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。
PC プリント	パソコン（PC）からプリンタドライバを使って MFP に印刷したいファイルのプリントデータを流し、MFP にてそのデータを画像ファイルに変換し、その画像データを印刷すること。

機密文書プリント	PC プリントのうち、プリンタドライバで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。
ボックス	画像ファイルを MFP 内部に保管するために、HDD 領域に作成されたディレクトリのこと。
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、調整等の保守管理を行う。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または代理店のサービス担当者である。
サービスモード	サービスエンジニアのために用意された MFP 機能を動作することができる操作パネル画面領域。
CE パスワード	サービスモードに入るときの認証時に照合する一種のパスワード。
残存画像ファイル	HDD データ領域に残存するファイルであり、通常の削除操作では削除できない画像ファイル。
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、電話番号などが含まれるファイル。
アカウントロック	パスワード認証の操作で連続して失敗した時などに、続けてパスワード認証をできなくしてしまうこと、またはその状態。

6 参照

[1] bizhub C250 / ineo+ 250　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 1.04　2006年11月14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17年7月　独立行政法人 情報処理推進機構　EC-01

[3] ITセキュリティ認証手続規程　平成17年7月　独立行政法人 情報処理推進機構　EC-03

[4] 評価機関承認手続規程　平成17年7月　独立行政法人 情報処理推進機構　EC-05

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[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2.1 1999年8月 CCIMB-99-031　(平成13年1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: セキュリティ機能要件 バージョン2.1 1999年8月 CCIMB-99-032　(平成13年1月翻訳第1.2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: セキュリティ保証要件 バージョン2.1 1999年8月 CCIMB-99-033　(平成13年1月翻訳第1.2版)

[11] ISO/IEC15408-1: 1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC15408-2: 1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC15408-3: 1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] JIS X 5070-1: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部: 総則及び一般モデル

[15] JIS X 5070-2: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部: セキュリティ機能要件

[16] JIS X 5070-3: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部: セキュリティ保証要件

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999

[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論 バージョン1.0 1999年8月　(平成13年2月翻訳第1.0版)

[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法

[20] CCIMB Interpretations-0407　平成16年8月

[21] 補足-0210 第2版、補足-0407　平成16年8月

[22] bizhub C250 / ineo+ 250 全体制御ソフトウェア　評価報告書　第3版　2006年11月15日　みずほ情報総研株式会社　情報セキュリティ評価室