認　証　報　告　書

評価対象

申請受付年月日（受付番号）	**平成16年4月1日（IT認証4025）**
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**	**日本名：**#4036 Multi Function Peripheral **全体制御ソフトウェア** **英名：**#4036 Multi Function Peripheral Control Software
TOE**のバージョン**	Macro System Controller　：　4036-10G0-18-00 Network Module　　：　4036-A0G0-04-00
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	**社団法人　電子情報技術産業協会　ITセキュリティセンター**

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16年9月15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セキュリティ評価機関に対する要求事項」で定める下記の規格に基づいて評価された。

① ISO/IEC 15408:1999 Information technology - Security techniques - Evaluation criteria for IT security
② JIS X 5070(2000) セキュリティ技術 ― 情報技術セキュリティの評価基準
③ Common Criteria for Information Technology Security Evaluation Version 2.1
④ 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
⑤ Common Methodology for Information Technology Security Evaluation Version 1.0
⑥ CCIMB Interpretations-0210

⑦　認証機関が公開する③、⑤及び⑥の翻訳文書

評価結果：合格

「日本名：#4036 Multi Function Peripheral 全体制御ソフトウェア、英名：#4036 Multi Function Peripheral Control Software」は、独立行政法人情報処理推進機構が定めるIT製品等のセキュリティ認証業務実施規程に従い、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 3
1.2.4 TOEの機能 4
1.3 評価の実施 9
1.4 評価の認証 9
1.5 報告概要 10
1.5.1 PP適合 10
1.5.2 EAL 10
1.5.3 セキュリティ機能強度 10
1.5.4 セキュリティ機能 10
1.5.5 脅威 12
1.5.6 組織のセキュリティ方針 13
1.5.7 構成条件 13
1.5.8 操作環境の前提条件 13
1.5.9 製品添付ドキュメント 14
2 評価機関による評価実施及び結果 16
2.1 評価方法 16
2.2 評価実施概要 16
2.3 製品テスト 16
2.3.1 開発者テスト 17
2.3.2 評価者テスト 18
2.4 評価結果 19
3 認証実施 19
4 結論 20
4.1 認証結果 20
4.2 注意事項 26
5 用語 27
6 参照 30

1 全体要約

1.1 はじめに

この認証報告書は、「日本名：#4036 Multi Function Peripheral 全体制御ソフトウェア、英名：#4036 Multi Function Peripheral Control Software」（以下「本TOE」という。）について社団法人 電子情報技術産業協会 ITセキュリティセンター（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。

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: 日本名：#4036 Multi Function Peripheral 全体制御ソフトウェア
英名：#4036 Multi Function Peripheral Control Software

バージョン: Macro System Controller ： 4036-10G0-18-00
Network Module ： 4036-A0G0-04-00

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

#4036 Multi Function Peripheral（以下MFPとする）とは、コピー、プリント、スキャンの各機能を選択、組み合わせて構成されるコニカミノルタビジネステクノロジーズ株式会社が提供するデジタル複合機である。本製品（日本名：#4036 Multi Function Peripheral 全体制御ソフトウェア、英名：#4036 Multi Function Peripheral Control Softwareは名称が異なるだけで同一物である。）は、MFPに搭載される制御ソフトウェアの中で、MFP本体操作パネルからの操作制御処理、ジョブのリソース管理、ジョブのシーケンス制御処理等を実施するソフトウェアコンポーネントである「Macro System Controller」及びクライアントPCからの操作制御処理を実施するソフトウェアコンポーネントである「Network Module」から構成される。本製品のセキュリティ機能は、MFPにおける特定の機能の利用にあたりMFPに取り込まれる機密性の高いド

キュメントデータの暴露に対する保護機能を提供する。特定の機能とは以下に示す機能である。

・ 親展プリント機能
  クライアントPCにてパスワードを設定し、MFPに送信して印刷待機状態にあるプリントデータに対して、MFP本体操作パネルからパスワードを入力して一致した場合に当該プリントデータが印刷される機能。
・ ボックス機能
  スキャンデータの一時格納領域として設定されるボックスへのアクセスを制御する機能。
・ メモリリコール OFF コピー機能
  通常、コピーを実行して印刷後には再印刷可能な状態になる当該コピーデータを、印刷終了後自動的に削除する機能。

想定される一般的な利用環境を図1-1に示す。

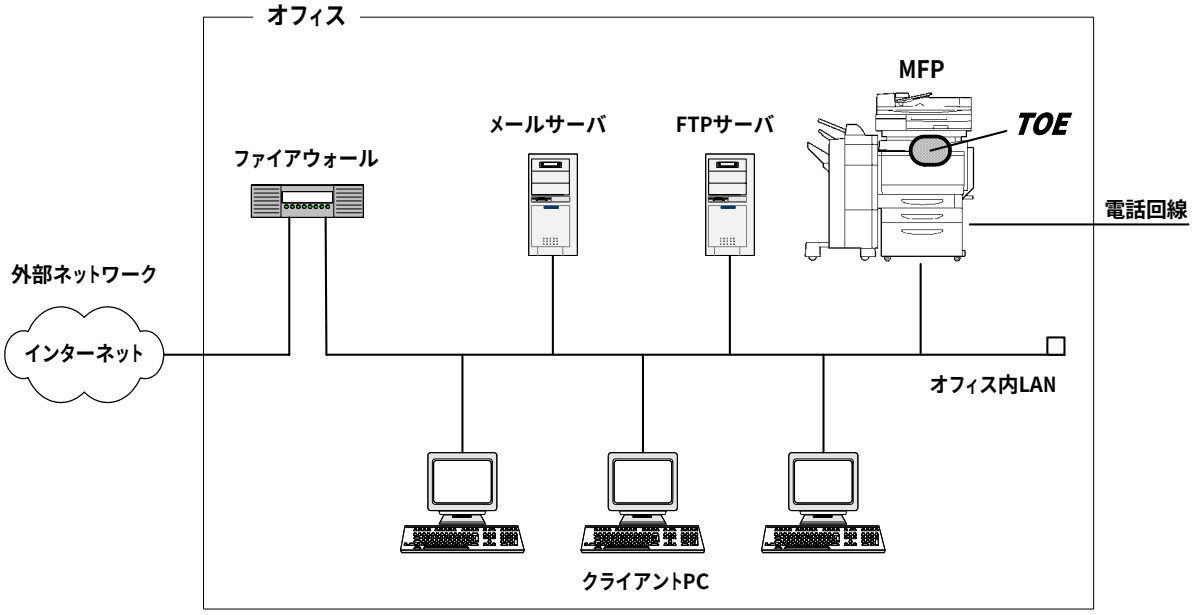

図1-1　想定されるMFPの利用環境の例

上図に示されるように、MFPは一般的なオフィスに設置される。オフィスは、MFPの利用・運用・保守に関わる者だけが入室することか可能な運用管理体制が敷かれる。オフィス内部のネットワークとしてオフィス内LANが存在する。MFPはオフィス内LANを介してクライアントPCと接続し、相互にデータ通信を行う。オフィス内LANにメールサーバ、FTPサーバが接続される場合は、MFPはこれらを利用してデータ通信を行うことも可能である。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に対するアクセス要求を遮断するための適切な設定が行われる。またオフィス内LANは、スイッチングハブ等の利用、オフィスの運用により、MFPとクライアントPCの間の通信データが盗聴されないネットワーク環境が整備されている。MFPに接続される電話回

線は、MFPの保守管理を行うサポートセンターとの通信に利用される。

また、HDDロック機能(パスワードの照合にて不成功試行を検出し、一定回数の不成功試行検出以降、照合機能をロックする機能)を有するHDDが搭載され、HDDが盗難された場合でも不当なアクセスから保護され、機密性が保たれる。

1.2.3 TOEの範囲と動作概要

TOEである「Macro System Controller」及び「Network Module」は、その他のMFP制御ソフトウェアコンポーネントと一体となってMFP本体内部のMFP制御コントローラで稼動するOS（VxWorks）上で動作する。このMFP制御ソフトウェアコンポーネントの構成図を図1-2に示す。TOEの物理的領域は、同図にて濃色で示される範囲である。

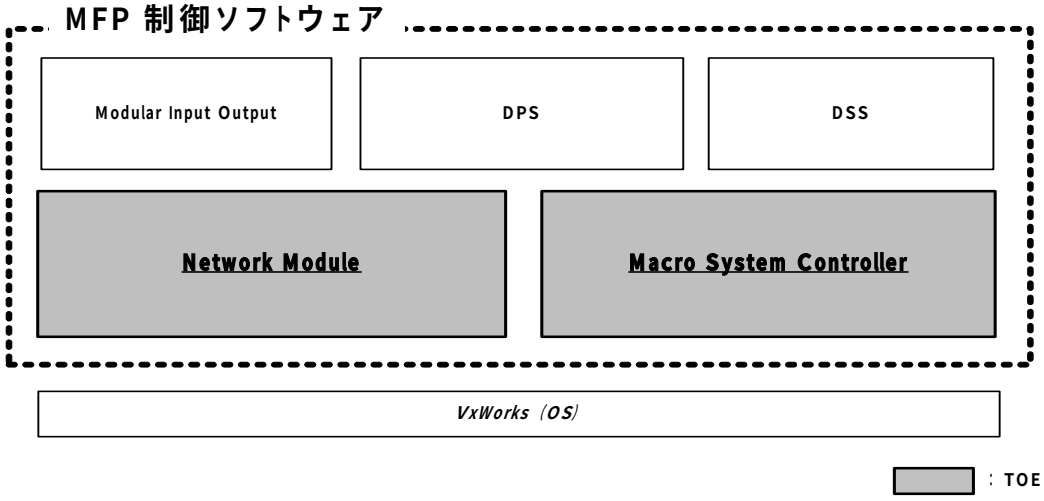

図1-2　MFP制御ソフトウェアコンポーネントの構成

以下、TOEが担う動作概要について説明する。

- Macro System Controller（MSC）

  取り込んだイメージデータをジョブとして登録し、ジョブのリソース、起動、シーケンスを管理するモジュール。MFP本体操作パネルにおけるLCD、LED、キー等の入力情報を処理し、処理に応じて他のソフトウェアコンポーネントに通知する。他のソフトウェアコンポーネントからのメッセージを処理してその他のソフトウェアコンポーネントへ通知する、またはMFP本体操作パネルに表示する。

- Network Module（NM）

  クライアントPCからの操作要求に対し、「Modular Input Output」がネットワークからデータを受け付け、処理・制御するソフトウェアコンポーネント。処理に応じて「VxWorks」、「Macro System Controller」に処理を依頼する。また「VxWorks」、「Macro System Controller」にて処理されたデータを受け付け、「Modular Input Output」に処理を依頼する。

TOEである「Macro System Controller」及び「Network Module」は、その他のMFP制御ソフトウェアコンポーネント及びOSと以下の図1-3に示される関係を持つ。

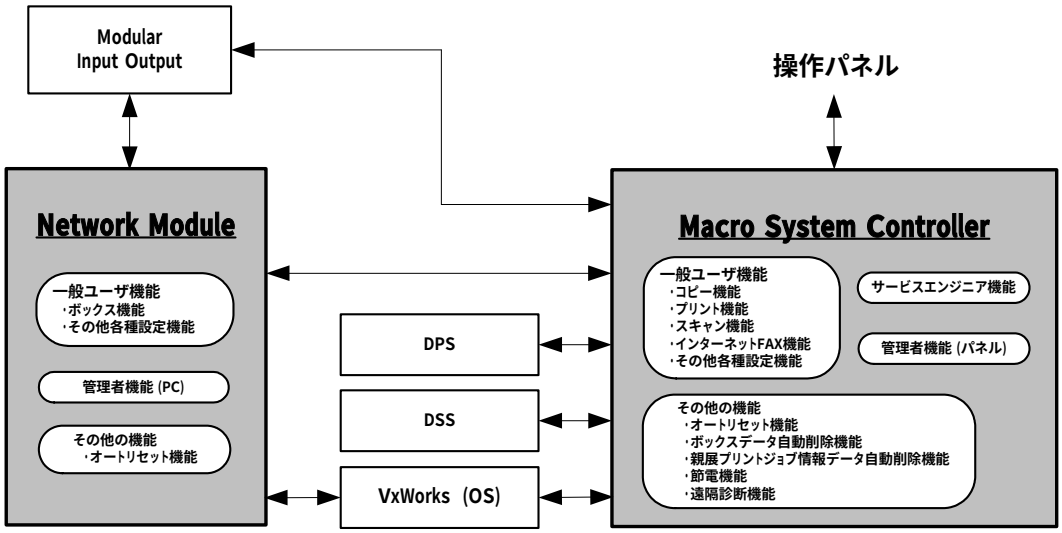

図1-3　TOE動作処理と関係するMFP制御ソフトウェアコンポーネント

1.2.4　TOEの機能

一般ユーザ及び管理者は、クライアントPC及びMFP本体操作パネルからTOEの搭載されたMFPの各種機能を使用する。サービスエンジニアは、MFP本体操作パネルよりサービスエンジニア向けの機能を使用することができる。以下、一般ユーザ及び管理者が操作する一般ユーザ機能、管理者だけが操作することが可能な管理者モードにおける諸機能（管理者機能（パネル)、管理者機能（PC))、サービスエンジニア向けの諸機能（サービスエンジニア機能）について説明する。なお、一般ユーザとはMFPが設置されるオフィス内に入室が許可されている、MFPを利用する者である。

1.2.4.1　一般ユーザ機能

(1) コピー機能

MFP本体操作パネルより、ドキュメントのスキャンを実行すると揮発性メモリにイメージデータを取り込んだ後、イメージデータを印刷する機能。

①メモリリコールコピー

コピーを実行すると、印刷終了後にコピージョブ情報データが印刷可能なジョブとして残り、何度でも再印刷することが可能なコピー機能。

②メモリリコール OFF コピー

コピーを実行すると、印刷終了後にコピージョブ情報データが自動的に削除されるコピー機能。利用者が自動削除を指定して実施される場合と、利用者に設定を委ねず、管理者の設定に基づき自動削除が実施される場合が存在する。

③画像蓄積コピー

コピー実行時に画像蓄積を行うことを選択の上でコピーを実行すると、印刷待機

状態となるコピー機能。ジョブバインド機能（後述）にて他のジョブと組み合わせて印刷する等の場合にて、本機能は利用される。なお、印刷待機状態となった本ジョブに対する印刷実行操作に対して特にアクセスの制限は設けていない。

(2) プリント機能

クライアントPCのプリンタドライバを使用して、MFPにプリントデータを送信すると、MFPは揮発性メモリに受信したプリントデータを印刷する。プリント機能には、以下に示すプリント方法がある。

①通常プリント

MFPのメモリに受信したプリントデータをそのまま印刷するプリント機能。

②リプリント

クライアントPC上で、「リプリント」を指定した場合、プリントデータの印刷を終了後もプリントデータをメモリに蓄積し、再印刷、または印刷仕上げ等の諸設定等を変更した上で何度でも印刷することができるプリント機能。印刷実行操作において特にアクセスの制限は設けていない。

③親展プリント

機密性の高いドキュメント等を印刷する場合、クライアントPCのプリンタドライバで「親展」を指定し、パスワードを設定した上で、MFPにプリントデータを送信する。TOEでこのプリントデータを受信すると、親展プリントジョブ情報データとして登録し、印刷待機状態になる。TOEは、MFP本体操作パネルから入力されるパスワードと親展プリントジョブ情報データのパスワードを照合し、これが一致した場合に待機状態が解除され、印刷が実行される。印刷の終了した親展プリントジョブ情報データは、自動的に削除される。

④HDD ストアプリント

MFPのHDDにプリントジョブ情報データを保管する機能。MFP本体操作パネルからの操作で印刷することができる。印刷実行操作において特にアクセスの制限は設けていない。

(3) ジョブバインド機能

メモリリコールされたコピーやリプリント等で印刷待機状態にあるジョブを選択し、順序を設定して1つのジョブとして印刷する機能。TOEは、このジョブバインド機能においてジョブの選択、印刷実行の受付処理を行う。

(4) スキャン機能

MFP本体操作パネルからスキャンを実行してイメージをデータとして取り込む機能。スキャンにより揮発性メモリに格納されたイメージデータは、E-mail、FTP等のデータ送信方法があり、スキャンと連動して利用される。またスキャンデータをMFP外に送信せず、MFPに内蔵されるHDDのボックスに保管することも可能である。

(5) インターネットFAX機能

インターネットFAX（添付される画像形式が規定されたE-mail）を受信し、印刷する機能。またスキャン機能によってMFPに取り込んだイメージデータをイン

ターネットFAXとして規定される画像圧縮形式の添付ファイルにしてE-mail送信する機能。

(6) ボックス機能

クライアントPCよりブラウザを用いて、スキャンされたイメージデータの保管領域であるボックスをHDDに作成（名称、パスワードの新規設定）し、イメージデータ（以降、ボックスデータとする）の格納されたボックスに対してクライアントPCよりブラウザを用いて以下に示す操作が提供される。

・ボックスデータのクライアントPCへのダウンロード
・ボックスデータの削除
・ボックスの削除
・ボックスの設定変更（名称の変更、パスワードの変更）

またMFP本体操作パネルよりボックスに格納されたスキャンデータに対して以下に示す操作が提供される。

・ ボックスデータのクライアント PC への E-mail 送信
・ ボックスデータのクライアント PC への FTP 送信
・ ボックスデータの名称変更
・ ボックスデータの削除

その他、クライアントPCより専用のアプリケーション（ボックスユーティリティ）を用いてボックスに対して以下の操作が提供される。

・ ボックスデータのプレビュー表示
・ ボックスデータの一覧表示（サムネイル付一覧表示）
・ ボックスデータのクライアント PC へのダウンロード
・ ボックスデータの名称変更
・ ボックスデータの削除

(7) その他各種設定機能

上記(1)～(6)の機能以外に一般ユーザが扱える機能として、MFP本体操作パネルからは、印刷における用紙選択、画質選択、倍率等の各種設定を行う複数の機能が存在する。またクライアントPCよりブラウザを利用して操作することができる機能に、MFPのシステム状態（デバイス構成、概要）の閲覧、ジョブ状況の閲覧、スキャン機能における送信方法、宛先の設定等を行う複数の機能が存在する。

1.2.4.2 管理者機能

TOEは、管理者だけが操作することが可能な管理者モードにて一般ユーザ機能を管理する管理機能（管理者機能）を提供する。以下、MFP本体操作パネルから実施可能な管理機能である管理者機能（パネル）、クライアントPCから実施可能な管理機能である管理者機能（PC）に分類して説明する。またクライアントPCより専用アプリケーションであるボックスユーティリティを用いて利用可能な管理機能である管理者機能（ボックスユーティリティ）についても説明する。

(1) パネル管理者機能

・管理者モードパスワードの変更機能
・不正使用防止動作設定機能
・アクセス不可状態解除機能（親展プリント、ボックスに対する各不正アクセス検出カウント値を0クリアする機能）
・オートリセット機能（後述の1.2.4.4項参照）の動作設定機能
・HDDロック動作設定機能
・SMTPサーバ、FTPサーバの設定機能
・メモリリコール設定データの設定機能
・管理者向け各種設定機能（親展プリントジョブ情報データの保管期間設定、ネットワークの諸設定、コピー枚数制限の設定、日付時刻の設定等）

(2) PC管理者機能

・ボックスデータの削除
・ボックスの削除
・ボックスの設定変更（名称の変更、パスワードの変更）
・オートリセット機能の動作設定
・SMTPサーバ、FTPサーバの設定機能
・メモリリコール設定データの設定機能
・管理者向け各種設定機能（ボックスデータの保管期間設定、親展プリントジョブ情報データの保管期間設定、ネットワークの諸設定、コピー枚数制限の設定、日付時刻の設定等）

(3) ボックスユーティリティ管理者機能

・ボックスデータのバックアップ機能
・バックアップされたボックスデータのリストア機能

1.2.4.3 サービスエンジニア機能

TOEは、MFP本体操作パネルから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一般ユーザ機能や管理者機能に対する管理機能（サービスエンジニア機能）を提供する。以下、本機能について説明する。

・ROMバージョン表示機能
・管理者モードパスワードの初期化機能
・サービスコード(サービスエンジニアのパスワード)の変更機能
・サービスエンジニア向け各種設定機能（一般ユーザに提供される各設定機能に対する動作設定機能、印刷枚数のカウンタ設定、各機能動作確認、センサチェック、HDD装着設定、HDDフォーマット、等）

1.2.4.4 その他の機能

一般ユーザ、管理者、及びサービスエンジニアが直接操作することによって動作する機能以外に、各利用者の設定に応じてTOEが自発的に動作する機能が存在する。以下にこの種の代表的な機能を説明する。

(1) オートリセット機能

無操作が継続し、設定された時間を経過すると、自動的に基本画面にリセットされる機能。MFP本体操作パネルからのアクセス、クライアントPCからの管理者モードへのアクセス中において発動する。発動までの時間（オートリセット設定データ）は、管理者が設定する。

(2) ボックスデータ自動削除機能

設定された保管期間を経過したボックスデータを削除する機能。保管期間の設定は、管理者が設定する。

(3) 親展プリント自動削除機能

設定された保管時間を経過した親展プリントジョブ情報データを削除する機能。保管時間の設定は、管理者が設定する。

(4) パワーセーブ機能

無操作が継続し、設定された時間を経過すると、自動的に印刷エンジン定着部のヒータの温度を調節し、電力消費を抑える以下の機能。本機能が作動すると、印刷待機状態で登録されているジョブは削除される。一般ユーザが本機能の作動開始までの時間を設定する。

・プレヒート機能：印刷エンジン定着部のヒータ温度を低下させる。
・スリープ機能　：印刷エンジン定着部のヒータを消す。

(5) 遠隔診断機能

サポートセンターからのアクセス要求を受け付け、MFPのトラブル発生回数、消耗品の消耗具合を示す値、印刷カウンタ値等の情報をサポートセンターに送信する。またMFPに特定の故障（重大な故障）が発生すると、自動的にサポートセンターへアクセスし、MFPの故障情報を送信する。本機能におけるデータの送受信は、電話回線やE-mailが利用される。

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セキュリティ認証申請等の手引き」[2]、「ITセキュリティ評価機関に対する要求事項」[3]、「ITセキュリティ認証申請者・登録者に対する要求事項」[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「#4036 Multi Function Peripheral 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:1.07」（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][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、「#4036 Multi Function Peripheral 全体制御ソフトウェア 評価報告書」（以下「本評価報告書」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、本評価報告書、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16年8月の評価機関による本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

本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

本STは、最小機能強度として、”SOF-基本”を主張する。

本TOEは、物理的な面と人的な面で十分なセキュリティを確保した条件下で運用されることを想定している。このため、脅威エージェントは低レベルの人物に特定することができる。従って、低レベルの攻撃力に対抗できるレベルである”SOF-基本”で満足される。

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) 一般ユーザ機能におけるセキュリティ機能

- メモリリコールOFF設定による残存コピーデータ保護機能
  管理者機能にてメモリリコールコピーをしないにした場合、コピー機能の利用にて取り込まれたコピージョブ情報データを印刷終了後、自動的に削除する機能。
- 親展プリントジョブに対する一般ユーザのアクセスを許可する識別認証
  親展プリントジョブ情報データを印刷する際、当該親展プリントジョブ情報データの正当な利用者である一般ユーザであることを識別認証する機能。認証に3回失敗すると、当該親展プリントジョブ情報データに対する認証機能はロックし、アクセスできなくなる。認証に成功すると、当該親展プリントジョブ情報データの印刷が開始される。
- ボックスの作成機能
  一般ユーザが、名称を指定し、ボックスを作成する機能。
- ボックスに対する一般ユーザのアクセスを許可する識別認証・アクセス制御機能
  ユーザボックスにアクセスする際、当該ユーザボックスの正当な利用者である一般ユーザであることを識別認証する機能。認証に3回失敗すると、当該ユーザボックスに対する認証機能はロックし、アクセスできなくなる。
  認証に成功すると、ボックス内のすべてのボックスデータのダウンロードが許可される。（なお、“Public”で示されるユーザボックスは、本セキュリティ機能の対象範囲外である。）
- アクセスを許可された一般ユーザのボックス管理機能

ボックスの正当な利用者である一般ユーザが、当該ボックスの設定（名称、パスワード）を変更する機能。

(2) 管理者機能におけるセキュリティ機能

- 管理者モードに対するアクセスを許可する識別認証機能
  - MFP本体操作パネル、またはクライアントPCよりブラウザを用いて管理者モードにアクセスする際、管理者であることを識別認証する機能。認証に3回失敗すると、当該認証機能はロックし、アクセスすることができなくなる。
  - クライアントPCよりボックスユーティリティを利用してボックスデータのバックアップ機能、リストア機能を実行する際、管理者であることを認証する機能。上記同様、認証に3回失敗すると、管理者の認証機能はロックし、アクセスすることができなくなる。
- 管理者モードにおけるセキュリティ関連機能

  MFP本体操作パネルから管理者モードにおいて操作できる以下の機能。
  - 管理者モードパスワードの変更機能
  - 不正使用防止動作設定機能
  - アクセス不可状態解除機能
  - オートリセット機能の動作設定機能
  - SMTP サーバ、FTP サーバの設定機能
  - メモリリコール設定データの設定機能

  クライアントPCから管理者モードにおいて操作できる以下の機能。
  - ボックスの設定変更機能（名称の変更、パスワードの変更）
  - オートリセット機能の動作設定機能
  - SMTP サーバ、FTP サーバの設定機能
  - メモリリコール設定データの設定機能

(3) サービスエンジニア機能におけるセキュリティ機能

- サービスモードへのアクセスを許可する識別認証機能

  サービスモードにアクセスする際、サービスエンジニアであることを識別認証する機能。認証に3回失敗すると、当該認証機能はロックされ、アクセスすることができなくなる。
- サービスエンジニア機能におけるセキュリティ関連機能

  サービスモードにおいて操作することができる以下の機能。
  - 管理者モードパスワードの初期化機能
  - サービスコードの変更機能

(4) その他の機能におけるセキュリティ機能

- オートリセット機能

  設定される一定時間、無操作状態が継続した場合にアクセス許可を取り消す機能

(MFP本体パネル基本画面に戻る、またはクライアントPCからの接続であれば接続を遮断する)。管理者モードへアクセスしている際に誤って離席してしまった場合の補助的なセキュリティ機能として有効である。

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.ACCESS-SECURE-PRINT	親展プリントジョブ情報データの不正な操作： 悪意をもった一般ユーザが、親展プリントジョブ情報データにMFP本体操作パネルよりアクセスし、他の一般ユーザが送信した親展プリントジョブ情報データを印刷することにより、親展プリントジョブ情報データが不正に暴露される。
T.ACCESS-BOX	ボックスデータの不正な操作： ・ 悪意を持った一般ユーザが、作成されたボックスにクライアント PC よりアクセスし、他の一般ユーザが利用するボックスのボックスデータをダウンロード、プレビュー、サムネイル表示することにより、ボックスデータが不正に暴露される。 ・ 悪意を持った一般ユーザが、作成されたボックスに MFP 本体操作パネルよりアクセスし、他の一般ユーザが利用するボックスのボックスデータを E-mail 送信、FTP 送信することにより、ボックスデータが不正に暴露される。 ・ 悪意を持った一般ユーザが、クライアント PC より作成されたボックスにアクセスし、ボックスデータをバックアップすることにより、ボックスデータが不正に暴露される。 ・ 悪意を持った一般ユーザが、クライアント PC よりバックアップされたボックスデータをリストアすることにより、ボックスデータが不正に改ざんされる。
T.ACCESS-COPY-DATA	残存するコピージョブ情報データに対する不正な操作： 悪意を持った一般ユーザが、MFP 本体操作パネルよりアクセスしてコピージョブ情報データを再印刷し、コピージョブ情報データが不正に暴露される。
T.SEND-BOX-DATA	ボックスデータの想定されない宛先への送信： ・ 悪意を持った一般ユーザが、MFP 本体操作パネルよりアクセスして MFP が利用する SMTP サーバ、FTP サーバの各設定データを変更することにより、ボックスデータが

	一般ユーザの意図しないサーバに送信されてしまい、ボックスデータが暴露される。 ・ 悪意をもった一般ユーザが、クライアント PC よりアクセスして MFP が利用する SMTP サーバ、FTP サーバの各設定データを変更することにより、ボックスデータが一般ユーザの意図しないサーバに送信されてしまい、ボックスデータが暴露される。

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を表1-2に示す。

表1-2 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.BEHAVIOR-FUNCTION	セキュリティ機能の動作設定機能 ・ セキュアな環境では、操作上の便宜を図るために不正使用防止機能を停止することができる。 ・ セキュアな環境では、操作上の便宜を図るためにメモリリコールコピー機能を動作することができる。

1.5.7 構成条件

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#4036 Multi Function Peripheralに搭載されるソフトウェア製品である。

#4036 Multi Function Peripheralは、販売商品名「bizhub C350」、「CF2203」、「8022」として消費者に提供されるMulti Function Peripheralである。

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1-3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1-3 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ついて、悪意を持った行為は行わない。
A.AUTH	パスワードに関する運用条件：

	TOEの利用において使用される各パスワードは、そのパスワードの所有者によって漏れることがないよう管理される。
A.HDD	MFPで利用されるハードウェア環境条件： ・TOE が搭載される MFP では、HDD ロック機能を有する HDD だけが利用される。 ・HDD ロック機能に利用される HDD ロックパスワードは、その所有者によって漏れることがないよう管理される。
A.NETWORK	MFPのネットワーク接続条件： ・MFPを利用する組織は、TOEが搭載されるMFPを設置するオフィス内LANにおいて盗聴されないネットワーク環境を構成する。 ・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.PHYSICAL	MFPの設置条件： TOEが搭載されるMFPは、一般ユーザ、管理者、サービスエンジニアだけが入ることが可能な物理的に保護された場所に設置される。
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、TOEの設置及びMFPの保守において課せられた役割として許可される一連の作業について、悪意を持った行為は行わない。
A.SETTING	セキュリティ機能の動作設定条件： TOE の利用者は、不正使用防止機能が必ず動作する状態で TOE を利用する。

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。

●日本語版

＜サービスエンジニア向けドキュメント＞

・bizhub C350サービスマニュアル [セキュリティ機能編] Ver1.30 2004.06

・設置チェックリスト バージョン：1.04

＜管理者・一般利用者向けドキュメント＞

・bizhub C350ユーザーズガイド [セキュリティ機能編] Ver1.05 2004.5

●英語版

＜サービスエンジニア向けドキュメント＞

・bizhub C350/CF2203/8022 Service Manual [Security Function] Ver1.10 2004.06

・Installation Checklistバージョン：1.04

＜管理者・一般利用者向けドキュメント＞

・bizhub C350 User's Guide [Security Function] Ver1.05 2004.6

・CF2203 User's Guide [Security Function] Ver1.05 2004.6

・8022 User's Guide [Security Function] Ver1.05 2004.6

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、本評価報告書において報告されている。本評価報告書では、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、本評価報告書による評価実施の履歴を示す。

評価は、平成16年4月に始まり、平成16年8月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成16年6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16年6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。

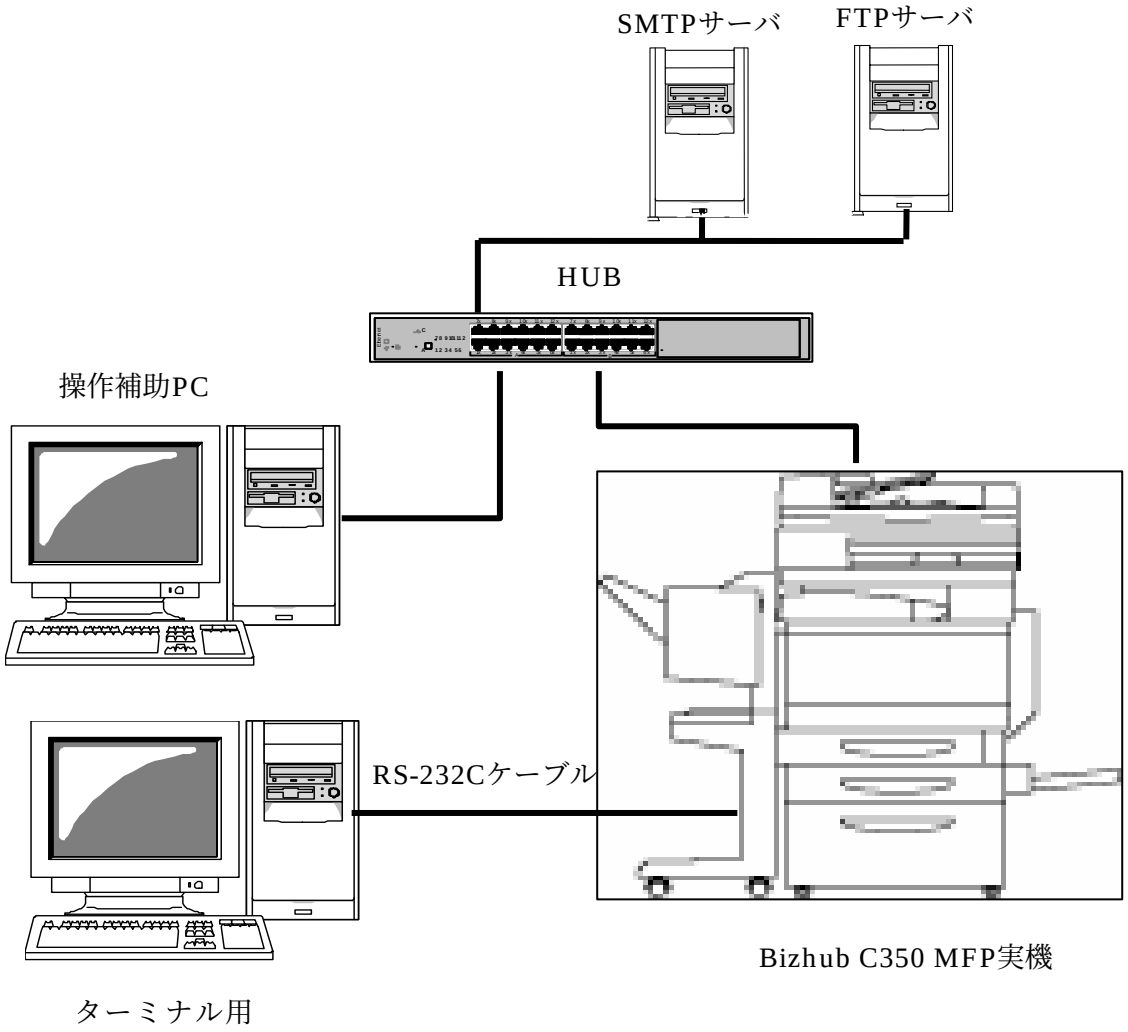

図2-1　開発者テストの構成図

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。

b.テスト手法

テストには、以下の手法が使用された。

①テスト項目は各セキュリティ機能（一般ユーザ機能におけるセキュリティ機

能、管理者機能におけるセキュリティ機能、サービスエンジニア機能におけるセキュリティ機能、オートリセット機能）をすべて網羅するように設定する。

②MFP本体操作パネルあるいはクライアントPCのブラウザ画面からの操作により、外部インタフェースより刺激(パラメタ)を与え、外部インタフェースの挙動を目視確認する。

③テスト結果の信頼性向上のために、また、目視では結果確認できないインタフェースについては、外部インタフェースの挙動の変化を目視確認する以外にデバック出力(ログ出力)によりテスト結果を確認する。

c.実施テストの範囲

テストは開発者によって29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。

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。

①テスト項目は各セキュリティ機能をすべて網羅するように設定する。

②MFP本体操作パネルあるいはクライアントPCのブラウザ画面からの操作により、外部インタフェースより刺激(パラメタ)を与え、外部インタフェースの挙動を目視確認する。

③テスト結果の信頼性向上のために、また、目視では結果確認できないインタ

フェースについては､外部インタフェースの挙動の変化を目視確認する以外にデバック出力(ログ出力)によりテスト結果を確認する。

c.実施テストの範囲

評価者が独自に考案したテストを3項目、開発者テストのサンプリングによるテストを29項目、計32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 独自に考案したテストでは､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 サンプリングテストでは､開発者が実施したセキュリティ機能に関連するすべてのテストを選択

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

本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本評価報告書で示されたように評価されていること。

④ 本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 本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及び本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

提出された本評価報告書、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 ([7][10][13][16]のいずれか) 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識別、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記述が理路整然と一貫性の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。
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。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_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。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_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。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.1.3E	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明記され、それらが脅威、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。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_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理路整然とし、完結しており、かつ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_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。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_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理路整然とし、完結しており、かつ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_SRE.1.1E	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はないため非適用であ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はないため非適用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。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_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結しており、理路整然とし、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。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。
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。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。
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。
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。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。
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。また、本評価時に行われたサイト訪問での調査方法も適切と判断される。
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。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。
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。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。
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が含まれて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。また、本評価時に行われたテスト実施方法も適切と判断される。
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。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。
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が記述され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。
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

本報告書で使用された用語を以下に示す。

VxWorks(OS)	MFP制御ソフトウェアが動作するために必要な根幹ソフト。オペレーティングシステム。MFPにおいて、ネットワーク機能、ファイルシステム機能、マルチプロセシング処理等のサービスを提供する。
Modular Input Output(MIO)	各種の外部インタフェース（ネットワークユニット、セントロI/F）から受け付けたデータを「DPS」、「DSS」、「Network Module」、「Macro System Controller」で扱うデータに変換するソフトウェアコンポーネント。WWWサーバ機能を実現する。またIPアドレス等ネットワークの諸設定処理を実施する。
DPS	クライアントPCからのプリント受け付け処理を実施するアプリケーションソフトウェアコンポーネント。
DSS	スキャンよって取り込まれた画像をE-mail送信、FTP送信等の処理を実施するアプリケーションソフトウェアコンポーネント。
ジョブ	コピー機能、スキャン機能、プリント機能等のMFPにおけ

	る一連の機能の動作単位。
親展プリント	クライアントPCからの印刷する場合の1つの形態。クライアントPC上のプリンタドライバでパスワードを設定してMFPにプリントデータを送信すると、MFPでは印刷が実行されずに待機状態になる。設定したパスワードをMFPに入力すると待機状態が解除されて印刷が実行される。
親展プリントジョブ情報データ	親展プリントとしてMFPが受信したプリントデータ。本TOEでは保護資産として扱う。
ボックス	ハードディスク（HDD）を搭載時、スキャンしたイメージデータをMFPに保管する領域として設定されるディレクトリ。個々の利用者がクライアントPCからのみ名称及びパスワードを設定することが可能である。なお、“ Public ”で示されるボックスは、共同利用されるため、パスワードを設定することはできない。名称変更を行うこともできない。
ボックスデータ	ボックスに格納されたイメージデータ。本STでは保護資産として扱う。
ボックスユーティリティ	クライアントPCからボックスにアクセスするための専用アプリケーション。本アプリケーションを利用してプレビュー表示、管理者操作によるボックス内データのバックアップ及びリストア操作等が行える。
メモリリコール設定データ	メモリリコールコピーの動作有無を決定するデータ。管理者が設定する。本データをOFFにすると、利用者に提供されるメモリリコールONコピー／メモリリコールOFFコピーの選択機能が一般ユーザに提供されなくなる。コピーを実行すると、印刷終了後に取り込まれたドキュメントのイメージデータを自動的に削除するメモリリコールOFFコピーとしてコピー機能が動作する。
管理者モード	認証された管理者にのみ提供される機能群。
管理者モードパスワード	管理者モードに設定されるパスワード。8桁の数字が設定可能である。
サービスモード	認証されたサービスエンジニアにのみ提供される機能群。
サービスコード	サービスモード、メンテナンスモード、初期化モードに設定されるパスワード。8桁の数字、“ ＊ ”、“ ＃ ”が設定可能であ

	る。
不正使用防止機能	管理者に動作設定管理される機能。本機能が有効になると、ボックス認証機能が動作し、更に管理者機能、親展プリント機能、ボックス機能における各認証機能にて、連続した各不成功認証試行を検出し、不成功認証回数に応じて各認証機能をロックする機能が動作する。
ボックス不正アクセス検出カウント値	不正使用防止機能が動作中にボックスの認証機能において認証試行に失敗した場合、不成功試行回数としてカウントされ保持される値。
親展プリント不正アクセス検出カウント値	不正使用防止機能が動作中に親展プリントの認証機能において認証試行に失敗した場合、不成功試行回数としてカウントされ保持される値。
アクセス不可状態解除機能	ボックス不正アクセス検出カウント値、親展プリント不正アクセス検出カウント値を0クリアする機能。ボックス、親展プリントに対する認証機能がロックした場合、本機能を実行することにより、ロックが解除される。
HDDロック機能	MFPにて利用されるHDDに実装されているセキュリティ機能。HDDにアクセスするためのパスワード（HDDロックパスワード）が設定可能であり、本機能を使用すると、アクセスする際にHDDロックパスワードを利用した認証機能が動作する。HDDが設置されたMFPであることが認証されない限りアクセスすることはできない。また一定回数の不成功試行が検出されると、それ以降の認証機能をロックし、一切のアクセスを遮断する。

6 参照

[1] #4036 Multi Function Peripheral 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:1.07（2004年8月5日）コニカミノルタビジネステクノロジーズ株式会社

[2] ITセキュリティ認証申請等の手引き 平成15年10月 独立行政法人 製品評価技術基盤機構 適合性評価センター

[3] ITセキュリティ評価機関に対する要求事項 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター 適合－部門－IT機関要求－02

[4] ITセキュリティ認証申請者・登録者に対する要求事項 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター 適合－部門－IT申請要求－02

[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

[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

[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

[11] ISO/IEC 15408-1 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[12] ISO/IEC 15408-2 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[13] ISO/IEC 15408-3 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

[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

[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-0210

[21] 補足-0210

[22] #4036 Multi Function Peripheral 全体制御ソフトウェア 評価報告書 第1.2版 2004年8月27日
社団法人 電子情報技術産業協会 ITセキュリティセンター