認　証　報　告　書

評価対象

申請受付年月日(受付番号)	**平成16年7月13日（IT認証4031）**
認証番号	C0026
認証申請者	**シャープ株式会社**
TOEの名称	AR-FR11
TOEのバージョン	VERSION M.20
PP適合	**なし**
適合する保証要件	EAL3
TOE開発者	**シャープ株式会社**
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17年6月2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 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

「AR-FR11 VERSION M.20」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 はじめに

この認証報告書は、「AR-FR11 VERSION M.20」（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シャープ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:	AR-FR11
バージョン:	VERSION M.20
開発者:	シャープ株式会社

1.2.2 製品概要

本製品は、コピー、プリント、スキャン、ファクスなどの複数の機能を備えた事務機械であるデジタル複合機（以下「MFD」という。）にセキュリティ機能を追加するためのアップグレードキットである。本製品はROM製品として提供されるファームウェアであり、このROM製品をMFD標準のROMと置き換えることによって、MFD標準ファームウェア相当の機能に加えて、セキュリティを考慮した拡張機能を提供する。

本製品が備えるこのセキュリティ機能によって、MFD内に一時的にスプール保存される実イメージデータ及びファイリング保存される実イメージデータが、権限のない人物に開示される危険性を減ずることができる。

1.2.3 TOEの範囲と動作概要

1.2.3.1 MFDの利用環境

想定する利用環境を図 1-1に示す。TOEは、図中MFD(1)及びMFD(2)に設置されているものとする。ただし以降の機能説明では、MFD(1)に設置されたTOEを対象とし、単に”MFD”と記述する場合、MFD(1)を意味するものとする。

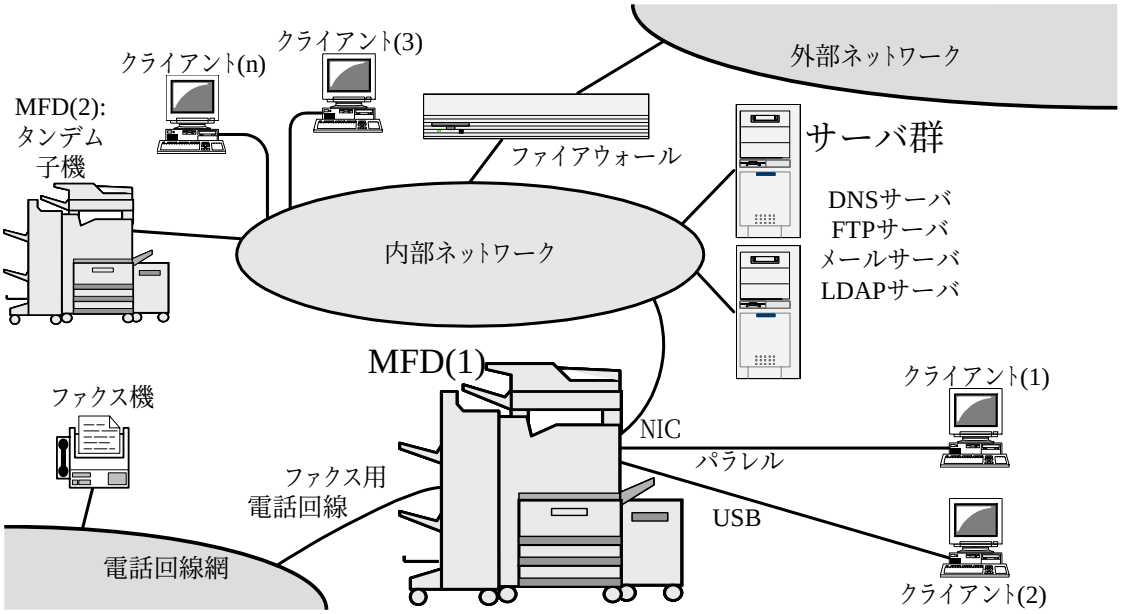

図 1-1 MFDの利用環境

図 1-1に示す環境の下、TOEがMFD全体を制御することによって、以下の機能を利用することができる。

(a) コピー
原稿を印刷する。このときタンデム子機(MFD(2))を併用することにより、ネットワークを介して親機(MFD(1))と子機(MFD(2))で分担した印刷も可能となる。

(b) プリンタ
パラレル、USB、またはネットワーク経由でクライアントから送付された実イメージデータを印刷する。

(c) ダイレクトプリント
FTP、E-mail、Webのプロトコルを利用してネットワーク経由で取得した実イメージデータを印刷する。

(d) スキャン送信
原稿から実イメージデータを取得し、ネットワーク経由でクライアントやサーバに送信する。

(e) ファクス送信
原稿から実イメージデータを取得し、電話回線経由で他のファクス機に送信する。

(f) ファクス受信

電話回線経由で他のファクス機から実イメージデータを受信し、印刷する。

(g) PC-FAX

クライアントからパラレル、USB、またはネットワーク経由で送付された実イメージデータを、電話回線経由またはネットワーク経由で送信する。

(h) ドキュメントファイリング

スキャン、コピー、プリント、またはPC-FAX時の実イメージデータをMFD内にファイリング保存する。またファイリング保存された実イメージデータを再操作する。

(i) バックアップ

前記ドキュメントファイリングによりMFD内にファイリング保存した実イメージデータをネットワーク経由でクライアントにバックアップする。また、バックアップした実イメージデータをMFD内にリストアする。

(j) ネットワーク管理

上記の各機能をネットワーク経由で使用するためのネットワーク関連設定（MFDや各サーバのアドレス設定など）を行う。

1.2.3.2 TOEの構成と動作概要

MFDの物理的構成を図 1-2に示す。TOEは、図中”AR-FR11”と記された網掛け部分であり、MFDのコントローラ基板を制御するファームウェアを格納した2枚のROM基板である。

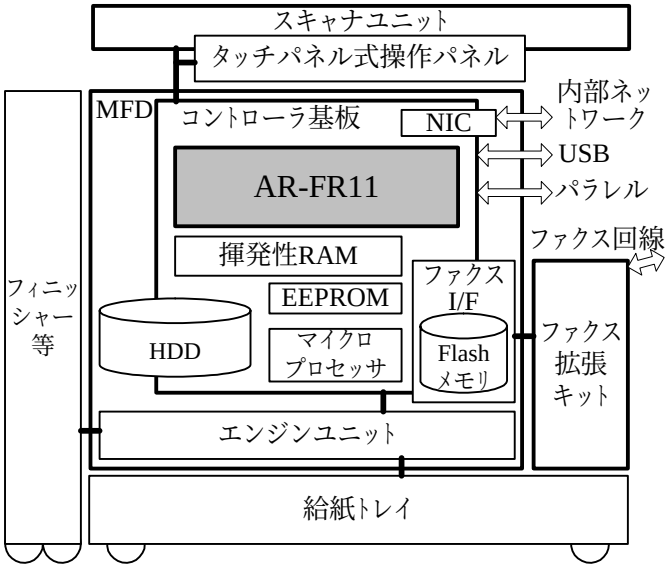

図 1-2 MFDの物理的構成とTOE

TOEの論理的構成を図 1-3に示す。図中、長方形はソフトウェア部分を、角を丸くした長方形はハードウェア部分を示す。

TOEは、図中”TOE”と記された網掛け部分である。この網掛け部分において、”TSF_”

で始まる識別名を付与された部分が、セキュリティ機能(TSF)を示す。

また、TOEの保護資産となる利用者データが、TOE外のHDD、Flashメモリ、及びEEPROM内に保持されており、これらもまた網掛けで示している。

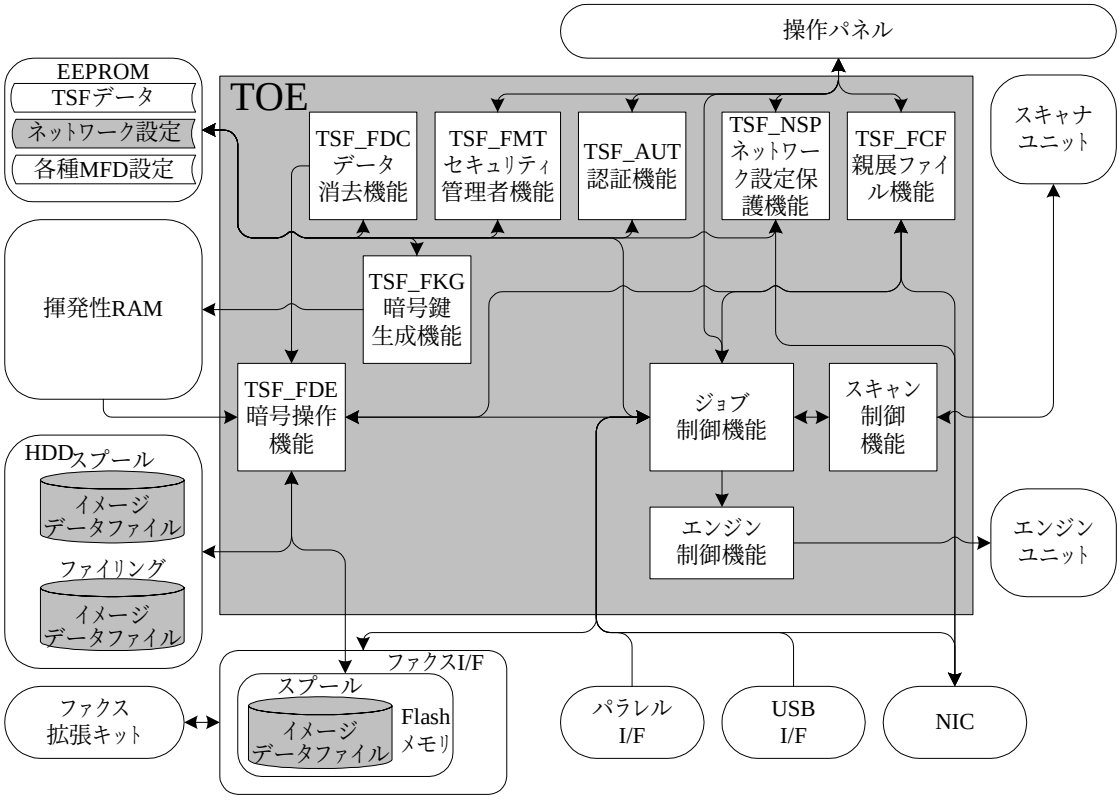

図 1-3　TOEの論理的構成

(1) MFD通常利用時

利用者は、操作パネルを使用して直接的に、あるいは、パラレルI/F、USB I/F、またはネットワーク経由で接続されたクライアントを使用して間接的に、MFDを操作する。このような操作により、実イメージデータを各種I/Fを介して印刷・送信したり、HDD内へのファイリング保存・再操作を行ったりする（下表を参照）。

実イメージデータの入力形態	実イメージデータの出力形態
・スキャナユニットによる原稿の読み取り ・ファクスI/Fによるイメージデータの受信 ・パラレルI/F、USB I/F、またはNICによるイメージデータの受信 ・HDD内にファイリング保存したイメージデータの取り出し	・エンジンユニットを介して、実イメージデータを印刷（コピー、プリンタ、ダイレクトプリント、ファクス受信） ・ファクスI/Fを介して、実イメージデータを他のファクス機に送信（ファクス送信、PC-FAX） ・NICを介して、実イメージデータをクライアントやサーバに送信（スキャン送信、PC-FAX、バックアップ） ・実イメージデータをHDD内にファイリング保存（ドキュメントファイリング）

この通常利用時に、TOEは、MSD内に一時的にスプール保存される実イメージデータとHDD内にファイリング保存される実イメージデータを各セキュリティ機能により保護しつつ、ジョブ制御機能、スキャン制御機能、及びエンジン制御機能を連動させて上記 1.2.3.1 (a)〜(i)の各機能を提供する。

(2) MFD管理時

キーオペレーターがMFDの操作パネルを使用して直接的に、また、Web-Adminがネットワーク経由で接続されたクライアントを使用して間接的に、MFDを管理する。

このときTOEは、各セキュリティ機能により、ネットワーク設定とTSFデータ(各セキュリティ機能に関わる情報)を権限のない人物によるアクセスから保護する。

1.2.4 TOEの機能

TOEが提供する機能の詳細を以下に示す。

(a) コピー機能

MFD標準ファームウェアと同様、原稿を読み取り、読み取った画像を印刷する機能である。主な追加機能を以下に挙げる。

- タンデムコピー: 内部ネットワークに接続された 2 台の MFD がある場合、原稿を読み取った MFD (親機) が他の MFD (子機) 宛に、内部ネットワーク経由で実イメージデータを転送し、利用者が指定したコピー部数を各々折半し分担して印刷出力する。ただし TOE は、標準ファームウェア MFD へ実イメージデータを転送しない。
- ファイリング: 通常の印刷出力に加え、コピー原稿の実イメージデータを MFD 内に保存する。保存したデータは、後でドキュメントファイリング機能により、印刷や削除ができる。

(b) プリンタ機能

MFD標準ファームウェアと同様、クライアントから送付されてくるプリントデータを印刷する機能である。クライアントにはMFD用のプリンタドライバをインストールしておくべきである。プリントデータはパラレル、USB、もしくは内部ネットワークより受信する。主な追加機能を以下に挙げる。

- タンデムプリント: タンデムコピー機能と同様で、プリントデータを受信した MFD が親機となり、クライアントの利用者が指定したプリント部数を子機と折半する。
- 印刷せずにホールド: 受信したデータから印刷可能な実イメージデータを生成し MFD 内に保存するが、印刷は実行しない。パスワードを付けて保存すれば 親展プリント として機能する。
- 印刷後ホールド: 通常の印刷出力に加え、実イメージデータを MFD 内に保存する。
- サンプルプリント: 指定部数のうち 1 部のみ印刷出力し、残部数印刷のために実イメージデータを MFD 内に保存する。大量のミスプリントを未然に防ぐのに役立つ。

MFD内に保存した実イメージデータに対し、ドキュメントファイリング機能により、印刷や削除を行う。

(c) ダイレクトプリント機能

MFD標準ファームウェアと同様、クライアント、FTPサーバまたはE-mail添付ファイルからプリントデータのファイルを取得し、印刷する機能であり、プリンタ機能と異なりプリンタドライバを必要としない。本機能には以下の種類がある。

- E-mail プリント、及び、インターネット FAX 受信: TOE がメールサーバを定期的に確認してメールを受信し、受信したメールに添付されたファイルを印刷する機能。インターネット FAX として送られたメールも同じ仕組みで処理する。
- FTP Pull プリント: 操作パネルからの操作により TOE が FTP サーバにアクセスし、ファイルを取得し印刷する機能。
- FTP Push プリント: TOE が内蔵する FTP サーバに対し、クライアントよりプリントデータを送信することにより印刷する機能。
- Web プリント: TOE が内蔵する Web サーバに対し、クライアントよりプリントデータを送信することにより印刷する機能。

(d) スキャン送信機能

MFD標準ファームウェアと同様、原稿をスキャンすることによりイメージデータを得て、そのイメージデータをE-mail/FTP送信、または、インターネットFAX送信する機能である。

E-mail/FTP送信とは、ファイルサーバー送信 (FTPサーバへ送信)、デスクトップ送信 (クライアントへFTP送信)、及びE-mail送信 (メールサーバへ送信) の総称である。デスクトップ送信を利用するためには、MFDネットワークスキャナ機能の付属ソフトウェアであるスキャンツールをクライアント上で稼動させておく必要がある。

(e) ファクス送信機能

MFD標準ファームウェアと同様、操作パネルにて指定した送信先ファクス機にファクス送信する機能である。主な追加機能を以下に挙げる。

- 時刻指定通信: 利用者が指定した送信予約日時の到来を待って送信を開始する。

(f) ファクス受信

MFD標準ファームウェアと同様、他機よりファクス受信し印刷する機能である。

(g) PC-FAX機能

PCFAX機能とも呼ばれる。MFD標準ファームウェアと同様、クライアントから送付されてくるイメージデータをパラレル、USB、もしくは内部ネットワークより受信し、ファクス送信またはインターネットFAX送信する機能である。クライアントにはMFD用のPC-FAXドライバをインストールしておくべきである。主な追加機能を以下に挙げる。

- ドキュメントファイリング: 通常の送信に加え、送信した実イメージデータを MFD 内に保存する。保存したデータは、後でドキュメントファイリング機能により、送信や削除ができる。

(h) ドキュメントファイリング機能

MFD標準ファームウェアと同様、MFD内のHDDに実イメージデータを保存し、その実イメージデータを操作パネル経由またはクライアントよりWeb経由で再操作できる機能を提供する。TOEはパスワード保護付きの保存モード (親展モード) を提供し、このモードで保存されたデータを 親展ファイル と呼ぶ。

実イメージデータを親展ファイルとして保存する手段には、以下の4通りがある。

- スキャン保存: スキャンして得た実イメージデータを HDD に保存するが、印刷や送信は実行しない。
- コピージョブ (ファイリング 指定): コピー機能を参照。
- プリンタジョブ (印刷せずにホールド、印刷後ホールド またはサンプルプリント 指定): プリンタ機能を参照。
- PC-FAX ジョブ (ドキュメントファイリング 指定): PC-FAX 機能を参照。

上に挙げた各操作においてTOEは、利用者が入力したパスワードを、実イメージデータとともに保存する。保存した親展ファイルを再操作するためには、操作パネルまたはクライアントのWebブラウザで、パスワード入力による認証を経なければならない。

再操作には以下が含まれる。

- 印刷: コピー機能と同様に、部数等を指定し、印刷する。タンデム印刷も可能である。
- 送信: ファクス送信、E-mail / FTP 送信、及び、インターネット FAX 送信が可能である。
- プレビュー: 実イメージデータの概略を表示する。Web 経由のみで可能。
- 属性変更: 親展ファイルを、親展でない (パスワードのない) ファイルに変更する。逆もまた可能。
- パスワード変更。
- 削除。

(i) バックアップ機能

MFD標準ファームウェアと同様、ドキュメントファイリング機能でHDD内に保存したファイルを、クライアントからの操作により、そのクライアント内にバックアップを取る機能、及び、再びHDDへ戻す機能である。前者をエクスポートあるいはバックアップと呼び、後者をインポートあるいはリストアと呼ぶ。

エクスポートの手順は以下の通り。

- 利用者がクライアントより TOE の Web にアクセスし、必要な操作 (HDD 内の対象ファイルの指定、パスワード入力等) を行う。

- TOE は、親展ファイルのパスワードの一致を確認の上、クライアントの Web ブラウザへ、暗号化されたままのファイルを送る。
- クライアントの Web ブラウザは、そのファイルをダウンロードし、保存する。

インポートの手順は以下の通り。

- 利用者がクライアントより TOE の Web にアクセスし、必要な操作 (クライアント側ファイル指定等) を行う。
- クライアントの Web ブラウザは、指定されたファイルを TOE へアップロードする。
- TOE はそのファイルを受け取り、暗号化されていなければ暗号化を行い、保存する。

(j) ネットワーク管理機能

MFD標準ファームウェアと同様、TOEのネットワーク機能を使用するために、MFDに付与するIPアドレス、TOEが参照すべきDNSサーバのIPアドレス、その他のネットワーク関連設定を行う機能である。

本機能の一部は、操作パネルでキーオペレーターに提供される。これは、TOEのキーオペレータープログラムUI内にあるネットワーク設定 というUIであり、ここでIPアドレス設定等、最低限の設定が可能である。また、タンデム設定は、このネットワーク設定でのみ可能である。

TOEはTCP/IP使用時に限り、リモート操作用Webを提供する。このWebが提供するページ群の一部は、管理用パスワードで保護されており、Webブラウザでアクセスしたときにパスワード入力を要する。本書では、この管理用パスワードで認証される利用者をWeb-Adminと呼び、保護されたページ群をWeb-Adminページと総称する。

本機能 (ネットワーク管理機能) の大部分はこのWebでWeb-Adminに提供される。ここではTOEがDNS、WINS、SMTP及びLDAPサーバを利用するための設定等が可能である。これらの設定を行うための設定フォームを含むページ、及び、それらフォームの送信先ページを、ネットワーク管理ページ と総称する。すべてのネットワーク管理ページはWeb-Adminページである。

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「（日本語版）デジタル複合機データセキュリティキット AR-FR11 セキュリティターゲット （英語版）Digital Multifunction Device Data Security Kit AR-FR11 Security Target」（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、「AR-FR11 VERSION M.20 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17年5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が設置される内部ネットワークは、外部ネットワークからのセキュリティの脅威から保護されている。このような環境下で想定される攻撃は、MFD（TOEを含む）への直接アクセスによるものか、または内部ネットワークを経由したものに制限される。つまりインターネット越しで外部からの攻撃を幅広く受け付けることは想定され

ない。したがって、攻撃者の攻撃能力を低（low attack potential）と想定することは妥当であり、最小機能強度としてSOF-基本を主張することは妥当である。

1.5.4 セキュリティ機能

TOEセキュリティ機能は、以下のとおりである。

(1) 暗号操作機能 (TSF_FDE)

MFD 内の MSD (HDD 及び Flash ﾒﾓﾘ) を制御するデバイスドライバ機能に介在することにより、MSD に書き込む実ｲﾒｰｼﾞデータを暗号化し、MSD から読み出した実ｲﾒｰｼﾞデータを復号する。

(2) 暗号鍵生成機能 (TSF_FKG)

暗号操作機能 (前項) で提供する暗号化、及び復号の暗号鍵を生成する。生成された暗号鍵は、揮発性 RAM に保存する。

(3) データ消去機能 (TSF_FDC)

ｼﾞｮﾌﾞ処理のために HDD または Flash ﾒﾓﾘ内にスプール保存されたｲﾒｰｼﾞデータがｼﾞｮﾌﾞ完了後に削除される際、及び、利用者が親展ﾌｧｲﾙ機能 (後述) で HDD 内に保存したｲﾒｰｼﾞデータが利用者の操作により削除される際、ランダム値または固定値を上書きすることにより、実ｲﾒｰｼﾞデータ領域を消去する (各ｼﾞｮﾌﾞ完了後の自動消去)。

また、未完のｼﾞｮﾌﾞのｲﾒｰｼﾞデータ、及び、利用者が保存したまま削除していないｲﾒｰｼﾞデータに対し、ランダム値または固定値を上書きすることにより、実ｲﾒｰｼﾞデータ領域を消去する (全データｴﾘｱ消去、ﾄﾞｷｭﾒﾝﾄﾌｧｲﾘﾝｸﾞデータ消去、及び、電源 ON 時の自動消去)。

以下の四つのデータ消去プログラムを提供する。

- 各ｼﾞｮﾌﾞ完了後の自動消去 (HDD と Flash ﾒﾓﾘ): ｼﾞｮﾌﾞ完了後、ｼﾞｮﾌﾞが使用した実ｲﾒｰｼﾞデータ領域に対し、消去を行う。後述の親展ﾌｧｲﾙ機能により保存された親展ﾌｧｲﾙが、利用者の操作により削除される場合も、同様に消去する。
- 全データｴﾘｱ消去 (HDD と Flash ﾒﾓﾘ): 管理者 (キーオペレーター) の操作により、残っているすべての実ｲﾒｰｼﾞデータ領域に対する消去を行う。TOE もしくは MFD を廃棄または所有者変更する際、管理者 (キーオペレーター) は本プログラムを実行すべきである。
- ﾄﾞｷｭﾒﾝﾄﾌｧｲﾘﾝｸﾞデータ消去 (HDD): 管理者 (キーオペレーター) の操作により、HDDに残っている実ｲﾒｰｼﾞデータに対する消去を行う。主として、利用者がHDDに保存したデータを一括消去するための機能だが、HDDにスプール保存されたｼﾞｮﾌﾞのｲﾒｰｼﾞデータを消去することも可能である。
  なお、全データｴﾘｱ消去とﾄﾞｷｭﾒﾝﾄﾌｧｲﾘﾝｸﾞデータ消去を、*データｴﾘｱ消去*と総称する。
- 電源 ON 時の自動消去 (HDD と Flash ﾒﾓﾘ): TOE の電源 ON 時 (スキャン送信またはﾌｧｸｽ送信の予約ｼﾞｮﾌﾞがある場合、及び、未出力のﾌｧｸｽ受信またはｲﾝﾀｰ

ネットFAX受信ジョブがある場合を除く) に、実イメージデータ領域に対する消去を行う。管理者 (キーオペレーター) は、本機能の有効化または無効化 (電源ON時に本プログラムを実行するか否か) 及び対象領域を設定できる。

(4) 認証機能 (TSF_AUT)

キーオペレーターコード (パスワード) によりキーオペレーターの識別認証を行う。

(5) セキュリティ管理者機能 (TSF_FMT)

TOEの運用に必要な、以下の管理者機能を提供する。

- 各ジョブ完了後の自動消去回数の変更機能
- データエリア消去回数の変更機能
- 電源ON時の自動消去の領域別有効設定の変更機能
- 電源ON時の自動消去回数の変更機能
- キーオペレーターコードの変更機能
- 親展ファイルのロック解除機能
- NICリセット (Web-Adminパスワードを含むネットワーク関連設定を初期化する)

(6) ネットワーク設定保護機能 (TSF_NSP)

MFDのネットワーク関連設定を、管理者以外が変更できないよう保護する。

(7) 親展ファイル機能 (TSF_FCF)

利用者がドキュメントファイリング機能によりMFD内にイメージデータを保存する際、パスワードによる保護を提供する。本機能によりパスワード保護されファイルとして保存されたイメージデータを、親展ファイルと呼ぶ。利用者は親展ファイル保存時にパスワードを設定し、TOEは再操作 (印刷や送信) の際にパスワードを要求し認証を行う。

本機能は、連続3回認証失敗した親展ファイルに対し、認証受付を拒絶する。これをロックと呼ぶ。

本機能を利用してプリンタジョブを親展プリントとすることが可能である。

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.RECOVER	攻撃者がMFDから物理的にMSDを取り出し、MSD内の実イメージデータを読み出し再生する。
T.SHUNT	攻撃者がMFDのネットワーク関連設定を変更することにより、利用者がMFDに送信させようとしている実イメージデータを、攻撃者が攻撃の手段とする機材へ送信させる。
T.SPOOF	利用者がMFD内に保存している実イメージデータを、攻撃者が

	その利用者になりすますことにより、印刷または送信する。

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、以下のシャープ社製MFDの標準ROMと置き換えることで動作する。

AR-555S、AR-625S、AR-705S、AR-555M、AR-625M、AR-705M、AR-550U、AR-620U、AR-700U、AR-550N、AR-620N、AR-700N、AR-550UJ、AR-620UJ、AR-700UJ、AR-550NJ、AR-620NJ、AR-700NJ

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.NETWORK	TOEを設置するMFDは、セキュアに管理された内部ネットワークに接続するものとし、外部ネットワークからのセキュリティの脅威から保護されているものとする。
A.OPERATOR	キーオペレーター及びWeb-Adminは、MFD及びTOEに対して不正をせず信頼できるものとする。
A.USER	TOE及びMFDの管理者を含む利用者は、パスワードを以下のように扱うものとする。 ・パスワードには容易に推測可能な値を設定しない。 ・パスワードは定期的に更新する。 ・パスワードは安全に管理する。

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。

(1) 日本語版

- 取扱説明書　データセキュリティキット AR-FR11, バージョン 0.04 （CINSJ2570FC52）

- 注意書　データセキュリティキット AR-FR11, バージョン 0.05
  （TCADZ1732FCZZ）
- AR-FR11　Web ヘルプ (全般), TOEに内蔵
- AR-FR11　Web ヘルプ (ドキュメントファイリング), TOEに内蔵

(2) 英語版

- AR-FR11 Data Security Kit Operation Manual, Version 0.04
  （CINSZ2571FC52）
- AR-FR11　Data Security Kit　Notice, Version 0.05
  （TCADZ1733FCZZ）
- AR-FR11　Help Overview (Top Page), TOEに内蔵
- AR-FR11　Help Overview (Document Filing), TOEに内蔵

なお、本TOEの使用にあたっては、MFD本体に付属する以下のドキュメントも併読する必要がある。

(1) 日本語版

- 取扱説明書　デジタル複合機 キーオペレータープログラム編, バージョン 1
  （CINSJ2495FC51）
- 取扱説明書　デジタル複合機
  形名
  AR-555S
  AR-625S
  AR-705S
  共通編/コピー編, バージョン 1
  （TINSJ2472FCZ1）
- 取扱説明書　デジタル複合機 プリンタ編, バージョン 3
  （AR555S-JP3-PRINTER）
- 取扱説明書　デジタル複合機 ネットワークスキャナ編, バージョン 1
  （AR555S-JP1-SCANNER）
- 取扱説明書　ファクス拡張キットAR-FX8, バージョン 3
  （TINSJ2562FCZZ）

(2) 英語版

- KEY OPERATOR'S GUIDE
  DIGITAL LASER COPIER/PRINTER
  DIGITAL MULTIFUNCTIONAL SYSTEM, Version 2
  （CINSE2499FC51）
- MODEL
  AR-M550U
  AR-M620U

AR-M700U
AR-M550N
AR-M620N
AR-M700N
DIGITAL LASER COPIER/PRINTER
DIGITAL MULTIFUNCTIONAL SYSTEM
OPERATION MANUAL
(for general information and copier operation), Version 6
（TINSE2476FCZ1）

- OPERATION MANUAL(for printer)
  DIGITAL LASER COPIER/PRINTER
  DIGITAL MULTIFUNCTIONAL SYSTEM, Version 3
  （ARM550N-EX3-PRINTER）
- OPERATION MANUAL(for network scanner)
  DIGITAL LASER COPIER/PRINTER
  DIGITAL MULTIFUNCTIONAL SYSTEM, Version 1
  （ARM550N-EX1-SCANNER）
- MODEL AR-FX8
  FACSIMILE EXPANSION KIT
  OPERATION MANUAL, Version 3
  （TINSE2565FCZZ）

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7月に始まり、平成17年5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11月及び平成17年1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17年1月、2月、及び3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中の(122)decode.exeは、テスト用の復号ソフトウェアを示す。また、(110)デバッグターミナル用PCに接続されている(12)HDDは、(10)MFD内蔵の(12)HDDを取り外してPCに接続したものである。

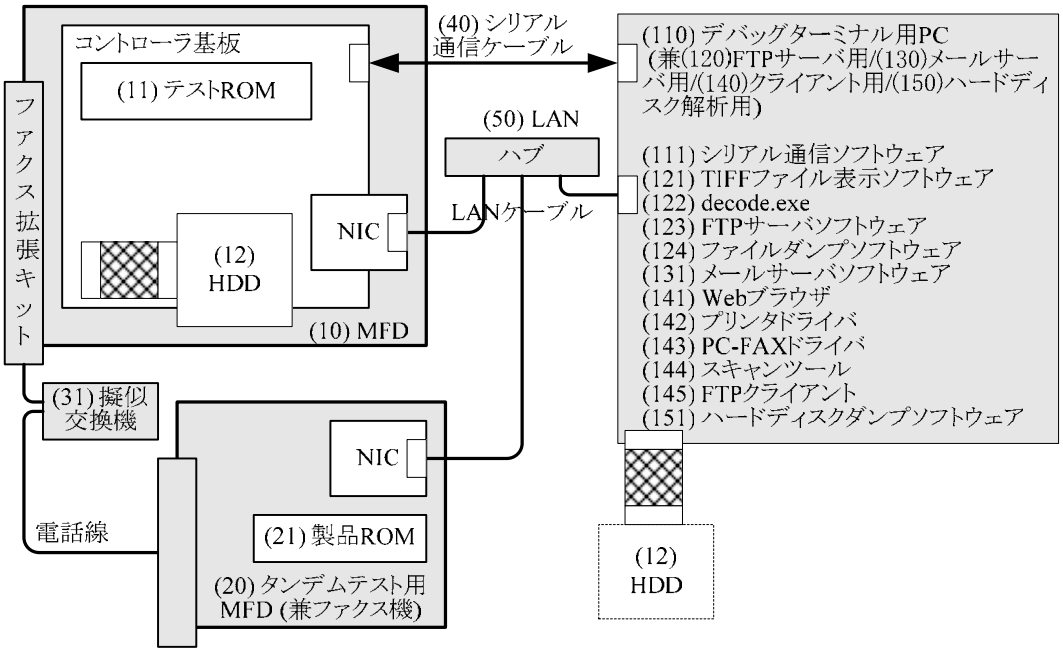

図 2-1　開発者テストの構成

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は図 2-1のとおりである。開発者テストは、STにおいて識別されているTOE構成と同等のハードウェア及びソフトウェア構成のテスト環境で実施されている。なお、図 2-1中の(11)テストROMはSTで識別されるTOEとは異なるが、これは製品ROM(TOE)にテスト用のデバッグ機能のみを追加したものであり、TOEと同等とみなすことができる。また、テスト構成には、STのTOE構成では識別されていないテスト用ツール・ソフトウェアも含まれているが、これらはセキュリティ機能のふるまいに影響を及ぼすものではない。

b.テスト手法

テストには、以下の手法が使用された。

①MFD（操作パネル、電源など）を手動で操作することによりセキュリティ機能の外部インタフェースを刺激し、操作パネルへの表示内容、デバッグターミナルへの出力内容、及びログファイルの内容からセキュリティ機能のふるまいを観察する。

②TOEのWebを操作することによりセキュリティ機能の外部インタフェースを刺激し、操作パネルへの表示内容、デバッグターミナルへの出力内容、ログファイルの内容、及びTOEのWebの出力内容からセキュリティ機能のふるまいを観察する。

③MFDに実イメージデータの読み取り・受信、及び印刷・送信を行わせるこ

とによりセキュリティ機能の外部インタフェースを刺激し、操作パネルへの表示内容、デバッグターミナルへの出力内容、ログファイルの内容、及びMFDから取り外したHDDのダンプ内容からセキュリティ機能のふるまいを観察する。

c.実施テストの範囲

テストは開発者によって48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

評価者が実施した独立テスト、侵入テストの構成をそれぞれ図 2-2、図 2-3に示す。図 2-2中の(122)decode.exeは、テスト用の復号ソフトウェアを示す。また、(110)デバッグターミナル用PCに接続されている(12)HDDは、(10)MFD内蔵の(12)HDDを取り外してPCに接続したものである。

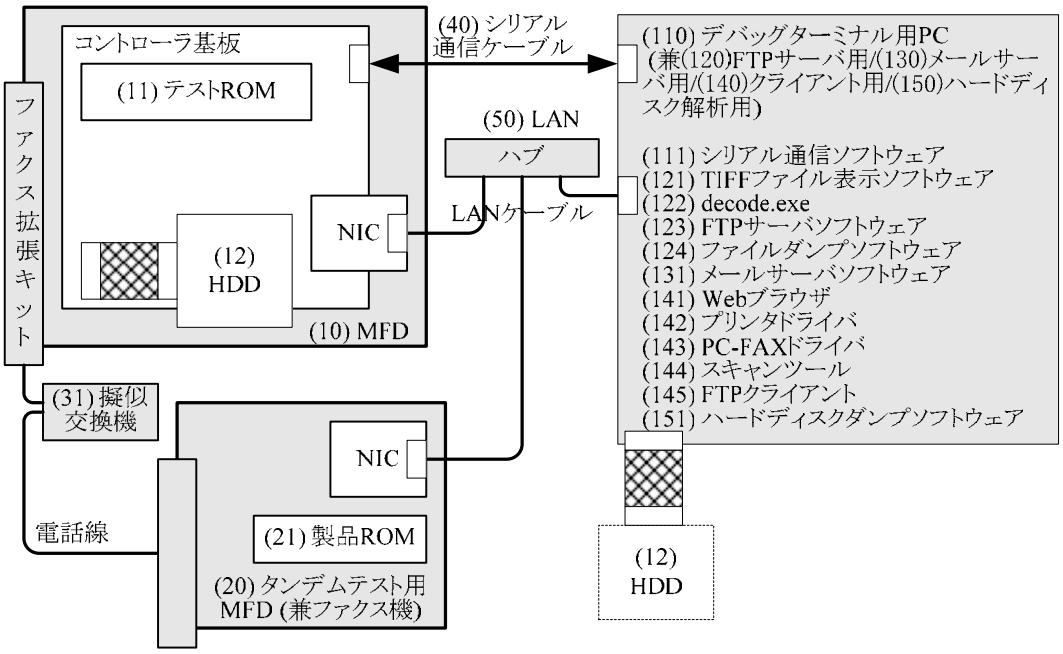

図 2-2　独立テストの構成

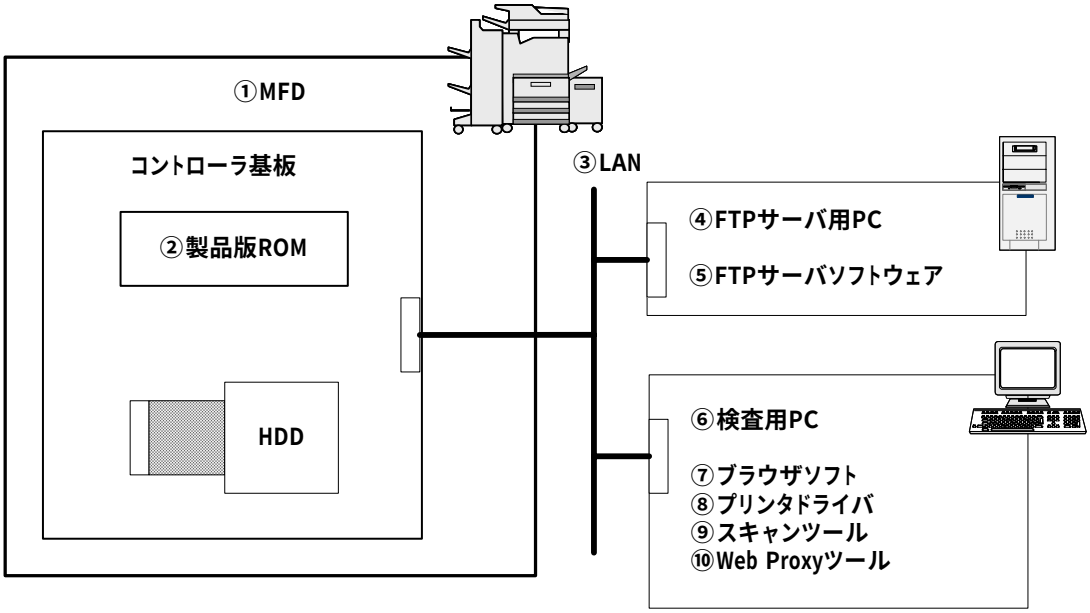

図 2-3　侵入テストの構成

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

評価者が実施した独立テストの構成（図 2-2）は開発者テストと同様の構成である。侵入テストの構成については図 2-3のとおりである。独立テスト及び侵入テストは、STにおいて識別されているTOE構成と同等のTOEテスト環境で実施されている。なお、テスト構成には、STのTOE構成では識別されていないテ

スト用ツールが含まれているが、これらはセキュリティ機能のふるまいに影響を及ぼすものではない。

b.テスト手法

テストには、以下の手法が使用された。

①MFD（操作パネル、電源など）を手動で操作することによりセキュリティ機能の外部インタフェースを刺激し、操作パネルへの表示内容、デバッグターミナルへの出力内容、及びログファイルの内容からセキュリティ機能のふるまいを観察する。

②TOEのWebを操作することによりセキュリティ機能の外部インタフェースを刺激し、操作パネルへの表示内容、デバッグターミナルへの出力内容、ログファイルの内容、及びTOEのWebの出力内容からセキュリティ機能のふるまいを観察する。

③MFDに実イメージデータの読み取り・受信、及び印刷・送信を行わせることによりセキュリティ機能の外部インタフェースを刺激し、操作パネルへの表示内容、デバッグターミナルへの出力内容、及びログファイルの内容からセキュリティ機能のふるまいを観察する。

④MFDのNICに対してポートスキャンを行い、その応答を観察する。

c.実施テストの範囲

評価者は、独自に考案した独立テストを22項目、開発者テストのサンプリングによるテストを14項目、侵入テストを7項目、計43項目のテストを実施した。

なお各評価者テストは、下記を考慮している。

【独自に考案した独立テスト】

① すべてのセキュリティ機能をテスト対象とすること
② すべての論理的TSFIをテスト対象とすること
③ 操作パネル一般UI及び操作パネル管理者UIの両方を対象とすること
④ 暗号操作及びデータ消去のテストでは、ジョブ、ファイリングの有無、使用するMSD（FlashメモリまたはHDD）の組み合わせに関して、開発者テストとは異なる組み合わせを採用すること

【開発者テストのサンプリングによるテスト】

① 開発者テスト項目数(48項目)の20%以上を確保すること
② すべてのセキュリティ機能を網羅すること
③ 対象とするMSDとして、スプール領域（HDD、Flashメモリ）及びファイリング領域（HDD）を含めること
④ 開発者テストの各分類（HDD取り外しテストを除く）からそれぞれ選択すること

【侵入テスト】

① TOEのWebへのアクセス時における認証セッションの脆弱性の確認
② 公知の脆弱性が顕在化していない論拠の実地検査

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。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.1.2E	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。
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明記され、それらが脅威、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。
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。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。
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。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。
ADO_DEL.1.2D	評価はワークユニットに沿って行われた。ただし出荷実績がないため、実際に配付手続きが使用されていることを確認する代わりに、適切な配付手続きが存在し使用される準備が十分に整っていることを、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。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。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。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。

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。
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。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_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。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_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。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。
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。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_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。

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。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.1.2E	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。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。

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。

イメージデータ	MFDにてコピー、プリント、スキャン、もしくはファクス送信のため、原稿画像を読み込みデジタル化したデータ。ファクス受信においては、電話回線を通じて受信したデータ、及びこのデータを伸張したデータ。また、これらを圧縮したデータもイメージデータと呼ぶ。
エンジン	給紙機能、排紙機能の機構を含み、受像紙に印刷画像を形成する装置。実イメージデータを印刷すると同時に、給紙トレイ及びフィニッシャー等を制御する。コピー、プリンタ、ダイレクトプリント、ファクス受信、及び、再操作の印刷の際に使用する。プリントエンジン、エンジンユニットともいう。
外部ネットワーク	組織の管理が及ばない、内部ネットワーク以外のネットワーク。
給紙トレイ	印刷するための用紙を収納し、印刷時にエンジンユニットへ送り出す。
キーオペレーター	TOEのセキュリティ管理者機能、あるいはMFD管理者機能にアクセス可能な、認証された利用者。MFD及びTOEの管

	理者。
キーオペレーターコード	キーオペレーターの認証の際に用いられるパスワード。
キーオペレータープログラム	TOEのセキュリティ管理者機能。MFD管理者機能でもある。キーオペレータープログラムにアクセスするためには、キーオペレーターとして識別認証されなければならない。
基板	プリント基板に部品を半田付け実装したものを指す。
コントローラ基板	MFD全体を制御する。TOE内のファームウェアを実行するためのマイクロプロセッサと揮発性RAM、設定を保存するEEPROMを有する。
実イメージデータ	イメージデータファイルから管理領域を除いた実イメージデータ部分。
ジョブ	MFD機能 (コピー、プリンタ、ダイレクトプリント、スキャン送信、PC-FAX送信、ファクス送信、ファクス受信) において、その機能の開始から終了までの流れ、シーケンス。また、機能動作の指示についてもジョブと呼ぶ場合がある。
全データエリア消去	MFDが搭載しているすべてのMSDについて、保存されているすべての実イメージデータを上書き消去する処理。
操作パネル	表示部、ボタンキー、タッチパネル上に形成されたボタンを含む、利用者I/Fのためのデバイス。または、そのユニット。
タッチパネル式操作パネル	ボタンキー及びタッチパネル付きLCDを持つ操作パネル。利用者I/Fを提供する。
スキャナユニット	原稿をスキャンして実イメージデータを得る。コピー、スキャン送信、ファクス送信及びスキャン保存の際に使用する。
内部ネットワーク	外部ネットワークからのセキュリティの脅威に対して保護されるネットワーク。それぞれの組織内部のイントラネットが、“内部ネットワーク” に該当する。
ファイリング	MFDが取り扱うイメージデータを、利用者が後で再操作(印刷、送信、等) できるようMFD内のHDDに保存する機能。ドキュメントファイリングともいう。
ファクス拡張キット	ファクス送受信機能を提供するオプション。ファクス送受信

及びファクスI/F	ジョブ処理に必要な実イメージデータを保持するFlashメモリを持つ。
フィニッシャー等	印刷済みの用紙に対し、ステープル綴じ、穴あけ等の仕上げを施すオプション類。
ネットワーク設定	MFDのネットワーク関連設定データのうち、本STが保護資産とするもの。
メモリ	記憶装置、特に半導体素子による記憶装置。
ユニット	プリント基板に脱着可能な標準品や、オプション品を装備し、動作可能状態とした単位。また、機構部を含んで動作可能状態とした単位。
EEPROM	不揮発性メモリの一種で、電気的に任意部分の書き換えを可能にしたROM (Electronically Erasable Programmable ROM)。
Flashメモリ	不揮発性メモリの一種で、電気的な一括消去及び任意部分の再書き込みを可能にしたROM (Flash Memory)。
HDD	ファクス送受信以外のジョブ処理に必要な実イメージデータを保持する。また、利用者がドキュメントファイリング機能により実イメージデータを保存することもできる。
I/F	インタフェース (Interface)の略。
LCD	液晶ディスプレイ (Liquid Crystal Display)の略。
MSD	大容量ストレージ機器 (Mass Storage Device)の略。本TOEの場合、HDD及びFlashメモリがMSDに相当する。
NIC	内部ネットワークに接続するためのイーサネットI/Fである。MFDの機種により、標準装備またはオプションとなる。ネットワークインタフェースカード (Network Interface Card) または ネットワークインタフェースコントローラ (Network Interface Controller)の略。
RAM	任意に読み書き可能なメモリ (Random Access Memory)。
ROM	読み出し専用メモリ (Read Only Memory)。
UI	利用者インタフェース (User Interface)の略。
Web-Admin	TOEがリモート操作用に提供するWebにおいて、MFDの管

理者として、管理用パスワードで認証される利用者。Admin
はAdministratorの意。

6 参照

[1] （日本語版）デジタル複合機データセキュリティキット AR-FR11 セキュリティターゲット バージョン 0.16 （2005年3月16日） シャープ株式会社,
（英語版）Digital Multifunction Device Data Security Kit AR-FR11 Security Target Version 0.16 (16 Mar. 2005) Sharp Corporation

[2] ITセキュリティ認証申請等の手引き 平成16年4月 独立行政法人情報処理推進機構 ITQM-23

[3] ITセキュリティ評価機関に対する要求事項 平成16年4月 独立行政法人情報処理推進機構 ITQM-07

[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16年4月 独立行政法人情報処理推進機構 ITQM-08

[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-0407

[21] 補足-0210 第2版 及び 補足-0407

[22] AR-FR11 VERSION M.20 評価報告書 第009版 2005年5月2日
みずほ情報総研株式会社 情報セキュリティ評価室