



認証報告書

独立行政法人情報処理推進機構
理事長 藤江 一正



評価対象

| | |
|-------------|---|
| 申請受付日（受付番号） | 平成25年3月13日（IT認証3446） |
| 認証番号 | C0438 |
| 認証申請者 | Dell Inc. |
| TOEの名称 | Dell C7765dn Color Multifunction Printer |
| TOEのバージョン | Controller ROM Ver. 2.205.5、IOT ROM Ver. 41.1.0、ADF ROM Ver. 12.5.0 |
| PP適合 | なし |
| 適合する保証パッケージ | EAL3 |
| 開発者 | 富士ゼロックス株式会社 |
| 評価機関の名称 | 一般社団法人 ITセキュリティセンター 評価部 |

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。

平成26年9月25日

技術本部
セキュリティセンター 情報セキュリティ認証室
技術管理者 山里 拓己

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

- ① 情報技術セキュリティ評価のためのコモンクライテリア バージョン3.1 リリース4
- ② 情報技術セキュリティ評価のための共通方法 バージョン3.1 リリース4

評価結果：合格

「Dell C7765dn Color Multifunction Printer」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、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 | 評価対象製品概要 | 1 |
| 1.1.1 | 保証パッケージ | 1 |
| 1.1.2 | TOEとセキュリティ機能性 | 1 |
| 1.1.2.1 | 脅威とセキュリティ対策方針 | 2 |
| 1.1.2.2 | 構成要件と前提条件 | 2 |
| 1.1.3 | 免責事項 | 2 |
| 1.2 | 評価の実施 | 2 |
| 1.3 | 評価の認証 | 3 |
| 2 | TOE識別 | 4 |
| 3 | セキュリティ方針 | 5 |
| 3.1 | セキュリティ機能方針 | 5 |
| 3.1.1 | 脅威とセキュリティ機能方針 | 6 |
| 3.1.1.1 | 脅威 | 6 |
| 3.1.1.2 | 脅威に対するセキュリティ機能方針 | 6 |
| 3.1.2 | 組織のセキュリティ方針とセキュリティ機能方針 | 8 |
| 3.1.2.1 | 組織のセキュリティ方針 | 8 |
| 3.1.2.2 | 組織のセキュリティ方針に対するセキュリティ機能方針 | 8 |
| 4 | 前提条件と評価範囲の明確化 | 9 |
| 4.1 | 使用及び環境に関する前提条件 | 9 |
| 4.2 | 運用環境と構成 | 9 |
| 4.3 | 運用環境におけるTOE範囲 | 12 |
| 5 | アーキテクチャに関する情報 | 13 |
| 5.1 | TOE境界とコンポーネント構成 | 13 |
| 5.2 | IT環境 | 14 |
| 6 | 製品添付ドキュメント | 15 |
| 7 | 評価機関による評価実施及び結果 | 16 |
| 7.1 | 評価方法 | 16 |
| 7.2 | 評価実施概要 | 16 |
| 7.3 | 製品テスト | 17 |
| 7.3.1 | 開発者テスト | 17 |
| 7.3.2 | 評価者独立テスト | 22 |
| 7.3.3 | 評価者侵入テスト | 24 |
| 7.4 | 評価構成について | 27 |
| 7.5 | 評価結果 | 28 |
| 7.6 | 評価者コメント/勧告 | 28 |

| | | |
|-----|------------------|----|
| 8 | 認証実施..... | 29 |
| 8.1 | 認証結果..... | 29 |
| 8.2 | 注意事項..... | 29 |
| 9 | 附属書..... | 30 |
| 10 | セキュリティターゲット..... | 30 |
| 11 | 用語..... | 31 |
| 12 | 参照..... | 34 |

1 全体要約

この認証報告書は、富士ゼロックス株式会社が開発した「Dell C7765dn Color Multifunction Printer、バージョン Controller ROM Ver. 2.205.5、IOT ROM Ver. 41.1.0、ADF ROM Ver. 12.5.0」（以下「本 TOE」という。）について一般社団法人 IT セキュリティセンター 評価部（以下「評価機関」という。）が平成 26 年 9 月 12 日に完了した IT セキュリティ評価に対し、その内容の認証結果を申請者である Dell Inc. に報告するとともに、本 TOE に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

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

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

1.1 評価対象製品概要

本 TOE の機能、運用条件の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 保証パッケージ

本 TOE の保証パッケージは、EAL3 である。

1.1.2 TOE とセキュリティ機能性

本 TOE は、コピー機能、プリンター機能、スキャナー機能、ファクス機能を有するデジタル複合機（以下「MFD」という。）である。

本 TOE は、コピー機能、プリンター機能、スキャナー機能、ファクス機能等の MFD の基本機能に加えて、基本機能で扱う文書データやセキュリティに影響する設定データ等を漏えいや改ざんから保護するセキュリティ機能を提供する。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で評価が行われた。本 TOE が想定する脅威及び前提については次項のとおりである。

1.1.2.1 脅威とセキュリティ対策方針

本 TOE は、以下の脅威を想定しており、それに対抗するセキュリティ機能を提供する。

TOE の保護資産である利用者の文書データ及びセキュリティに影響する設定データは、TOE の操作や、MFD 内の内部ハードディスク装置からの直接読出し、TOE が設置されているネットワーク上の通信データへのアクセスによって、不正に暴露されたり改ざんされたりする脅威がある。

そのため TOE は、それらの保護資産の不正な読出しや改ざんを防止するために、識別認証、アクセス制御、内部ハードディスク装置や通信データの暗号化等のセキュリティ機能を提供する。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定する。

本 TOE は、TOE の物理的部分やインタフェースが不正なアクセスから保護されるような環境に設置されることを想定している。また、TOE の運用にあたっては、ガイダンス文書に従って TOE を適切に設定し、維持管理しなければならない。

1.1.3 免責事項

本 TOE には、以下に示す運用や機能は保証の対象外である。

本評価では、カスタマーエンジニア操作制限をはじめとする設定条件が適用された構成だけが TOE として評価されている。従って、「7.4 評価構成について」に示す設定を変更した場合、それ以降は本評価による保証の対象外となる。

TOE は、ダイレクトファクス機能を提供しているが、その機能は本体認証時に限定され、外部認証時は評価の対象外である。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価・認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって本 TOE に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 26 年 9 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、所見報告書及び関連する評価証拠資料を検証し、本 TOE の評価が所定の手続きに沿って行われたことを確認した。また、TOE の評価が CC ([4][5][6]または[7][8][9]) 及び CEM ([10][11]のいずれか) に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 TOE識別

本 TOE は、以下のとおり識別される。

| | | |
|--------|--|--------------|
| TOE名称： | Dell C7765dn Color Multifunction Printer | |
| バージョン： | Controller ROM | Ver. 2.205.5 |
| | IOT ROM | Ver. 41.1.0 |
| | ADF ROM | Ver. 12.5.0 |
| 開発者： | 富士ゼロックス株式会社 | |

本 TOE の範囲にはファクス機能が含まれているが、オプションのファクスボードは含まれていない。

製品が評価・認証を受けた本 TOE であることを、利用者は以下の方法によって確認することができる。

ガイドンスに記載された手順に従って操作パネルを操作し、画面に表示された機種名とバージョン情報、または、設定値リストのプリント出力に記述された機種名とバージョン情報を、ガイドンスの当該記載と比較することにより、設置された製品が評価を受けた本 TOE であることを確認する。

3 セキュリティ方針

本章では、本 TOE が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

TOE は、コピー機能、プリンター機能、スキャナー機能、ファクス機能等の MFD 機能を提供しており、利用者の文書データを内部のハードディスク装置に蓄積したり、ネットワークを介して利用者の端末や各種サーバとやりとりしたりする機能を有している。

TOE は、それらの MFD 機能を使用する際に、利用者の識別認証とアクセス制御、ハードディスク装置の蓄積データの暗号化、暗号通信プロトコルといったセキュリティ機能を適用することで、保護資産である利用者の文書データ及びセキュリティに影響する設定データが、不正に暴露されたり改ざんされたりすることを防止する。また、TOE は、セキュリティ機能に関する監査ログを記録する機能を備えている。

なお、TOE は、使用に関して以下の役割を想定し、役割に応じたアクセス制御機能を提供する。

- ・一般利用者

一般利用者は、TOE が提供するコピー機能、プリンター機能、スキャナー機能、ファクス機能等の利用者である。

- ・システム管理者（機械管理者+SA）

システム管理者は、TOE のセキュリティ機能の設定を行うための特別な権限を持つ利用者である。システム管理者には、すべての管理機能を使用できる「機械管理者」と、一部の管理機能を使用できる「SA」が含まれる。

- ・カスタマーエンジニア

カスタマーエンジニアは、MFD の保守や修理を行うエンジニアである。

また、TOE は、組織のセキュリティ方針により、ファクスで使用する公衆電話網から内部ネットワークにアクセスすることを防止する機構と、ハードディスク装置に蓄積されたデータを削除する際の上書き消去及び自己テスト機能を備えている。

3.1 セキュリティ機能方針

TOE は、3.1.1 に示す脅威に対抗し、3.1.2 に示す組織のセキュリティ方針を満たすセキュリティ機能を具備する。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

本 TOE は、表 3-1 に示す脅威を想定し、これに対抗する機能を備える。

表3-1 想定する脅威

| 識別子 | 脅威 |
|------------|---|
| T.CONSUME | TOEの利用を許可されていない者が、TOEを不正に利用するかもしれない。 |
| T.DATA_SEC | TOEの利用を許可されている利用者が、許可されている権限範囲を超えて、文書データ及びセキュリティ監査ログデータを不正に読み出すかもしれない。 |
| T.CONFDATA | TOEの利用を許可されている一般利用者が、システム管理者のみアクセスが許可されているTOE設定データに対して、不正な読み出しや設定の変更を行うかもしれない。 |
| T.RECOVER | 攻撃者が、内部ハードディスク装置を取り出して、内部ハードディスク装置上の利用済み文書データや文書データ、及びセキュリティ監査ログデータを不正に読み出して漏洩するかもしれない。 |
| T.COMM_TAP | 攻撃者が、内部ネットワーク上に存在する文書データ、セキュリティ監査ログデータ及びTOE設定データを盗聴や改ざんをするかもしれない。 |

3.1.1.2 脅威に対するセキュリティ機能方針

本 TOE は、表 3-1 に示す脅威に対し、以下のセキュリティ機能方針で対抗する。

(1) 脅威「T.CONSUME」「T.DATA_SEC」「T.CONFDATA」への対抗

TOE は、「ユーザー認証機能」、「システム管理者セキュリティ管理機能」、「カスタマーエンジニア操作制限機能」及び「セキュリティ監査ログ機能」で対抗する。

「ユーザー認証機能」は、識別認証の成功した利用者だけに TOE の利用を許可する。また、識別認証された利用者が、親展ボックスや文書データを操作する際には、当該利用者に許可された操作だけが実行できる。

利用者の識別認証は、利用者 ID と 9 文字以上のパスワードを使用する。また、スマートカード(CAC/PIV)に格納された X.509 デジタル証明書を使用することもできる。

「システム管理者セキュリティ管理機能」は、セキュリティ機能に関する TOE 設定データの参照と設定変更及びセキュリティ機能の有効/無効の設定変更を、識別認証されたシステム管理者だけに許可する。

「カスタマーエンジニア操作制限機能」は、カスタマーエンジニアの操作制限の有効/無効を制御する TOE 設定データについて、その参照と設定変更を識別認証されたシステム管理者だけに許可する。

「セキュリティ監査ログ機能」は、利用者のログイン/ログアウト、ジョブ終了、設定変更等の監査ログを取得し、その読出しを識別認証されたシステム管理者だけに許可する。これにより、利用者へのなりすましなどの不正操作を検出できる。なお、監査ログを格納する領域が満杯になった時は、最も古い監査ログに上書きして記録される。

以上により、TOE の正当な利用者に対して利用者毎の権限範囲で許可された操作だけが実行可能であり、TOE の不正な利用や保護資産の不正アクセスが防止される。

(2) 脅威「T.RECOVER」への対抗

TOE は、「ハードディスク蓄積データ暗号化機能」で対抗する。

「ハードディスク蓄積データ暗号化機能」は、コピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能、ファクス機能及びダイレクトファクス機能といった MFD 基本機能の動作時に、文書データを内部ハードディスク装置に蓄積する際に、文書データの暗号化を行う。また、セキュリティ監査ログ機能で生成した監査ログデータを内部ハードディスク装置に蓄積する際に、監査ログデータの暗号化を行う。

暗号アルゴリズムは 256bit の AES である。暗号鍵は、TOE 設置時にシステム管理者によって設定された 12 桁の英数字から成る暗号化キーを元に、TOE 起動時に富士ゼロックス社の独自方式に従って生成され、電源オフにより消去される。

以上により、内部ハードディスク装置に蓄積された文書データは暗号化によって不正な読出しが防止される。

(3) 脅威「T.COMM_TAP」への対抗

TOE は、「内部ネットワークデータ保護機能」で対抗する。

「内部ネットワークデータ保護機能」は、TOE と利用者端末（以下、「クライアント」という。）や各種サーバとの通信時に、暗号通信プロトコルを適用する。対応している暗号通信プロトコルは、SSL/TLS (SSL 3.0、TLS 1.0、TLS 1.2)、IPsec、SNMPv3、S/MIME である。

以上により、内部ネットワークでやり取りされる文書データ、セキュリティ監査ログデータ及び TOE 設定データは、暗号通信プロトコルが適用され、盗聴や改ざんが防止される。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 組織のセキュリティ方針

本 TOE の利用に当たって要求される組織のセキュリティ方針を表 3-2 に示す。

表3-2 組織のセキュリティ方針

| 識別子 | 組織のセキュリティ方針 |
|-------------|--|
| P.FAX_OPT | TOEは、公衆電話回線網から内部ネットワークへのアクセスができないことを保証しなければならない。 |
| P.VERIFY | TOEは、TSF の実行コードおよびTSFデータの完全性に関し自己テストをしなければならない。 |
| P.OVERWRITE | TOEは、内部ハードディスク装置に蓄積される利用済み文書データの上書き消去をしなければならない。 |

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

TOE は、表 3-2 に示す組織のセキュリティ方針を満たす機能を具備する。

(1) 組織のセキュリティ方針「P.FAX_OPT」への対応

TOE の「ファクスフローセキュリティ機能」は、指定されたファクスモデムからのみファクスデータを受信し、そのデータをファクス機能以外へ渡さない構造により、公衆回線網から受信したデータを、いかなる場合においても内部ネットワークへの送信に受け渡さない。これにより、公衆電話回線網から内部ネットワークへのアクセスができないことを保証する。

(2) 組織のセキュリティ方針「P.VERIFY」への対応

TOE の「自己テスト機能」は、起動時に Controller ROM のチェックサムを照合する。また、NVRAM と SEEPROM に格納された TSF データをチェックし異常を検出する。これにより、TOE セキュリティ機能の実行コードとデータの完全性が検査される。

(3) 組織のセキュリティ方針「P.OVERWRITE」への対応

TOE の「ハードディスク蓄積データ上書き消去機能」は、MFD 基本機能の終了後に文書データが削除される際に、文書データが格納されていた内部ハードディスク装置の領域を上書き消去する。これにより、内部ハードディスク装置に蓄積された利用済み文書データは上書き消去される。

4 前提条件と評価範囲の明確化

本章では、想定する読者が本 TOE の利用の判断に有用な情報として、本 TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

本 TOE を運用する際の前提条件を表 4-1 に示す。これらの前提条件が満たされない場合、本 TOE のセキュリティ機能が有効に動作することは保証されない。

表4-1 前提条件

| 識別子 | 前提条件 |
|-----------|---|
| A.ADMIN | システム管理者は、TOEセキュリティ機能に関する必要な知識を持ち、課せられた役割に従い、悪意をもった不正を行わないものとする。 |
| A.USER | TOE 利用者は、組織の方針および製品のガイダンス文書に従い、TOEの使用方法及び注意事項に関する教育を受け、その能力を習得する。 |
| A.SECMODE | システム管理者はTOEを運用するにあたり、組織のセキュリティポリシー及び製品のガイダンス文書に従ってTOEを正確に構成設置し、TOEとその外部環境の維持管理を遂行するものとする。 |
| A.ACCESS | TOEを監視下に置くか、TOEの物理的なコンポーネントとデータインタフェースへの許可されないアクセスに対する保護を提供する制限された環境に設置する。 |

4.2 運用環境と構成

TOE は、一般的な業務オフィスにおいて、ファイアウォールなどで外部ネットワークの脅威から保護された内部ネットワークに接続され、さらにファクスボードを介して公衆電話回線網に接続されて利用されることを想定している。本 TOE の一般的な運用環境を図 4-1 に示す。

内部ネットワークには、Mail サーバ、FTP サーバ、SMB サーバ、LDAP サーバ、Kerberos サーバ、OCSP サーバといったサーバコンピュータ、及び一般利用者用のクライアント、システム管理者用のクライアントが接続され、TOE と文書データ等の通信を行う。

TOE の利用者は、MFD の操作パネル、内部ネットワークに接続された一般利用者クライアント、システム管理者クライアントを操作して、TOE を使用する。一般利用者クライアントは、USB を経由して TOE を利用することもできる。

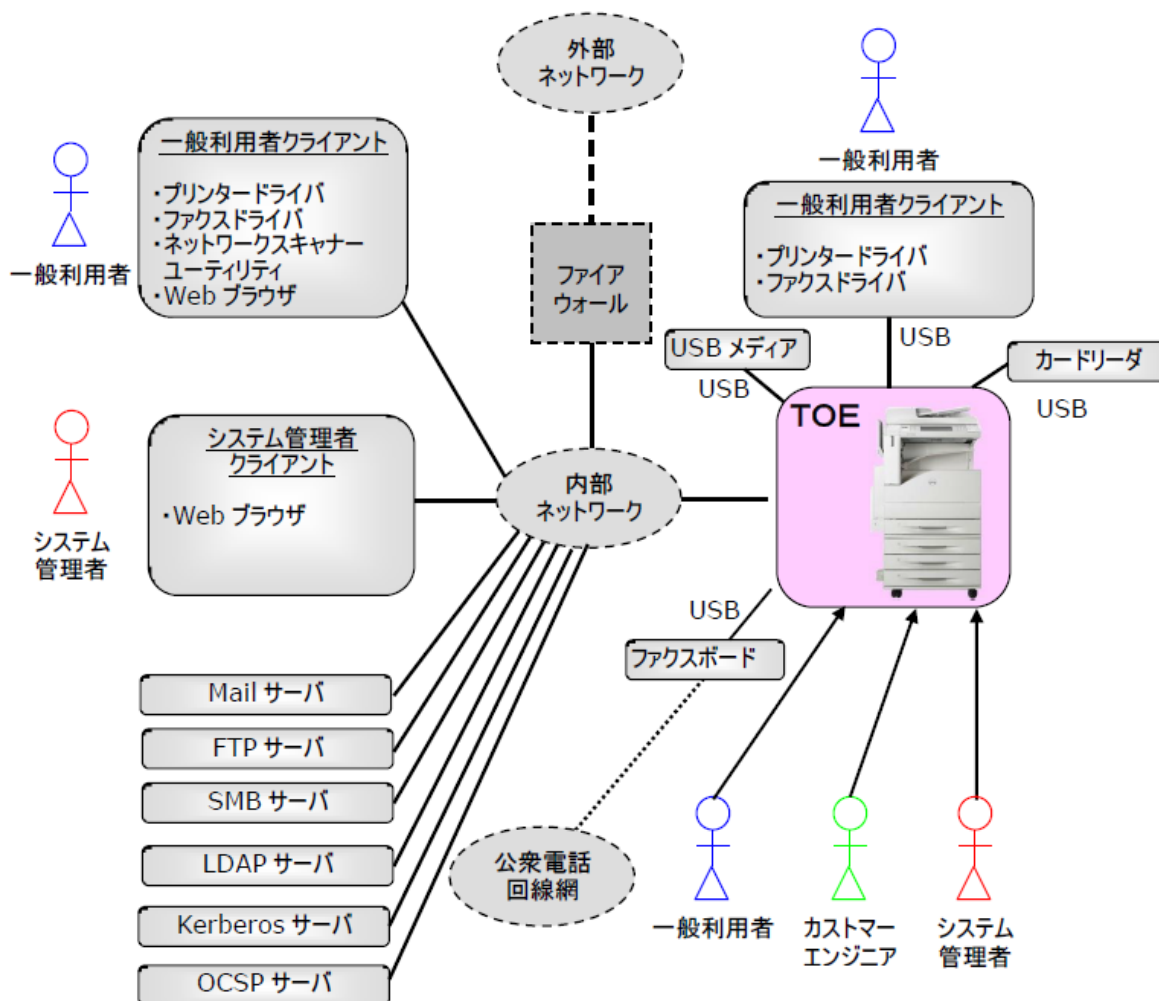


図 4-1 TOE の運用環境

TOEの運用環境の構成品について以下に示す。

(1) ファクスボード

TOEとUSBで接続するファクスボードは別売りである。ファクス機能を使用したい利用者は、指定されたファクスボードを別途購入する必要がある。

(2) 一般利用者クライアント

一般利用者が使用する汎用のPCであり、USBまたは内部ネットワークを介してTOEと接続する。以下のソフトウェアが必要である。

- ・ OSは、Windows XP、Windows Vista、Windows 7のいずれか。
- ・ プリンタードライバ、ファクスドライバ

内部ネットワーク接続の場合には、上記に加えて、以下のソフトウェアが必要である。

- ・ Webブラウザ(OS附属のもの)
- ・ ネットワークスキャナーユーティリティ

(3) システム管理者クライアント

システム管理者が使用する汎用のPCであり、内部ネットワークを介してTOEと接続する。以下のソフトウェアが必要である。

- ・ OSは、Windows XP、Windows Vista、Windows 7のいずれか。
- ・ Webブラウザ(OS附属のもの)

(4) LDAPサーバ、Kerberosサーバ

ユーザー認証機能として「外部認証」を設定した場合、LDAPサーバ、Kerberosサーバのいずれかの認証サーバが必要となる。ユーザー認証機能として「本体認証」を設定した場合は、どちらも必要ない。

また、LDAPサーバは、「外部認証」時に、SA役割を判別するための利用者属性を取得するためにも使用される。従って、Kerberosサーバによる認証の場合であっても、SA役割を使用する場合には、LDAPサーバが必要である。

LDAPサーバ及びKerberosサーバとして、本評価では以下のソフトウェアを使用する。

- ・ Windows Active Directory

(5) Mailサーバ、FTPサーバ、SMBサーバ

TOEは、Mailサーバ、FTPサーバ、SMBサーバと文書データをやりとりする基本機能を持つ。それらのMFDの基本機能を利用する際に、必要に応じてこれらのサーバを設置する。

(6) OCSPサーバ

OCSPサーバは、OCSP(Online Certificate Status Protocol)プロトコルで、X.509デジタル証明書（以下「証明書」という。）の失効情報を提供するサーバである。TOEの設定で、証明書の失効確認を有効にした場合に必要である。本評価では以下のソフトウェアを使用する。

- ・ Windows Active Directory

(7) カードリーダー

スマートカード(CAC/PIV)対応の読み取り装置である。TOEの設定で、スマートカード認証機能を有効にした場合に必要である。本評価では以下の機器を使用する。

・ SCR331、SCR3310 v2.0

(8) USBメディア

USBメディアは、一般に販売されているUSB flash drive (USBメモリ)である。TOEは、USBメディアに格納された文書データのプリントや、スキャンした文書データをUSBメディアに格納する基本機能を提供している。これらのMFDの基本機能を利用する際に、必要に応じてUSBメディアを用意する。

なお、本構成に示されているTOE以外のハードウェア及び連携するソフトウェアの信頼性は本評価の範囲ではない（十分に信頼できるものとする）。

4.3 運用環境におけるTOE範囲

本TOEの評価されたセキュリティ機能には、以下の制約条件がある。

① プリンター機能

TOEのプリンター機能には、TOEが一般利用者クライアントから受信した印刷データを、一旦、内部ハードディスク装置に蓄積して操作パネルから印刷指示をした時点で印刷を行う「蓄積プリント」と、受信すると即時に印刷する「通常プリント」がある。本評価では、「蓄積プリント」だけが評価の対象であり、「通常プリント」は評価の対象外である。本評価の対象となる設定がされたTOEでは、一般利用者クライアントから「通常プリント」を実行しても、TOEにおいて必ず自動的に「蓄積プリント」を実行する。

②外部認証時

TOEのユーザー認証機能では、TOE内に登録した情報を使用して識別認証を行う「本体認証」と、TOE外の認証サーバ(LDAPまたはKerberosプロトコル)を使用して識別認証を行う「外部認証」をサポートしている。TOEで「外部認証」を使用している場合、以下の制約がある。「本体認証」の場合には、これらの制約はない。

- ・ 外部認証時、MFD基本機能のダイレクトファクス機能は評価対象外である。
- ・ 外部認証時、一般利用者クライアントのネットワークスキャナーユーティリティの使用は、評価対象外である。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成を説明する。

5.1 TOE境界とコンポーネント構成

図 5-1 に、TOE である MFD の構成を、MFD 以外の IT 環境と共に示す。図 5-1 で、MFD は、コントローラボード、操作パネル、内部ハードディスク装置、ADF、IIT、IOT の部分である。ファクスボードは TOE の範囲に含まれていない。

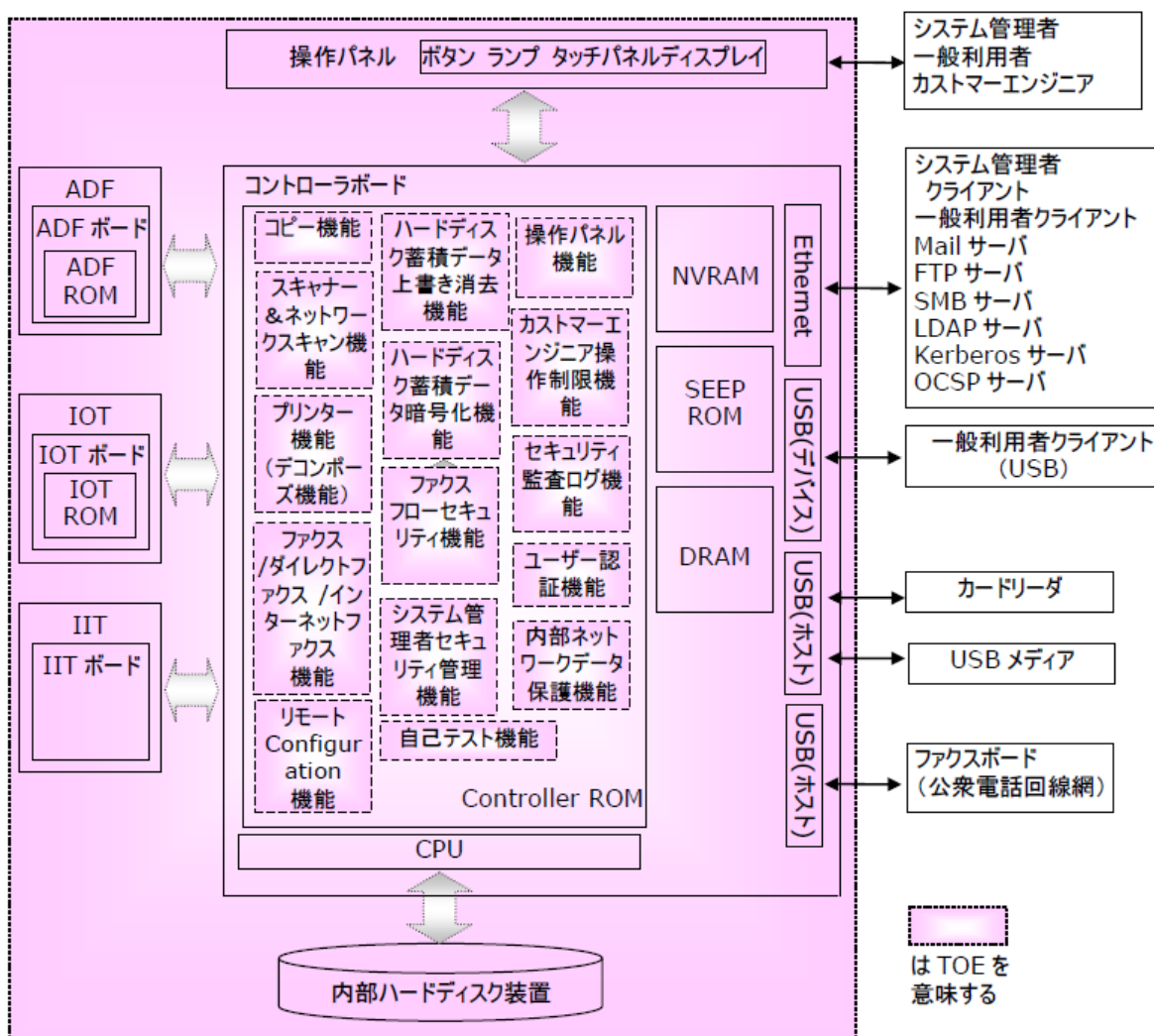


図 5-1 TOE 境界

TOE の機能は、3 章で説明したセキュリティ機能と、それ以外の MFD の基本機能で構成される。MFD の基本機能については、11 章の用語説明を参照。

TOE のセキュリティ機能は、利用者が MFD の基本機能を使用する際に適用される。以下、セキュリティ機能と MFD の基本機能の関係について説明する。

- ① 利用者が、MFDの基本機能、システム管理者セキュリティ管理機能、セキュリティ監査ログ機能の中の監査ログを参照する機能を使用する際には、ユーザー認証機能が適用され、識別認証された利用者はその役割に応じた操作を許可される。識別認証された利用者には、その役割に応じたメニューが表示され、MFDの基本機能、システム管理者セキュリティ管理機能、セキュリティ監査ログ機能が使用できる。利用者の操作入力は、権限に照らし合わせて許可／不許可が判断され、実行される。また、これらの機能を使用する際に、セキュリティ監査ログ機能によって、監査ログが生成される。
- ② ①の利用時に、内部ハードディスク装置に格納される文書データ及び監査ログに対しては、ハードディスク蓄積データ暗号化機能が適用され、文書データを削除する際には、ハードディスク蓄積データ上書き消去機能が適用される。これらの処理は、利用者が意識して蓄積や削除した文書データだけでなく、コピー機能等の処理の都合で利用者が意識することなく一時的に内部ハードディスク装置に蓄積された文書データも対象となる。
- ③ ①の利用時に、MFDとその他のIT機器が内部ネットワークを經由して通信する場合には、内部ネットワークデータ保護機能が適用される。また、ファクスに対しては、ファクスフローセキュリティ機能が適用される。

5.2 IT環境

TOEの設定で外部認証を選択した場合は、TOEは、TOE外の認証サーバ(LDAPサーバまたはKerberosサーバ)から利用者の識別認証の結果を取得する。ただし、機械管理者は、TOE外の認証サーバでは識別認証されず、TOE内に登録した機械管理者の情報を使用して識別認証される。また、認証サーバとしてLDAPサーバとKerberosサーバのいずれを使用する場合であっても、TOEは、LDAPサーバから取得した利用者属性を使用して、利用者がSA役割であるかどうかを判断する。

TOEの設定でスマートカード認証が有効の場合には、TOEは、操作パネルからの利用者を、スマートカード(CAC/PIV)に格納された証明書を使用して、Kerberosサーバと連携して識別認証する機能を提供する。さらに、TOEの設定で証明書の失効確認が有効の場合には、OCSPサーバを使用して証明書の失効確認を行う。

MFDと内部ネットワークで接続する各種サーバやクライアントは、各種暗号通信プロトコルを使用して通信を行う。まず、TOEは、各種サーバやクライアントに対してIPsecを使用する。さらに、クライアントに搭載されるWebブラウザに対してはSSL/TLS、Mailサーバとやり取りするメールに対してはS/MIME、ネットワーク管理にはSNMPv3を使用する。また、TOEと認証サーバ間の通信は、LDAP(SSL/TLS)、Kerberosプロトコルを用いて、識別認証に関するデータを暗号化する。

6 製品添付ドキュメント

本 TOE に添付されるドキュメントの識別を以下に示す。TOE の利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

- Dell C7765dn Color Multifunction Printer User's Guide
(KB3206EN0-5)
(SHA1ハッシュ値 ; ffa87cc19460eeda82c42194b6dfdb1e2eefb5fb)
- Dell C5765dn/C7765dn Security Function Supplementary Guide
(KE3036EN0-1)
(SHA1ハッシュ値 ; 930f93de08df2629aed52f9de314e7df2adccffd)
- Dell C7765dn Smart Card Installation and Configuration Guide
(KE3037EN0-3)
(SHA1ハッシュ値 ; 40524e2e02908e5479b981e205b7d75440c5f084)

※SHA1 ハッシュ値について

ガイドンスは MFD 製品に同梱の CD に格納されている。本評価では、CD に格納されたガイドンスファイルの SHA1 ハッシュ値を計算し比較することで、ガイドンスの完全性が保証されるという評価がされている。

7 評価機関による評価実施及び結果

7.1 評価方法

評価は、CC パート 3 の保証要件について、CEM に規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告された。評価報告書では、本 TOE の概要と、CEM のワークユニットごとの評価内容及び判断結果を説明する。

7.2 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 25 年 3 月に始まり、平成 26 年 9 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 25 年 7 月、同年 11 月、平成 26 年 1 月及び同年 2 月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付・開発セキュリティの各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成 26 年 1 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。

7.3 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評価に基づく侵入テストを実行した。

7.3.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価者が評価した開発者テストの内容を以下に説明する。

(1) 開発者テスト環境

開発者が実施したテストの構成を図 7-1 に示す。

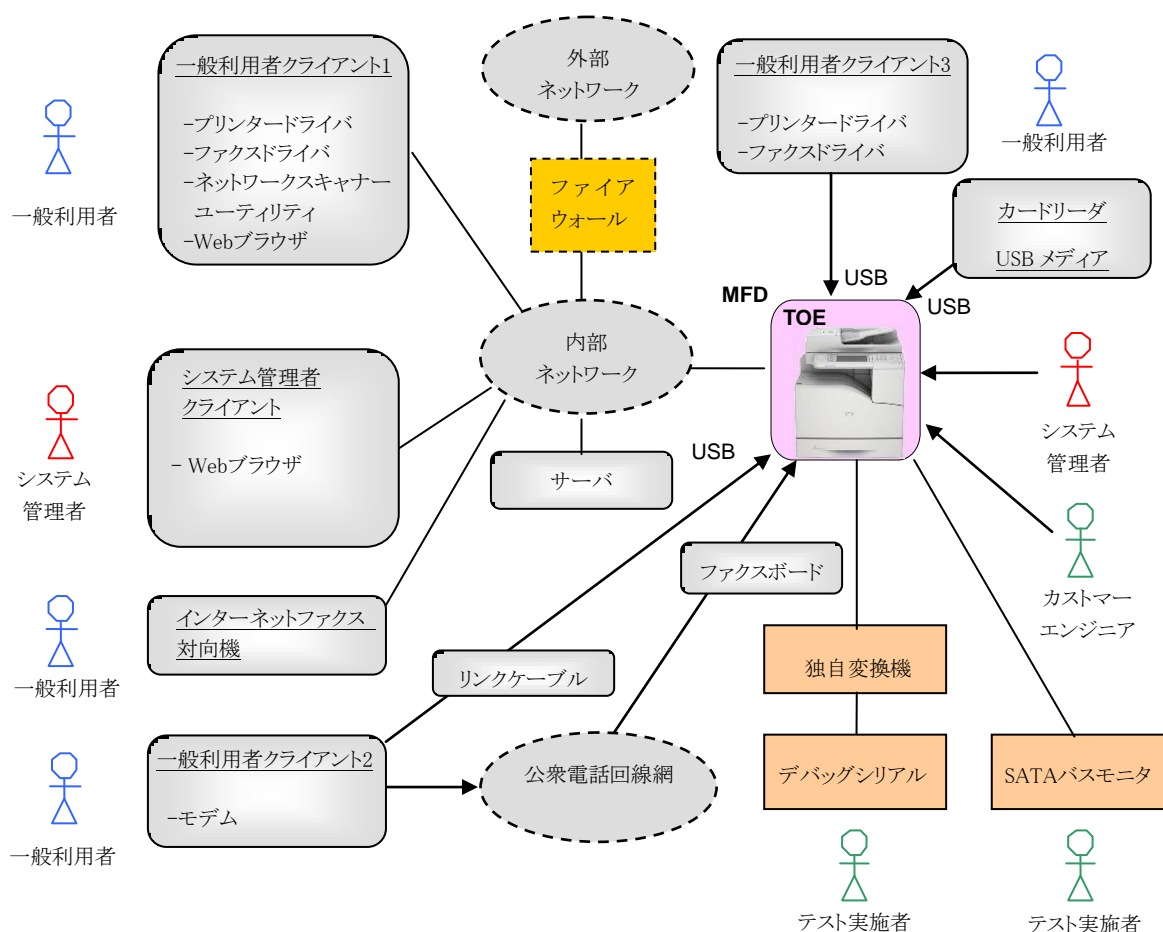


図7-1 開発者テストの構成図

開発者がテストした TOE は、2 章の TOE 識別と同一の TOE である。開発者テストの構成要素を表 7-1 に示す。

表7-1 開発者テストの構成要素

| 名称 | 詳細 |
|---------------|---|
| MFD | Dell C7765dn Color Multifunction Printer |
| サーバ | <p>各種サーバとして使用。以下の2機種を使用</p> <p>a) Microsoft Windows Server 2008 R2 SP1搭載PC</p> <ul style="list-style-type: none"> ・ Mailサーバ : Xmail Version 1.27 ・ FTP、SMB、LDAPサーバ : OS標準搭載ソフトウェア <p>b) Microsoft Windows Server 2012 搭載PC</p> <ul style="list-style-type: none"> ・ Kerberosサーバ、OCSPサーバ : OS標準搭載ソフトウェア |
| システム管理者クライアント | <p>システム管理者クライアントとして使用。以下の3機種を使用</p> <p>a) Microsoft Windows 7 Professional SP1搭載PC</p> <p>Webブラウザ : Microsoft Internet Explorer 8</p> <p>b) Microsoft Windows XP Professional SP3 搭載PC</p> <p>Webブラウザ : Microsoft Internet Explorer 6</p> <p>c) Microsoft Windows VISTA Business SP2 搭載PC</p> <p>Webブラウザ : Microsoft Internet Explorer 7</p> |
| 一般利用者クライアント1 | <p>一般利用者クライアント（内部ネットワーク経由の接続）として使用。以下の3機種を使用</p> <p>a) Microsoft Windows 7 Professional SP1搭載PC</p> <p>Webブラウザ : Microsoft Internet Explorer 8</p> <p>b) Microsoft Windows XP Professional SP3 搭載PC</p> <p>Webブラウザ : Microsoft Internet Explorer 6</p> <p>c) Microsoft Windows VISTA Business SP2 搭載PC</p> <p>Webブラウザ : Microsoft Internet Explorer 7</p> <p>さらに、上記のa) b) c)いずれも、以下のソフトウェアを使用</p> <ul style="list-style-type: none"> ・ プリンタードライバ/ファクスドライバ : PCL6 Driver Version 6.5.1 ・ ネットワークスキャナーユーティリティ : Version 1.9.10 |
| 一般利用者クライアント2 | <p>ファクス送受信と、MFDのファクス接続用USBポートが他用途に使用できないことの確認に使用</p> <ul style="list-style-type: none"> ・ Microsoft Windows XP Professional SP3 搭載 PC <p>※PCのモデムポートを公衆電話回線網に接続。PCのUSBポートを、リンクケーブル（USBケーブル）を介してMFDのファクスボード用USBポートに接続</p> |

| 名称 | 詳細 |
|----------------|--|
| 一般利用者クライアント3 | 一般利用者クライアント（プリンター用のUSBポート経由の接続）として使用 <ul style="list-style-type: none"> ・ Microsoft Windows XP Professional SP3 搭載PC ・ プリンタードライバ/ファクスドライバ：PCL6 Driver Version 6.5.1 |
| SATAバスモニタ | 内部ハードディスク装置の接続されたSATAバスのデータをモニタするツール <ul style="list-style-type: none"> ・ 専用機器（Catalyst Enterprises社製 ST2-32-2-A）を接続したWindows XP搭載PC ・ 専用ソフトウェア：Serial ATA Analyzer V1.984.0401 |
| デバッグシリアル | MFDのデバッグ用端末。端末(PC)のシリアルポートを、独自変換機を経由して、MFDのデバッグ用の端末ポートと接続 <ul style="list-style-type: none"> ・ Microsoft Windows XP Professional 搭載PC ・ 端末ソフトウェア：Tera Term Pro Version 2.3 |
| 独自変換機 | MFDとデバッグシリアルを接続するための、富士ゼロックス製の独自の変換基板 |
| 公衆電話回線網 | 電話回線疑似交換機を使用（ハウ社N4T-EXCH） |
| ファクスボード | 富士ゼロックス製のMFDのオプション <ul style="list-style-type: none"> ・ Fax ROM Ver 1.1.13 |
| インターネットファクス対向機 | 富士ゼロックス製のMFDであるWorkCentre 5325を使用 |
| カードリーダー | 以下の2機種を使用 <ul style="list-style-type: none"> ・ SCM製 SCR331 ・ SCM製 SCR3310 V2.0 |

外部ネットワークとファイアウォールは、テスト内容に影響しないことを、評価者が評価している。

開発者テストは本 ST において識別されている TOE 構成と同等の TOE テスト環境で実施されている。

(2) 開発者テスト概説

開発者テストの概説は以下のとおりである。

a) テスト概要

開発者テストの概要は、以下のとおりである。

<開発者テスト手法>

- ① MFD の操作パネル、システム管理者クライアント、一般利用者クライアントから MFD の基本機能やセキュリティ管理機能を操作して、その結果の MFD のふるまい、パネル表示、監査ログ内容を確認する。
- ② ハードディスク蓄積データ上書き消去機能の確認のために、テスト用ツールである SATA バスモニタを使用して、内部ハードディスク装置へ書き込まれるデータと、書き込み後の内部ハードディスク装置の内容を読み出して観測する。
- ③ ハードディスク蓄積データ暗号化機能の確認のために、デバッグ用のシリアルポートを使用して、内部ハードディスク装置に格納された文書データ等を直接参照し、暗号化されていることを観測する。また、暗号化された内部ハードディスク装置を、暗号鍵の異なる MFD の内部ハードディスク装置と入れ替えても、操作パネルにエラーが表示され、使用できないことを確認する。
- ④ ハードディスク蓄積データ暗号化機能の確認のために、生成された暗号鍵と暗号化されたデータを、指定されたアルゴリズムによって算出された既知のデータと比較し、仕様どおりの暗号鍵生成アルゴリズムと暗号アルゴリズムであることを確認する。
- ⑤ IPSec 等の暗号通信プロトコル機能の確認のために、後述するテストツールを使用して、仕様どおりの暗号通信プロトコルであることを観測する。また、様々な Web 入力や印刷ジョブコマンドに対する保護機能を確認する。
- ⑥ 一般利用者クライアント 2 を公衆電話回線網経由で接続し、MFD とのファクス送受信に使用する。また、ファクスフローセキュリティ機能の確認のために、一般利用者クライアント 2 から公衆電話回線網を経由して TOE にダイヤルアップ接続ができないことを観測する。さらに、一般利用者クライアント 2 からファクスボード接続用の USB ポートに直接接続しても、TOE の操作ができないことを観測する。

<開発者テストツール>

開発者テストにおいて利用したツールを表 7-2 に示す。

表7-2 開発テストツール

| ツール名称 | 概要・利用目的 |
|---------------------------------------|---|
| SATA バスモニタ (PC+専用機器) ※構成は表7-1参照 | MFD内の内部ハードディスク装置接続用のSATAバスのデータをモニタし、内部ハードディスク装置に書き込まれるデータを観測する。また、内部ハードディスク装置に書き込まれたデータを読み出す。 |

| ツール名称 | 概要・利用目的 |
|--|--|
| プロトコルアナライザ (Wireshark Version 1.8.2) | 内部ネットワーク上の通信データをモニタし、暗号通信プロトコルが、仕様通りにIPsec、SSL/TLS、SNMPv3であることを確認する。 |
| メーラー (Microsoft Windows Live Mail 2011) | TOEとメールサーバを介して、電子メールを送受信し、S/MIMEによる暗号化と署名が仕様通りであることを確認する。 |
| HTTPデバッガ (Fiddler 4.4.5.5) | Webブラウザ（クライアント）とWebサーバ（MFD）間の通信を仲介し、その間の通信データの参照と変更を行うツール。 |
| デバッグシリアル +独自変換機 ※構成は表7-1参照 | 内部ハードディスク装置に書き込まれたデータを読み出して、その内容を確認する。 |

<開発者テストの実施内容>

各種インタフェースより、MFDの基本機能とセキュリティ管理機能を操作し、様々な入力パラメタに対して、適用されるセキュリティ機能が仕様通りに動作することを確認した。なお、ユーザー認証機能については、利用者の役割毎に、本体認証、外部認証（LDAPサーバ）、外部認証（Kerberosサーバ）、スマートカード認証の各場合について、仕様通りに動作することを確認した。

また、MFD本体の電源OFFによる上書き消去処理の中断と電源ONによる再開などのエラー時に関するふるまいが、仕様通りに動作することを確認した。

b) 開発者テストの実施範囲

開発者テストは開発者によって87項目実施された。

カバレッジ分析によって、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た。深さ分析によって、TOE設計に記述されたすべてのサブシステムとサブシステムインタフェースが十分にテストされたことが検証された。

c) 結果

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、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

7.3.2 評価者独立テスト

評価者は、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実行されることを再確認するサンプリングテストを実施するとともに、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることをより確信するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

評価者が実施した独立テストの構成は、図 7-1 に示した開発者テストの構成と、以下を除いて同じである。

- ・ ファクス対向機（一般利用者クライアント 2）及びインターネットファクス対向機として、富士ゼロックス製の MFD である Dell C7765dn Color Multifunction Printer (TOE)を使用。
- ・ カードリーダーとして、SCM 製 SCR3310 V2.0 だけを使用。

評価者は、ファクスやインターネットファクスの通信相手の違いは、TOE のセキュリティ機能に影響ないと判断している。また、評価者は、カードリーダーは同じ会社の製品で機能が同じであることから、開発者がテストをした機種から 1 機種を選択しテストすることで、十分であると判断している。

なお、開発者独自のデバッグ環境（デバッグシリアルと独自変換機）をはじめとするテストツールは、開発者テストに用いられたものを利用しているが、それらの妥当性確認及び動作試験は、評価者によって実施されている。

独立テストは、本 ST において識別されている TOE の構成と同一の環境で実施された。

(2) 独立テスト概説

評価者の実施した独立テストは以下のとおりである。

a) 独立テストの観点

評価者が、開発者テスト及び提供された評価証拠資料から考案した独立テストの観点を以下に示す。

<独立テストの観点>

- ① 開発者テストにおいて、セキュリティ機能のふるまいについて厳密なテストが実施されていないインタフェースが存在するため、テストされていないパラメタのふるまいを確認する。

- ② サンプルングテストでは、以下の観点で開発者テストの項目を抽出する。
- ・ すべてのセキュリティ機能と外部インタフェースを確認する。
 - ・ すべての利用者種別と、親展ボックス及びプライベートプリントの組合せのアクセス制御を確認する。
 - ・ すべての認証方式（本体認証、Kerberos による外部認証、LDAP による外部認証、スマートカード認証）を確認する。

b) 独立テスト概要

評価者は、独立テストの観点に基づいて、開発者テストのサンプルングテストと追加の独立テストを考案した。評価者が実施した独立テストの概要は以下のとおりである。

<独立テスト手法>

開発者テストと同じ手法を使用して、開発者と同じテスト及び入力パラメータを変更したテストを実施する。

<独立テストツール>

開発者テストと同じツールを使用した。

<独立テストの実施内容>

評価者は、独立テストの観点に基づいて、76 項目のサンプルングテストと、6 項目の追加の独立テストを実施した。

独立テストの観点とそれに対応した主なテスト内容を表 7-3 に示す。

表7-3 実施した主な独立テスト

| 観点 | テスト概要 |
|-----|---|
| 観点① | パスワード変更や入力時の長さ制限の限界値のふるまいが、仕様どおりであることを確認する。 |
| 観点① | システム管理者の親展ボックスに対するアクセス制御が、仕様どおりであることを確認する。 |
| 観点① | アカウントロック状態の判定や、複数の利用者アカウントのロック状態の管理が、仕様どおりであることを確認する。 |
| 観点① | TOE内に文書データが存在している状態で、所有者の利用者登録を削除する際のふるまいが、仕様どおりであることを確認する。 |

c) 結果

評価者が実施したすべての独立テストは正しく完了し、評価者は TOE のふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが一致していることを確認した。

7.3.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

- ① 公知の脆弱性情報であるネットワークサービスの不正利用、Web の各種脆弱性、SSL 通信時に安全でない暗号が選択される可能性について、本 TOE にも該当する懸念がある。
- ② 公知の脆弱性情報より、PDF ファイルによる予期しない処理の実行、印刷ジョブコマンドによる不正なアクセスについて、本 TOE にも該当する懸念がある。
- ③ 操作パネル等の Web 以外のインタフェースについても、制限値を超えた長さの入力や、想定外の文字コード入力に対して、TOE が予期しない動作をする懸念がある。
- ④ 証拠資料に対する脆弱性分析より、USB ポートによる不正アクセスの懸念がある。
- ⑤ 証拠資料に対する脆弱性分析より、設定データが格納された NVRAM、SEEPROM が初期化された場合、セキュリティ機能が無効化される懸念がある。
- ⑥ 証拠資料に対する脆弱性分析より、親展ボックスの文書データに対して、複数の利用者のアクセスが競合した場合に、保護資産である文書データの不整合が生じる懸念がある。
- ⑦ 初期化処理中の不正アクセスや、MFD のシステムクロックの電池切れによってセキュリティ機能が誤った動作を行う懸念がある。

なお、暗号鍵については、設定する暗号化キーや暗号鍵の生成メカニズムの分析から、想定されている攻撃者の攻撃能力では暗号鍵の入手や推測ができないことが評価されている。

b) 侵入テストの概要

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

<侵入テスト環境>

評価者独立テスト環境と同じ環境で実施した。ただし、侵入テスト用のツールを搭載したPCを追加して使用した。侵入テストで使用したツールの詳細を表7-4に示す。

表7-4 侵入テストツール

| 名称 | 概要・利用目的 |
|------------------------------|---|
| 侵入テスト用PC | Windows XP、Windows 7、Windows VISTAを搭載したPCであり以下の侵入テスト用ツールを動作させる。 |
| Nmap Ver.6.25 | 利用可能なネットワークサービスポートを検出するツール。 |
| Fiddler V2.4.4.5 | Webブラウザ（クライアント）とWebサーバ（TOE）間の通信を仲介し、その間の通信データの参照と変更を行うツール。 |
| ContentsBridge Version 7.3.0 | 富士ゼロックス社製のPC用のプリントソフト。 |
| Metasploit Ver.4.6.2 | PDFの脆弱性を検査するための検査データの作成に使用。 |

<侵入テストの実施内容>

懸念される脆弱性と対応する侵入テスト内容を表7-5に示す。

表7-5 侵入テスト概要

| 脆弱性 | テスト概要 |
|------|--|
| 脆弱性① | <ul style="list-style-type: none"> ・NmapをTOEに対して実施し、オープンされているポートが悪用できないことを確認した。 ・Webブラウザ及びFiddlerを使用して、Webサーバ（TOE）に各種入力を行い、識別認証のバイパス、バッファオーバーフロー、各種インジェクション等の公知の脆弱性がないことを確認した。 ・暗号通信プロトコルに関して、クライアントとして使用するPCの設定を推奨されない値に変更しても、TOEが指定する暗号通信プロトコル以外は通信できないことを確認した。 |
| 脆弱性② | <ul style="list-style-type: none"> ・不正な処理を含むPDFファイルを入力しても、処理が実行されないことを確認した。 |

| | |
|------|--|
| | <ul style="list-style-type: none"> ・印刷ジョブコマンドで、ディレクトリを探索しても、保護資産にアクセスできないことを確認した。 |
| 脆弱性③ | <ul style="list-style-type: none"> ・操作パネル、一般利用者クライアント（ネットワークスキャナーユーティリティ、プリンタードライバ）より、規定外の文字長、文字コード、特殊キーを入力しても、エラーとなることを確認した。 |
| 脆弱性④ | <ul style="list-style-type: none"> ・TOEが備える各種USBポートに対して、侵入テスト用クライアントを接続してTOEにアクセスを試みても、プリンターやファクス等の意図された機能以外の利用はできないことを確認した。 |
| 脆弱性⑤ | <ul style="list-style-type: none"> ・NVRAMやSEEPROMを設定のされていない新品と交換しても、エラーとなりTOEが使用できないことを確認した。 |
| 脆弱性⑥ | <ul style="list-style-type: none"> ・親展ボックスの文書データに対して、複数の利用者がアクセスしても、他で操作中の場合はアクセスが拒否されることを確認した。 |
| 脆弱性⑦ | <ul style="list-style-type: none"> ・電源投入直後のMFDの初期化処理中は、操作を受け付けないことを確認した。 ・MFDのシステムクロック用の電池が切れた状態で電源を投入すると、エラーが表示されMFDが使用できないことを確認した。 |

c) 結果

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

7.4 評価構成について

本評価の前提となる TOE の構成条件は、6 章に記述したガイダンス「Security Function Supplementary Guide」に記述されているとおりである。本 TOE のセキュリティ機能を有効にし、安全に使用するために、システム管理者は、当該ガイダンスの記述のとおり TOE を設定しなければならない。

TOE の設定値の中には、セキュリティ機能を有効にするための設定の他に、以下のような設定も含まれている。

- カスタマーエンジニア操作制限機能：[有効]
- 蓄積プリント機能：[プライベートプリントに保存]

さらに、外部認証時には以下の設定が必要である。

- ダイレクトファクス機能：外部認証時は [無効] に設定
- ネットワークスキャナーユーティリティの使用（WebDAV 設定）
：外部認証時は [無効] に設定

これらの設定値をガイダンスと異なる値に変更した場合には、本評価による保証の対象ではない。

7.5 評価結果

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

評価では以下について確認された。

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

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

- ・ EAL3 パッケージのすべての保証コンポーネント

評価の結果は、第 2 章に記述された識別に一致する TOE によって構成されたものみに適用される。

7.6 評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

8 認証実施

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

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

8.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本 TOE が CC パート 3 の EAL3 に対する保証要件を満たすものと判断する。

8.2 注意事項

本 TOE に興味のある調達者は、「1.1.3 免責事項」、「4.3 運用環境における TOE 範囲」及び「7.4 評価構成について」の記載内容を参照し、本 TOE の評価対象範囲や運用上の要求事項が、各自の想定する運用条件に合致しているかどうか注意が必要である。

特に、保守機能を有効化した場合、それ以降の運用での本 TOE のセキュリティ機能への影響については本評価の保証の範囲外となるため、保守の受け入れについては管理者の責任において判断されたい。

9 附属書

特になし。

10 セキュリティターゲット

本 TOE のセキュリティターゲット[12]は、本報告書とは別文書として以下のとおり本認証報告書とともに提供される。

Dell C7765dn Color Multifunction Printer セキュリティターゲット, **Version 1.1.3**, 2014 年 9 月 8 日, 富士ゼロックス株式会社

11 用語

本報告書で使用された CC に関する略語を以下に示す。

| | |
|-----|--|
| CC | Common Criteria for Information Technology Security Evaluation (セキュリティ評価基準) |
| CEM | Common Methodology for Information Technology Security Evaluation (セキュリティ評価方法) |
| EAL | Evaluation Assurance Level (評価保証レベル) |
| PP | Protection Profile (プロテクションプロファイル) |
| ST | Security Target (セキュリティターゲット) |
| TOE | Target of Evaluation (評価対象) |
| TSF | TOE Security Functionality (TOEセキュリティ機能) |

本報告書で使用された TOE に関する略語を以下に示す。

| | |
|---------|---|
| ADF | Auto Document Feeder (自動原稿送り装置) |
| CAC | Common Access Card (共通アクセスカード) |
| IIT | Image Input Terminal (画像入力ターミナル) |
| IOT | Image Output Terminal (画像出力ターミナル) |
| MFD | Multi Function Device (デジタル複合機) |
| NVRAM | Non Volatile Random Access Memory (不揮発性ランダムアクセスメモリ) |
| PIV | Personal Identity Verification (個人識別認証) |
| SA | System Administrator privilege (SA役割) |
| SEEPROM | Serial Electronically Erasable and Programmable Read Only Memory (シリアルバスに接続された電氣的に書き換え可能なROM) |

本報告書で使用された用語の定義を以下に示す。

| | |
|---------------|---|
| SA | 一部の管理機能が使用できるシステム管理者。SAの役割は、利用組織の必要に応じて機械管理者が設定する |
| TOE設定データ | TOEのセキュリティ機能に影響を与える可能性のある設定データ |
| USBメディア | USB Flash Drive (USBメモリ) であり、スキャンした文書データの書き込みや、格納された文書データのプリントに使用する |
| 暗号化キー | システム管理者が設定する12桁の英数字。内部ハードディスク装置の暗号化時に、このデータをもとに暗号鍵を生成する |
| 一般利用者 | TOEが提供するコピー機能、プリンター機能、スキャナー機能、ファクス機能等の基本機能の使用を許可された利用者 |
| インターネットファクス機能 | 公衆電話回線網を使用することなく、インターネットを經由してファクスの送受信を行う機能 |

| | |
|--------------------------|---|
| 外部認証 | 外部の認証サーバ (LDAPサーバまたはKerberosサーバ) に登録されている利用者情報を使用して、TOEの利用者を識別認証する機能。利用者情報としては、利用者IDとパスワード (LDAPサーバ及びKerberosサーバ) または証明書 (Kerberosサーバの場合のみ) を使用する |
| カスタマーエンジニア | MFDの保守/修理を行うエンジニア |
| 機械管理者 | すべての管理機能が使用可能なシステム管理者 |
| コピー機能 | 一般利用者がMFDの操作パネルから指示をして、IITから原稿を読み取り、IOTから印刷する機能 |
| システム管理者 | TOEのセキュリティ機能の設定や、その他機器設定を行うための特別な権限を持つ管理者。「機械管理者」と「SA」の総称 |
| 親展ボックス | 文書データを蓄積するためにMFDの内部ハードディスク装置に作成される論理的なボックス。スキャナー機能やファクス受信により読み込まれた文書データを登録ユーザー別や送信元別に蓄積できる |
| スキャナー機能 | 一般利用者がMFDの操作パネルから指示して、IITから原稿を読み込み、MFD内部の親展ボックスまたは外部のUSBメディアに蓄積する機能。蓄積された文書データは、ネットワークスキャナーユーティリティやWebブラウザから取り出す |
| スマートカード (CAC/PIV) | 米国政府で採用されているスマートカード |
| スマートカード認証 | スマートカード(CAC/PIV)に格納された証明書を使用して、KerberosサーバやOCSPサーバ(証明書の失効確認設定が有効の場合)と連携して、TOEの利用者を識別認証する機能 |
| セキュリティ監査ログデータ | 障害や構成変更、ユーザー操作など、デバイス内で発生した重要な事象を時系列に記録したもの |
| 操作パネル | MFDの操作に必要なボタン、ランプ、タッチパネルディスプレイが配置されたパネル |
| ダイレクトファクス機能 | 一般利用者が、一般利用者クライアントから文書データをMFDに送り、紙に印刷することなく、公衆電話回線網を使用してファクス送信する機能 |
| 蓄積プリント | 印刷データを一時的にMFDの内部ハードディスク装置に蓄積し、一般利用者が操作パネルから印刷指示をした時に印刷を行う。「プリンター機能」の説明参照 |
| 通常プリント | 印刷データをMFDが受信するとすぐに印刷を行う。「プリンター機能」の説明参照 |
| ネットワークスキャナー機能 | 一般利用者が、MFDの操作パネルから指示して、IITから原稿を読み込み、MFDの設定情報に従って自動的にFTPサーバ、SMBサーバ、Mailサーバに送信する機能 |
| ネットワークスキャナーユーティリティファクス機能 | MFD内の親展ボックスに保存されている文書データを、一般利用者クライアントから取り出すためのソフトウェアファクス送受信を行う機能。ファクス送信は、操作パネルからの一般利用者の指示に従い、IITから原稿を読み込み、公衆電話回線網を経由して、接続された相手機に文書データを送信する。ファクス受信は、公衆電話回線網により接続された相手機から送られた文書データを受信し、IOTから印刷を行う |

| | |
|-------------------------|---|
| ファクスドライバ | 印刷と同じ操作で、一般利用者クライアント上からMFDへ文書データを送信し、直接ファクス送信する（ダイレクトファクス機能）ためのソフトウェア |
| プリンター機能 | 一般利用者が、印刷データを一般利用者クライアントからMFDへ送信して、IOTから印刷を行う機能。 プリンター機能には、「通常プリント」と「蓄積プリント」がある。本評価では、蓄積プリントだけが評価の対象である。また、外部のUSBメディアに格納された文書データを操作パネルから指定して印刷を行う機能も含まれる |
| プリンタードライバ | 一般利用者クライアント上の文書データを、MFDが解釈可能なページ記述言語で構成された印刷データに変換するソフトウェア |
| 文書データ | MFDのコピー機能、プリンター機能、スキャナー機能、ファクス機能が処理する文字や画像の情報を含むデータの総称 |
| 本体認証 | TOEに登録された利用者IDとパスワードを使用して、TOEの利用者を識別認証する機能 |
| リモート Configuration機能 | 利用者クライアントのWebブラウザを介して、TOEの状態確認、設定変更、文書データの取出し、印刷要求ができるサービス |

12 参照

- [1] ITセキュリティ評価及び認証制度の基本規程, 平成26年3月, 独立行政法人情報処理推進機構, CCS-01
- [2] ITセキュリティ認証等に関する要求事項, 平成26年4月, 独立行政法人情報処理推進機構, CCM-02
- [3] ITセキュリティ評価機関承認等に関する要求事項, 平成25年4月, 独立行政法人情報処理推進機構, CCM-03
- [4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001
- [5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002
- [6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003
- [7] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-001, (平成24年11月, 翻訳第1.0版)
- [8] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能コンポーネント, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-002, (平成24年11月, 翻訳第1.0版)
- [9] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証コンポーネント, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-003, (平成24年11月, 翻訳第1.0版)
- [10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004
- [11] 情報技術セキュリティ評価のための共通方法: 評価方法, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-004, (平成24年11月, 翻訳第1.0版)
- [12] Dell C7765dn Color Multifunction Printer セキュリティターゲット, Version 1.1.3, 2014年9月8日, 富士ゼロックス株式会社
- [13] Dell C7765dn Color Multifunction Printer 評価報告書, 第1.16版, 2014年9月12日, 一般社団法人ITセキュリティセンター 評価部