認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司　原紙押印済

評価対象

申請受付日（受付番号）	**平成21年9月30日** (IT**認証**9272)
認証番号	C0250
認証申請者	**富士ゼロックス株式会社**
TOE**の名称**	Xerox 4112/4127 Copier/Printer
TOE**のバージョン**	Controller+PS ROM Ver. 1.211.8 IOT ROM Ver. 46.18.0 IIT ROM Ver. 15.6.1 IIT Option ROM Ver. 14.0.4 ADF ROM Ver. 12.2.7
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22年3月12日

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 改訂第2版 (翻訳第2.0版)
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 改訂第2版 (翻訳第2.0版)

評価結果：合格

「Xerox 4112/4127 Copier/Printer」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件

を満たした。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「Xerox 4112/4127 Copier/Printer」（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富士ゼロックス株式会社に報告するとともに、本TOEに関心を持つ利用者や運用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、本書と共に、対応するSTを併読されたい。本TOEの動作条件や運用のための前提についての詳細、本TOEが対抗する脅威への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、及びセキュリティ仕様の概要と十分性の根拠は、STにおいて詳述されている。

本認証報告書は、特に本TOEを購入し、運用する消費者サイトのシステム管理者等を読者として想定している。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。

1.1.1 評価保証レベル

本TOEが適合を主張する評価保証レベルは、EAL3適合である。

1.1.2 PP適合

適合するPPはない。

1.2 評価製品

1.2.1 製品名称

本TOEは、以下の製品のセキュリティ機能である。

製品名称：	Xerox 4112/4127 Copier/Printer	
バージョン：	Controller+PS ROM	Ver. 1.211.8
	IOT ROM	Ver. 46.18.0
	IIT ROM	Ver. 15.6.1
	IIT Option ROM	Ver. 14.0.4
	ADF ROM	Ver. 12.2.7
開発者：	富士ゼロックス株式会社	

1.2.2 製品概要

Xerox 4112/4127 Copier/Printerである本TOEは、コピー機能、プリンター機能、スキャナー機能等を有するデジタル複合機（MFD）である（以下、これら2機種を総称してMFDと呼ぶ）。ただし、本TOEは、ファクス機能は有さない。

本TOEは、一般的な業務オフィスに設置され、利用者クライアント（一般利用者クライアント及びシステム管理者クライアント）やサーバと接続された内部ネットワークと接続されて利用されることを想定している。

本TOEは、MFD全体の制御を行う一般機能、及び左記一般機能の使用に関わる文書データ等を脅威から保護するセキュリティ機能を提供している。

本TOEは、一般機能として下記の機能を提供している。

*コピー機能

*プリンター機能

*スキャナー機能

*CWIS機能
一般利用者が操作パネルから指示してスキャンし、MFDの親展ボックスに格納された文書データを、Webブラウザを使用して一般利用者クライアントから取り出す機能。また、システム管理者が、Webブラウザを使用して、TOE設定データの確認や書き換えを行う機能。

*ネットワークスキャン機能
一般利用者が操作パネルから指示してMFDにスキャンした文書データを、MFDに設定されている情報に従い、FTPサーバ、Mailサーバ、またはSMBサーバに送信する機能

1.2.3 TOE範囲とセキュリティ機能

TOEは、1.2.2で説明した一般機能と下記(1)～(7)のセキュリティ機能を提供している。

TOEの下記セキュリティ機能は、上記一般機能の使用に関連した文書データや利用済みの文書データを漏洩等の脅威から保護したり、TOEのセキュリティ機能の使用に関連するTOE設定データやセキュリティ監査ログデータを変更や漏洩の脅威から保護するためのものである。

(1) ハードディスク蓄積データ上書き消去機能
コピー、プリンター及びスキャナー等の各機能の動作後、ハードディスク装置に蓄積された利用済みの文書データの上書き消去を行う機能

(2) ハードディスク蓄積データ暗号化機能
コピー、プリンター、スキャナー等の各機能の動作時にハードディスク装置に蓄積される文書データや、ハードディスク装置に蓄積されるセキュリティ監査ログデータの暗号化を行う機能

(3) ユーザー認証機能
許可された一般利用者だけにTOEの機能を使用する権限を持たせるために、操作パネルまたは一般利用者クライアントから、ユーザーIDとユーザーパスワードを入力させて識別認証する機能。また、TOEのセキュリティ機能に関する設定の参照及び変更をシステム管理者に制限するために、操作パネルまたはシステム管理者クライアントから、システム管理者IDとパスワードを入力させて識別認証する機能。

(4) システム管理者セキュリティ管理機能
操作パネルまたはシステム管理者クライアントから、上記ユーザー認証機能により認証されたシステム管理者のみが、TOEのセキュリティ機能に関する設定の参照及び変更を行えるようにする機能

(5) カストマーエンジニア操作制限機能
カストマーエンジニアがTOEのセキュリティ機能に関する設定の変更をできないようにする、システム管理者のみが行える設定機能

(6) セキュリティ監査ログ機能
いつ、誰が、どのような作業を行ったかという事象や重要なイベント（構成管理など）を、追跡記録するための機能

(7) 内部ネットワークデータ保護機能
内部ネットワーク上に存在する通信データである文書データ、セキュリティ監査ログデータ、及びTOE設定データを保護する機能

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セキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[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「Xerox 4112/4127 Copier/Printer　セキュリティターゲット」（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]のいずれか）附属書A、CCパート2（[6][9]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]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、「Xerox 4112/4127 Copier/Printer　評価報告書」（以下「評価報告書」という。）[13]に示されている。なお、評価方法は、CEM（[11][12]のいずれか）に準拠する。

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、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、特に問題点は見られなかった。評価は、平成22年3月の評価機関による評価報告書の提出をもって完了し、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。

2 TOE概要

2.1 セキュリティ課題と前提

TOEが解決すべき課題と、必要とする前提を以下に示す。

2.1.1 脅威

本TOEは、表2-1に示す脅威を想定し、これに対抗する機能を備える。
攻撃者は低レベルの攻撃能力を持つ者であり、TOEの動作について公開されている情報知識を持っていると想定する。

表2-1 想定する脅威

識別子	脅 威
T.RECOVER	攻撃者が、内部ハードディスク装置を取り出して、その内容を読み取るために市販のツール等に接続して、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するかもしれない。
T.CONFDATA	攻撃者が、操作パネルやシステム管理者クライアントから、システム管理者のみアクセスが許可されている、TOE設定データにアクセスして設定の変更、または不正な読み出しを行うかもしれない。
T.DATA_SEC	攻撃者が、操作パネルやWebブラウザから、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.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。
T.CONSUME	攻撃者が、TOEにアクセスしTOEの利用を不正に行うかもしれない。

2.1.2 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は存在しない。

2.1.3 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2-3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2-3　TOE使用の前提条件

識別子	前提条件
A.ADMIN	システム管理者は、TOEの機器管理に課せられた役割を遂行するために、TOEセキュリティ機能に関する必要な知識を持ち、悪意をもった不正を行わないものとする。
A.SECMODE	システム管理者は、TOEを運用するにあたり、下記の通りに設定するものとする。 *本体パネルからの認証時のパスワード使用設定：有効にする *システム管理者パスワード長：9文字以上 *システム管理者認証失敗によるアクセス拒否設定：有効にする *システム管理者認証失敗によるアクセス拒否回数設定：5 *カストマーエンジニア操作制限設定：有効にする *ユーザー認証設定：有効にする（ローカル認証を選択） *ユーザーパスワード(一般利用者とSA)文字数制限設定：9文字以上 *プライベートプリント設定：認証成功のジョブを蓄積にする *監査ログ設定：有効にする *SNMPv3通信設定：有効にする *SNMPv1/v2c通信設定：無効にする *SNMPv3認証パスワード：8文字以上 *SSL/TLS通信設定：有効にする *IPSec通信設定：有効にする *S/MIME通信設定：有効にする *SMB通信設定：NetBEUIを無効にする *ハードディスク蓄積データ上書き消去設定：有効にする *ハードディスク蓄積データ暗号化設定：有効にする *ハードディスク蓄積データ暗号化キー：12文字 *時刻指定文書削除設定：有効にする

2.1.4　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。読者は、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。

* Xerox 4112/4127 Copier/Printer Administrator Guide

* Xerox 4112/4127 Copier/Printer User Guide
* Xerox 4112/4127 Copier/Printer Security Function Supplementary Guide

2.1.5 構成条件

本TOEは、コピー機能、プリンター機能、スキャナー機能等を有するMFDである。

本TOE以外に、リモートのクライアントPC（一般利用者クライアント及びシステム管理者クライアント）から使用する場合のOSとして、Windows 2000、Windows XP、またはWindows VISTAのインストールが必要である。

一般利用者クライアントにおいては、上記OSがインストールされた汎用のPC上に、プリンタードライバー、及びネットワークスキャナユーティリティがインストールされていることが必要である。

2.2 セキュリティ対策

TOEは、2.1.1の脅威に対抗し、2.1.2の組織のセキュリティ方針を満たすために以下のセキュリティ機能を具備する。

まず、内部ハードディスク装置に蓄積される文書データや利用済み文書データを不正に読み出す脅威に対しては、TOEのセキュリティ機能であるハードディスク蓄積データ暗号化機能とハードディスク蓄積データ上書き消去機能により対抗する。

ハードディスク蓄積データ暗号化機能は、システム管理者により「ハードディスク蓄積データ暗号化機能設定」が有効に設定されると、コピー機能、プリンター機能、スキャナー機能、及びネットワークスキャン機能の動作時に、内部ハードディスク装置に文書データを蓄積する際に、文書データの暗号化を行う。

例えば、同一原稿の複数部数のコピーが指示された場合、コピー対象として読み込まれた文書データは、MFDの内部ハードディスク装置に蓄積され、指定部数回、内部ハードディスク装置から読み出されて印刷される。この場合、上記のように読み込まれ、蓄積される文書データは暗号化され、さらに、内部ハードディスク装置から印刷のために読み出される度に復号される。印刷されて利用済みになった文書データは暗号化され、内部ハードディスク装置に蓄積される。

ハードディスク蓄積データ上書き消去機能は、システム管理者により「ハードディスク蓄積データ上書き消去機能設定」が有効に設定されると、コピー機能、プリンター機能、スキャナー機能、及びネットワークスキャン機能の各ジョブの完了後に、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に対して、内部ハードディスク装置の文書データ領域を上書きにより消去する。

なお、上記各ジョブの完了時には、利用済みになった文書データがハードディスク蓄積データ暗号化機能により暗号化された後、内部ハードディスク装置に蓄積されるため、暗号化された利用済み文書データに対して上書き消去を行うこととなる。

また、権限のない人にMFDの機能を使用され、文書データにアクセスされる脅威に対しては、許可されている一般利用者のみがMFDの機能を使用し、当該一般利用者の権限の範囲内でのみ文書データにアクセスが行われるように、ユーザー認証機能により、操作パネルまたは一般利用者クライアントからユーザIDとパスワードを入力させ、当該一般利用者の識別認証を行うことにより対抗する。

また、TOE設定データへの不正アクセスの脅威に対しては、システム管理者のみに特別な権限を持たせるために、ユーザー認証機能により、操作パネルまたはシステム管理者クライアントからシステム管理者IDとパスワードを入力させ、認証されたシステム管理者のみが、システム管理者セキュリティ管理機能により、TOEのセキュリティ機能に関する設定の参照と変更を行う権限を許可されることにより対抗する。

なお、カストマーエンジニア操作制限機能は、システム管理者により「カストマーエンジニア操作制限機能設定」が有効に設定されると、カストマーエンジニアがTOEのセキュリティ機能の設定の変更ができないように、カストマーエンジニアのシステム管理者モードへの操作を制限する機能であり、本機能も有効に設定し、TOE設定データへの不正アクセスの脅威に対抗する。

また、内部ネットワーク上に存在する文書データ、TOE設定データ、及びセキュリティ監査ログデータの盗聴や改ざんの脅威に対しては、内部ネットワークデータ保護機能により対抗する。

内部ネットワークデータ保護機能は、TOEとリモート（一般利用者クライアント、システム管理者クライアント、サーバ）間で暗号化通信プロトコル（IPSec、SSL/TLS等）により、セキュアなデータ通信を確立し、文書データ、TOE設定データ、及びセキュリティ監査ログデータといった通信データを盗聴や改ざんの脅威から保護する。

また、セキュリティ監査ログ機能により、すべてのTOE利用者に対して、いつ、誰がログインし、どのような作業を行ったかという事象や重要なイベント（設定変更、ユーザー操作等）を追跡記録し、不正アクセスへの対抗に使用する。セキュリティ監査ログデータの読み出しは、認証されたシステム管理者に限定される。なお、取得されたセキュリティ監査ログデータは、MFDの内部ハードディスク装置に蓄積される際に、TOEのハードディスク蓄積データ暗号化機能により暗号化され、保護される。

3 評価機関による評価実施及び結果

3.1 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ている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

3.2 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21年9月に始まり、平成22年2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21年12月に開発現場へ赴き、図面、記録、現物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21年12月及び平成22年2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。

3.3 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定に基づく侵入テストを実行した。

3.3.1 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。評価した開発者テストの概要を以下に示す。

1) 開発者テスト環境

開発者が実施したテストの構成を図3-1に示す。

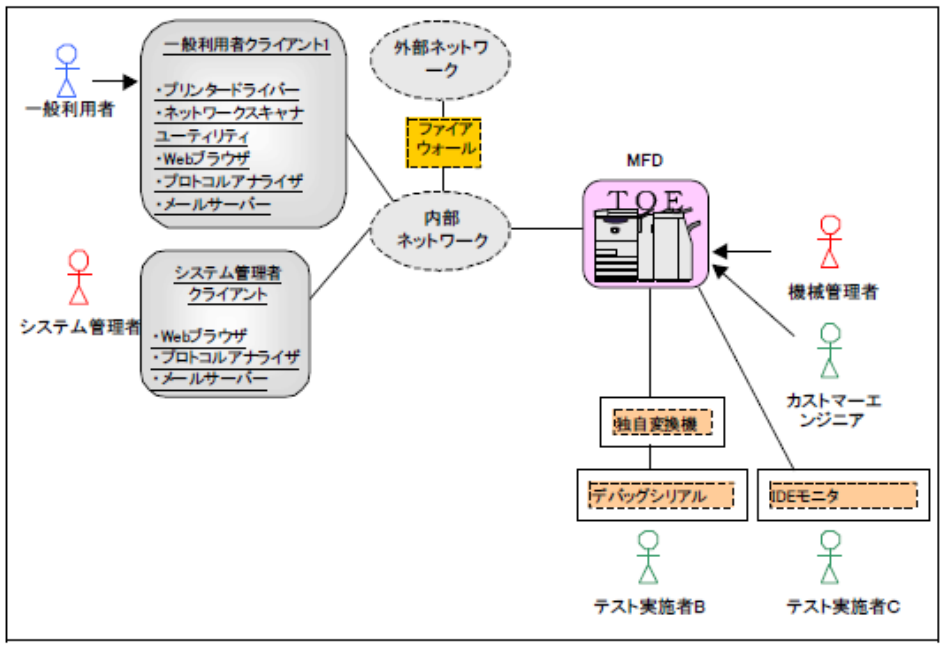

図3-1　開発者テストの構成

開発者テストは、STにおいて識別されているTOE構成（TOEを含むTOE利用のための構成）と同等のTOEテスト環境で実施されている。

本TOEは、Xerox 4112/4127 Copier/Printerの2機種であるが、セキュリティ機能が搭載されるコントローラソフトウェアは共通しており、本開発者テストではXerox 4127 Copier/Printerのみが使用された。

また、STでは利用者クライアント（一般利用者クライアント及びシステム管理者クライアント）のOSとして、Windows2000、WindowsXP、またはWindowsVistaをインストールすることが記載されているが、本開発者テストはWindowsXPがインストールされた利用者クライアントのみで実施された。

これは、TOEがOSの標準通信プロトコル機能の上にセキュリティ機能を実装し上記3つのOSは標準通信プロトコル機能が共通しているため、標準通信プロトコル機能とTOEのセキュリティ機能の連携について、WindowsXPでテストし確認できれば、他の2つのOSについても問題ないと判断されたためである。なお、他の2つのOSの標準通信プロトコル機能自体については、開発者として別途テストを実施しており、問題ないことが確認されている。

2) 開発者テスト概説

開発者の実施したテストは以下のとおり。

a. テスト概要

開発者テストで実施されたテストの概要は以下のとおり。

（1）TOEのシステム管理関連のTSFIには、MFDの操作パネル及びシステ

ム管理者クライアントのWebブラウザから、システム管理者として認証（TSFI使用）された後アクセスできる。また、一般利用者が操作パネルまたは一般利用者クライアント（プリンタードライバー等）からユーザー認証（TSFI使用）された後、TOEの一般機能を使用すると、自動的にTOEのセキュリティ機能（ハードディスク蓄積データ上書き消去機能等）が動作することとなる。上記の方法でTSFIにデータを入力する等の刺激を与え、TOEのセキュリティ機能をテストした。

（2）TOEのセキュリティ機能のテスト結果の観測のため、図3-1のデバッグシリアル、及びIDEモニタが使用された。デバッグシリアルは、MFDに独自変換機を介して接続され、ハードディスク蓄積データ上書き消去機能、及びハードディスク蓄積データ暗号化機能の実行によるハードディスク内の最終的なデータの状態を確認するために使用された。また、IDEモニタは、MFD内のコントローラボードとハードディスクの間のIDEバスに接続され、IDEバスを流れる通信データをモニタリングすることにより、ハードディスク蓄積データ上書き消去機能、及びハードディスク蓄積データ暗号化機能の実行による通信データの内容を確認するために使用された。

（3）ハードディスクのエラーを擬似的に発生させるために、HDD電源OFF用スイッチ付きの中継ケーブルをハードディスクに接続し、ハードディスクデータ上書き消去機能の動作エラーに関するテスト（電源OFFによる動作エラー後、電源ONにより、動作再開）を実施した。

（4）TOEの内部ネットワークデータ保護機能（IPSec等の暗号化プロトコル）のテスト結果の観測のため、内部ネットワーク上の通信パケットを確認するためのツールが使用された。

b. 実施テストの範囲

テストは開発者によって50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。

c. 結果

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

3.3.2 評価者独立テスト

評価者は、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることの再確認のための独立テストを実施した。評価者が実施した独立テストの概要を以下に示す。

1) 評価者独立テスト環境

評価者が実施したテストの構成は、図3-1に示した開発者テストの構成と同等である図3-2に示した構成である。評価者テストは、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。

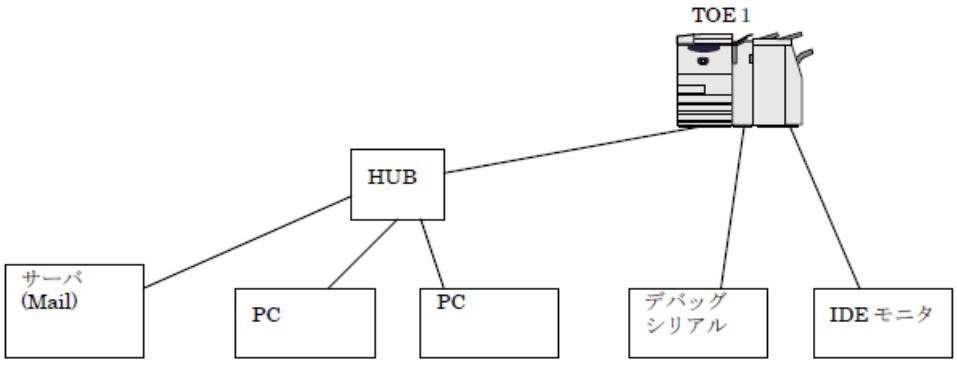

図3-2　評価者テストの構成

なお、本評価者テストは、TOEとしてXerox 4127 Copier/Printerのみ、クライアントPCにおけるOSとしてWindowsXPのみで実施されたが、STで識別されているすべての種類で実施していない妥当性の根拠は、開発者テスト（3.3.1 1)）記載のものと同一である。

2) 評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

a. 独立テストの観点

評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点での独立テストを考案した。

（1）開発者テストのサンプリングという観点では、開発者が実施したすべてのテスト項目をテストした。

（2）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、パラメタの限界値分析の観点で、6項目を独立テストとして取り上げた。

b. テスト概要

評価者が実施した独立テストの概要は以下のとおり。

（1）開発者テストのサンプリングテストにおいては、3.3.1 2) a.記載の開発者テストのテスト手法（デバッグシリアル、IDEモニタ等を使用）と同等のテスト手法により、テストを実施した。

（2）評価者独自テストとしては、ユーザー認証機能のインタフェースのパラメタ限界値分析として、システム管理者（機械管理者、SA）のIDやパスワードの入力、及びパスワードの変更に関する設定可能範囲外のデータ入力時のふるまい等の妥当性をテストした。

c. 結果

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

3.3.3 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の可能性について、必要と思われる侵入テストを考案し実施した。評価者侵入テストの概要を以下に示す。

1) 評価者侵入テスト概説

評価者の実施した侵入テストは以下のとおり。

a. 懸念される脆弱性

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

評価者は、探索した公知情報から本TOE運用における潜在的な脆弱性16件(Web経由でのクロスサイトスクリプティング、開放ポートによる不正侵入関係、SSL/TLS通信やIPSec通信の脆弱性、クライアントからの識別認証の迂回、不正実行可能ファイルのアップロード、リブート前パスワード残存)を、また、提供された証拠資料から本TOE運用における潜在的な脆弱性37件を識別し、悪用可能性を判定するために侵入テストが必要であると判断した。

証拠資料から識別された上記潜在的な脆弱性37件の概要を以下に示す。

*保守用ローカルインタフェースによる不正侵入関係

*TOE設定不適切や不正設定データ入力による非セキュア関係

*認証迂回（システム管理者クライアント、一般利用者クライアント）

*初期化プロセスへの侵入

*複数システム管理者の同時操作による非セキュア

*入力フォームへの不正入力関係（システム管理者クライアント、一般利用者クライアント）

*USBポートからの侵入関係

*CWISからのプリント要求インタフェースの不正使用

*操作パネルでの不正操作・設定関係

*CWISからの不正設定関係

*親展ボックスへの同時アクセスでの不整合

b. 実施テストの範囲

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

侵入テストは、上記a.で識別された53件の潜在的な脆弱性に対して、相互類似も考慮し、14項目としてまとめられ、詳細にテストされた。

主な侵入テストは以下のとおりである。

*MFDのLANポートからの不要なポート開放に関するポートスキャン調査

*USBポートからのTOE不正アクセス試行

*システム管理者クライアントのWebブラウザからの不正試行（ユーザ認証URLを記録し認証迂回、操作パネルや別のシステム管理者クライアントとの同時TOE設定操作、入力フォームにスクリプト等不正データ入力、パラメタ入力で制限を越えた種類・値を入力）

*TOE設定データ格納媒体のすり替え

*一般利用者クライアントのWebブラウザからの不正試行（URLを記録し認証迂回、プリント要求で不正プログラム混入、初期化処理中のTOEアクセス）

* SSL/TLSやIPSecの通信ネゴシエーション不成立時の非セキュア通信

c. 結果

実施した評価者侵入テストでは、想定する攻撃能力を超える潜在的な脆弱性は確認されなかった。

3.4 評価結果

3.4.1 評価結果

評価報告書をもって、評価者は本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。

3.4.2 評価者コメント/勧告

特になし。

4 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 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。
② 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。
③ 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は、特に存在しなかった。

5 結論

5.1 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。

5.2 注意事項

特になし。

6 用語

本報告書で使用されたCCに関する略語を以下に示す。

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

本報告書で使用されたTOEに関する略語を以下に示す。

CWIS	Centre Ware Internet Service（センターウェアインターネットサービス）
ADF	Auto Document Feeder（自動原稿送り装置）
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）。本報告書では、Xerox 4112/4127 Copier/Printerの2機種を指す。
PDL	Page Description Language（ページ記述言語）

本報告書で使用された用語の定義を以下に示す（順不同。左記用語を理解するための関連用語を含む）。

一般利用者	MFDのコピー機能、スキャナー機能、及びプリンター機能を利用する者。
機械管理者	MFDの機械管理やTOEセキュリティ機能の設定を行う管理者。
SA(System Administrator)	機械管理者から、MFDの機械管理やTOEセキュリティ機能の設定を許可された者。
システム管理者	MFDの機械管理やTOEセキュリティ機能の設定を行う管理者。機械管理者とSAの総称。
カストマーエンジニア	MFDの保守/修理を行うエンジニア。
攻撃者	悪意を持ってTOEを利用する者。
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。

一般利用者クライアント	一般利用者がMFDを利用するためのクライアント。
システム管理者クライアント	システム管理者が利用するクライアント。システム管理者はWebブラウザを使いMFDに対して、TOE設定データの確認や書き換えを行う。
利用者クライアント	一般利用者クライアントとシステム管理者クライアントの総称。
システム管理者モード	一般利用者がMFDの機能を利用する動作モードとは別に、システム管理者がTOEの使用環境に合わせて、TOE機器の動作設定やTOEセキュリティ機能設定の参照/更新といった、設定値の変更を行う動作モード。
センターウェアインターネットサービス（CWIS）	MFDのスキャナー機能によりスキャンして親展ボックスに格納された文書データを、取り出す機能を提供する。さらに、システム管理者に、Webブラウザを使いMFDに対して、TOE設定データの確認や書き換えを行う機能を提供する。
プリンタードライバー	一般利用者クライアント上のデータを、MFDが解釈可能なページ記述言語(PDL)で構成された印刷データに変換するソフトウェアで、一般利用者クライアントで使用。
ネットワークスキャナユーティリティ	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。
デコンポーズ機能	ページ記述言語(PDL)で構成された印刷データを解析し、ビットマップデータに変換する機能。
デコンポーズ	デコンポーズ機能により、ページ記述言語(PDL)で構成されたデータを解析し、ビットマップデータに変換すること。
プリンター機能	利用者クライアントから送信された印刷データをデコンポーズして印刷する機能。
プリンター制御機能	プリンター機能を実現するために装置を制御する機能。
コピー機能	操作パネルからの一般利用者の指示に従い、IITで原稿を読み込み、IOTより印刷を行う機能。 同一原稿の複数部のコピーが指示された場合、IITで読み込んだ文書データは、一旦MFDの内部ハードディスク装置に蓄積され、指定部数回、内部ハードディスク装置から読み出されて印刷される。
スキャナー機能	操作パネルからの一般利用者の指示に従い、IITで原稿を読み込み、MFDの内部ハードディスク装置に作られた親展ボックスに蓄積する。 蓄積された文書データは、一般的なWebブラウザを使用

	して、CWISやネットワークスキャナユーティリティの機能により取り出す。
ネットワークスキャン機能	操作パネルからの一般利用者の指示に従い、IITで原稿を読み込み後にMFDに設定されている情報に従って、FTPサーバ、SMBサーバ、Mailサーバへ文書データの送信を行う機能。
親展ボックス	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。スキャナー機能により読み込まれた文書データや親展ボックスを使った印刷のための文書データを蓄積することができる。
文書データ	一般利用者がMFDのコピー機能、プリンター機能、スキャナー機能を利用する際に、MFD内部を通過する全ての画像情報を含むデータを、総称して文書データと表記する。文書データには以下のようなものが含まれる。 *コピー機能を使用する際に、IITで読み込まれ、IOTで印刷されるビットマップデータ *プリンター機能を利用する際に、一般利用者クライアントから送信される印刷データ、及びそれをデコンポーズした結果作成されるビットマップデータ *スキャナー機能を利用する際に、IITから読み込まれ内部ハードディスク装置に蓄積されるビットマップデータ
利用済み文書データ	MFDの内部ハードディスク装置に蓄積された後、利用が終了しファイルとしては削除されたが、内部ハードディスク装置内には、データ部が残存している状態の文書データ。
TOE設定データ	TOEによって作成された、及びTOEに関して作成されたデータであり、TOEの動作に影響を与える可能性のあるもの。具体的には、内部ハードディスク蓄積データ上書き情報、ハードディスク暗号化情報、システム管理者情報、カストマーエンジニア操作制限情報、本体パネルからの認証時のパスワード使用情報、システム管理者IDとパスワード情報、システム管理者認証失敗によるアクセス拒否情報、内部ネットワークデータ保護情報、セキュリティ監査ログ情報、親展ボックス情報、ユーザー認証情報。
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、「いつ」「何(誰)が」、「どうした」、「その結果」という形式で時系列に記録したもの。

上書き消去	内部ハードディスク装置上に蓄積された文書データを削除する際に、そのデータ領域を特定データで上書きすること。
外部ネットワーク	TOEを管理する組織では管理ができない内部ネットワーク以外のネットワーク。
内部ネットワーク	TOEが設置される組織の内部にあり、MFDへアクセスが必要なリモートの高信頼なサーバやクライアントPCとMFD間のチャネル。

7 参照

[1] Xerox 4112/4127 Copier/Printer セキュリティターゲット バージョン 1.0.9 2010年1月27日 富士ゼロックス株式会社

[2] ITセキュリティ評価及び認証制度の基本規程 平成19年5月 独立行政法人 情報処理推進機構 CCS-01

[3] ITセキュリティ認証申請手続等に関する規程 平成19年5月 独立行政法人 情報処理推進機構 CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程 平成19年5月 独立行政法人 情報処理推進機構 CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 1 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 2 September 2007 CCMB-2007-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 2 September 2007 CCMB-2007-09-003

[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3.1 改訂第1版 2006年9月 CCMB-2006-09-001 (平成19年3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: セキュリティ機能コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-002 (平成20年3月翻訳第2.0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: セキュリティ保証コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-003 (平成20年3月翻訳第2.0版)

[11] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 3.1 Revision 2 September 2007 CCMB-2007-09-004

[12] 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2版 2007年9月 CCMB-2007-09-004 (平成20年3月翻訳第2.0版)

[13] Xerox 4112/4127 Copier/Printer 評価報告書 第1.2版 2010年2月10日 一般社団法人 ITセキュリティセンター 評価部