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

原紙押印済

評価対象

申請受付日（受付番号）	平成24年12月3日 (IT認証2437)
認証番号	C0402
認証申請者	理想科学工業株式会社
TOEの名称	【日本】RISO セキュリティパッケージ 【英語】RISO Security Package
TOEのバージョン	2.0
PP適合	なし
適合する保証パッケージ	EAL3
開発者	理想科学工業株式会社
評価機関の名称	株式会社 ECSEC Laboratory 評価センター

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25年8月20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3
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3

評価結果：合格

「【日本】RISO セキュリティパッケージ 【英語】 RISO Security Package」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

この認証報告書は、理想科学工業株式会社が開発した「【日本】RISO セキュリティパッケージ 【英語】RISO Security Package、バージョン 2.0」(以下「本 TOE」という。）について株式会社 ECSEC Laboratory 評価センター（以下「評価機関」という。）が平成 25 年 8 月 8 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理想科学工業株式会社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、市販される本 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、理想科学工業株式会社製のデジタル複合機（以下「MFP」という。）のためのデータ保護オプションソフトウェア製品である。

本 TOE を MFP にインストールすることにより、MFP 内の HDD に保存されたプリント機能とコピー機能が扱う文書データ（以下「文書データ」という。）を削除する際に上書き消去する機能と、それらの文書データを HDD に保存する際に暗号化する機能が追加される。

これらのセキュリティ機能により、廃棄あるいはリース・レンタル契約終了により返却された MFP から、プリント機能とコピー機能が扱う文書データが取り出されて漏えいすることを防止する。ただし、MFP のスキャン機能で生成する画像ファイル（以下「スキャンファイル」という。）に対しては、上書き消去や暗号化の機能は適用されない。

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 の保護資産であるプリント機能とコピー機能が扱う文書データは､廃棄あるいはリース・レンタル契約終了により返却された MFP から取り出されて漏えいする脅威がある。そのため TOE は、それらの文書データを削除する際には格納されている HDD 領域を上書き消去することで、HDD から文書データを復元することを防止するセキュリティ機能を提供する。

そのほかに、TOE は、一般的な調達者のニーズを想定し、HDD に格納する文書データを暗号化する機能も提供している。

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 を搭載した MFP は、物理的な不正なアクセスから保護された環境に設置されることを想定している。本 TOE を搭載することのできる MFP は、理想科学工業株式会社製の以下の機種である。

・日本国内向け

ORPHIS X7200/X7250/X7250A/X9050
ORPHIS EX7200/EX7250/EX7250A/EX9000/EX 9050/EX7200L

・海外向け

ComColor 3010/3010R/7010/7010R/3050/3050R/7050/7050R/9050/9050R
ComColor 3110/3110R/3150/3150R/7110/7110R/7150/7150R/9110/9110R/
9150/9150R/2150

1.1.3 免責事項

本 TOE の上書き消去や暗号化の機能は、以下のデータには適用されない。

- スキャン機能で生成するスキャンファイル
- プリント機能で､IPPやLPRなどのRAWポート以外の通信プロトコルを使用した場合の文書データ

また、本 TOE には、利用者パスワード等を管理する利用者管理機能が含まれているが、その機能は本評価による保証の対象ではない。

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 25 年 8 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]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。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。認証機関が指摘した問題点は、すべて解決され、かつ、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：	【日本】RISO セキュリティパッケージ 【英語】RISO Security Package
バージョン：	2.0
開発者：	理想科学工業株式会社

本 TOE は、以下のソフトウェア及びガイダンスから構成される。

表2-1 TOEの構成品

構成品名称	バージョン	説明
SNSO	1.0.4	TOEのソフトウェア
【日本】RISO セキュリティパッケージ 取扱説明書 セキュリティガイド 【英語】RISO Security Package Security Guide	050-36055-300 050-36056-306	TOEのガイダンス

(注)「SNSO」は TOE のソフトウェアの名称。TOE のソフトウェアは、RISO セキュリティパッケージのバージョン 1.0 とバージョン 2.0 で同一である。

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。

TOE のソフトウェアは、ガイダンスに記載された手順に従って、TOE を搭載した MFP パネルの画面にファームバージョンを表示させ、その内容を確認する。ファームバージョンが TOE のソフトウェアのバージョンである。

TOE のガイダンスは、表紙に記載された名称と部品番号を確認する。部品番号が、ガイダンスのバージョンである。

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、プリンタ機能、コピー機能、スキャン機能を提供する、理想科学工業株式会社製の MFP 用のデータ保護オプションソフトウェアである。

TOE のセキュリティ機能は、プリンタ機能とコピー機能が扱う文書データを削除する際に上書き消去することで、廃棄やリース返却された MFP からプリンタ機能とコピー機能が扱う文書データが漏えいすることを防止する。

また、TOE は調達者の一般的なニーズを想定して、プリンタ機能とコピー機能が扱う文書データを HDD に保存する際に暗号化する機能も提供する。

なお、本 TOE を搭載可能な MFP では、製品仕様として、スキャン機能で生成するスキャンファイルは不特定の利用者が取得可能である。そのため、本 TOE では、スキャンファイルは秘匿する必要はなく、本 TOE の保護対象ではないという考え方がされている。

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.REMOVE	＜HDDの取り出し＞ 悪意を持つ者が、廃棄されたMFP や、リース・レンタル契約終了により返却されたMFP からHDD を取り出し、HDD に残る文書データを漏洩する。

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.REMOVE」への対抗

本 TOE は、「残存データ上書き消去機能」と「利用者データ一括上書き消去機能」で本脅威に対抗する。

TOE の「残存データ上書き消去機能」は、MFP のプリント機能とコピー機能が終了または中止して文書データが不要になった時や、利用者がボックスに保存された文書データを削除指示した際に、文書データが保存されていた HDD の領域を自動的に上書きし、情報の再現を不可能にする。

TOE の「利用者データ一括上書き消去機能」は、MFP の管理者や保守員が一括削除を指示した際に、HDD に保存された文書データを一括消去する。消去の際には、文書データが保存されていた HDD の領域を上書きし、情報の再現を不可能にする。

なお、「残存データ上書き消去機能」「利用者データ一括上書き消去機能」のどちらの機能も、上書き消去中に MFP の電源が切れた場合は、次の電源投入時に自動的に上書き処理を再開する。

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。本セキュリティ方針は、本 TOE の対抗する脅威には直接は関与しないが、本 TOE の利用者が一般的に自らの組織に課すセキュリティ方針を開発者が想定したものである。

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
OSP.CRYPTO	文書データを、暗号化されていない状態でHDDに保存してはならない。

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「OSP.CRYPTO」への対応

本 TOE は、「HDD 保存データ暗号化／復号機能」で本方針を満足する。

TOE の「HDD 保存データ暗号化／復号機能」は、文書データを MFP に内蔵された HDD に書き込む際に暗号化を行い、それらの文書データを読み出す際に復号する。

使用する暗号アルゴリズムは、128bit の AES である。暗号鍵は、MFP の起動時に独自アルゴリズムで生成し、MFP の電源オフで消滅する。

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	＜信頼できる管理者＞ 管理者は、課せられた役割を遂行するための作業において、悪意を持った行為を行わない。
A.PORT	＜プリンタのポート＞ プリント機能の通信プロトコルはRAWポートを使用する。 （注）自分の文書データをTOEのセキュリティ機能で保護したい利用者は、プリンタドライバ等の設定でRAWポートを使用するように設定し、IPPやLPRなど他の通信プロトコルを使用してはならない。
A.ACCESS.MANAGED	＜設置場所＞ TOE を搭載したMFP は、悪意を持つ者による物理的なアクセスを制限できる、管理された環境に設置される。

4.2 運用環境と構成

本 TOE は、理想科学工業株式会社製 MFP のオプションソフトウェアである。本 TOE を搭載することのできる MFP 機種を以下に示す。

・日本国内向け

ORPHIS X7200/X7250/X7250A/X9050

ORPHIS EX7200/EX7250/EX7250A/EX9000/EX9050/EX7200L

・海外向け

ComColor 3010/3010R/7010/7010R/3050/3050R/7050/7050R/9050/9050R

ComColor 3110/3110R/3150/3150R/7110/7110R/7150/7150R/9110/9110R/9150/9150R/2150

本 TOE を搭載した MFP の一般的な運用環境を図 4-1 に示す。この構成は MFP 本体の利用形態に依存し、本 TOE を導入することに伴う追加の条件はない。

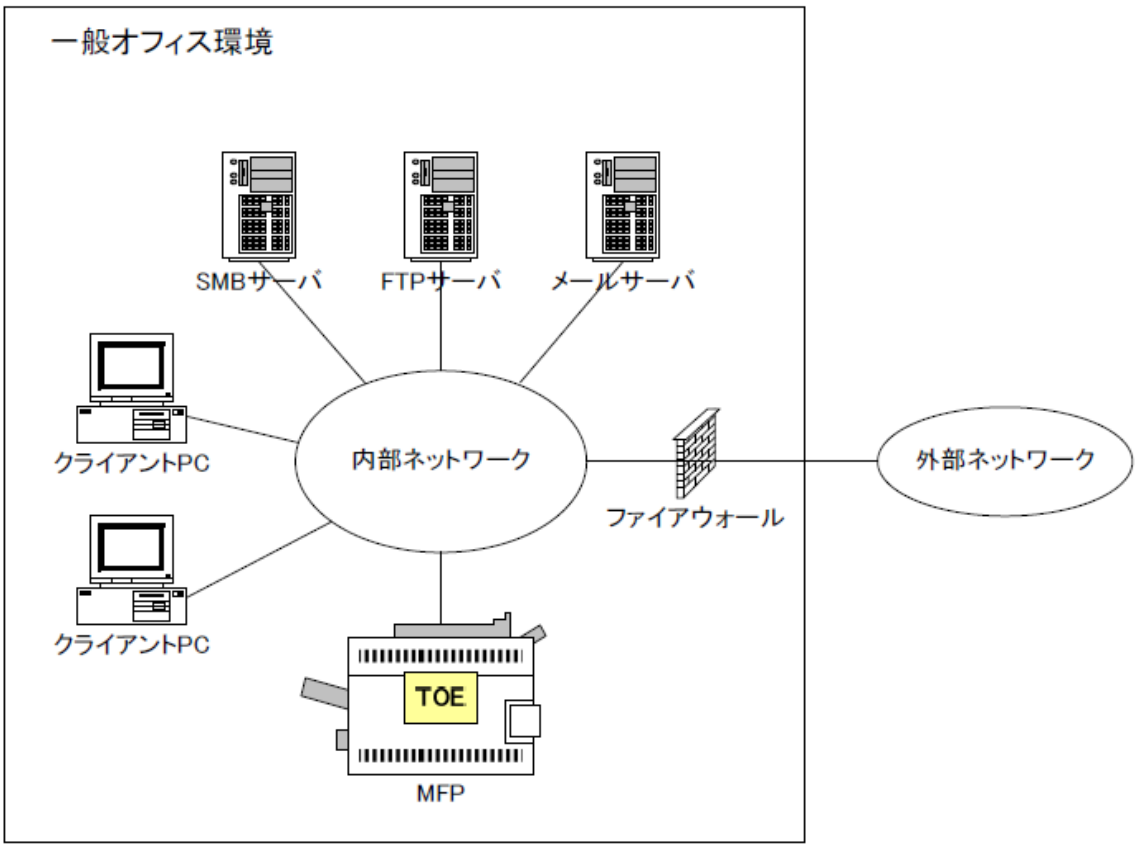

図4-1 TOEの運用環境

TOE の運用環境の構成品について以下に示す。

(1) クライアント PC

MFP 用のプリンタドライバを搭載し、MFP にプリントを要求する。また、MFP の設定やボックスに保存された文書データの操作を行うことができる。

(2) SMB サーバ、FTP サーバ、メールサーバ

MFP から送信されたスキャンファイルを受信、保存する。

なお、TOE を搭載する MFP や、本構成に示されている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 は、MFP のスキャン機能や、RAW ポート以外の通信プロトコルを使用した場合のプリント機能に対しては、上書き消去や暗号化の機能を適用しない。これらの制約条件の順守は利用者の責任となる。

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 は、本 TOE を搭載した MFP 内の主要な部分の構成及び MFP とネットワークで接続されたクライアント PC を示したものである。図 5-1 の中で、TOE は「残存データ上書き消去機能」「利用者データ一括上書き消去機能」「HDD 保存データ暗号化／復号機能」「利用者管理機能」を含む黄色の四角で囲まれた部分である。

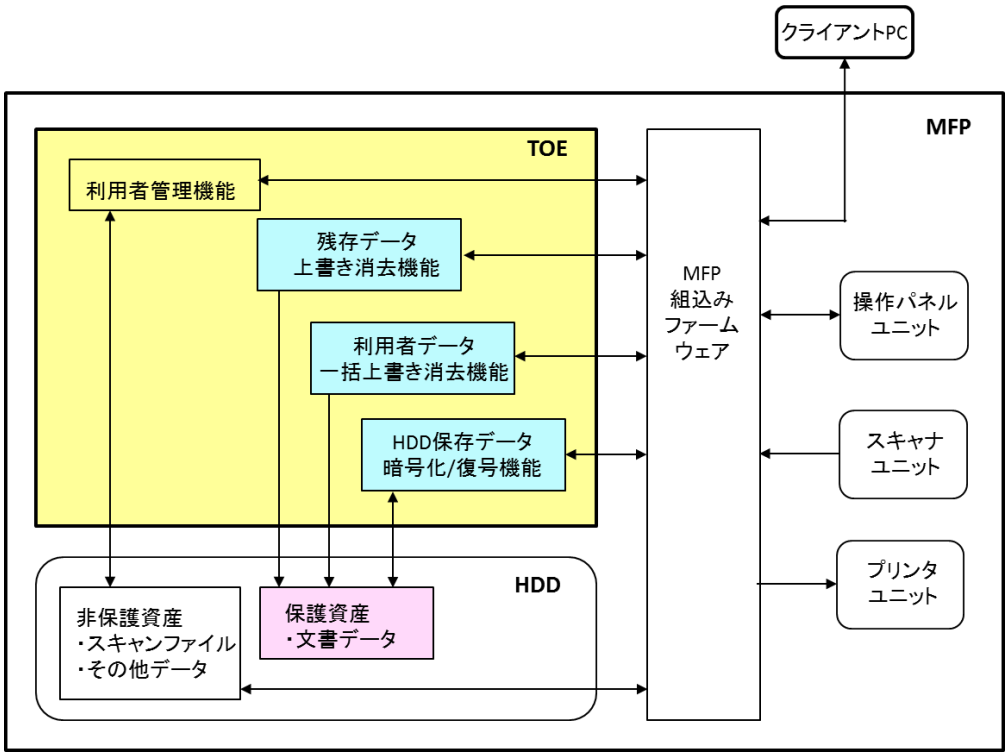

図5-1　TOE境界

「MFP 組込みファームウェア」は、MFP にあらかじめ組込まれている MFP 全体を制御するソフトウェアであり、TOE の機能は MFP 組込みファームウェアから呼び出されて動作する。TOE の機能と MFP 組込みファームウェアの関係を以下に示す。

(1) 残存データ上書き消去機能

本セキュリティ機能は、MFP のプリント機能やコピー機能の処理終了の際に、MFP 組込みファームウェアから呼び出されて、HDD 上の不要となった文書データを利用者が意識することなく自動的に上書き消去する。本セキュリティ機能が呼び出される場合を以下に示す。

・ プリントやコピーの処理が正常に終了した場合

・ プリントやコピーの処理がエラーにより異常終了した場合
・ プリントやコピーの処理が利用者によって取り消された場合
・ 利用者がボックスに保存された文書データを削除した場合

なお、本セキュリティ機能の実行中に MFP の電源が切れた場合には、次に MFP が起動した時に自動的に再開される。

(2) 利用者データ一括上書き消去機能

本セキュリティ機能は、管理者や保守員が MFP コマンドで指示した場合に、MFP 組込みファームウェアから呼び出されて、HDD に保存されたすべての文書データを上書き消去する。本セキュリティ機能が呼び出される場合を以下に示す。

・ 管理者が、MFPの「ユーザ情報を全て削除する」コマンドを実行した場合
・ 保守員が、MFPの「ファクトリーデフォルト」コマンドを実行した場合
・ 保守員が、MFPの「HDD初期化」コマンドを実行した場合

なお、本セキュリティ機能の実行中に MFP の電源が切れた場合には、次に MFP が起動した時に自動的に再開される。

(3) HDD 保存データ暗号化／復号機能

本セキュリティ機能は、MFP のプリント機能とコピー機能の処理中に文書データを HDD に読み書きする際に、MFP 組込みファームウェアから呼び出されて、文書データの暗号化と復号を行う。

(4) 利用者管理機能

本機能は、TOE の中に存在しているが、保護資産である文書データとは関係がなく、評価対象のセキュリティ機能には含まれていない。本機能は、利用者のログインやログアウトの際に、MFP 組込みファームウェアから呼び出されて、利用者パスワードの暗号化機能など、利用者情報の管理機能を提供する。

5.2 IT環境

本 TOE は、MFP に搭載されたオペレーティングシステム（以下「OS」という。）上で動作し、MFP 組込みファームウェアから呼び出されて動作する。ただし、図 5-1 では OS の記述は省略されている。

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。

【日本】RISO セキュリティパッケージ取扱説明書 セキュリティガイド
050-36055-300

【英語】RISO Security Package Security Guide
050-36056-306

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 24 年 12 月に始まり、平成 25 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 25 年 1 月、2 月及び同年 7 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 25 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。

また、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。

これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

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定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

開発者テストは、TOE の動作対象 MFP の代替えとしてシミュレーション環境を使用し、それに TOE を追加した構成で実施された。

開発者テストの対象の TOE は、2 章の TOE 識別と同一の TOE である。

開発者テストで使用したシミュレーション環境の構成を表 7-1 及び表 7-2 に示す。TOE を搭載可能な MFP は、ORPHIS X シリーズ（ComColor 30xx、70xx、90xx シリーズを含む）と ORPHIS EX シリーズ（ComColor 31xx、71xx、91xx シリーズを含む）の 2 つに分類することができる。開発者はそれぞれのシミュレーション環境でテストを実施している。

表7-1　TOEのテスト環境（ORPHIS Xシリーズ）

※対象MFP:
ORPHIS　X7200/X7250/X7250A/X9050
ComColor 3010/3010R/7010/7010R/3050/3050R/7050/7050R/9050/9050R

構成品	概要
MFPハードウェア	MFPを制御するCPUやメモリ等を含む回路基板。 ・ORPHIS Xシリーズ用コントロール基板（HDD含む） (注) 操作パネルユニットやプリンタユニット等は非搭載。
MFP用OS	MFPのコントロール基板上で動作するOS。 ・ORPHIS Xシリーズ用OS（2.6.18）
MFP組込みファームウェア	MFP全体の機能を制御するソフトウェア。 ・PMS 10.4.3
MFPハードウェアの一部の代替機能	ハードウェア非搭載部分の代替えソフトウェアと周辺装置。 ・エンジンシミュレータ 1.24 ・ディスプレイ、キーボード、マウス

表7-2　TOEのテスト環境（ORPHIS EXシリーズ）

※対象MFP:

ORPHIS　EX7200/EX7250/EX7250A/EX9000/EX9050/EX7200L

ComColor 3110/3110R/3150/3150R/7110/7110R/7150/7150R/9110/9110R/9150/9150R/2150

構成品	概要
MFPハードウェア	MFPを制御するCPUやメモリ等を含む回路基板。 ・ORPHIS EXシリーズ用コントロール基板（HDD含む） (注) 操作パネルユニットやプリンタユニット等は非搭載。
MFP用OS	MFPのコントロール基板上で動作するOS。 ・ORPHIS EXシリーズ用OS（2.6.32.26）
MFP組込みファームウェア	MFP全体の機能を制御するソフトウェア。 ・PMS 1.10.0
MFPハードウェアの一部の代替機能	ハードウェア非搭載部分の代替えソフトウェアと周辺装置。 ・エンジンシミュレータ 1.74 ・ディスプレイ、キーボード、マウス

評価者は、次のような評価により、TOE の動作対象 MFP の代替えとして、2 つのシミュレーション環境のテストで十分であると判断している。

- TOEはMFP用OS上で動作しており、ハードウェアを制御している部分は存在しない。そのため、MFP用OSが制御しているプリンタユニット等のハードウェアを代替機能で置き換えても、TOEのセキュリティ機能には影響しない。
- MFP用OS及びOSが動作するコントロール基板は、TOE動作対象のMFP機種に搭載されているものと同じである。
- TOEがMFP組込みファームウェアに提供しているインタフェースは、MFP組込みファームウェアに依存しない仕様になっている。

したがって、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とみなすことができる。

(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＞

インタフェースの応答で観測可能なふるまいについては、テストプログラムを用いて、インタフェースへの入力に対する出力を確認した。

インタフェースの応答で観測できないふるまいについては、以下のように、ツールを使用してデータを確認した。

① 上書き消去機能については、OS コマンドを用いて HDD のデータをダンプした。
② 暗号化機能については、OS コマンドを用いて暗号鍵や暗号化したデータの内容を表示し、別ツールで算出した暗号鍵や暗号化データと比較した。

＜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 7-3 に示す。

表7-3　開発者テストツール

ツール名称	概要・利用目的
test_MDL	開発者が作成したテストプログラム。インタフェースへのパラメタの入力とその応答の表示を行う。
openssl バージョン0.9.8c-4、 または、 バージョン1.0.0h	暗号アルゴリズムの検証に使用。当ツール及びTOEで暗号化したデータの比較を行う。 (注) ツールの2つのバージョンは、暗号アルゴリズムの処理は同じであり、テスト結果には影響しない。
各種OSコマンド	TOEのデータやHDD上のデータの表示等を行う。

＜開発者テストの実施内容＞

インタフェースに対して、各種入力に対する応答やツールで取得したデータ内容を表示させ、あらかじめ期待されたテスト計画書の値と比較し、一致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129項目実施された。カバレージ分析によって、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ル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を表 7-4 及び表 7-5 に示す。評価者は、開発者テストと同様のシミュレーション環境に加えて、MFP 実機を使用した。なお、シミュレーション環境やテストプログラムは、開発者テストに用いられたものを利用しているが、それらの仕様と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。

表7-4　独立テストの構成（ORPHIS Xシリーズ）

名称	概要
シミュレーション環境	表7-1のORPHIS Xシリーズ用開発者テスト環境と以下を除いて同じ。 ・ORPHIS Xシリーズ用スキャナユニットを追加。
MFP実機	シミュレーション環境の他に、以下のMFP機種を使用。 ・ORPHIS X7250
クライアントPC	シミュレーション環境に対して、ネットワークを介して、プリントを依頼する。 ・WindowsXP Pro SP2搭載PC ・ORPHIS Xシリーズプリンタドライバ Ver.4.30.02

表7-5　独立テストの構成（ORPHIS EXシリーズ）

名称	概要
シミュレーション環境	表7-2のORPHIS EXシリーズ用開発者テスト環境と以下を除いて同じ。 ・MFP組込みファームウェアは、PMS 4.34.0を使用。 ・ORPHIS EXシリーズ用スキャナユニットを追加。
MFP実機	シミュレーション環境に加えて、以下のMFP機種を使用。 ・ORPHIS EX 9050
クライアントPC	シミュレーション環境に対して、ネットワークを介して、プリントを依頼する。 ・Windows7搭載PC ・ORPHIS EXシリーズプリンタドライバ Ver.1.04.04

まず評価者は、MFP 実機を使用し、2 章の TOE 識別と同一の TOE を格納した媒体を用いて、インストールテスト等を実施した。評価者が使用した MFP 実機は、ORPHIS X7250 と ORPHIS EX 9050 である。評価者は、ORPHIS X シリーズと ORPHIS EX シリーズに含まれる機種はプリント機能等の処理速度が異なるだけで、機種の違いは TOE の機能に影響しないことから、両シリーズの代表機種をテストすることで問題ないと判断している。

次に評価者は、TOE をインストールした HDD を MFP 実機から取り外し、シミュレーション環境に取り付けてテストを実施した。評価者がテストしたシミュレーション環境の構成は、表 7-1 及び表 7-2 に示した開発者テストの構成と同様である。

開発者テスト環境に追加したスキャナユニットは、TOE の動作対象 MFP に搭載されるものと同じであり、テスト構成として妥当である。また、スキャナユニットの有無の違いは開発者テストの確認には影響を与えないことが評価されている。

ORPHIS EX シリーズ用のテスト構成では、MFP 組込みファームウェアのバージョンが評価者テストと開発者テストで違いがある。評価者は、TOE の設計仕様を分析し、TOE が提供しているインタフェースは、MFP 組込みファームウェアのバージョンの違いには影響しないと判断している。また、評価者が異なるバージョンをテストすることで、実際に影響がないことを確認することになる。

独立テストは、本 ST において識別されている TOE の構成と同じ環境で実施されたとみなすことができる。

(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 開発者テストでTOEのふるまいが確認されていないテスト条件が存在するため、パラメタ、初期条件、同時実行条件を変更したテストを行う。

② 開発者テストでTOEのふるまいの厳格な確認が不足しているテストが存在するため、確認項目を追加したテストを行う。

③ 開発者はTOEのインタフェースをテストプログラムから呼び出している。それに加えて、MFPの利用者向けインタフェースを刺激して、TOEのインタフェースが仕様どおりに呼び出されて動作することを確認する。

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リ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＞

シミュレーション環境において、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タを変更したテストを実施する。

シミュレーション環境において、MFPパネルに相当する部分の操作、MFPのスキャナユニットからの原稿読み取り操作、クライアントPCからのプリント依頼やボックス操作を行い、OSコマンド等を用いてTOE部分のふるまいを確認する。

＜独立テストツール＞

独立テストにおいて使用したツールは､表7-3に示した開発者テストツールと同じである。

＜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、20項目のサンプリングテストと、8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テスト内容を表7-6に示す。

表7-6　実施した独立テスト

項番	観点	テスト概要
1	観点①	暗号化処理中にパディングが発生するサイズの平文が、正しく暗号化・復号される事を確認する。
2	観点①	開発者テストとは異なる乱数シードを使用し、異なる暗号鍵が生成され、正しく暗号化・復号が実行される事を確認する。
3	観点①	異なるファイルに対する暗号化・復号・上書き削除を同時に実行して、正しく実行される事を確認する。
4	観点①	上書き削除の対象のファイルの中に多数の不連続な頁番号が存在している場合、全ての頁が正しく上書き削除される事を確認する。
5	観点①	一括上書き削除の対象のファイルの中に多数の不連続な頁番号が存在している場合、全ての頁が正しく上書き削除される事を確認する。
6	観点①	開発者がテストしてないファイル識別子が使われた場合に、正しく上書き削除されることを確認する。
7	観点②	ファイル名の変更を伴う処理において、ファイル名変更処理の途中でデータが複製されていないことを確認する。データが複製されると上書きされない可能性がある。
8	観点③	MFPの利用者インタフェースに相当するインタフェースを刺激して、TOEのセキュリティ機能が確実に呼び出されることを確認する。

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 評価対象外の MFP 組込みファームウェア部分の不具合等により、TOE 仕様上想定されていないジョブ ID やページ番号が使われると、上書き削除されない可能性がある。
② 同じファイル名を生成するような 2 つの暗号化処理が同時に行われ、大きなサイズの暗号化データを格納したファイルが、小さなサイズの暗号化データで上書きされると、ファイルが縮小してデータが切り捨てられ、上書き削除の対象とならないデータが生成される可能性がある。
③ 暗号鍵の乱数性が不十分な場合、暗号鍵を推定され、暗号化データを復号される可能性がある。
④ TOE が想定していない通信プロトコルが MFP に存在する場合、TOE 機能がバイパスされる可能性がある。
⑤ MFP の通信プロトコルに公知の脆弱性が存在する可能性がある。
⑥ TOE を実行するプロセスが異常終了してコアダンプが出力される場合、コアダンプから保護対象のデータが漏えいする可能性がある。
⑦ 暗号化処理中のファイルに上書き削除を要求すると、上書き削除が先に終了し、上書きされないデータが残存する可能性がある。

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検出するために、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テスト環境に、以下に示す侵入テスト用ツールを追加して使用した。

表 7-1　侵入テストで追加したツール

名称	概要・利用目的
評価者作成テストプログラム	TOE内の暗号鍵生成関数を、シードを変更しながら繰返し呼び出し、応答された暗号鍵をファイルに保存する。
nmap バージョン5.21、 または、 バージョン6.01	MFPのオープンポートを検出する。 (注) ツールの2つのバージョンは、オープンポート検出機能は同じであり、テスト結果には影響しない。

＜侵入テストの実施項目＞

懸念される脆弱性と対応する侵入テスト内容を表 7-2 に示す。

表 7-2　侵入テスト概要

項番	脆弱性	テスト概要
1	脆弱性①	上限を超えるジョブIDを指定した場合に、上書き削除されることを確認する。 (注) テストの結果、上書き削除は失敗し暗号化ファイルが残存する。しかし、残存した暗号化ファイルは、一括上書き削除を行うと上書き削除される。
2	脆弱性①	上限を超えるページ番号を指定した場合に、上書き削除されることを確認する。 (注) 項番1と同じ結果が得られた。
3	脆弱性②	同じファイル名を生成する暗号化処理を、ほぼ同時に連続して実行しても、先に実行したファイルが残され、上書きされていないことを確認する。 (注) 後から実行した方はエラーとなる。
4	脆弱性③	評価者テストプログラムを用いて128bitの暗号鍵を157個以上（20,000bit以上）生成し、生成された暗号鍵が統計的に十分な乱数になっていることを確認する。
5	脆弱性④⑤	MFP実機にポートスキャンを実施し、オープンポートが仕様どおりであり、MFPに侵入できないことを確認する。
6	脆弱性⑥	TOEを実行するプロセスを強制終了させてもコアダンプを出力しないことを確認する。
7	脆弱性⑦	暗号化処理中に上書き削除を要求しても、暗号化処理が終了した後に上書き削除が実行されることを確認する。

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 TOE のセキュリティ機能には設定項目は存在しないため、評価者の評価した TOE の構成は、運用環境で使用可能な構成と同じである。

なお、評価者は、表 7-1、表 7-2、表 7-4 及び表 7-5 に示したテスト構成を評価することで、TOE の動作対象として ST に示されたすべての MFP 機種に対して、TOE の動作が保証できると判断している。

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のみに適用される。

7.6 評価者コメント/勧告

本 TOE において、脅威に対抗するための機能は、「残存データ上書き消去機能」「利用者データ一括上書き消去機能」である点に注意が必要である。

そのため、以下の運用が必須であり、それらの運用をしなくても暗号化機能があるから安全であると誤解してはならない。

- MFP を廃棄やリース返却する際には、利用者データ一括上書き消去機能を実施すること。
- 故障等により HDD 交換の必要が生じた場合には、ガイダンスに従って、利用者自らまたは利用者が保守員に委託して、安全な方法で HDD を処分すること。

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 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 及び評価報告書において、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、本認証報告書を発行した。

8.1 認証結果

提出された評価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 の運用や評価範囲には、「1.1.3 免責事項」、「4.1 使用及び環境に関する前提条件」及び「7.6 評価者コメント/勧告」に記載した制約条件がある。それらの運用条件の順守や本評価で保証されていない機能の扱いは、TOE の利用者の責任となる。

本 TOE の導入を検討している調達者は、それらの制約条件が受け入れ可能かどうか注意する必要がある。

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。

RISO セキュリティパッケージ セキュリティターゲット, Version 1.04, 2013 年 7 月 29 日, 理想科学工業株式会社

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。

MFP	Multi Function Printer（デジタル複合機）

本報告書で使用された用語の定義を以下に示す。

MFP組込みファームウェア	MFPにあらかじめ搭載されているファームウェア。TOEは含まれていない。
コントロール基板	MFP全体を制御する回路基板。CPU、メモリ、HDD、入出力インタフェース等を搭載。
スキャナユニット	MFPの構成品であり、紙原稿を読み取りデジタルデータに変換する装置。
スキャンファイル	スキャン機能で生成したPDF・TIFF・JPEG形式のファイル。スキャンファイルは、MFPでプリントすることやボックスに保存することはできない。
操作パネルユニット	MFP の構成品であり、液晶ディスプレイ、LED、テンキー、ボタンなどを備えた、操作を行うための入出力装置。
プリンタユニット	MFPの構成品であり、画像データを紙媒体に印字する装置。
文書データ	プリンタ機能やコピー機能でMFP内に保存される画像データ。プリンタ機能やコピー機能でボックスに保存される画像データや、プリンタ機能やコピー機能の処理の都合で一時的にHDDに保存される画像データも含まれる。
ボックス	文書データを保存するためのMFP内の領域。利用者は、プリント機能やコピー機能の中で指示することにより文書データをボックスに保存しておき、その後、プリントしたり削除したりすることができる。

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24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25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 3, July 2009, CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003

[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3版, 2009年7月, CCMB-2009-07-001, (平成21年12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3版, 2009年7月, CCMB-2009-07-002, (平成21年12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3版, 2009年7月, CCMB-2009-07-003, (平成21年12月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

[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3版, 2009年7月, CCMB-2009-07-004, (平成21年12月, 翻訳第1.0版)

[12] RISO セキュリティパッケージ セキュリティターゲット, Version 1.04, 2013年7月29日, 理想科学工業株式会社

[13] 【日本】RISO セキュリティパッケージ 【英語】RISO Security Package 評価報告書, 第1.2版, 2013年8月8日, 株式会社 ECSEC Laboratory 評価センター