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8月7日** (IT**認証**9260)
認証番号	C0258
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**	1.0
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 電子商取引安全技術研究所　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22年6月17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

「【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、「【日本】RISO セキュリティパッケージ 【英語】RISO Security Package」（以下「本TOE」という。）について株式会社 電子商取引安全技術研究所　評価センター（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である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、市販される本TOEを購入する一般消費者を読者と想定している。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：　【日本】RISO セキュリティパッケージ
　　【英語】RISO Security Package
バージョン：　1.0
開発者：　理想科学工業株式会社

1.2.2 製品概要

RISO セキュリティパッケージである本 TOE は、理想科学工業株式会社が提供するデジタル複合機 ORPHIS X7200/X7250/X7250A/X9050（以上、日本国内向け）、ComColor 3010/3010R/7010/7010R/3050/3050R/7050/7050R/9050/9050R（以上、海外向け）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。（以下、上記のデジタル複合機を「MFP」という。）

本 TOE は、MFP に対して、MFP に内蔵されたハードディスク（HDD）に保存されたプリント機能とコピー機能が取り扱う画像データ及び一時画像データを削除する時に、このデータを再現できないように上書き消去する機能と、前記のデータをハードディスクに対して書き込みと読み出しを行う場合にこれを暗号化／復号する機能を提供する。本 TOE がインストールされた MFP は、MFP の利用者以外の者が、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 のハードディスクから、プリント機能とコピー機能が取り扱う画像データ及び一時画像データを取り出して、これに含まれる情報を不正に取得することを防ぐことができる。

ただし、スキャナユニットから読みこまれてスキャン機能が扱うデータは、本TOEによる保護の対象外である。

1.2.3 TOE範囲とセキュリティ機能

TOE の論理的な範囲を図 1-1 に示す。図 1-1 は、MFP の主要な部分の構成を示したものである。ただし、「クライアント PC」は MFP とネットワークで接続された利用者端末である。TOE は、図 1-1 の中の「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」を含む黄色の四角で囲まれた部分である。

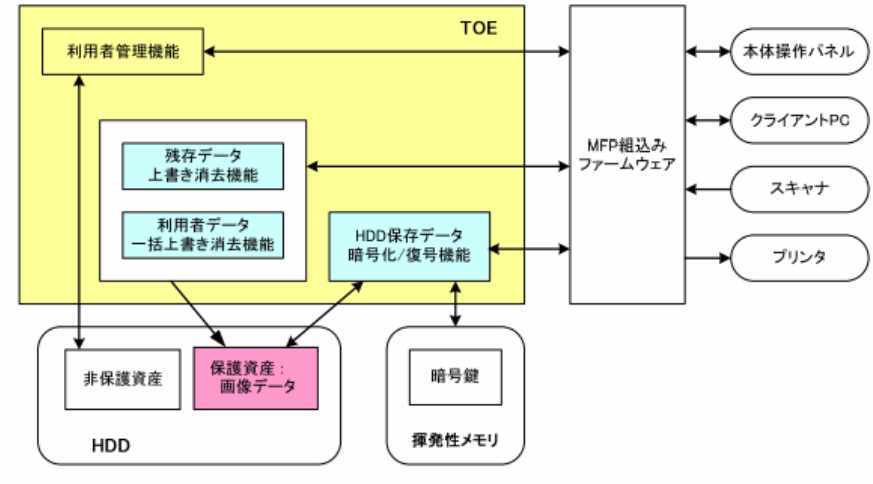

図1-1　TOEの範囲

MFP は、プリント機能、コピー機能、スキャン機能、ボックス保存機能などの基本機能を利用者に提供する。利用者が MFP の提供するインタフェースを操作して MFP の基本機能を使用すると、MFP の基本機能を実現する MFP 組込みファームウェア部分は、必要に応じて TOE の提供する機能を呼び出す。

本 TOE は、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 からハードディスクを取り出し、ハードディスクに残るプリント機能とコピー機能が取り扱う画像データ及び一時画像データを読み取ることによって、画像データに含まれる機密情報が取得される脅威を想定する。この脅威に対抗するために、MFP の基本機能が MFP に内蔵されたハードディスクから同データを削除する場合や読み書きする場合に 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」のセキュリティ機能を提供する。

また、本 TOE を運用する組織が保持する組織のセキュリティ方針としてハードディスク（HDD）に保存するデータを暗号化することを要求すると想定し、その方針を満たすために「HDD 保存データ暗号化／復号機能」を提供する。

図 1-1 にある「利用者管理機能」は、TOE の範囲に含まれているが、評価対象のセキュリティ機能ではなく、かつ、上記のセキュリティ機能にも関係しない。

TOE が提供するセキュリティ機能の概要を以下に示す。

1. 残存データ上書き消去機能

   MFP に内蔵されたハードディスクに保存されたプリント機能とコピー機能が取り扱う画像データ及び一時画像データが、不要になった時や利用者から削除指示があった時に、このデータが保存されていたハードディスク上の領域に値を上書きし、情報が再現できないように消去する機能。以下の場合に、上記の画像データ及び一時画像データに対して上書き消去が行われる。

   [自動的に残存データ上書き消去機能が実行される場合]
   - 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
   - 残存データ上書き消去機能の実行中にMFPの電源が切れ、次にMFPが起動した場合
   - 利用者がプリントやコピーの処理を取り消した場合

   [手動操作に伴って残存データ上書き消去機能が実行される場合]
   - 利用者が、ハードディスク上へ画像データを長期保存するための領域であるボックスに保存された画像データを、削除する要求操作を行った場合

2. 利用者データ一括上書き消去機能
   利用者から、MFP に内蔵されたハードディスクに保存されたプリント機能とコピー機能が取り扱う画像データ及び一時画像データの領域を一括削除する指示があった時に、このデータが保存されていたハードディスク上の領域に値を上書きし、情報が再現できないように消去する機能。以下の場合に、上記画像データ及び一時画像データに対して一括上書き消去が行われる。

   ・ 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

   上記の利用者の指示による利用者データ一括上書き消去機能の実行中に MFP の電源が切れた場合は、次に MFP が起動した時に、上記の処理が完了しなかった利用者データ一括上書き消去機能がもう一度、自動的に実行される。

3. HDD保存データ暗号化／復号機能
   プリント機能とコピー機能が取り扱う画像データや一時画像データをMFPに内蔵されたハードディスクに保存する場合、このデータを暗号化してから保存する機能。同様に、プリント機能とコピー機能がハードディスク上の暗号化された画像データや一時画像データを使用する場合、これを復号する機能。

なお、スキャン機能で生成した画像データ及び一時画像データは、TOE セキュリティ機能の対象としない。つまり、本 TOE はスキャン機能で生成した画像データ及び一時画像データに対し上書き消去と暗号化／復号を行わない。

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「ORPHIS X、ComColor シリーズ RISO セキュリティパッケージ 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、「【日本】RISO セキュリティパッケージ【英語】RISO Security Package バージョン1.0 評価報告書」（以下「評価報告書」という。）[12]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、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22年5月の評価機関による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。

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。

表2-1 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に残る画像データを漏洩する。

2.1.2 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針を表2-2に示す。

表2-2 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	暗号化されていない画像データや一時画像データを、HDDに保存してはならない。 （注） 本方針が対象としている画像データ及び一時画像データは秘匿性があると組織が認識したものである。つまり、本TOEでスキャンの対象となるデータは除外される。

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	＜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。

識別子	前提条件
A.PORT	＜プリンタドライバのポート＞ プリンタドライバの送信ポートは、RAWポートが使用される。 （注）クライアントPCからネットワークを経由してMFPへ送信されるプリント用の画像データは、MPFに搭載された理想科学工業社製のプログラムが受信し、処理しなければならない。上記のプログラムはRAWポートを使用するため、クライアントPCのプリンタドライバがプリント用の画像データをMFPのRAWポートへ送信するよう設定する。他の通信プロトコル（IPP: Internet Printing Protocol、LPR: Line PRinter daemon プロトコル）が使用する通信ポートへ送信するよう設定してはならない。
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。

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。TOEの管理者は、前提条件を満たすため、下記のドキュメントを十分に理解し、これを遵守することが要求される。なお、下記のドキュメントに記述されている一般利用者に関係する使用方法や注意事項の内容は、管理者から周知されることを意図している。

＜管理者向けドキュメント＞

- 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
  品番 050-36055-105 （※日本国内用の取扱説明書）
- RISO Security Package Security Guide
  品番 050-36056-101 （※海外用の取扱説明書）

2.1.5 構成条件

本 TOE は、MFP のオプションに位置づけられたソフトウェアである。本評価は以下のハードウェア及びソフトウェア上での動作を対象とする。なお、本構成に示されるハードウェア及びソフトウェアの信頼性は本評価の範囲外である。

- 理想科学工業株式会社が提供する日本国内向けのデジタル複合機
  ORPHIS X7200/X7250/X7250A/X9050
- 理想科学工業株式会社が提供する海外向けのデジタル複合機
  ComColor 3010/3010R/7010/7010R/3050/3050R/7050/7050R/9050/9050R

2.2 セキュリティ対策

TOEは、具備したセキュリティ機能により以下のように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。

1. 脅威「T.REMOVE」に対抗するセキュリティ機能

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 のハードディスクに残った画像データや一時画像データに含まれる機密情報を取得する脅威に対抗するために、TOE は、2 つの上書き消去機能、「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」を提供する。この 2 つの上書き消去機能は、ハードディスク上に保存されたプリント機能とコピー機能が取り扱う画像データ及び一時画像データが不要になった時点で、再現できないように上書き消去することによって、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 のハードディスクには上記のデータを存在させない。これにより、悪意を持つ者が MFP に内蔵されたハードディスクから機密情報を取り出すことを防止する。

TOE が提供する上書き消去機能の詳細を以下に示す。

1) 「残存データ上書き消去機能」

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によって自動的に同データの削除が要求された場合と、MFP の利用者の操作から同データの削除が要求された場合に、呼び出されて実行される。プリント機能やコピー機能の処理が終了するたびに、同機能が取り扱う画像データ及び一時画像データを逐次、上書き消去することによって、MFP に内蔵するハードディスク上に不要な画像データ及び一時画像データが存在しないようにする。ハードディスク上のボックスへ長期保存している画像データも、その画像データが不要になったときに、利用者がデータ消去をしたタイミングで残存データ上書き消去機能が呼び出され、上書き消去を実行する。

上書き消去の処理は、以下の手順にしたがって実行される。

- 暗号化や復号などの処理が削除対象ファイルを使用中の場合は、その処理が終了するまで待機する。
- ハードディスク上の削除対象ファイルの全ての領域を0x00で上書きする。
- ハードディスク上の削除対象ファイルの全ての領域を0xFFで上書きする。
- ハードディスク上の削除対象ファイルの全ての領域をランダム値で上書きする。

・ ランダム値が正しく書き込まれたことを確認（ベリファイ）する。
・ 削除対象ファイルを削除する。

上記の上書き消去の手順が全て終了する前に MFP の電源が切れた場合は、次に MFP の電源が投入された時に、自動的に再度、残存データ上書き消去機能を実行し、上書き消去をやり直す。

2) 「利用者データ一括上書き消去機能」

利用者データ一括上書き消去機能は、管理者や保守員が、MFP の表示パネルを操作して、MFP に内蔵されたハードディスクに保存されたプリント機能とコピー機能が取り扱う画像データ及び一時画像データを一括削除する命令を要求した場合に、呼び出されて実行される。これにより、MFP を廃棄したりリース・レンタル契約終了により返却したりするときには、一般利用者がボックスに保存し明示的に消去していない、プリント機能とコピー機能が取り扱う画像データ及び一時画像データは、すべて上書き消去される。

上書き消去の処理は、「残存データ上書き消去機能」に記述した手順と同じ手順で行われる。上書き消去の手順が全て終了する前に MFP の電源が切れた場合は、次に MFP の電源が投入された時に、自動的に再度、残存データ上書き消去機能を実行し、上書き消去をやり直す。管理者が MFP の廃棄前に利用者データ一括上書き消去機能を実行し、その途中で MFP の電源が切れた場合は、利用者データ一括上書き消去機能を再度実行するよう、指示がガイダンスに記述されている。

2. 組織のセキュリティ方針「OSP.CRYPTO」を実現するセキュリティ機能

本 TOE では、MFP の基本機能がプリント機能とコピー機能が取り扱う画像データや一時画像データをハードディスクに書き込む場合は必ず暗号化を行い、MFP の基本機能が、同様の画像データや一時画像データをハードディスクから読み出す場合は必ず復号することにより、組織のセキュリティ方針「OSP.CRYPTO」を満たしている。

TOE が提供する暗号化／復号機能の詳細を以下に示す。

1) 「HDD 保存データ暗号化／復号機能」

HDD 保存データ暗号化／復号機能は、プリント機能、コピー機能、ハードディスク上のボックスへ画像データを長期保存する機能（ボックス保存機能）が、プリント機能とコピー機能が取り扱う画像データ及び一時画像データをハードディスクへ書き込んだり、ハードディスクから読み出したりする際に、必ず呼び出されて

実行される。HDD 保存データ暗号化／復号機能は、暗号鍵長 128bit の AES 暗号アルゴリズムを使用する。TOE は、同データをハードディスクへ書き込む直前に暗号化を行い、そのデータをハードディスクから読み出した直後に復号を行う。これにより、同データは常に暗号化されてハードディスクへ保存され、暗号化されていない同データがハードディスクに保存されることはない。

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8月に始まり、平成22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21年10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22年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。

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

開発者テストは、MFPの実機のみの構成と、MFP本体のファームウェアが搭

載されたコントロール基板やエンジンシミュレータ（ソフトウェア）などを組み合わせたシミュレーション用の構成において、実施された。

MFP実機のみの構成では、TOEが搭載されるMFPとして、ORPHISX/ComColorシリーズX7250のみが選択されている。評価者は、以下の理由から、1機種だけのテストで問題ないと判断している。

RISO製のMFPORPHISX/ComColorシリーズ（ORPHIS X7200/X7250/X7250A/X9050, ComColor 3010/3010R/7010/7010R/3050/3050R/7050/7050R/9050/9050R）は、全て同一の機能仕様、上位設計を元に共通のMFP本体のファームウェアが開発・実装されている。そのため、ハードウェア構成が異なるが、コピー機能やプリント機能の処理速度が異なるだけであり、得られるテスト結果は同一である。

テストに使用したシミュレーション環境は、以下のとおりである。

- MFPの実機に実装されるハードディスクと同一のパーティション／ディレクトリ構造等を持つハードディスクを使用した。ハードディスクには、TOEの運用環境と同一のOSがインストールされている。上記のハードディスクをMFP本体のファームウェアが搭載されたコントロール基板に接続し、動作させる。
- シミュレーション環境のMFP本体のファームウェアには、MFPのハードウェアなしで動作できるようにエンジンシミュレータが組み込まれている。同ファームウェアは実機と異なるものの、ハードウェアの動作が直接にTOEのふるまいへ影響を及ぼす部分はないため、シミュレーション環境におけるTOEの動作は、TOEの運用環境におけるそれと一貫している。
- MFPの表示パネルは、タッチパネルではなく、ディスプレイ上へウィンドウとして表示される。タッチパネルへの手入力の代わりに、マウスでの入力が可能となっている。機能を代替しているのみであり、TOEの運用環境と一貫している。
- OSのコマンド等を入力するテストに使用するため、実機では無効化されているキーボードが有効化されている。

以上より、シミュレーション環境はTOEの運用環境を正しくシミュレートするため、TOEは、実機と同一のふるまいを行うことができる。よって、シミュレーション環境におけるテストから得られる結果は、実機のテスト結果と同一である。

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。

■ テスト手法について

TOEのセキュリティ機能のインタフェースの入力パラメタへ、あるジョブIDや頁番号などを入力し、パイプ名などの出力パラメタやインタフェースの戻り値が期待どおりに得られることを確認する。ただし、TOEは、MFP内にオプション機能としてインストールされるため、TOEの入出力インタフェースに対して、直接、値を入力する等のテストを行うことができない。そこで、開発者が作成したシミュレーション環境及びシミュレータを使用して、TOEに対してテストを実施した。

■ テスト環境、使用したツールについて

開発者がテストで使用した環境、ツールを表3-1、表3-2に示す。

表3-1：開発者テスト（MFP実機）のハードウェア／ソフトウェア構成

種別	仕様
ハードウェア	ORPHISX/ComColorシリーズX7250 型番：SE-H301　　製造番号：33200241
ソフトウェア	Linux Debian 4.0, kernelバージョン 2.6.18（OS）
	PMS バージョン10.4.3 （MFP本体ファームウェア)

表3-2：開発者テスト（シミュレーション）のハードウェア／ソフトウェア構成

種別	仕様
ハードウェア	ORPHISX/ComColorシリーズPMS基板
	HDD 型番：WD1600AAJS　　製造番号：WCAS2A274819
ソフトウェア	Linux Debian 4.0, kernel バージョン 2.6.18
	PMS バージョン10.4.3 （MFP 本体ファームウェア)
	エンジンシミュレータ バージョン 1.24
	test_MDL （開発者が作成したテスト用ドライバ）
	gdb バージョン 6.4.90-debian （TOEのふるまいの検証に使用するデバッガ）
	openssl バージョン 0.9.8c-4 （TOEの暗号化機能のふるまいの検証に使用するツールキット）

テスト用ドライバ「test_MDL」が、TOEのセキュリティ機能のインタフェースへ、テスト用のパラメタなどを元に生成した値を入力し、同インタフェースからの応答はテストドライバが受け取って画面に表示する。

■ テストの観点について

TOEのセキュリティ機能のインタフェースに対して、必要な入力パラメタを与えて機能を呼び出すテスト手法を採用した。テストの対象としたセキュリティ機能のインタフェースを以下に示す。

① 画像データの暗号化、一時画像データの暗号化
② 画像データの復号、一時画像データの復号
③ 画像ファイルの上書き消去、一時画像ファイルの上書き消去（ハードリンクの削除を含む）
④ 画像ファイルのコピー（実体をコピーするのではなく、ハードリンクを生成すること）
⑤ 暗号鍵生成
⑥ 上書き消去再開

上記のTOEのセキュリティ機能のインタフェース毎に、正常終了や異常終了となるようなパラメタの範囲や初期条件をテスト項目として作成する。開発者テストでは、作成したテスト項目について全数検査を実施した。

テスト結果をテスト用ドライバの表示等から直接観察できない場合は、代替手法を用いて間接的に確認する。主な代替手法は、以下のとおりである。

・ 暗号鍵生成
デバッガを用いて、生成された暗号鍵が保存されている変数の値を表示させる。
・ 画像データの暗号化
実績のあるオープンソースツールの暗号化結果と比較検証を行う。
・ 画像ファイルの上書き消去
上書き消去を実施するモジュールに組み込まれたデバッグ機能により、0x00、0xff、乱数の3回の上書き消去のそれぞれにおいて、一旦動作を停止させ、上書き消去対象ファイルが保存されたハードディスクのセクタをダンプする。

b. 実施テストの範囲

テストは開発者によって129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、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、開発者テストと同様の構成である。評価者テストは本STにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

なお、評価者テストも、TOEが搭載されるMFPとして、ORPHISX/ComColorシリーズX7250のみが選択されているが、「3.3.1 開発者テスト」に記載された理由から、問題ないと判断している。

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。

■ 開発者テストのサンプルを使用したテスト

TOEが、開発者がテストしたとおりにふるまうことの確信を得るために、サンプルテストを行う。開発者の実施したテスト129項目の中からテスト項目を抽出し、手動で実施する。評価者は、以下の方針に基づいて、サンプルテストのテスト項目を決定する。

① セキュリティ機能を保証する上で意味のない項目を除外する。
② 全てのSFRについて、SFR実施のふるまい１つにつき、少なくとも1

つテストをサンプルに含める。

③ 全てのTSFモジュールについて、１つのモジュールにつき、少なくとも1つのテストをサンプルに含める。

④ 全てのTSFIについて、1つのTSFIにつき、少なくとも1つテストをサンプルに含める。

⑤ 本TOEの最も複雑なふるまい「SFR実施TSFIのSFR実施のふるまい」のうち、より複雑な状況（初期条件や同時実行など）のテストをサンプルに含める。

⑥ TSFIを直接刺激できない場合の代替手段によるテストをサンプリング対象に含める。

⑦ 費用対効果の悪いテスト項目は除外する。

⑧ 開発者テスト 129項目の中からテスト項目をランダムに選び、上記の条件に当てはまるテスト項目が、開発者テストの40%程度のサンプリング率になるよう調整する。

以上の方針に基づいて、サンプリングテストのテスト項目を作成した。その結果、テスト項目は54項目となり、サンプリング率は41.9%となった。

■ 評価者が考案した独立テスト

TOEが、仕様のとおりにふるまうことの確信を得るためのテストである。評価者は、開発者がテストしていないパラメタ値や、開発者が厳密に確認していないふるまいについて、以下の方針に基づいて、独立テストのテスト項目を決定する。

① サンプリングテストのテスト項目のうち、パラメタや初期条件、同時実行条件を変えることによって、実装レベルで異なるふるまいが行なわれる可能性があるものを独立テストの項目とする。

② 開発者のテストにおいて、厳格さが不足しているテストを独立テストの項目とする。これらのテスト項目に関係するインタフェースは、厳密にテストする。

以上の方針に基づいて、独立テストのテスト項目を考案した。その結果、テスト項目は7項目となった。

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。

■ テスト手法について

テストの実施手法は、「3.3.1 開発者テスト」と同様に、TOEのセキュリティ機能のインタフェースへの入力と出力から確認する。独立テストに使用した環境、及びツールを以下に示す。テスト結果をテスト用ドライバの表示等から直接観察できない場合は、「3.3.1 開発者テスト」に記載された代替手法と同様の方法を用いて、間接的に確認する。

■ 独立テストで使用したツールについて

表3-2のツールに加えて、評価者が独立テストで使用した環境、ツールを表3-3に示す。

表3-3：独立テストで使用したツール等

ソフトウェア名称	備考
xdol	評価者が作成したテスト用ドライバ。 「RISO暗号鍵生成アルゴリズムを実行する関数」を、シードを変更しながら157回呼び出し、応答された暗号鍵をファイルに保存する。
Syslog バージョン1.4.1-18	TOEが呼び出された事を検証する代替手法に使用するOS機能

■ 独立テストの概要について

独立テストにおいて行ったサンプルテストの概要と、評価者が考案した独立テストの概要を以下に示す。

① 開発者テストのサンプルを使用したテスト

開発者テスト 129項目から、前記の「a. 独立テストの観点」に基づいて抽出したサンプルテストのテスト 54項目について、手動でテストを実施した。

② 評価者が考案した独立テスト

評価者が考案した以下の表3-4に示す7項目について、手動でテストを実施した。

表3-4：評価者が考案した独立テストの概要

No.	テストの概要
IND-01	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。

No.	テストの概要
IND-02	開発者テストとは異なる乱数シードを使用して、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。
IND-03	異なるファイルに対する暗号化／復号を同時に実行して、正しく暗号化／復号される事を確認する。
IND-05	残存データ上書き消去機能において、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消去される事を確認する。
IND-06	利用者データ一括上書き消去機能において、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消去される事を確認する。
IND-07	識別子”page”とは異なる識別子が使われた場合に、全ての一時画像ファイルが正しく上書き消去される事を確認する。
IND-08	ファイル名の変更を伴う画像ファイルの入れ替え処理の前後において、画像ファイルを保存したハードディスクの位置が変化しない事を確認する。

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。

① バックドアの設置
② 期待されていないジョブIDの指定
③ 期待されていない頁番号の指定
④ 識別されていないネットワークサービス用ポートの存在
⑤ TOEインストール判断のバイパス
⑥ コアダンプによる漏えい
⑦ 暗号化処理中の上書き消去処理要求

⑧ RISO暗号鍵生成アルゴリズムが生成する暗号鍵の乱数性
⑨ 暗号化処理中の暗号化処理要求

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。

■ 侵入テスト環境

評価者が実施したテストの構成は、開発者テストの構成に加えて、MFPとLAN接続された表3-5に示すクライアントPC及びツールを使用する。

表3-5：侵入テストのハードウェア／ソフトウェア構成

種別	仕様
ハードウェア	TOSHIBA Dynabook MNCD1PTN.004
ソフトウェア	Windows XP Pro SP2 **バージョン** 5.1.2600
	nmap バージョン 5.21 (ポートスキャンツール)

■ 懸念される脆弱性ごとのテスト概要

懸念される脆弱性ごとのテスト概要を表3-6に示す。

表3-6：懸念される脆弱性とテスト概要

識別子	テスト概要	懸念される脆弱性との対応
VAN-01	ジョブIDの上限許容値を超える値を入力し、上書き消去のバイパスを試みる。	② 期待されていないジョブIDの指定
VAN-02	頁番号の上限許容値を超える値が入力し、上書き消去のバイパスを試みる。	③ 期待されていない頁番号の指定
VAN-03	同一のジョブID・頁番号（・識別子）に対して、ほぼ同時に複数の暗号化を要求し、画像ファイルのサイズの切り捨てにより、上書き消去されないハードディスク領域の生成を試みる。	⑨ 暗号化処理中の暗号化処理要求
VAN-04	RISO暗号鍵生成アルゴリズムによって生成される暗号鍵の乱数性を確認する。	⑧ RISO暗号鍵生成アルゴリズムが生成する暗号鍵の乱数性
VAN-05	MFPにポートスキャンを実施し、OSに侵入を試みる。	① バックドアの設置 ④ 識別されていないネットワークサービス用ポートの存在

識別子	テスト概要	懸念される脆弱性との対応
VAN-06	TOEプロセスのコアダンプの出力を試みる。	⑥ コアダンプによる漏えい
VAN-08	暗号化実行中のジョブID・頁番号（・識別子）に対して上書き消去を要求し、ファイル後半部分の上書き動作のバイパスを試みる。	⑦ 暗号化処理中の上書き消去処理要求
VAN-10	MFPのユーザインタフェースを刺激して、セキュリティ機能を適用していないインタフェースを探索する。	⑤ TOEインストール判断のバイパス

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持つ攻撃者が悪用可能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

消費者に喚起すべき評価者勧告はとくにない。

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 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。

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。

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

- 本TOEが対処する脅威は、廃棄時のHDDからの情報漏洩である。MFP運用における利用者のログイン機能やアクセス制限機能、ボックス機能の共有については、本評価の対象に含まれていない。MFPの運用については、管理者や一般利用者は、MFPの基本機能のガイダンスや組織のセキュリティ担当者の指示に従い、適切な操作や管理を行う必要がある。
- 本TOEのセキュリティ機能が保護する資産は、プリント機能とコピー機能が取り扱う画像データ及び一時画像データのみであり、MFP内に保存されている利用者の認証等の情報や設定に関する情報、スキャン機能で生成した画像データ及び一時画像データは対象外である。

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）
SFR	Security Functional Requirement（セキュリティ機能要件）
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。

HDD	Hard Disk Drive（ハードディスクドライブ）
IPP	Internet Printing Protocol（標準的な印刷用プロトコル）
LAN	Local Area Network（内部ネットワーク）
LPR	Line PRinter daemon（UNIX系の印刷用サーバサービス）
MFP	Multiple Function Peripheral（デジタル複合機） プリント機能のほかに、コピー、スキャンなど複数の機能を 1 台に搭載した機器。
PC	Personal Computer（コンピュータ）
PMS	MFP本体のファームウェア名称

本報告書で使用された用語の定義を以下に示す。

RAWポート	プリンタドライバからMFPにデータを送信する通信ポートの 1 つ。プリンタドライバを標準設定でインストールした場合に選択されるポートである。
RISO暗号鍵生成アルゴリズム	理想科学工業社製の暗号鍵の生成方式
コアダンプ	プログラムが異常終了した場合に、使用中のメモリの内容をそのまま記録したファイル。特定のプロセスのメモリイメージ（あるいはその一部）やレジスタの内容などの情報が格納されている。
サムネイル画像	印刷されるページの見本画像
シード	乱数シード、乱数種、ランダム・シード(Random seed)。擬似乱数生成の元となる値

ジョブID	MFPが実行する仕事（プリント、コピー、スキャン）の処理単位に割り当てられた番号。
ネットワークサービス	WebサーバやFTPサーバなどのネットワークを経由して通信を用いて利用するサービス
ハードリンク	コンピュータのファイルシステム上のファイルやディレクトリ等の資源とその資源につけられた名前の結びつける仕組み。名前を持つファイルは少なくともひとつのハードリンクを持っている。ファイルは複数のハードリンクを持つこともある。
バックドア	制限や認証、許可などの正規の手続きを踏まずにコンピュータ内部に入り、利用することが可能な、あらかじめコンピュータ内に設けられた接続機能
パディング	データを固定長として扱いたいときに、短いデータの前や後に無意味なデータを追加して長さを合わせる処理
ボックス	利用者がプリンタ出力用の画像ファイルをMFPに内蔵されたハードディスクに保管できる仮想的に区分けされた保存場所。
一時画像データ	コピー機能の実行中にMFP内部で一時的に生成される二次元画像データ。
一般利用者	MFPのプリント機能、コピー機能、スキャン機能などの基本機能を利用する者。
画像データ	二次元画像データ部分の総称。サムネイル画像や、ボックスに保存されたデータも含む。
管理者	MFPの運用管理を行う者。
平文データ	暗号化されていないデータ
保守員	MFPの設置・保守を行う者。通常は、理想科学工業株式会社もしくはMFPの保守を委託されている企業の技術者。
乱数シード	上記の「シード」の項目を参照。
利用者	MFPの使用を許可され、使用する者。操作可能な機能により、一般利用者、管理者に分類される。

7 参照

[1] ORPHIS X、ComColor シリーズ RISO セキュリティターゲット バージョン 1.07 2010年4月10日 理想科学工業株式会社

[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] 【日本】RISO セキュリティパッケージ【英語】RISO Security Package バージョン1.0 評価報告書 第2.1版 2010年5月31日 株式会社 電子商取引安全技術研究所 評価センター