認 証 報 告 書

独立行政法人情報処理推進機構
理事長　富田 達夫

原紙押印済

評価対象

申請受付日（受付番号）	平成27年3月5日 (IT認証5536)
認証番号	C0498
認証申請者	株式会社リコー
TOEの名称	日本版名称：セキュリティカード タイプM19 海外版名称：DataOverwriteSecurity Unit Type M19
TOEのバージョン	1.02
PP適合	なし
適合する保証パッケージ	EAL2
開発者	株式会社リコー
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28年3月9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

「日本版名称：セキュリティカード タイプM19, 海外版名称：DataOverwriteSecurity Unit Type M19」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 2
2　TOE識別 3
3　セキュリティ方針 4
3.1　セキュリティ機能方針 4
3.1.1　脅威とセキュリティ機能方針 4
3.1.1.1　脅威 4
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 4
3.1.2.1　組織のセキュリティ方針 4
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 4
4　前提条件と評価範囲の明確化 6
4.1　使用及び環境に関する前提条件 6
4.2　運用環境と構成 6
4.3　運用環境におけるTOE範囲 6
5　アーキテクチャに関する情報 7
5.1　TOE境界とコンポーネント構成 7
5.2　IT環境 8
6　製品添付ドキュメント 9
7　評価機関による評価実施及び結果 10
7.1　評価機関 10
7.2　評価方法 10
7.3　評価実施概要 10
7.4　製品テスト 11
7.4.1　開発者テスト 11
7.4.2　評価者独立テスト 13
7.4.3　評価者侵入テスト 14
7.5　評価構成について 15
7.6　評価結果 15
7.7　評価者コメント/勧告 16

8　認証実施 17
8.1　認証結果 17
8.2　注意事項 17
9　附属書 18
10　セキュリティターゲット 18
11　用語 19
12　参照 20

1 全体要約

この認証報告書は、株式会社リコーが開発した「日本版名称：セキュリティカード タイプ M19, 海外版名称 : DataOverwriteSecurity Unit Type M19 バージョン 1.02」（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 28 年 3 月に完了した 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株式会社リコー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、本書とともに提供され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、EAL2 である。

1.1.2 TOEとセキュリティ機能性

本 TOE は、MFP をより安全に使用するためのオプションキットであり、その実態は MFP 内で動作するソフトウェアである。本 TOE は SD メモリカードに記録された状態で配付される。SD メモリカードを MFP に搭載した状態で MFP を動作させることにより、本 TOE は MFP により読み込まれて動作する。

本 TOE は、MFP から指定された HDD 上の領域を上書き消去する。

本 TOE を搭載可能な MFP は、本 TOE と同様の上書き消去の機能を持つ。本 TOE を搭載することで、MFP は自身の上書き消去の機能は使わずに本 TOE の上書き消去の機能を使う。そのことにより、評価により保証された上書き消去の機能が動作しているという信頼が得られる。

こ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 は脅威を想定しない。本 TOE は、セキュリティ機能として、MFP から指示された HDD 上の領域を上書き消去する機能を持つ。この機能は、MFP を利用する際の調達者の要求を満足するためのものである。

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、MFP に搭載された状態で運用される。対象となる MFP は「4.2 運用環境と構成」参照。

本 TOE は、MFP の動作中に MFP への電源の供給が途絶えることのないような環境で運用されることを想定する。

1.1.3 免責事項

MFP の指示の通りに HDD の領域を上書き消去する機能のみが保証の対象である。MFP の指示が適切かどうかは保証の対象外である。

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 28 年 3 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。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： 日本版名称：セキュリティカード タイプM19
海外版名称：DataOverwriteSecurity Unit Type M19
バージョン： 1.02
開発者： 株式会社リコー

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。

ガイダンスに記載された手順に従って MFP を操作して、画面に表示された名称とバージョンがガイダンスで示されているものと一致することを確認する。

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。

本 TOE は、MFP から指定された HDD 上の領域を上書き消去する機能を持つ。この機能により、MFP が指定した HDD 上の領域に存在するデータの漏洩を防止する。

3.1 セキュリティ機能方針

TOE は、脅威は想定せず、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、脅威を想定しない。

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 3-1 に示す。

表3-1　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.UNREADABLE	TOEはMFPから指示されたHDD上の領域の情報を読み取れないようにしなければならない。 この方針は、MFPを運用する調達者が要求すると考えられる要件から導かれる。

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 3-1 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.UNREADABLE」への対応

本 TOE は、MFP から指示された HDD 上の領域を上書き消去する機能を持つ。この機能により、P.UNREADABLE は実現される。

この機能において、以下の上書きの方式を指定できる。ただし、TOE 外の機能である MFP の HDD に書き込むデータを暗号化する機能の影響により、指定した上書きの方式に準拠しない場合がある。(「8.2 注意事項」参照)

- NSA 方式
  NSA 方式は以下の手順でデータを上書きする。
  - 乱数2回上書き
  - Null(0) 1回上書き
- DoD 方式
  DoD 方式は以下の手順でデータを上書きする。
  - 固定値1回上書き
  - 上記の固定値の補数1回上書き
  - 乱数1回上書き
  - HDDの内容を読み込んで、正しく上書きされたかを検証
- 乱数書込み方式
  乱数を指定された回数(1~9 回)上書きする。
- BSI/VSITR 方式
  0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA の順番で 7 回上書きする。

(注) 「一括消去機能」(「5.1 TOE 境界とコンポーネント構成」参照)を使用する場合のみ指定可能。

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.MODE.AUTOMATIC	TOEが逐次消去による上書き消去を完了する前に、MFPの電源の切断によりTOEの動作が中断されることはないものとする。 逐次消去とは、MFPのHDD上に不要なデータが発生する度にその領域の上書きをTOEに指示することである。
A.MODE.MANUAL	TOEの一括消去が完了する前に、利用者の意図に反して、一時停止ボタン操作やMFPの電源の切断により一括消去が一時停止されることはないものとする。 一括消去とは、MFPがHDDの全領域の上書きをTOEに指示することである。
A.MFP	TOEを搭載するMFPは、正しくセットアップされ、故障が発生していない状態で運用されるものとする。

4.2 運用環境と構成

本 TOE は「RICOH MP CW2201/CW1201 シリーズ」のいずれかの MFP に搭載されて運用される。

なお、MFP の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(TOE の範囲外)の指示の通りに HDD の領域を上書き消去する。MFP(TOE の範囲外)の指示には、HDD の領域の特定も含まれる。

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（サブシステム）を説明する。

5.1 TOE境界とコンポーネント構成

TOE の構成を図 5-1 に示す。

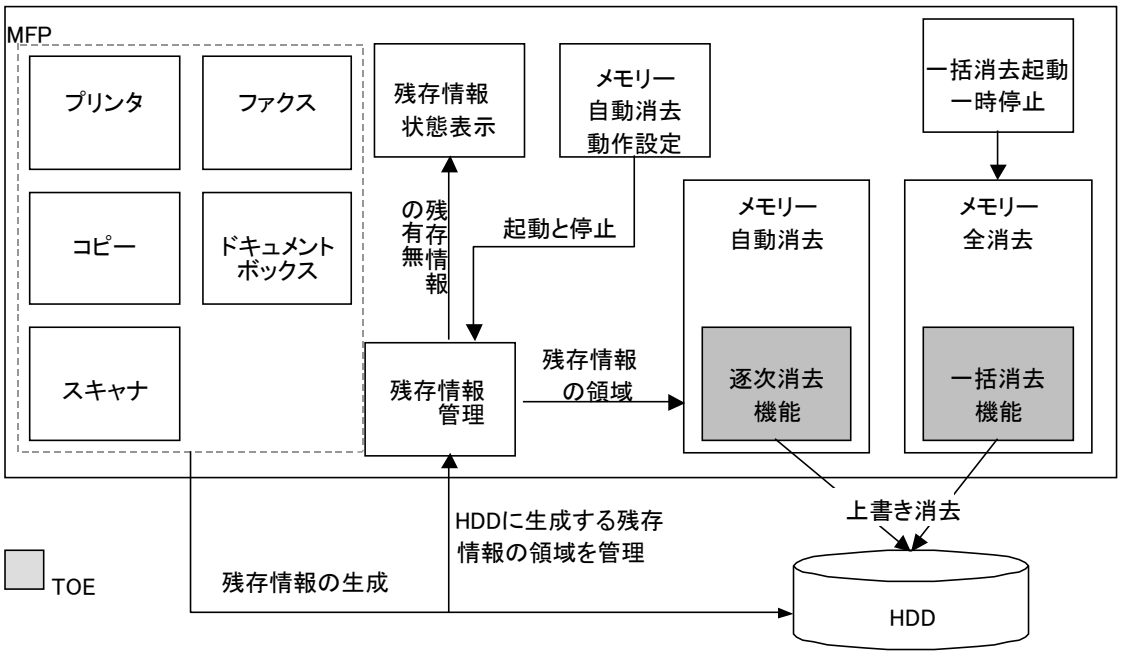

図5-1　TOEの構成と動作環境

TOE を構成するコンポーネントである、逐次消去機能、一括消去機能について説明する。

- 逐次消去機能

  MFPの「残存データ管理」からHDD上の残存データの領域の上書き消去の指示を受けると、その領域に対して上書き消去を実施する。

- 一括消去機能

  MFPの「一括消去起動・一時停止」から一括消去起動の指示を受けると、HDDの全領域の上書き消去を実施する。MFPからの指示で一時停止することも可能。

5.2 IT環境

本 TOE は MFP 内で動作する。MFP 内では、本 TOE の他に MFP を制御するソフトウェアが動作しており、本 TOE は MFP を制御するソフトウェアからの指示で動作する。

- 残存データ管理

  HDD上の残存データが存在する領域を管理する機能。MFPの機能の利用により発生したHDD上の残存データはこの「残存データ管理」に通知され、「残存データ管理」からTOEの「逐次消去機能」に上書きの指示をする。

  「残存データ」は、以下のようなデータである。

  - MFPはコピー、プリンタ、スキャナ、ファクス、及びドキュメントボックスの機能を提供する。MFPは、これらの機能を実行する際に、ドキュメントの全部あるいは一部の情報を含む一時的な作業用データを、HDD上に作成する。これらの機能が終了し、不要になった一時的な作業用データは、「残存データ」となる。
  - MFPはドキュメントボックスの機能によりHDD上にドキュメントを蓄積することができる。利用者がMFPに対して蓄積されたドキュメントを削除することを指示した場合、削除の対象となったドキュメントは「残存データ」となる。

- メモリー自動消去動作設定

  「残存データ管理」による上書きの指示をするかしないかの設定をする。

- 一括消去起動・一時停止

  TOEの「一括消去機能」に対し、起動または一時停止の指示をする。

- 残存データ状態表示

  MFPの操作パネルに残存データ状態を表わすアイコンを表示する機能。残存データ状態アイコンは、残存データの有無と上書き消去中の3種類の状態を表わす。

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。

日本語版のドキュメント

- セキュリティカード タイプM19 使用説明書 D3BS-7000

英語版のドキュメント

- DataOverwriteSecurity Unit Type M19 Operating Instructions D3BS-7002

7 評価機関による評価実施及び結果

7.1 評価機関

評価を実施した株式会社 ECSEC Laboratory 評価センターは、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）と相互承認している認定機関（独立行政法人評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

7.2 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。

7.3 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 27 年 3 月に始まり、平成 28 年 3 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 27 年 10 月及び平成 28 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 27 年 10 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。

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。

7.4 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・追加テストを実行した。脆弱性評定の結果、侵入テストは必要ないと判断された。

7.4.1 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、以下の MFP に TOE を設置して実施された。

- RICOH MP CW2201 (システムバージョン 0.20)

また、テストの操作や結果の観察のために以下のテストツールが用いられた。

- テスト用 PC

  RS232C またはイーサネット経由にて MFP と接続されるターミナルソフトウェアを使用

- SATA プロトコルアナライザ

  Catalyst Enterprises, Inc. 製 ST2-31-4-A(DE)

- その他

  MFP をブートモードで起動するためのブートサーバ、メール送信機能使用時のメールサーバ

TOE の動作環境である MFP としては、ST において識別されている MFP のうちの特定の機種の特定のバージョンが用いられた。ST において識別されている MFP の TOE と関係する部分の動作は機種やバージョンによらず共通であるという理由により、ST において識別されている MFP と同等の環境でテストが実施されたことが評価者により判断された。

したがって、開発者テストは 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たとみなせる。

(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＞

テストにおける TSFI の刺激及び観察には以下の手法が用いられた。「テスト用の TOE」と「OS の動作を観察できるようなモードにした MFP」については、TOE の動作確認に適していることが評価者により確認されている。

- MFP の操作パネルからの操作及びパネルへの表示の確認。
- ログを出力する機能を追加したテスト用の TOE、OS の動作を観察できるようなモードにした MFP を使い、MFP に接続されたテスト用 PC から TOE や MFP の OS の動作を確認。
- SATA プロトコルアナライザによる HDD とのインタフェースをモニタ。

(補足) 開発者テスト環境のブートサーバとメールサーバについて。
ブートサーバは、MFP を OS の動作を観察できるようなモードにするために使われた。
メールサーバは、MFP の操作により MFP からメールが送信されるようなテストがあるために用意された。

＜開発者テストの実施内容＞

TSFI の刺激は MFP の操作により行われた。MFP の操作は、各 TSFI のパラメタを網羅するように行われた。

テスト用 PC から TOE や MFP の OS の動作を確認することにより、意図したパラメタの通りに TOE が動作していることが確認された。また、実際に正しく上書きをしているかどうかが SATA プロトコルアナライザによるモニタリングにより確認された。

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57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ているかどうかが検証された。その結果、セキュリティ機能の動作に関係する一部のパラメタについてはテストの十分性に疑問があることがわかり、評価者独立テストにより補われた。

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。

7.4.2 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

評価者が実施したテストの構成は、MFP として以下のものが使われた以外は、開発者テストと同様の構成である。MFP が開発者テストの構成と異なることが TOE のテストに影響しないことは評価者により判断された。

- RICOH MP CW1201 (システムバージョン 0.22)
- RICOH MP CW2201 (システムバージョン 0.22)

テストツールとして開発者テストで使われたテストツールと同様のものが使われたが、テストツールの動作確認は評価者によって実施されている。

(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 開発者テストのサンプリングに関しては、すべてのセキュリティ機能とインタフェースが対象となることを考慮し、十分な量のテストを選択する。

② パラメタの網羅性やインタフェースを使用するタイミングの観点で開発者テストの十分性に懸念がある場合、それを補うためのテストを独自に考案する。

b) 独立テスト概要

評価者が実施した独立テストの概要は以下のとおりである。

＜独立テスト手法＞

開発者テストと同じ手法で実施した。

＜独立テストツール＞

開発者テストと同じツールを用いた。

＜独立テストの実施内容＞

独立テストの観点とそれに対応したテスト内容を表 7-1 に示す。

表7-1 実施した独立テスト

観点	テスト概要
①	開発者が実施したテスト項目から、テストの観点に基づいてテスト項目を抽出して開発者と同じテストを実施し、開発者と同じ結果が得られることを確認する。実施したテストは19項目である。
②	逐次消去の実行中に上書きの方式を変更した場合に、期待通りの方式で上書き消去がされることを確認する。
②	同時に複数の逐次消去を実施した場合に、複数の対象が上書き消去されることを確認する。
②	逐次消去・一括消去において、開発者テストでは上書きの回数のパラメタが十分にテストされたか懸念がある。そのため、上書きの回数を開発者テストとは異なる値にして、期待通りの回数で上書き消去が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。

7.4.3 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が存在するかどうかの分析を実施した。

分析の結果、以下のような理由で評価者は本 TOE の範囲においてはそのような脆弱性はないということを結論付けた。そのため、評価者侵入テストは不要であった。

- 本 TOE が MFP 内のソフトウェアであり、MFP の機能の利用に伴い間接的に動作するものであるといった使用環境である。

- そのような使用環境であることを考慮すると、想定される攻撃レベルで可能な範囲での本 TOE へのアクセスに関しては、本 TOE のふるまいは開発者テストと評価者独立テストで十分に検証されている。

(1) 結果

評価者の分析により、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。

7.5 評価構成について

本 TOE は、「4.2 運用環境と構成」で示した MFP の機種に搭載されることを想定している。評価構成は、それらの MFP の一部の機種に TOE を搭載した構成である。

この評価構成での評価で、「7.4.1 開発者テスト」に示した理由により、「4.2 運用環境と構成」で示したどの MFP を使用した場合も保証できることが評価者により判断された。

7.6 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。

・ PP 適合：なし

・ セキュリティ機能要件：　コモンクライテリア　パート 2　拡張

・ 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。

・ EAL2 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。

7.7 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。

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、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 EAL2 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

- 評価により保証されたのは、本TOEによる上書き消去が「MFPの指示通り」に実施されるということのみである。
- MFP の指示が適切かどうかは保証の対象外である。例えば、MFP が本 TOE に対して実施する上書き消去の指示に関して、以下のことは保証の対象外である。
  - MFP の利用により発生する残存データの領域を正しく指定しているか
  - 適切なタイミングで上書き消去の指示をしているか
- 本 TOE のセキュリティ機能が有効に動作するために、動作環境である MFP の機能が正しく動作することが必要である。例えば、以下の MFP の機能が該当する。
  - 逐次消去の有効・無効設定を MFP の管理者に限定する。

- TOE が動作しているかどうかを判別できるような表示をする。
- MFP の故障など TOE が正しく動作できないような状況において、MFP の管理者に適切に通知する。
- 上書き消去方式または乱数上書き回数として想定される範囲の入力のみができるようにする。
  なお、TOE のインタフェースは想定される範囲外(乱数上書き回数として 9 よりも大きい値など)の入力も受け付ける仕様となっている。

本評価では動作環境である MFP の機能は保証されないため、MFP の機能が正しく動作することについては調達者の責任となる。そのための適切なガイダンスが提供されることは評価者により判断されている。

- TOE 外の機能として MFP の HDD に書き込むデータを暗号化する機能があり、かつその機能が動作している場合は、逐次消去機能(メモリー自動消去)において上書きするデータが暗号化されて書き込まれる。そのため、逐次消去機能で NSA、DoD 方式を指定した場合、これらの方式には準拠しないことになる。(定数や補数のように定められているデータを書き込む際に、実際に書き込まれるデータが暗号化の機能で変更されるため。)

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。

セキュリティカード タイプ M19　DataOverwriteSecurity Unit Type M19
セキュリティターゲット バージョン 3.03　2016 年 02 月 24 日
株式会社リコー

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）
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。

DoD	Department of Defense (アメリカ国防総省)
HDD	Hard Disk Drive
MFP	Multi Function Product (デジタル複合機)
NSA	National Security Agency (アメリカ国家安全保障局)
OS	Operating System
SATA	Serial Advanced Technology Attachment (HDDのインタフェースの方式の一つ)

本報告書で使用された用語の定義を以下に示す。

SDメモリカード	SDメモリカードはセキュアデジタルメモリカードである。高い機能を持ったメモリー装置で、切手サイズで、MFPにTOEや他のアプリケーションを供給するために使用される。
ドキュメントボックスの機能	MFPの機能。 紙原稿をスキャンしてMFP内のHDDに蓄積することと、コピー、プリンタ、ファクス及びドキュメントボックスの各機能でMFP内のHDDに蓄積した文書を印刷、削除することができる。

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27年6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27年10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27年10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 Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: 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] セキュリティカード タイプM19　DataOverwriteSecurity Unit Type M19　セキュリティターゲット バージョン 3.03　2016年02月24日　株式会社リコー

[13] 日本版名称：セキュリティカード タイプM19 海外版名称：DataOverwriteSecurity Unit Type M19 Ver.1.02 評価報告書 第2.1版（VST-ETR-0002-01）
2016年3月1日　株式会社 ECSEC Laboratory 評価センター