imagio セキュリティカード タイプ 9

DataOverwriteSecurity Unit Type I

セキュリティターゲット

作成者	:	株式会社リコー
作成日付	:	2013 年 11 月 5 日
バージョン	:	2.00

更新履歴

バージョン	日付	作成者	詳細
2.00	2013-11-05	株式会社リコー	公開版

目次

図一覧

表一覧

1 ST 概説

本章は、ST 参照、TOE 参照、TOE 概要、および TOE 記述について記述する。

1.1 ST 参照

本書を識別するための情報を以下に示す。

タイトル : imagio セキュリティカード タイプ 9
DataOverwriteSecurity Unit Type I
セキュリティターゲット

バージョン : 2.00

発行日 : 2013 年 11 月 5 日

作成者 : 株式会社リコー

1.2 TOE 参照

TOE は、株式会社 リコー製の imagio セキュリティカード タイプ 9 および DataOverwriteSecurity Unit Type I であり、下記の製造者、TOE 名称、およびバージョンで識別する。imagio セキュリティカード タイプ 9 は日本国内で販売する際の製品名称であり、DataOverwriteSecurity Unit Type I は海外で販売する際の製品名称で、ソフトウェアは同じものである。

製造者 : 株式会社 リコー

TOE 名称 : <日本版名称> imagio セキュリティカード タイプ 9
<海外版名称> DataOverwriteSecurity Unit Type I

バージョン : 1.02m

1.3 TOE 概要

本節では、TOE の概要として TOE 種別、要求される TOE 以外のハードウェア/ソフトウェア、TOE の使用方法、および TOE の主要なセキュリティ機能を記す。

1.3.1 TOE 種別

TOE は、株式会社リコー製のデジタル複合機（Multi Function Product：以下、MFP という）のオプション製品であり、MFP のメモリー上のデータを上書き消去するソフトウェアである。
上書き消去とは、メモリー上のデータに特定の値を上書きして再利用できないようにすることである。

1.3.2 要求される TOE 以外のハードウェア/ソフトウェア

TOE を使用するためには株式会社 リコー製の MFP が必要である。リコー製 MFP は、MFP 機種ごとにオプション製品のリスト(搭載可能なオプション製品が記載されている製品情報)が用意されている。TOE が搭載可能な MFP では、このリストに TOE がオプション製品として記載されている。MFP の利用者は、MFP のオプション製品のリストを参照することで、TOE が搭載可能な MFP を識別できる。

本 TOE を搭載する MFP については、附属書 A に記載する。

MFP は、ドキュメントを入力、出力、および蓄積する能力を持った IT 製品であり、これら能力を組合せてコピー、プリンタ、スキャナ、ファクス、およびドキュメントボックスの機能を利用者に提供する。
MFP は、前述した各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、内蔵するハードディスク(以下、HDD という)上に一時的な作業用データを作成する。また、ドキュメントボックス機能で蓄積しているドキュメントを削除した場合は、論理的な削除を実行するのでドキュメントの実体データは HDD に残る。これらの一時的な作業用データや実体データの情報を残存データと言う。

1.3.3 TOE の使用方法

TOE は、MFP のオプション製品であり、SD カードに記録して配付される。TOE を利用するためには、カスタマー・エンジニアに TOE を設置してもらう必要がある。
TOE の機能が活性化されると、MFP は操作パネルに TOE の機能に関連するボタンとアイコンを表示する。
利用者は、MFP の操作パネルから TOE の設定や機能を選択して利用する。

1.3.4 TOE の主要なセキュリティ機能

TOE は、MFP が指定する HDD 上の領域を上書き消去し、その領域にある情報を無効化する。

1.4 TOE 記述

本節では TOE の物理的範囲、ガイダンス文書、および TOE の論理的範囲について記す。

1.4.1 TOE の物理的範囲

TOE は、MFP にロードして使用するソフトウェアである。MFP の利用環境、および MFP における TOE の位置づけを明らかにして TOE の物理的範囲を示す。

1.4.1.1 MFP の利用環境

MFP は、オフィスに設置し、利用者の必要に応じてネットワークや電話回線との接続、あるいはクライアント PC を USB 接続して利用することを想定する。
ネットワーク接続した TOE は、クライアント PC、FTP サーバー、SMB サーバー、SMTP サーバーと通信をすることができる。電話回線を接続した TOE は、ファクスの送受信をすることができる。MFP の利用環境を図 1 に示す。

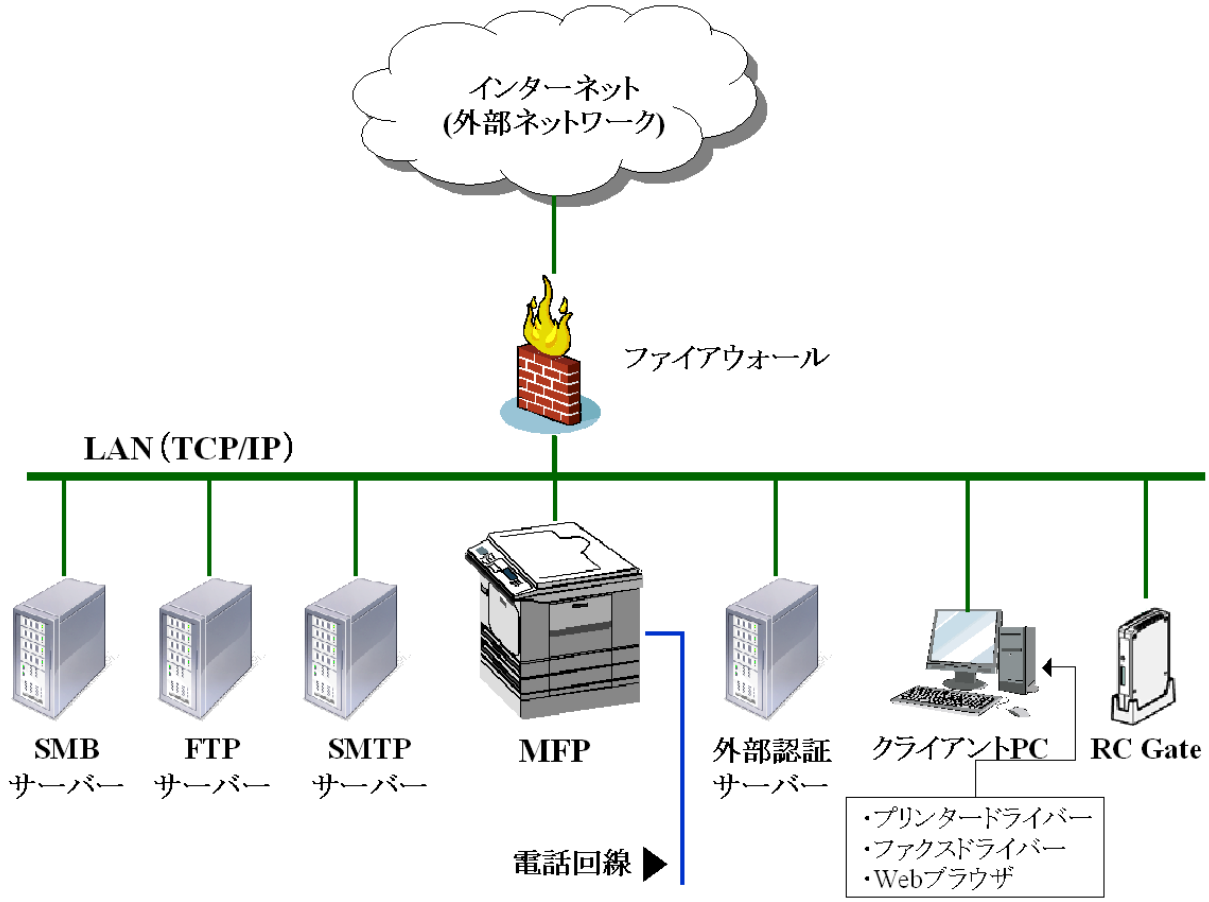

図 1：MFP の利用環境

1.4.1.2 MFP における TOE の位置づけ

MFP を構成するハードウェアには、操作パネル、エンジンユニット、ファクスユニット、コントローラボード、HDD、ネットワークユニット、USB ポート、SD CARD スロットがある。MFP のハードウェア構成を図 2 に示す。

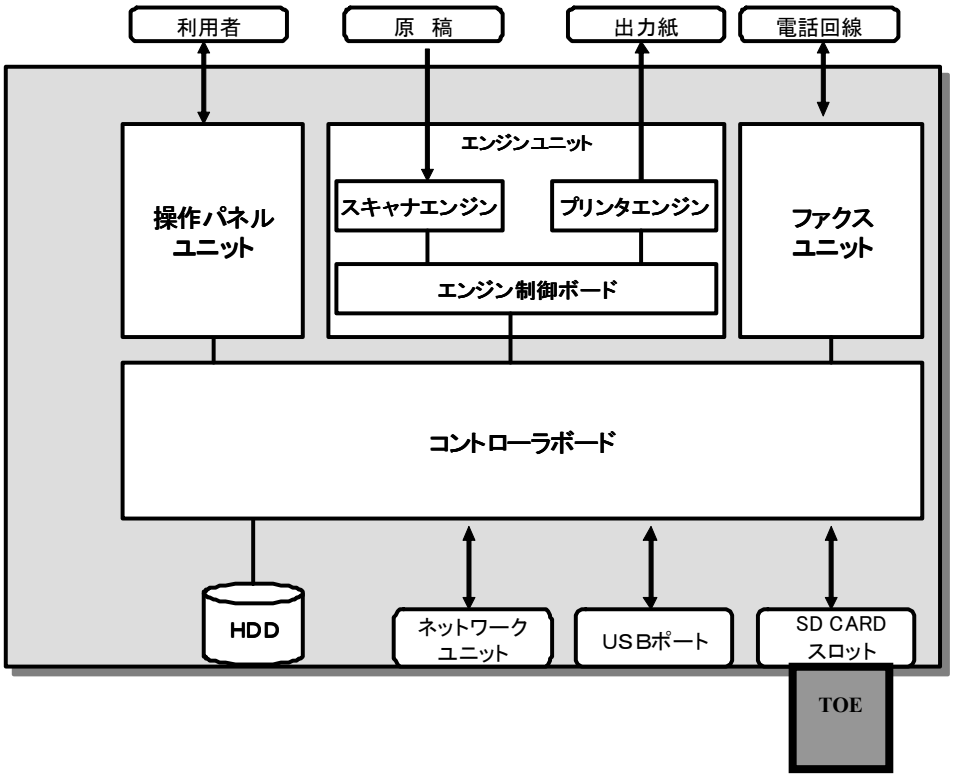

図 2：MFP のハードウェア構成と TOE

MFP を制御するためのファームウェアは、コントローラボード上のメモリーにインストールされている。TOE を記録した SD カードは、MFP の SD CARD スロットに挿入される。TOE は MFP によって SD カードからロードされ、MFP のファームウェアと通信し、HDD に記録されている情報を上書き消去する。

1.4.2 ガイダンス文書

TOE が、利用者に配付される際に同梱される文書は下に示すガイダンス文書である。

ガイダンス文書は日本向け製品には日本語版ガイダンス文書が同梱され、海外向け製品には英語版ガイダンス文書が同梱される。英語版ガイダンス文書は日本語版ガイダンス文書を元に翻訳したもので、記載内容は同じである。

- 日本語版ガイダンス文書名
  imagio セキュリティカード タイプ 7
  imagio セキュリティカード タイプ 9
  使用説明書　　D377-7902
  本製品をお使いのお客様へ Notes for Users　　D377-7925
- 英語版ガイダンス文書名
  DataOverwriteSecurity Unit Type H
  DataOverwriteSecurity Unit Type I
  Operating Instructions　　D377-7940

Notes for Users D377-7250
本製品をお使いのお客様へ Notes for Users D377-7925

1.4.3 TOE の論理的範囲

TOE の機能は逐次消去機能、および一括消去機能である。以下に、逐次消去機能、および一括消去機能について記す。
TOE 外である MFP が利用者に提供するメモリー自動消去機能、およびメモリー全消去機能については「1.4.4 TOE に係わる MFP の機能」に記す。

逐次消去機能

TOE は MFP から指定された HDD 上の領域に利用者が選択した方法で特定のデータを上書きすることによって残存データを消去する。MFP は、メモリー自動消去機能で不要となった HDD 上のデータ領域を、本機能で上書き消去する領域として指定する。

一括消去機能

TOE は MFP からの指示で HDD 上の全領域に利用者が選択した方法で特定のデータを上書きすることですべてのデータを消去する。MFP は、操作パネルから利用者が一括消去の起動を選択した時に、TOE へ一括消去の指示をする。

1.4.4 TOE に係わる MFP の機能

TOE の逐次消去機能と一括消去機能は、それぞれ MFP のメモリー自動消去機能とメモリー全消去機能を構成する下位機能である。また、逐次消去機能と一括消去機能は、MFP の残存データ管理機能、逐次消去動作設定機能、一括消去起動・一時停止機能、残存データ状態表示機能と関連する。TOE の機能と TOE に係わる MFP の機能を図 3 に示し、以下に各機能について解説する。

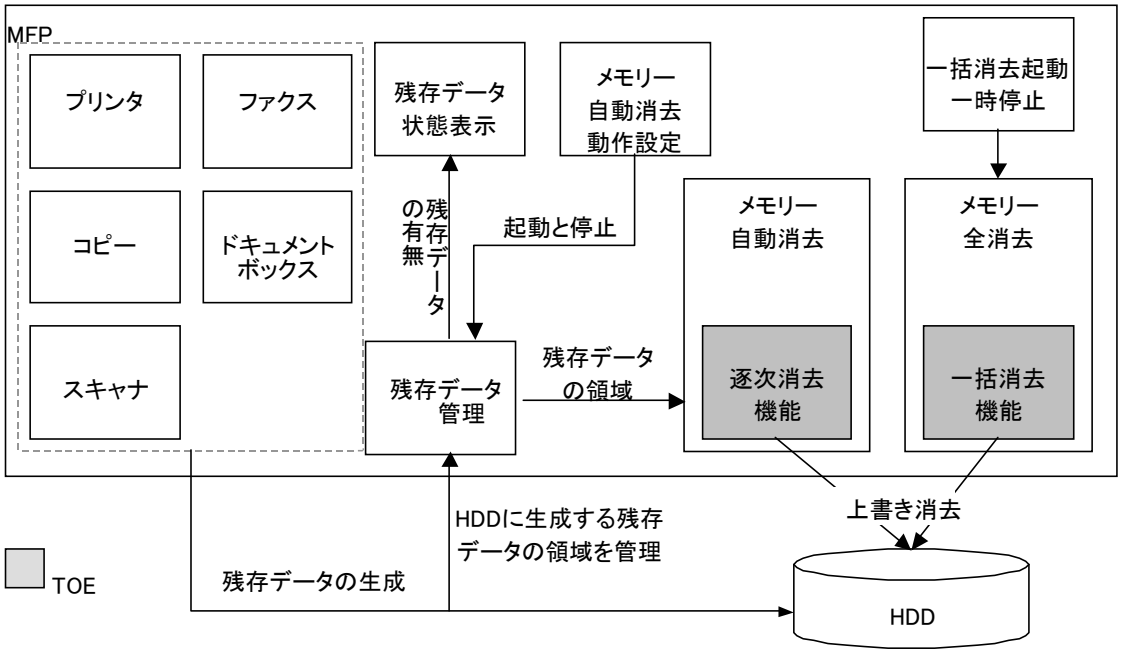

図 3：TOE の機能と TOE に係わる MFP の機能

メモリー自動消去機能

HDD 上に残存データが生成すると、TOE の逐次消去機能を使って上書き消去する機能。残存データの有無は、残存データ管理機能で管理しされている。

メモリー全消去機能

利用者が一括消去の起動を選択すると、TOE の一括消去機能を使って HDD 上の全ての領域を上書き消去する機能。

本機能は MFP を廃棄する、あるいは他部署に MFP を移管するといったときに、MFP の HDD に蓄積している文書や MFP の許可利用者の情報を無効化するために使用する。

残存データ管理機能

HDD 上の残存データが存在する領域を管理する機能。TOE の逐次消去機能で MFP から指示される HDD 上の残存データ領域は、本機能で管理している残存データ領域である。

メモリー自動消去動作設定機能

MFP の操作パネルからメモリー自動消去機能の有効/無効を設定する機能。
メモリー自動消去動作設定は、MFP がメモリー自動消去機能の有効/無効の設定を MFP の管理者だけに許可される。

一括消去起動・一時停止機能

メモリー全消去の起動と一時停止の操作を管理者だけに許可する機能。本機能の操作は、MFP の操作パネルから行う。

残存データ状態表示機能

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。

2 適合主張

本章は、CC 適合主張、PP 適合主張、セキュリティ要件パッケージ適合主張、および適合主張根拠について記す。

2.1 CC 適合主張

本 ST 及び TOE の CC 適合主張は以下のとおりである。

- 適合を主張する CC のバージョン
  パート1:
  概説と一般モデル 2012 年 9 月 バージョン 3.1 改訂第 4 版 [翻訳第 1.0 版] CCMB-2012-09-001
  パート2:
  セキュリティ機能コンポーネント 2012 年 9 月 バージョン 3.1 改訂第 4 版 [翻訳第 1.0 版] CCMB-2012-09-002
  パート3:
  セキュリティ保証コンポーネント 2012 年 9 月 バージョン 3.1 改訂第 4 版 [翻訳第 1.0 版] CCMB-2012-09-003
- 機能要件:パート2拡張
- 保証要件:パート3適合

2.2 PP 適合主張

本 ST が適合を主張する PP はない。

2.3 セキュリティ要件パッケージ適合主張

本 ST が適合を主張するセキュリティ要件は次のとおりである。

- 適合する機能要件のパッケージはない。
- 保証要件のパッケージは「EAL3」適合である。

2.4 適合主張根拠

本 ST が適合を主張する PP はないため、適合主張する根拠はない。

3 セキュリティ課題

本章は、脅威、組織のセキュリティ方針、および前提条件について記す。

3.1 脅威

TOE および TOE の運用環境が対抗する脅威はない。

3.2 組織のセキュリティ方針

本節では、TOE が従わなければならない組織のセキュリティ方針を識別する。

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。

3.3 前提条件

本節では、TOE の環境に関わる前提条件を識別する。

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。

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。

4 セキュリティ対策方針

本章は、TOE のセキュリティ対策方針と運用環境のセキュリティ対策方針について記す。

4.1 TOE のセキュリティ対策方針

本節では、TOE で対応するセキュリティ対策の方針を識別する。

O.OVERWRITE

TOE は、MFP が指定する HDD 上の領域の情報を漏えいさせないようにするため、その領域を上書き消去して情報を無効化する。

4.2 運用環境のセキュリティ対策方針

本節では、運用環境におけるセキュリティ対策の方針を識別する。

OE.MODE.AUTOMATIC

MFP の電源を切断する際には、利用者は操作パネル上のアイコンを確認し、逐次消去による上書き消去が完了している状態で電源を切断する。

OE.MODE.MANUAL

一括消去を行なう際には、利用者は一括消去が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時停止されないように MFP を管理する。

4.3 セキュリティ対策方針根拠

セキュリティ対策は、「3 セキュリティ課題」で規定した組織のセキュリティ対策方針を実現するもの、あるいは前提条件を充足するためのものである。セキュリティ対策方針とそれらに対応する組織のセキュリティ方針と前提条件の関係を表 1 に記す。

表 1：セキュリティ対策方針とセキュリティ課題の対応関係

セキュリティ課題 / セキュリティ対策方針	P.UNREADABLE	A.MODE.AUTOMATIC	A.MODE.MANUAL
O.OVERWRITE	X		
OE.MODE.AUTOMATIC		X	
OE.MODE.MANUAL			X

P.UNREADABLE

P.UNREADABLE は O.OVERWRITE によって実施される。なぜなら、O.OVERWRITE によって、MFP から指定された HDD の領域が上書き消去されることで、その領域の情報が読み出されなくなることが保証されるからである。

A.MODE.AUTOMATIC

A.MODE.AUTOMATIC は OE.MODE.AUTOMATIC によって実現できる。なぜなら、MFP の電源を切断する際に TOE の上書き消去の完了を待つことで、TOE の上書き消去が中断されないことが保証されるからである。

A.MODE.MANUAL

A.MODE.MANUAL は OE.MODE.MANUAL によって実現できる。なぜなら、一括消去の最中に MFP が利用者の管理下に置かれることで、利用者の意図に反して一括消去が一時停止されることが防止されるからである。

5 拡張コンポーネント定義

本章で、セキュリティ機能コンポーネントの拡張コンポーネントと、セキュリティ保証コンポーネントの拡張コンポーネントについて記す。

5.1 セキュリティ機能コンポーネントの拡張コンポーネント

本 ST では、下記の事由により CC パート2に定義されたセキュリティ機能コンポーネントの拡張コンポーネントとして FDP_SIP.1 を定義する。

拡張コンポーネントの必要性とファミリ追加の理由

TOE は、高信頼 IT 製品が指定する資源の一部領域あるいは全部のデータを無効化する。この資源は TSF の制御下にない。一方、既存の CC コンポーネントには、データを無効化するファミリとして FDP_RIP が存在するが、FDP_RIP が無効化するのは TSF 制御資源内のデータである。TOE が無効化する対象と FDP_RIP が無効化する対象は異なり、FDP_RIP のコンポーネントを詳細化できない。よって、拡張コンポーネントが必要である。
また、FDP_RIP にコンポーネントを追加した場合、TOE が無効化するデータが、TSF 制御資源内に全部あるいは一部が含まれると誤解を招くことが考えられるため、新たなファミリを追加する必要がある。新たなファミリは、SIP と定義する。

適用クラスの理由

TOE が高信頼 IT 製品に指定され上書き消去するデータのほとんどは、高信頼 IT 製品の利用者データであるため、拡張コンポーネントのクラスは利用者データの保護を規定する FDP クラスが妥当である。

FDP_SIP 指定された情報の保護

■ ファミリのふるまい

このファミリは、高信頼 IT 製品が指定する資源上のデータが無効であることを要求する。

■ コンポーネントのレベル付け

FDP_SIP.1 指定された資源にあるデータを再利用できないことを TSF が保証することを要求する。

■ 管理:FDP_SIP.1

予見される管理アクティビティはない。

管理アクティビティがない理由は、TOE が提供する機能の管理は高信頼 IT 製品が行い、TOE の機能を利用できるのは高信頼 IT 製品だけであるため管理の必要はない。

■ 監査:FDP_SIP.1

予見される監査はない。

FDP_SIP.1　　指定された情報の保護

下位階層:　　なし

依存性　:　　なし

FDP_SIP.1.1　　TSF は、指定された資源のどの情報の内容も上書き消去することを保証しなければならない。

5.2　セキュリティ保証コンポーネントの拡張コンポーネント

セキュリティ保証コンポーネントの拡張はない。

6 セキュリティ要件

本章は、セキュリティ機能要件、セキュリティ保証要件、およびセキュリティ要件根拠について記す。

6.1 セキュリティ機能要件

本節では、本 TOE が提供するセキュリティ機能要件を示す。

FDP_SIP.1　　指定された情報の保護

下位階層:　　なし

依存性　:　　なし

FDP_SIP.1.1　　TSF は、指定された資源のどの情報の内容も上書き消去することを保証しなければならない。

6.2 セキュリティ保証要件

本 TOE のセキュリティ保証要件は、CC パート 3 で規定している評価保証レベル EAL3で必要とするセキュリティ保証要件だけである。以下に本 TOE が必要とするセキュリティ保証要件を表 2 に示す。

表 2：TOE セキュリティ保証要件

保証クラス	保証コンポーネント	
ADV: 開発	ADV_ARC.1	セキュリティアーキテクチャ記述
	ADV_FSP.3	完全な要約を伴う機能仕様
	ADV_TDS.2	アーキテクチャ設計
AGD: ガイダンス文書	AGD_OPE.1	利用者操作ガイダンス
	AGD_PRE.1	準備手続き
ALC: ライフサイクルサポート	ALC_CMC.3	許可の管理
	ALC_CMS.3	実装表現の CM 範囲
	ALC_DEL.1	配付手続き
	ALC_DVS.1	セキュリティ手段の識別
	ALC_LCD.1	開発者によるライフサイクルモデルの定義
ASE: セキュリティターゲット評価	ASE_CCL.1	適合主張
	ASE_ECD.1	拡張コンポーネント定義
	ASE_INT.1	ST 概説
	ASE_OBJ.2	セキュリティ対策方針
	ASE_REQ.2	派生したセキュリティ要件
	ASE_SPD.1	セキュリティ課題定義

保証クラス	保証コンポーネント	
	ASE_TSS.1	TOE 要約仕様
ATE: テスト	ATE_COV.2	カバレージの分析
	ATE_DPT.1	テスト: 基本設計
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テストーサンプル
AVA: 脆弱性評定	AVA_VAN.2	脆弱性分析

6.3 セキュリティ要件根拠

本節では、セキュリティ要件根拠についてセキュリティ機能要件根拠、依存性の検証、およびセキュリティ保証要件根拠について記す。

6.3.1 セキュリティ機能要件根拠

本 TOE のセキュリティ対策方針は O.OVERWRITE であり、セキュリティ機能要件は FDP_SIP.1 である。これらは対応関係にある。すなわち、本 TOE のセキュリティ機能要件は、1つ以上のセキュリティ対策方針に対応することになり、セキュリティ機能要件は必要性があると言える。
また、O.OVERWRITE は、MFP が指定する HDD 上の領域の情報を暴露させないため、その領域を無効化することを要求しているのに対して、FDP_SIP.1 は、指定された領域の情報を上書き消去する。よって、O.OVERWRITE の要求は、FDP_SIP.1 で十分満たされると言える。

6.3.2 依存性の検証

本 TOE のセキュリティ機能要件である FDP_SIP.1 に依存性は、なしとなっている。よって本 TOE のセキュリティ要件の依存性は満たされていると言える。

6.3.3 セキュリティ保証要件根拠

本 TOE は市販製品である MFP のオプションである。MFP はオフィスに設置し、基本的な攻撃能力を持った攻撃者からの攻撃を想定する。したがって、TOE は、オフィスにおいて基本的な攻撃能力を持った攻撃者の攻撃に対抗できることを保証する必要がある。
EAL3は、セキュリティ機能とそのアーキテクチャの検証、セキュリティ機能を確実に使用するためのガイダンス文書の検証、開発環境と配付経路のセキュリティ対策の検証、構成要素の構成管理の検証、セキュリティ機能とアーキテクチャに基づいたテストの検証を行う。
これら検証のパッケージは、オフィスにおける一般的な商用製品への基本的な攻撃能力を持った攻撃者の攻撃に対して対抗できることを保証するのに十分であると言える。
したがって、EAL3の選択は妥当である。

7 TOE 要約仕様

TOE のセキュリティ機能要件 FDP_SIP.1 より導かれるセキュリティ機能は、SF.OVERWRITE である。
以下に、SF.OVERWRITE の解説と、SF.OVERWRITE による FDP_SIP.1 の実現方法を記載する。

SF.OVERWRITE

TOE は、MFP が指定した HDD 領域を上書き消去する。MFP が指定する上書き消去領域の取得方法には、逐次消去と一括消去がある。以下に、逐次消去と一括消去について記す。

- 逐次消去
  TOE は、MFP の残存データ管理機能が管理している HDD 上の残存データ領域の有無の情報を常に監視し、残存データが存在することを見つけ出したときに、残存データ領域を上書き消去する。
- 一括消去
  TOE は、MFP から HDD の一括消去指示を受けたときに、HDD の一括消去をする。また、TOE は一括消去のキャンセルを受け付ける。キャンセルを受け付けた場合は、一括消去処理を中断する。

上書き消去の手段には、NSA 方式、DoD 方式、および乱数書き込み方式がある。いずれの方式で上書き消去するかは MFP から TOE に指定される。以下に各方式について記す。

- NSA 方式
  乱数で2回上書きし、Null（0）で1回上書きする。
- DoD 方式
  固定値で1回上書きし、その固定値の補数で1回上書きし、さらに乱数で1回上書きし、最後に検証する。
- 乱数書き込み方式
  1から9回のうち指定された回数だけ乱数で上書きする。
  乱数上書き回数は、MFP から指定される。

FDP_SIP.1 の実現方法

FDP_SIP.1 は、高信頼 IT 製品である MFP から指定された資源（HDD）上の領域のデータを上書き消去することを要件としている。
SF.OVERWRITE は、逐次消去あるいは一括消去によって MFP から指定された HDD 上の領域を、NSA 方式、DoD 方式、および乱数書き込み方式のうち、MFP から指定される方式で上書きして、HDD 上のデータを無効化することで実現する。

8 付録

8.1 用語集

本 ST における用語を表 3 にて解説する。

表 3：本 ST で使用する用語

用語	定義
MFP	デジタル複合機(Multi Function Product)。 1 台でコピー、プリンタなどの 2 種類以上の機能を持った印字装置のことである。
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、ファクスおよ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。

附属書 A

本 TOE は、表 4 に挙げる MFP に搭載して使用することを想定している。

表 4: TOE を搭載可能な MFP

日本国内での製品名称	海外での製品名称
RICOH MP C3503、RICOH MP C3003	Ricoh MP C3003、Ricoh MP C3003G、 Ricoh MP C3503、Ricoh MP C3503G、 Savin MP C3003、Savin MP C3003G、 Savin MP C3503、Savin MP C3503G、 Lanier MP C3003、Lanier MP C3003G、 Lanier MP C3503、Lanier MP C3503G、 nashuatec MP C3003、nashuatec MP C3503、 Rex-Rotary MP C3003、 Rex-Rotary MP C3503、 Gestetner MP C3003、 Gestetner MP C3503、 infotec MP C3003、 infotec MP C3503