imagio セキュリティカード タイプ F,

Data OverWriteSecurity Unit F

セキュリティターゲット

作成者: 株式会社リコー 平林治之
作成日付: 2007 年 01 月 17 日
バージョン: 1.00

更新履歴

バージョン	日付	作成者	詳細
0.01	2006-12-08	平林治之	新規作成
0.02	2006-12-27	平林治之	表 1 海外製品名称の記載
1.00	2007-01-17	佐藤専	誤植を修正

目次

図一覧

表一覧

1 ST 概説

1.1 ST 識別

本書とTOE を識別するための情報を以下に示す。

ST のタイトル: imagio セキュリティカード タイプ F,
Data OverWriteSecurity Unit F
セキュリティターゲット

ST バージョン: 1.00

ST 作成日付: 2007 年 01 月 17 日

ST 作成者: 株式会社リコー 平林治之

製品名称: imagio セキュリティカード タイプ F,
Data OverWriteSecurity Unit F

注意 :これ以降、上記製品を総称して,"データオーバーライトモジュール"とする。

“imagio セキュリティカード タイプF”は日本の製品名称である。

“Data OverWriteSecurity Unit F”は海外の製品名称である。

これらのTOE は、x86 系のCPU を搭載したMFP を対象とする。

TOE 識別: データオーバーライトモジュールのソフトウェア

TOE バージョン: 1.05

CC バージョン: CC バージョン 2.3, ISO/IEC 15408:2005

注意:日本語訳は以下の資料を使用する。

-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 2.3 2005 年8 月 CCMB-2005-08-001

-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:セキュリティ機能要件 バージョン2.3 2005 年8 月 CCMB-2005-08-002

-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:セキュリティ保証要件 バージョン2.3 2005 年8 月 CCMB-2005-08-003

-補足-0512

キーワード: デジタル複合機、ドキュメント、コピー、プリンタ、スキャナ、ネットワーク、オフィス、ハードディスク、セキュリティ、上書き、残存情報保護

1.2 ST 概要

本 ST は、株式会社リコー製デジタル複合機（Multi Function Product、以降 MFP と記す）に搭載する「データオーバーライトモジュールのソフトウェア(以降 DOMS と記す)」について記述したものである。MFP は、コピー機能、プリンタ機能、およびスキャン機能で構成される OA 機器である。本 TOE は、MFP に装着さ

れ、より安全に使用するためのオプションキットであり MFP から指定された HDD 上の領域を上書き消去する。

1.3 CC 適合

本書は、以下を満たしている。

- CC パート 2 拡張
- CC パート 3 適合
- EAL3 適合

本書において適合する PP はない。

1.4 参考資料

本書を作成するときに参考にした資料は以下のとおりである。

- 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
  2005 年 8 月 バージョン 2.3 CCMB-2005-08-001
  (平成 17 年 12 月翻訳第 1.0 版 独立行政法人情報処理推進機構 セキュリティセンター)
- 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: セキュリティ機能要件
  2005 年 8 月 バージョン 2.3 CCMB-2005-08-002
  (平成 17 年 12 月翻訳第 1.0 版 独立行政法人情報処理推進機構 セキュリティセンター)
- 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: セキュリティ保証要件
  2005 年 8 月 バージョン 2.3 CCMB-2005-08-003
  (平成 17 年 12 月翻訳第 1.0 版 独立行政法人情報処理推進機構 セキュリティセンター)
- 補足-0512
  (平成 17 年 12 月 独立行政法人情報処理推進機構 セキュリティセンター
  情報セキュリティ認証室)

2 TOE 記述

2.1 TOE の概要

2.1.1 製品種別

本 TOE の製品種別は、MFP のオプションとして取り付けられるソフトウェア製品である。このソフトウェア製品は、お客様のところで設置される。

2.1.2 TOE の位置付け

TOE は、MFP から指示された領域の情報を再利用できなくするために、その情報を上書き消去する目的で使用される。

MFP で使用する HDD は RAW 領域と UNIX 領域に分かれている。TOE は MFP の共有メモリ上にある HDD の RAW 領域の管理情報を監視して、MFP から上書き消去の指示があった領域を見付けるとその領域を上書き消去する。また TOE は MFP から UNIX 領域の情報を上書き消去する指示を受けて、その領域を上書き消去する。さらに TOE は、リース/レンタル契約終了による返却、他部門への譲渡あるいは廃棄される際に、MFP に内蔵された HDD に記録された情報から秘密が漏洩しないようにするため、HDD 上の全ての情報を上書き消去する機能を持っている。

どの情報を上書き消去するかは MFP が決定し、TOE に指示する。

MFP は作業用として一時的にイメージデータを HDD 上に作成する。コピー、プリンタ、およびスキャナ、の処理が終了すると、MFP は上記の一時的に作成されたイメージデータを削除する。

また、利用者からイメージデータの蓄積を指示されると、MFP は HDD 上にイメージデータを保存する。利用者から蓄積されたデータの削除を指示されると、MFP は上記の保存されたイメージデータを削除する。

データの削除とは、コピー、プリンタ、スキャナ、およびドキュメントボックスの機能にとって必要の無くなった情報を、これらの機能からは見た目上存在しないものとすることである。MFP が削除したイメージデータはこれらの機能からは使用されなくなるが、その内容は実際には HDD 上に存在する。MFP はイメージデータとして記録されていた情報が削除されると、それを残存情報として管理する。MFP は、その機能によって RAW 領域あるいは UNIX 領域のどちらかにデータを保存する。MFP は RAW 領域の残存情報の有無を TOE に知らせるために、その管理情報を共有メモリに記録する。また、MFP は UNIX 領域に残存情報が存在すると、その上書き消去を TOE に指示する。

2.1.3 TOE が搭載される MFP の利用環境

TOE は MFP 上で動作するソフトウェアであり、MFP の機能を拡張するオプションとして提供される。MFP は基本的なコピー機能だけでなく、1 台でプリンタ、スキャナといった何種類かの機能を持っている。本 TOE は一般的なオフィスで使用されている MFP に搭載して使用されることを想定している。MFP は内部に HDD を備えている。HDD はコピーやプリンタのイメージデータを保存するのに使用する。オフィスの稼働時には MFP はそのオフィスの関係者の監視下にあるが、夜間および休日には無人のオフィスに部外者が侵入し、HDD を取り出すかもしれない。

想定されるMFP の利用環境を図 1 に示す。

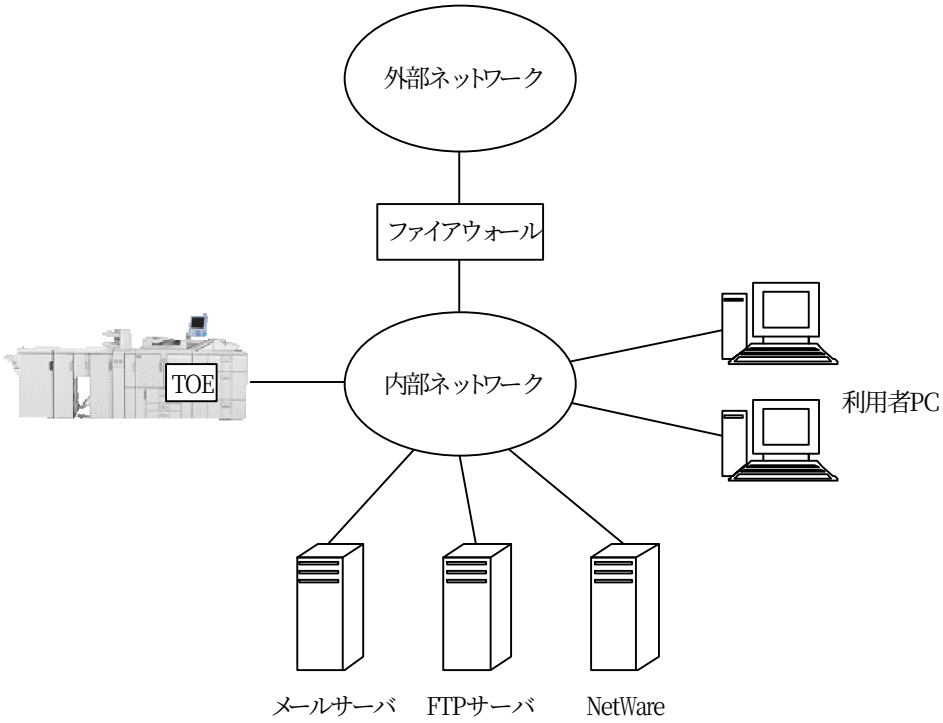

図 1: MFP の利用環境

MFP の利用環境には以下のものが接続される。

- 利用者 PC:
  MFP に対して文書の印刷を要求する。また、スキャンしたイメージデータや MFP に蓄積されたイメージデータを受け取ることができる。
- メールサーバ、FTP サーバ、NetWare サーバ:
  MFP でスキャンしたイメージデータをメールサーバ、FTP サーバ、NetWare サーバに送ることができる。

内部ネットワークに接続された機器を保護するため、外部ネットワークとの間にはファイアウォールが設置される。

本 TOE は表 1 に挙げるモデルの MFP に搭載して使用することを想定している。

表 1: TOE を搭載可能な MFP

	国内製品名称	海外製品名称
モデル 1	リコー imagio MP 9000 リコー imagio MP 1100 リコー imagio MP 1350	RICOH Aficio MP 9000/MP 1100/MP 1350 LANIER LD190/LD1110/LD1135 LANIER MP 9000/MP 1100/MP 1350 SAVIN 8090/8110/8135 Nashuatec MP 9000/MP 1100/MP 1350 Rex Rotary MP 9000/MP 1100/MP 1350 Gestetner DSm790/DSm7110/DSm7135 Gestetner MP 9000/MP 1100/MP 1350 infotec IS 3090/IS 3110/IS 3135

2.2 TOE の物理的範囲

リコーMFP はハードウェアとソフトウェアで構成される。

ハードウェアは、プリントエンジン、スキャナユニット、オペレーションパネル、HDD、コントローラボードで構成される。

プリントエンジンはプリント、およびコピーのデータを印刷し、同時に給紙および排紙の制御をする。

スキャナユニットは紙文書からイメージデータを取り込む。コピー、およびスキャンするイメージデータの取り込みに使用する。

オペレーションパネルは、一般利用者および管理者に伝える情報を表示し、また、一般利用者および管理者からの入力を受け付ける。一般利用者および管理者はオペレーションパネルを操作して MFP の機能を利用することができる。

HDD にはイメージデータが保存される。プリント、コピー、およびスキャンする際に、MFP が作業用として一時的にイメージデータを保存する。また、一般利用者の指示によって蓄積されるイメージデータもここに保存される。

コントローラボードは、MFP 全体を制御する。MFP 内のソフトウェアを実行するためのプロセッサとRAM、MFP のオペレーティングシステム(OS)や各種アプリケーションモジュール等、MFP のソフトウェアが記録された ROM、MFP の設定情報が記録される NV-RAM、利用者 PC や各種サーバと接続するためのホストインターフェイスを持つ。また、機能を追加するためのソフトウェアが記録されたSD メモリーカードを取り付けることができる。DOMS は SD メモリーカードに記録されてコントローラボードに取り付けられる。

図 2 に MFP のハードウェア構成を示す。

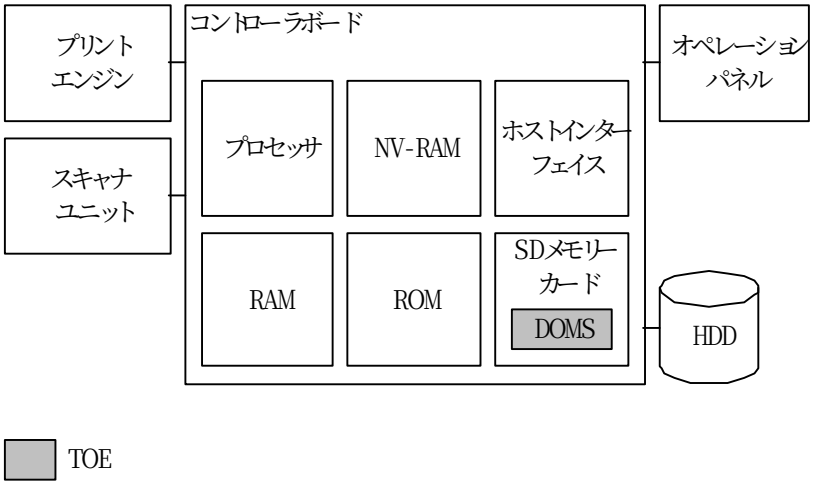

図 2: MFP のハードウェア構成

ソフトウェアは OS、コモンサービスモジュール(CSM)、アプリケーションモジュールで構成される。

OS は HDD 等のハードウェアを管理し、これらのハードウェア資源を操作するためのインターフェイスを提供する。OS は NetBSD を基にしたリコー独自の OS である。

アプリケーションモジュールは、一般利用者に対してコピー、プリンタ、スキャナ等の機能を提供する。これらのモジュールは、一般利用者の操作を受けて必要な処理をCSM に要求することで、それぞれの機能を実現する。

CSM はアプリケーションモジュールによって使用される共通の機能を提供する。また、CSM はイメージデータや残存情報が存在する HDD の領域の管理や、残存情報の状態のオペレーションパネルへの表示等の機能も提供する。

SCS は CSM の一種で、MFP 上で動作しているアプリケーションを把握し、設定情報を管理する。また、管理者からの要求があった時に、DOMS の一括消去機能を起動する。

HDD は RAW 領域と UNIX 領域に分かれており、MFP の機能によってそれぞれ異なる領域にデータを保存する。

IMH は CSM の一種で、OS を通してプリントエンジン、およびスキャナユニットとコントローラボード間のイメージデータの転送を制御する。IMH はまた、HDD の RAW 領域上のイメージデータおよび残存情報の有無を管理し、その管理情報を共有メモリに記録する。

ZFSD は CSM の一種で、HDD の UNIX 領域を監視し、使用されなくなったファイルが発生した時に DOMS に通知する。

DOMS には CSM の機能を拡張する 3 つのモジュール、HSM、ZFE、HDE が含まれる。

HSM は共有メモリに記録された HDD の RAW 領域の管理情報を監視し、MFP が情報を削除した領域の記録を見付けると、OS を通してその記録が指している HDD の領域を上書き消去する。

ZFE は、ZFSD から UNIX 領域の不要ファイルの通知を受けると、そのファイルを上書き消去する。

HDE は、管理者からの要求によって SCS から呼び出されると、HDD 上の全ての領域を上書き消去する。

図 3 に MFP のソフトウェア構成を示す。

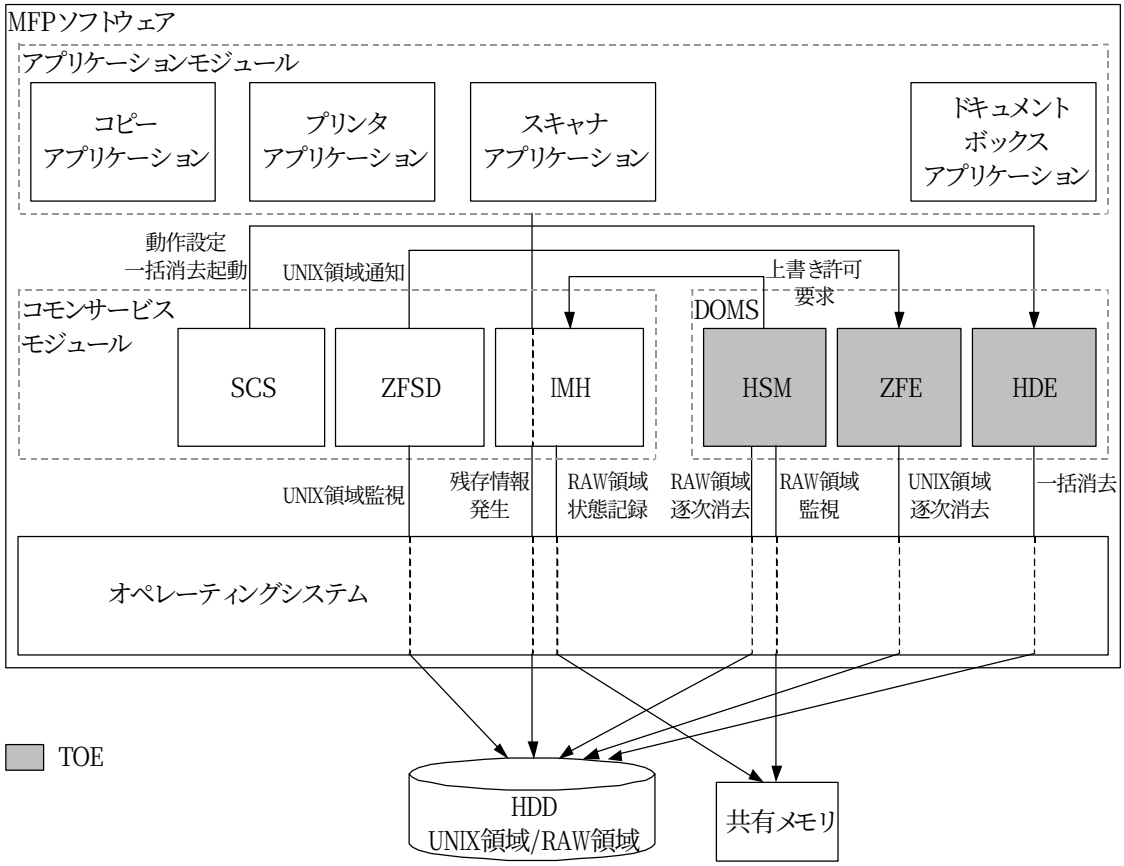

図 3: MFP のソフトウェア構成

2.3 TOE の論理的範囲

[TOE の論理的範囲]

TOE は共有メモリ上にある HDD の RAW 領域の管理情報を監視し、MFP から上書き消去の指示がある領域を見付けてその領域を上書き消去するために RAW 領域逐次消去機能を提供する。また MFP から UNIX 領域の情報の上書き消去の指示を受けて、その領域を上書き消去するために UNIX 領域逐次消去機能を提供する。TOE はまた、HDD 上の全ての情報を復元不能にするために、一括消去機能を提供する。

[MFP の論理的範囲]

MFP は一般利用者に対し、プリンタ、コピー、およびスキャナの機能を提供する。これらの機能は、HDD 上に作業用データを保存する。作業終了とともにこのデータは使用されなくなり、残存情報となる。

MFP はドキュメントボックス機能をも提供する。この機能は一般利用者の操作によって HDD 上にイメージデータを蓄積する。蓄積されたイメージデータが必要無くなった時には、一般利用者の操作によって削除され、残存情報となる。

MFP は HDD の RAW 領域および UNIX 領域上の残存情報の有無を管理する。MFP は RAW 領域の残存情報の有無を TOE に知らせるために、その管理情報を共有メモリに記録する。また、UNIX 領域に残存情報が存在することを検知すると、MFP はその情報の上書き消去を TOE に指示する。

MFP はまた、TOE の逐次消去機能のふるまいを制御するために、逐次消去動作設定の機能を提供する。また、TOE の一括消去機能のふるまいを制御するために、一括消去起動の機能を提供する。さらに、残存情報の状態を利用者が確認できるようにするために、残存情報状態表示の機能をも提供する。

図 4 は MFP および TOE の提供する機能とその関連を表す。

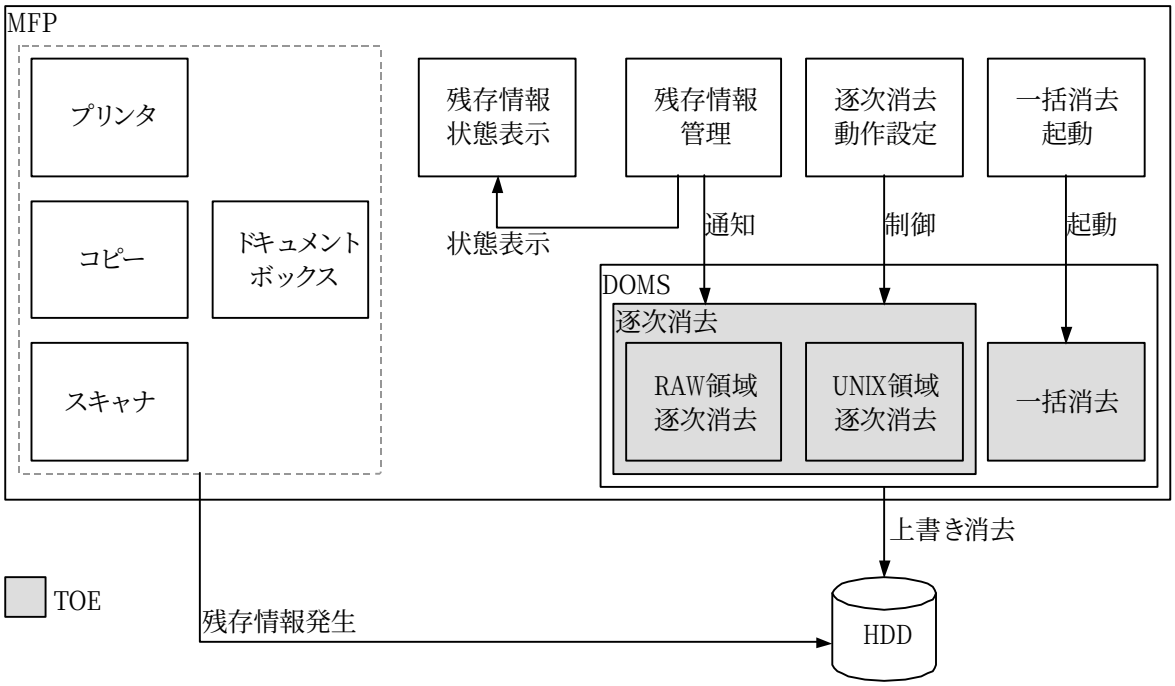

図 4: MFP および TOE の 機能とその関連

2.3.1 TOE の機能

以下に TOE が提供する機能の詳細を記述する。

[逐次消去]

HSM は、共有メモリ上に記録された HDD の RAW 領域の管理情報を監視し、その記録が示している HDD 上の領域に対する上書き消去の許可を IMH に要求する。IMH から許可を受けると、HSM は指定された消去方法でその領域を上書き消去する。上書き消去が完了すると、HSM はその領域に対する上書き消去の終了を IMH に通知し、HDD の RAW 領域の管理情報の監視を再開する。

ZFE は、ZFSD から UNIX 領域上の不要なファイルの存在の通知を受けると、指定された消去方法でその領域を上書き消去する。

逐次消去の方法として以下のような 3 種類の上書き消去方法がある。

- NSA 方式
  乱数で 2 回上書きし、NULL(0)データで 1 回上書きする

- DoD 方式
  固定値で 1 回上書きし、固定値の補数を取りその値で 1 回上書きし、乱数で上書きし、その後検証を行なう。
- 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

[一括消去]

HDE は MFP から呼び出されると指定された消去方法によって HDD の全領域を上書き消去する。また、MFP からの指示により一括消去を中止することができる。

一括消去の方法として以下のような 3 種類の上書き消去方法がある

- NSA 方式
- DoD 方式
- 乱数書込み方式

2.3.2 MFP の機能

以下に、TOE の範囲外として MFP が提供し、TOE に関連する機能を記述する。

[残存情報管理]

MFP は、HDD の RAW 領域に存在する残存情報の状態を管理し、その管理情報を HSM に通知するために共有メモリに記録する。また、MFP は UNIX 領域を監視し、不要なファイルを見付けると ZFE にそのことを通知する。

[逐次消去動作設定]

管理者だけが MFP のオペレーションパネルを操作して TOE の逐次消去機能のふるまいを制御することができる。この機能によって管理者が制御できる項目は以下のものである。

- 逐次消去を有効化または無効化する。
- NSA 方式、DoD 方式、乱数書込み方式の 3 つから逐次消去に用いる上書き消去方式を選択する。
- 乱数書込み方式を選択した場合は、乱数を書込む回数を 1 回から 9 回までの範囲で指定する。

[一括消去起動・中止]

管理者だけが MFP のオペレーションパネルを操作して TOE の一括消去機能を起動することができる。MFP は NV-RAM に記録された設定値を工場出荷時の値に戻す。これによって TOE の逐次消去機能は無効に、上書き消去方式は NSA 方式に、また、乱数書き込み方式の書き込み回数が 3 回に設定される。その後、MFP は一括消去以外の処理を停止し、TOE の一括消去機能を起動する。起動する際には、一括消去機能の以下のふるまいを指定する。

- NSA 方式、DoD 方式、乱数書込み方式の 3 つから一括消去に用いる上書き消去方式を選択する。
- 乱数書込み方式を選択した場合は、乱数を書込む回数を 1 回から 9 回までの範囲で指定する。

また、一括消去の最中に管理者は一括消去を中止することができる。

[残存情報状態表示]

DOMS が稼動中であるとき、MFP のオペレーションパネルには残存情報の状態を表わすアイコンが表示される。HDD 上に残存情報が存在する時、オペレーションパネルには残存情報があることを示すアイコンが表示される。DOMS が残存情報を消去している最中には、残存情報があることを示すアイコンが点滅する。HDD 上に残存情報が存在しない時は、残存情報が存在しないことを示すアイコンが表示される。これにより、一般利用者および管理者は残存情報の有無を簡単に確認できる。アイコンの表示は、DOMS が正しくインストールされ、上書き消去機能が機能していることをも示す。

[MFP の一般機能]

MFP はコピー/プリンタ/スキャナ/ドキュメントボックス等の機能を持つ。これらの機能は HDD 上の RAW 領域あるいは UNIX 領域に作業用データを作成、またはイメージデータを蓄積する。これらのデータが不要になると、MFP はこれらのデータを残存情報として管理し、TOE に上書き消去を指示する。

[その他]

もし消去処理中に電源が切断された場合、電源が再び投入された後で、MFP は TOE の上書き消去処理を再開する。

コピー/プリンタ/スキャナ/ドキュメントボックスのジョブは TOE より優先度が高い。TOE の上書き消去が動作しはじめたときに他のジョブが同時に起動した場合、TOE はそのジョブが終わるのを待って、消去を開始する。他のジョブが TOE の消去処理中に始まった時は、TOE は一時停止して、そのジョブの終了後に再開する。

TOE が上書き消去中に HDD への書き込みを失敗した場合、MFP は停止される。

2.4 用語解説

本 ST を明確に理解するために、表 2 において特定の用語の意味を定義する。

表 2: DOMS に関連する特定の用語

用語	定義
MFP	デジタル複合機(Multi Function Product)。 1 台でコピー、プリンタ等 2 種類以上の機能を持ったプリンタのことである。この ST の TOE はリコー製 MFP に使用する。
DOMS	データオーバーライトモジュール(Data Overwrite Modules)。 データの痕跡の解析をさせない事を目的として、HDD の領域を上書き消去する機能を持っている。DOMS は NSA 方式、DoD 方式、乱数書込み方式によって対象エリアの上書き消去を行なう。
HSM	DOMS を構成するモジュールの 1 つ。MFP によって上書き消去を指示された RAW 領域上のデータの逐次消去を行なう。
ZFE	DOMS を構成するモジュールの 1 つ。MFP によって上書き消去を指示された UNIX 領域上のデータの逐次消去を行なう。

用語	定義
HDE	DOMS を構成するモジュールの 1 つ。HDD の一括消去を行なう。
CSM	コモンサービスモジュール(Common Service Module)。 コピーやプリンタのようなアプリケーションモジュールで使用される一般的な機能を提供する。またイメージデータの管理機能は CSM に含まれる。
SCS	CSM の一種で、MFP 上で動作しているアプリケーションを把握し、設定情報を管理する。また、管理者からの要求があった時に、DOMS の一括消去機能を起動する。
IMH	CSM の一種で、OS を通してプリントエンジン、およびスキャナユニットとコントローラボード間のイメージデータの転送を制御する。IMH はまた、HDD の RAW 領域上のイメージデータおよび残存情報の有無を管理し、その管理情報を共有メモリに記録する。
ZFSD	CSM の一種で、HDD の UNIX 領域を監視し、使用されなくなったファイルが発生した時に DOMS に通知する。
残存情報	残存情報とは、MFP がイメージデータを削除することによって発生した不要な情報のことである。通常、”削除”プロセスが論理的にイメージデータを削除するが、HDD には物理的なデータ消去の痕跡が残る。これらの痕跡が残存情報である。
UNIX 領域	OS のファイルシステムによって管理されている HDD 上の領域。この領域にあるデータは通常のファイル操作によってアクセスできる。
RAW 領域	OS のファイルシステムによって管理されていない HDD 上の領域。この領域にあるデータは OS のファイル操作の機能を使わずに CSM が独自の方法で管理する。
ドキュメントボックス	ドキュメントボックスは、MFP 内の論理的なボックスのことでドキュメントの電子ファイルが保存されている。ドキュメントボックスのオプションが入っている時に利用できる。
NetBSD	UNIX の互換 OS で、フリーウェアで移植性が高い。
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。
NSA 方式	NSA 方式は以下の方法で上書き消去を行なう。 - 乱数を 2 回上書き - NULL(0)を 1 回上書き
DoD 方式	DoD 方式は、以下の方法で上書き消去を行なう。 - 固定値データを 1 回上書き - 固定値の補数を取りその値で 1 回上書き - 乱数で 1 回上書き - さらに最後に検証を実行
乱数方式	乱数を指定された回数(1~9 回)上書きする。

用語	定義
上書き消去方式	上書き消去方式には 3 種類ある。3 種類については以下の通りである。 - NSA 方式 - DoD 方式 - 乱数書込み方式 逐次消去、および一括消去それぞれについて、上記の上書き消去方式を選ぶことができる

3 TOE セキュリティ環境

3.1 前提条件

この章では、TOE の環境に関わる前提条件を識別し、記述する。

A.BREAK **TOE の動作が中断されることはないものとする。**

TOE が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.CANCEL **TOE の一括消去が中止されることはないものとする。**

TOE の一括消去が完了する前に利用者の意図に反して一括消去が中止されることはないものとする。

3.2 脅威

TOE および環境が対抗する脅威はない。

3.3 組織のセキュリティ方針

この章では、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し、記述する。

OSP.RESIDUAL **TOE は MFP から指示された HDD 上の領域から情報を読み出せないようにしなければならない。**

TOE は MFP から指示された HDD 上の領域から情報を読み出せないようにしなければならない。

4 セキュリティ対策方針

4.1 TOE のセキュリティ対策方針

この章では、3.3 章で述べた組織のセキュリティ方針を実施する、TOE のセキュリティ対策方針を記述する。

O.OVERWRITE TOE は MFP から上書き消去を指示された領域の情報が読み出されないことを保証する。

TOE は、MFP から指示された HDD 上の情報が読み出されないようにするために、その情報を上書き消去する。

4.2 環境のセキュリティ対策方針

4.2.1 IT 環境のセキュリティ対策方針

前提条件や脅威に対する IT 環境のセキュリティ対策方針はない。

4.2.2 非 IT 環境のセキュリティ対策方針

この章では、3 章で記述した前提や脅威に対する IT 以外の環境のセキュリティ対策方針を記述する。

OE.POWER 利用者は上書き消去が完了していない状態では電源を切断しない。

MFP の電源を切断する際には、利用者はオペレーションパネル上のアイコンを確認し、上書き消去が完了している状態で電源を切断する。

OE.CANCEL 利用者は一括消去が中止されないように MFP を管理する。

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中止されないように MFP を管理する。

5 IT セキュリティ要件

5.1 TOE セキュリティ機能要件

この章では、4.1 章で規定されたセキュリティ対策方針を実現するための、TOE の機能要件が記載される。[CC]で定義された割付と選択操作を行なった部分は、**[太文字と括弧]**で識別される。

FPT_RVM.1	**TSP の非バイパス性**
下位階層:	なし
FPT_RVM.1.1	TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。
依存性:	なし

5.2 最小機能強度主張

本 TOE の最小機能強度を SOF-基本とする。

5.3 TOE セキュリティ保証要件

本 TOE の評価保証レベルは EAL3 である。TOE の保証コンポーネントを表 3.に示す。これは評価保証レベルの EAL3 によって定義されたコンポーネントのセットであり、他の要件は追加していない。

表 3: TOE セキュリティ保証要件(EAL3)

保証クラス	保証コンポーネント	
ACM: 構成管理	ACM_CAP.3	許可の管理
	ACM_SCP.1	TOE の CM 範囲
ADO: 配付と運用	ADO_DEL.1	配付手続き
	ADO_IGS.1	設置、生成、及び立上げ手順
ADV: 開発	ADV_FSP.1	非形式的機能仕様
	ADV_HLD.2	セキュリティ実施上位レベル設計
	ADV_RCR.1	非形式的対応の実証
AGD: ガイダンス文書	AGD_ADM.1	管理者ガイダンス
	AGD_USR.1	利用者ガイダンス
ALC: ライフサイクルサポート	ALC_DVS.1	セキュリティ手段の識別
ATE: テスト	ATE_COV.2	カバレージの分析
	ATE_DPT.1	テスト:上位レベル設計
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テスト−サンプル
AVA: 脆弱性評定	AVA_MSU.1	ガイダンスの検査
	AVA_SOF.1	TOE セキュリティ機能強度評価
	AVA_VLA.1	開発者脆弱性分析

5.4 TOE の明示されたセキュリティ機能要件

この章では、セキュリティ対策方針を実現するための TOE の明示された機能要件を記述する。

FDP_SIP.1　指定された情報の保護

下位階層:　なし

FDP_SIP.1.1　TSF は、指定された資源のどの情報の内容も利用できなくすることを保証しなければならない。

依存性:　なし

5.5 環境に対するセキュリティ要件

環境に対する機能要件はない。

6 TOE 要約仕様

6.1TOE セキュリティ機能

SF.OVERWRITE

TSF には、逐次消去処理機能、一括消去処理機能という2 種類の上書き消去機能がある。

(1) 逐次消去処理機能

TSF は、共有メモリ上に記録されたHDD のRAW 領域の管理情報を監視し、その記録が示しているHDD 上の領域を上書き消去する。

TSF はまた、UNIX 領域において MFP から指示された情報を上書き消去する。

HDD の上書き消去には、後述する上書き消去方式を用いる。

(2) 一括消去処理機能

TSF は、HDD 上の全てのデータを上書き消去する。また、MFP からの指示により一括消去を中止することができる。HDD の上書き消去には、後述する上書き消去方式を用いる。

[上書き消去方式]

上述の逐次消去処理機能および一括消去処理機能は、HDD の上書き消去に以下の 3 種類の上書き消去方式のいずれかを用いる。

- NSA 方式
- DoD 方式
- 乱数書込み方式

(a) 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

(b) 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を取りその値で 1 回上書き
- 乱数 1 回上書き
- 最後に検証を実行

(c) 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。

上書き消去方式に乱数書込み方式を選択した場合には、乱数を上書きする回数を 1～9 回の範囲で指定する。

6.2 機能強度の主張

確率的または順列的メカニズムによって実現されるセキュリティ機能は存在しない。

6.3 保証手段

この章では TOE の保証手段を記述する。以下の表 4 に示される保証手段は、5.3 章で記述された TOE セキュリティ保証要件を満たすものである。

表 4: EAL3 の保証要件と保証手段

保証クラス	保証コンポーネント	保証手段
ACM: 構成管理	ACM_CAP.3 ACM_SCP.1	imagio セキュリティカード タイプ F, Data OverWriteSecurity Unit F 構成管理書
ADO: 配付と運用	ADO_DEL.1	imagio セキュリティカード タイプ F, Data OverWriteSecurity Unit F 配付手続き書
	ADO_IGS.1	imagio セキュリティカード タイプ F, Data OverWriteSecurity Unit F 製造手順書 imagio セキュリティカードタイプ F サービスマニュアル Data OverWriteSecurity Unit F Service Manual
ADV: 開発	ADV_FSP.1 ADV_HLD.2	Zoffy V3 システム設計 MH設計仕様書 B0.HDD 上書き消去 機能仕様 MH設計仕様書 B0.HDD 上書き消去 I／F:コマンド仕様 LPUX 仕様 05 ライブラリ HDD 消去ライブラリI/F 仕様 ZOFFY-V3 UNIX ファイルシステム領域逐次消去処理 システム基本設計書 ZOFFY-V2/V3 HDD 一括消去処理 システム基本設計書
	ADV_RCR.1	imagio セキュリティカード タイプ F, Data OverWriteSecurity Unit F 表現対応分析書

保証クラス	保証 コンポーネント	保証手段
AGD: ガイダンス文書	AGD_ADM.1	imagio セキュリティカード タイプ F 使用説明書 Data OverWriteSecurity Unit F Operating Instructions
	AGD_USR.1	
ALC: ライフサイクルサポート	ALC_DVS.1	imagio セキュリティカード タイプ F, Data OverWriteSecurity Unit F 開発セキュリティ
ATE: テスト	ATE_COV.2	imagio セキュリティカード タイプ F, Data OverWriteSecurity Unit F テスト分析書
	ATE_DPT.1	
	ATE_FUN.1	
	ATE_IND.2	TOE
AVA: 脆弱性評定	AVA_MSU.1	imagio セキュリティカード タイプ F, Data OverWriteSecurity Unit F 脆弱性評定書
	AVA_SOF.1	
	AVA_VLA.1	

7 PP 主張

本 ST において適合するPP はない。

8 根拠

8.1セキュリティ対策方針根拠

この章では、4 章で識別したセキュリティ対策方針が適切で、3 章で記述されたセキュリティ環境の全ての面を扱っていることを実証する。

表 5 は、各セキュリティ対策方針が少なくとも 1 つの脅威あるいは前提条件を扱い、かつ、各脅威および前提条件が少なくとも1 つのセキュリティ対策方針によって扱われていることを示す。

表 5: セキュリティニーズとセキュリティ対策方針の関連

	O.OVERWRITE	OE.POWER	OE.CANCEL
OSP.RESIDUAL	X		
A.BREAK		X	
A.CANCEL			X

OSP.RESIDUAL 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.BREAK は OE.POWER 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.CANCEL は OE.CANCEL 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中止されることが防止されるからである。

8.2セキュリティ要件根拠

8.2.1 機能要件根拠

この章では、5 章で指定されたセキュリティ機能要件が 4 章で識別された TOE および IT 環境のセキュリティ対策方針を達成していることを実証する。

表 6 は TOE セキュリティ機能要件が TOE および IT 環境のセキュリティ対策方針に対応することを示す。

表 6: セキュリティ対策方針と機能要件の関連

	FDP_SIP.1	FPT_RVM.1
O.OVERWRITE	X	X

O.OVERWRITE は FDP_SIP.1 によって達成される。なぜなら、この要件が、MFP によって指示された情報が利用できなくなること、すなわち、MFP によって指示された情報を誰も読み出すことができなくなることを保証するからである。さらに、FPT_RVM.1 によりTSP はバイパスされないことが保証される。

8.2.2 最小機能強度レベル根拠

本 TOE は市販製品である MFP のオプションである。TOE の動作環境である MFP は一般的なオフィスで使用されることを想定しているため、本 TOE の最小機能強度は SOF-基本が妥当である。

8.2.3 セキュリティ機能要件の依存性

TOE セキュリティ機能要件の依存性について表 7 に示す。表 7 には、CC が要求する依存性に対して、ST の中で満たしている依存性を示す。

表 7: TOE セキュリティ機能要件の依存性対応表

TOE セキュリティ機能要件	CC が要求する依存性	ST の中で満たしている依存性
FDP_SIP.1	なし	なし
FPT_RVM.1	なし	なし

上記表 7 に示すように、FDP_SIP.1 と FPT_RVM.1 には CC が要求する依存性がない。従って、TOE セキュリティ機能要件が満たさなければならない依存性はない。

8.2.4 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。TOE の動作環境である MFP は一般的なオフィスで使用されることを想定しており、本 TOE は中レベル以上の攻撃能力を持つ攻撃者は想定していない。

また、TOE はデータの上書き消去という簡単なメカニズムによってセキュリティ機能を実現している。この機能は確率的または順列的メカニズムを含まず、上位レベル設計の評価(ADV_HLD.2)はそのような正当性を示すのに十分である。さらに、TSF を回避あるいは改ざんするような攻撃には高い攻撃能力が要求され、これは今回の評価の対象外である。すなわち、一般的なニーズには明白な脆弱性の分析(AVA_VLA.1)で十分である。

一方で、攻撃をより困難にするために関連情報の秘密を守る必要があり、開発環境についてもセキュアな環境であることを保証すること、すなわち開発セキュリティ(ALC_DVS.1)は重要である。

従って、評価期間およびコストを考慮すると、本 TOE に対する評価保証レベルは EAL3 が妥当である。

8.2.5 セキュリティ要件の相互サポート

セキュリティ要件の相互サポートの関係を表 8 に示す。

表 8: セキュリティ要件の相互サポート

機能要件	迂回	非活性化	改ざん
FDP_SIP.1	FPT_RVM.1	なし	なし

【迂回】

TOE が起動されれば、FDP_SIP.1 は必ず呼び出されるため迂回できない。

【非活性化】

TOE が起動されれば、FDP_SIP.1 は必ず呼び出されるため非活性化できない。

【改ざん】

本 TOE には不正なサブジェクトが存在しない。そのため、TSF が改ざんされることはない。

8.2.6 明示されたセキュリティ要件根拠

本 TOE で採用している機能要件 FDP_SIP.1 は拡張要件である。本 TOE は MFP と連携して MFP の残存情報を利用できなくすることを目的としており、FDP_RIP.1 がこれに近い要件である。しかし、残存情報の管理は MFP が行なっており、TOE は MFP からの指示を受けて情報を上書き消去しているため、FDP_RIP.1 を適用するのはふさわしくない。そのため、FDP_RIP.1 を基本として TOE に適したセキュリティ要件を拡張した。また、この明示されたセキュリティ要件は、CC パート2 のセキュリティ要件と同じスタイル、同等の詳細レベルで拡張した。

この明示されたセキュリティ要件は、上記で述べたように FDP_RIP.1 の残存情報と判断する部分のセキュリティ機能を除いたセキュリティ機能となっている。

基本にした FDP_RIP.1 では、依存性や特別な保証要件が求められていない。従って、この明示されたセキュリティ要件もそれらを必要としない。

さらに、この明示されたセキュリティ要件の保証については、EAL3 のパッケージに含まれる保証要件で十分と判断する。なぜならば、この明示されたセキュリティ要件のために特有な文書による証拠が必要ないことが自明であるからである。

8.3TOE 要約仕様根拠

8.3.1 TOE セキュリティ機能の根拠

この章では、6.1 章で定義された TOE セキュリティ機能が 5.1 章で指定された TOE セキュリティ機能要件を実現することを実証する。

表 9 は TOE セキュリティ機能が TOE セキュリティ機能要件に対応することを示す。

表 9: TOE セキュリティ機能要件と TOE セキュリティ機能の関連

	SF.OVERWRITE
FDP_SIP.1	X
FPT_RVM.1	X

SF.OVERWRITE は、上書き消去することで MFP によって指示された情報が利用できなくなることを保証する。これによって、FDP_SIP.1 が実現される。

SF.OVERWRITE は起動されると必ず実行される。これによって、FPT_RVM.1 が実現される。

8.3.2 機能強度主張の根拠

6.2 章に示すように、確率的または順列的メカニズムを含むセキュリティ機能は無い。従って、この ST には機能強度主張は必要ない。

8.3.3 セキュリティ機能の組合せ根拠

8.3.1 に示す通り、TOE は 1 つのセキュリティ機能を持つ。これは、この ST にはセキュリティ機能の相互サポートがないことを示す。従って、セキュリティ機能は、それ単独でセキュリティ機能要件を満たすように機能する。

8.3.4 保証手段の根拠

6.3 章において、EAL3 で必要とされる全てのセキュリティ保証要件に対して、保証手段となる文書および TOE が対応付けられている。また、各文書および TOE によって、セキュリティ保証要件が要求する証拠は網羅されている。従って、TOE セキュリティ保証要件は満たされている。

8.4PP 主張根拠

本 ST において適合するPP はない。

9 付録

9.1参考文献

ISO/IEC 15408, Information technology – Security techniques – Evaluation criteria for IT security,

ISO/IEC 15408-1:2005(E), Part 1: Introduction and general model,

ISO/IEC 15408-2:2005(E), Part 2: Security functional requirements,

ISO/IEC 15408-3:2005(E), Part 3: Security assurance requirements.

9.2略語

CC	コモンクライテリア (Common Criteria)
CE	カスタマエンジニア (Customer Engineer)
HDD	Hard Disc Drive の略
MFP	デジタル複合機(Multi Function Product)
OS	オペレーティングシステム (Operating System)
PP	プロテクションプロファイル (Protection Profile)
SF	セキュリティ機能 (Security Function)
ST	セキュリティターゲット (Security Target)
TOE	評価対象 (Target of Evaluation)
TSF	TOE セキュリティ機能 (TOE Security Function)