Security Target for

imagio Security Card Type D,

DataOverwriteSecurity Unit Type C

Author: Haruyuki HIRABAYASHI, Atsushi SATOH, RICOH COMPANY, LTD.
Date: 2006-11-22
Version: 1.03

This document is a translation of the evaluated and certified security target written in Japanese

Revision history

Version	Date	Author	Description
1.00	2006-08-11	Atsushi SATOH	First draft.
1.01	2006-08-29	Atsushi SATOH	Revise CC version.
1.02	2006-11-09	Haruyuki HIRABAYASHI	Revise deliverable descriptions.
1.03	2006-11-22	Haruyuki HIRABAYASHI	Revise the pointed out descriptions.

Table of Contents

List of Figures

List of Tables

1 ST introduction

1.1 ST identification

The information to identify this document and the TOE is shown below.

ST title: Security Target for
imagio Security Card Type D,
DataOverwriteSecurity Unit Type C

ST version: 1.03

Date: 2006-11-22

Author: Haruyuki HIRABAYASHI, Atsushi SATOH, RICOH COMPANY, LTD.

Product: imagio Security Card Type D,
DataOverwriteSecurity Unit Type C

Note: Hereafter these products are called with a generic name "Data Overwrite Module".

"imagio Security Card Type D" is a name in Japan.

"DataOverwriteSecurity Unit Type C" is a name in other countries.

The TOE is applied to the MFP with x86 type CPU.

TOE: Software of Data Overwrite Module

TOE version: V0.04

CC version: CC version 2.3, ISO/IEC 15408:2005

Note: The following documents are used as the Japanese translations.

-Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCIMB-2005-08-001

-Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCIMB-2005-08-002

-Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCIMB-2005-08-003

-Interpretations-0512

Keywords: Digital MFP, document, copier, printer, facsimile, fax, scanner, network, office, hard disk, security, overwrite, protection for residual information

1.2 ST overview

This ST describes the data overwrite module software (hereinafter: DOMS) mounted in Multi-functional printers (hereinafter: MFP) produced by Ricoh Co., Ltd. The MFP is an OA device consisting of a copy function, print function, scan function and facsimile function. This TOE is an option kit, which is installed in the MFP for safer use, and its function is to overwrite designated areas of the HDD for erasing by the MFP.

1.3 CC conformance

This document meets the followings:

- CC part 2 extended
- CC part 3 conformant
- EAL3 conformant

There are no Protection Profiles claimed to which this ST is conformant.

1.4 Reference

The following documents are referred to write this document.

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model
  August 2005 Version 2.3 CCIMB-2005-08-001
  (December 2005 1.0 edition of Japanese translation, Information technology Promotion Agency, Security Center)
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements
  August 2005 Version 2.3 CCIMB-2005-08-002
  (December 2005 1.0 edition of Japanese translation, Information technology Promotion Agency, Security Center)
- Common Criteria for Information Technology Security Evaluation Part 2: Security assurance requirements
  August 2005 Version 2.3 CCIMB-2005-08-003
  (December 2005 1.0 edition of Japanese translation, Information technology Promotion Agency, Security Center)
- Interpretations-0512
  (December 2005, Information technology Promotion Agency, Security Center)

2 TOE description

2.1 TOE overview

2.1.1 Product type

The product classification of this TOE is a software product attached as an option of the MFP. This software product is installed at the location of the customer.

2.1.2 Positioning of the TOE

The TOE is used for the purpose of overwriting area of the HDD for erasing information to prevent reuse of information in the area designated by the MFP.

The HDD used by the MPF is divided into the RAW area and UNIX area. The TOE monitors the managed information of the RAW area of the HDD in the shared memory of the MFP. If an area is discovered for which there has been a direction from the MFP to carry out overwrite and erasing, that area is overwritten and erased. In addition, the TOE receives an instruction from the MFP to overwrite for erasing information of the UNIX area and carry out the instruction. Moreover, in order to prevent leaking of confidential information from the information recorded in the HDD housed in the MFP, it has a function to overwrite for erasing all information on the HDD in the case of return, assignment to another department or disposal due to termination of the lease/rental agreement.

The MFP determines what information to be overwritten and indicates the information to the TOE.

In the case of copying, printing, scanning and facsimile transfer/reception, the MFP composes temporary image data on the HDD for operational use. When copying, printing, scanning and facsimile processing has finished; the MFP erases the above-mentioned temporarily composed image data.

In addition, if the user indicates storage of image data, the MFP stores the image data on the HDD. If the user indicates erasing of stored image data, the MFP erases the above-mentioned stored image data. When the data is erased, the information that is no longer necessary for the copy, printer, scanner, facsimile and document box functions are treated as non-existent from the standpoint of those functions. Although the image data erased by the MFP can no longer be used by these functions, its contents actually exist on the HDD. If the information stored as image data is erased, the MFP manages that data as residual information. By means of that function, the MFP stores the data either in the RAW area or in the UNIX area. In order that the MFP can inform the TOE of the presence/absence of residual information in the RAW area, it stores that management information in the shared memory. If residual information exists in the UNIX area, the MFP indicates overwrite for erasing to the TOE.

2.1.3 Operational environment of MFP on which TOE is mounted

The TOE is software that operates on the MFP, and is provided as an option to extend the functions of the MFP. The MFP does not only consist of the basic copy function. It has several varieties of functions on a single unit, including facsimile, printer, and scanner. This TOE has been conceived for mounting and use on an MFP used in a conventional office setting. The MFP contains an internal HDD. The HDD is used for storing image data of the copier and printer. During office operational times, the MFP is under the supervision of the concerned parties in the office. However, at night or on holidays, there is a possibility of an outsider entering the deserted office and removing the HDD.

The conceived operational environment of the MFP has been shown as a diagram (Figure 1).

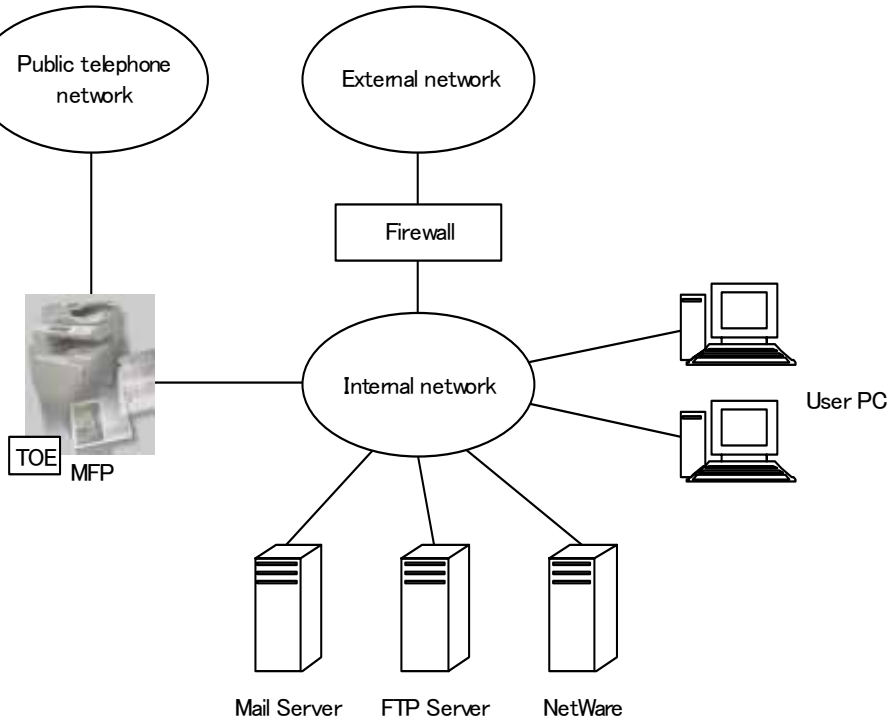

Figure 1: Environment for the usage of MFP

The following items are connected to the operational environment of the MFP.

- User PC:
  Requests that the MFP print documents and send facsimile messages. It can also received scanned data and image data stored to the MFP.
- Mail server, FTP server, NetWare server:
  It is possible to send image data scanned by the MFP to a mail server, FTP server or NetWare server.
- Public telephone line:
  Carries out transfer and receipt of facsimile messages.

A firewall is installed between the internal network and the external network in order to protect the devices connected to the internal network. In addition, public telephone lines can only be used for transmission/reception of facsimile messages. It is not possible to use those lines to invade the MFP or internal network.

This TOE has been conceived for mounting and using in the MFP models shown in the Table (Table 1).

Table 1: Target MFP of the TOE

	Product names in Japan	Product names in other country
Model 1	Ricoh imagio Neo C600Pro Ricoh imagio Neo C600 Ricoh imagio Neo C600 model 75	Ricoh Aficio 3260C, Aficio Color5560 Lanier LC155, Lanier LD160c Savin C6045, Savin SDC555 Nashuatec DSc460, Nashuatec CS555 RexRotary DSc460, RexRotary CS555 Gestetner DSc460, Gestetner CS555 infotec ISC 4560/5560
Model 2	Ricoh imagio Neo 603 Ricoh imagio Neo 603 model 75 Ricoh imagio Neo 753 Ricoh imagio Neo 753 model T Ricoh imagio Neo 753 model 75	Ricoh Aficio 2051/2060/2075 Lanier LD151/LD160/LD175 Savin 4051/4060/4075 Nashuatec DSm651/DSm660/DSm675 RexRotary DSm651/DSm660/DSm675 Gestetner DSm651/DSm660/DSm675 infotec IS 2151/2160/2175
Model 3	Ricoh imagio MP 6000 Ricoh imagio MP 6000 SP Ricoh imagio MP 7500 Ricoh imagio MP 7500 T Ricoh imagio MP 7500 SP	Ricoh Aficio MP 5500/5500SP/6500/6500SP/ 7500/7500SP Lanier-US LD255/LD255sp/LD265/ LD265sp/LD275/LD275sp Lanier-EU MP 5500/6500/7500 Lanier-AUS MP 5500/6500/7500 Savin 8055/8055sp/8065/8065sp/8075/8075sp Nashuatec MP 5500/6500/7500 RexRotary MP 5500/6500/7500 Gestetner MP 5500/6500/7500 Gestetner-US DSm755/DSm755sp/DSm765/ DSm765sp/DSm775/DSm775sp infotec IS 2255/2265/2275

2.2 Physical boundary of the TOE

The Ricoh MFP is composed of hardware and software.

The hardware is composed of the printer engine, scanner unit, facsimile unit, operation panel, HDD and controller board.

The print engine prints out data from printer and copier functions and received data by the facsimile unit while controlling paper feed and paper eject.

The scanner unit takes image data from paper documents into MFP. It is used for take image data from the copier, scanner and facsimile transmission functions into controller board.

The facsimile unit carries out transmission and reception of facsimile messages.

The operation panel displays the information to general users and administrator and also received instructions input by general users and administrator. General users and administrator operate the operation panel to use the functions of the MFP.

The HDD is used for storing image data. During printing, copying, scanning or facsimile transmission/reception, the MFP temporarily stores image data for working. Also general users use the HDD to keep their data until making use of the data.

The controller board controls whole of the MFP. In the MFP, the controller board is equipped with the processor and RAM to execute software, ROM on which the software such as operating system (OS) and the various application modules are stored, NV-RAM on which setting information for MFP is recorded, and the host interface to connect to the user PC and servers. DOMS is saved in the SD memory card, and the SD memory card is attached the controller board.

Figure 2 shows the structure of the MFP hardware.

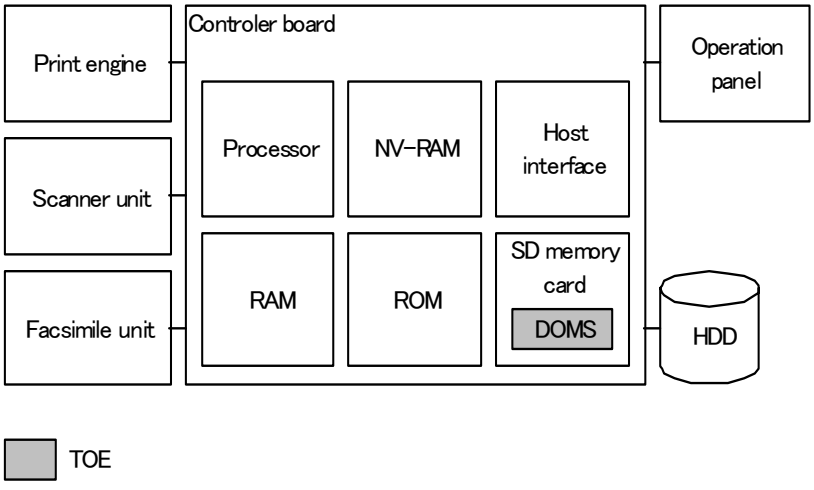

Figure 2: Structure of MFP hardware

The software is composed of the OS, common service module (CSM), and application modules.

The OS manages the HDD and other hardware and provides the interfaces for operation of these hardware resources. The OS is an original Ricoh OS with NetBSD as its basis.

The application modules supply such functions as copying, printing, facsimile and scanning to general users. These modules receive controls from general users and request the required processes from the CSM to realize the various functions.

The CSM supplies the common functions that are used by the application modules. The CSM supplies such functions as management of the areas of the HDD on which image data and residual information exist, and display on the operation panel of the condition of residual information.

The SCS is a type of CSM. It grasps the applications operating on the MFP to manage setting information. Moreover, in case of requests from general users, it starts the DOMS general erasure function.

The HDD is divided into the RAW area and UNIX area, storing data in one of these areas according to MFP functions.

The IMH is a type of CSM. It uses the OS to control transfer of image data between the scanner unit or facsimile unit and the controller board. The IMH also manages the existence or non-existence of image data and residual information in the RAW area of the HDD, storing that management information to the shared memory.

The ZFSD is a type of CSM. It monitors the UNIX area of the HDD and informs the DOMS when files that are no longer used.

DOMS includes three modules (HSM, ZFE, HDE) that are used to extend the functions of the CSM.

The HSM monitors the management information of the RAW area in the HDD recorded in the shared memory. When the HSM finds a record, which indicates that the information has been erased by the MFP, it overwrites for erasing the area of the HDD indicated by the record via the OS.

When the ZFE receives a notice of a discarded file in the UNIX area from the ZFSD, the ZFE overwrites for erasing that file.

When the HDE is called by the SCS due to a request from the administrator, the HDE overwrites for erasing all areas on the HDD. Figure 3 shows the structure of the MFP software.

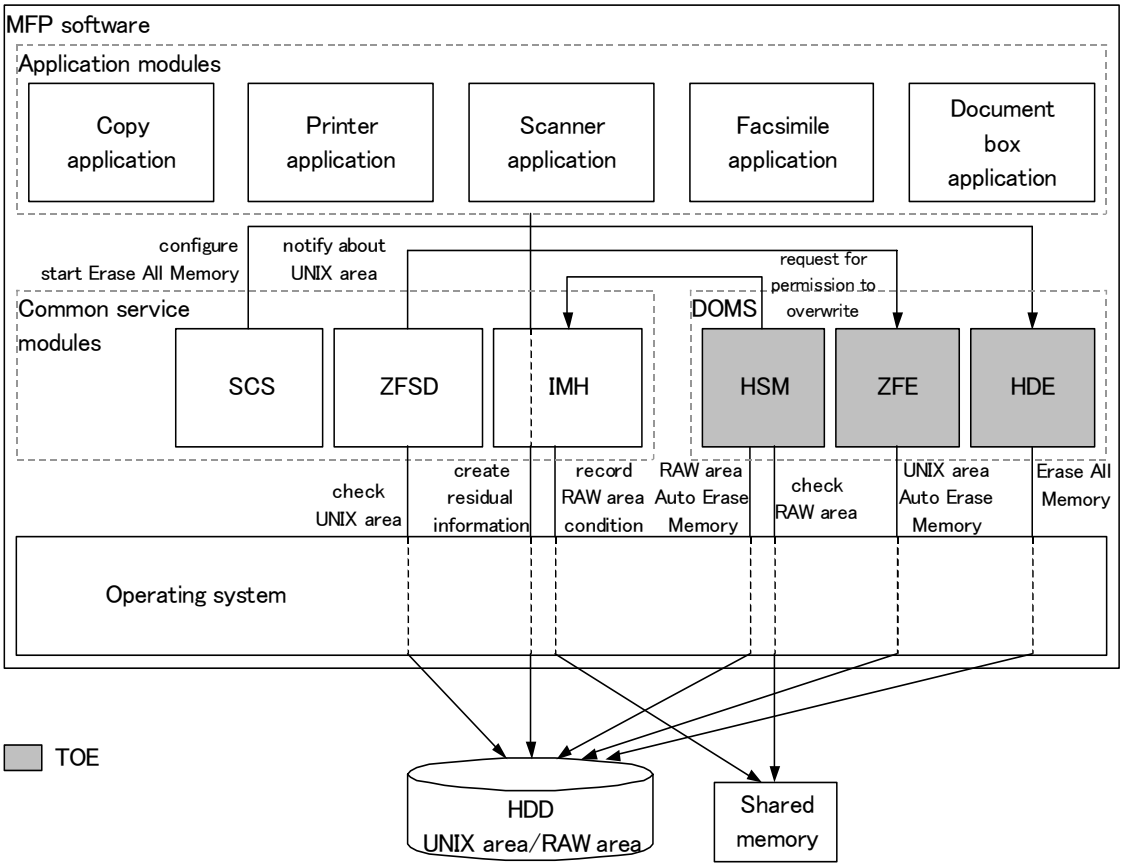

Figure 3: Structure of MFP software

2.3 Logical boundary of the TOE

[Logical boundary of the TOE]

The TOE provides RAW area Auto Erase Memory function that monitors management information of HDD RAW area on the shared memory, finds the area ordered to overwrite by the MFP, and overwrites the area. Also, the TOE provides UNIX area Auto Erase Memory function to overwrite the area in response to the order from the MFP to overwrite information on UNIX area. Furthermore, the TOE provides Erase All Memory function to make all information on HDD unavailable.

[Logical boundary of the MFP]

The MFP provides printer, copier, scanner, and facsimile functions to users. These functions store working data on the HDD. When the operation is finished, the data becomes disused, and remains as residual information.

The MFP also provides document box function. This function stores image data on the HDD by user's operation. When the stored image data becomes not needed, the data is deleted by user's operation, and remains as residual information.

The MFP manages existence or non-existence of residual information on the HDD RAW area and UNIX area. The MFP records management information of residual information to the shared memory to notify the TOE of existence of residual information on RAW area. Also, The MFP orders the TOE to overwrite the information when the MFP finds existence of residual information on UNIX area.

Furthermore, the MFP provides the configuration function to control the behaviour of Auto Erase Memory of the TOE. Also, the MFP provides the configuration function to control the behaviour of Erase All Memory of the TOE. The MFP provides also the function indicating condition of residual information for users to be able to check residual information.

Figure 4 shows the MFP and the TOE functions and its relations.

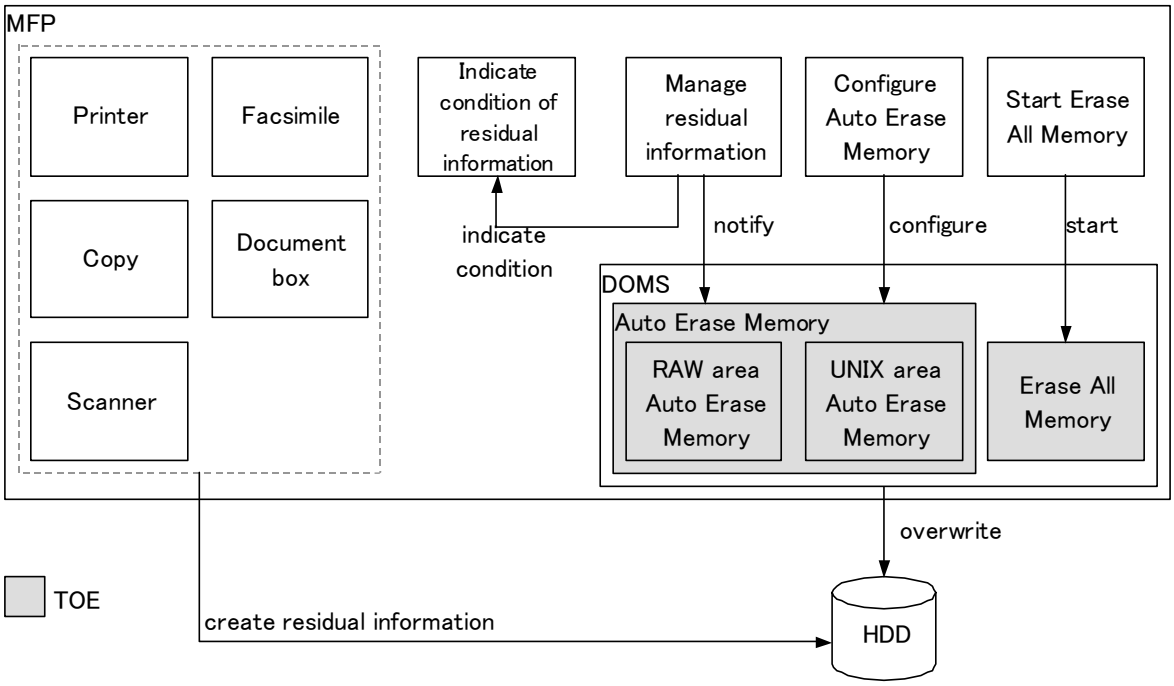

Figure 4: MFP and the TOE functions and its relations

2.3.1 TOE functionality

The following describes details of the functions provided by the TOE.

[Auto Erase Memory]

HSM monitors management information of HDD RAW area recorded in the shared memory, and requests permission to overwrite the HDD area designated by the management information to IMH. When IMH permits, HSM overwrites the area with specified method. At the end of overwriting, HSM notifies IMH of end of overwriting the area, and restarts to monitor management information of HDD RAW area.

When notified of existence of disused file on UNIX area by ZFSD, ZFE overwrites the area by specified method.

There are following three methods for Auto Erase Memory.

- NSA method
  overwrite twice with random numbers, and once with Null (0).
- DoD method
  overwrite once with fixed numbers, once with complement of the fixed numbers, once with random numbers, and check at last.
- Random Numbers method
  overwrite specified times (from one to nine times) with random numbers.

[Erase All Memory]

When called by the MFP, HDE overwrites all the area of the HDD by specified overwriting method. Erase All Memory can be cancelled by the order from the MFP.

There are following three methods for Erase All Memory.

- NSA method
- DoD method
- Random Numbers method

2.3.2 MFP functionality

The MFP provides functions out of the TOE but related to the TOE as below.

[Management of residual information]

The MFP manages existence of residual information on HDD RAW area, and records the management information on the shared memory to notify HSM. Also, the MFP monitors UNIX area, and notifies ZFE when disused file is found.

[Configuration of Auto Erase Memory]

Only the administrator can control the behaviour of Auto Erase Memory function of the TOE through the operation panel of the MFP. The administrator can control following items by this function.

- activate or deactivate Auto Erase Memory.
- select one of three methods, NSA method, DoD method, and Random Numbers method for Auto Erase Memory.
- specify number of times from one to nine for overwriting when Random Numbers method is selected.

[Start / Cancel of Erase All Memory]

Only the administrator can start Erase All Memory function of the TOE through the operation panel of the MFP. The MFP resets the configuration values recorded in NV-RAM to factory default. Thereby the Auto Erase Memory of the TOE is deactivated, overwriting method is set to NSA method, and the number of times for Random Numbers method is set to three. Then, the MFP stops all jobs other than Erase All Memory, and starts Erase All Memory. When starting Erase All Memory, those following behaviours are specified.

- select one of three methods, NSA method, DoD method, and Random Numbers method for Erase All Memory.
- specify number of times from one to nine for overwriting when Random Numbers method is selected.

Also, the administrator can cancel Erase All Memory during overwriting.

[Indicating condition of residual information]

When the DOMS is active, the icon indicating condition of residual information is shown on the operation panel of the MFP. When the residual information exists on the HDD, the icon indicating existence of residual information is shown on the operation panel. During overwriting the residual information, the icon blinks. When the residual information does not exist on the HDD, the icon indicating non-existence of residual information is shown. Thereby, users and the administrator can confirm easily the existence of residual information. Showing the icon indicates that the DOMS is installed correctly and overwrite function is activated.

[General functions of MFP]

The MFP has the copier/printer/scanner/facsimile/document box functions. Those functions create working data or store image data on HDD RAW area or UNIX area. Those data becomes disused, the MFP manages those data as residual information, and orders the TOE to overwrite them.

[Miscellaneous]

If the power is turned off during overwriting, the MFP restarts overwriting process of the TOE after the power is turned on. The job of copier/printer/scanner/facsimile/document box has high priority over the TOE. When the other job is started at the same time with the TOE overwriting, the TOE waits for the end of the job and start overwriting. When the other job is started during overwriting, the TOE is suspended and restarted after the end of the job.

If the writing on the HDD is failed during the TOE overwriting, the MFP is aborted.

2.4 Terminology

For clear understanding of this ST, the meaning of terminology is defined in Table 2.

Table 2: Terminology related to DOMS

Term	Definition
MFP	Multi-Functional Printer. It is the printer that has multiple functions such as copier, printer in a single machine. The TOE of this ST is used in the MFP manufactured by Ricoh.
DOMS	Data Overwrite Modules. It has the function to overwrite HDD area for preventing analysis of a footprint of data. DOMS overwrites target area with NSA method, DoD method, or Random Numbers method.

HSM	One of modules composing DOMS. It automatically overwrites the data on RAW area specified by the MFP.
ZFE	One of modules composing DOMS. It automatically overwrites the data on UNIX area specified by the MFP.
HDE	One of modules composing DOMS. It performs Erase All Memory.
CSM	Common Service Modules. They provide common services used by applications such as copier or printer. The management function of image data is also included in the CSM.
SCS	One of CSM. It perceives applications running on the MFP, and manages configuration information. Also, it starts Erase All Memory function of DOMS in response to the administrator's request.
IMH	One of CSM. It controls transmission of image data between the controller board and the print engine, the scanner unit, or the facsimile unit. Also, it manages existence of image data and residual data information on RAW area, and records the management information on the shared memory.
ZFSD	One of CSM. It monitors UNIX area on the HDD, and notifies DOMS of existence of disused files.
Residual information	The residual information is the disused information generated with deletion of image data by the MFP. Generally, “delete” process logically removes image data, but residual of deleted data actually exists. Those footprints are residual information.
UNIX area	HDD area managed by OS file system. The data that exists on the area can be accessed by normal file operation.
RAW area	HDD area not managed by OS file system. The data that exists on the area is managed by CSM in its way without OS file operation.
Document box	It is the logical box in which the electronic files of documents are stored. It can be used when the document box option is attached.
NetBSD	UNIX compatible OS. It is the free software and has high portability.
SD memory card	SD memory card is the secure digital memory card. It is a memory device with high functionality, small as postage stamps. It is used to provide the TOE or other applications to the MFP.
NSA method	NSA method overwrites with following process: - overwrite twice with random numbers. - overwrite once with NULL (0).
DoD method	DoD method overwrites by following process: - overwrite once with fixed numbers. - overwrite once with complement of the fixed numbers. - overwrite once with random numbers. - Furthermore, carrying out final verification.
Random numbers method	overwrite specified times (from one to nine times) with random numbers.
overwriting method	There are three overwriting methods as follows : - NSA method.

	- DoD method. - Random Numbers method. Those above methods can be selected for each function, Auto Erase Memory and Erase All Memory.

3 TOE security environment

3.1 Assumptions

In this section, the assumptions concerning the environment of the TOE are identified and described.

A.BREAK **It is assumed that the execution of the TOE is not aborted.**

The execution of the TOE is not aborted by turning off the power of the MFP before the TOE finishes overwriting.

A.CANCEL **It is assumed that the execution of Erase All Memory is not cancelled.**

The execution of Erase All Memory is not cancelled without user's intent before the function is finished.

3.2 Threats

There are no threats countered by the TOE or the environment.

3.3 Organisational security policies

In this section, the organisational security policy with which the TOE shall comply is identified and described.

OSP.RESIDUAL **The TOE shall prevent from retrieving information on the HDD area specified by the MFP.**

The TOE shall prevent from retrieving information on the HDD area specified by the MFP.

4 Security objectives

4.1 Security objectives for the TOE

In this section, the security objective for the TOE is described. The security objective for the TOE covers the organisational security policy described in section 3.3.

O.OVERWRITE The TOE shall ensure that the information on the area ordered by the MFP to overwrite cannot be retrieved.

The TOE overwrites the information on the HDD specified by the MFP to prevent from retrieving.

4.2 Security objectives for the environment

4.2.1 Security objectives for the IT environment

There are no security objectives for the IT environment.

4.2.2 Security objectives for the non-IT environment

In this section, the security objectives for the non-IT environment are described. The security objectives for the non-IT environment cover the assumptions or threats described in section 3.

OE.POWER User shall not turn off the power of the MFP before overwriting is finished.

When turning off the power of the MFP, user confirms the icon shown on the operation panel and turns off the power on the condition that the overwriting is finished.

OE.CANCEL User shall manage the MFP to prevent the function Erase All Memory from being cancelled.

When performing Erase All Memory, user manages the MFP to prevent the function from being cancelled without his/her intent.

5 IT security requirements

5.1 TOE security functional requirements

In this section, the TOE security functional requirement to achieve the security objective described in section 4.1 is identified and described. The parts against which the assignment and selection operations defined in [CC] are performed are identified with **[bold letters and brackets]**.

FPT_RVM.1	**Non-bypassability of the TSP**
Hierarchical to:	No other components.
FPT_RVM.1.1	The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
Dependencies:	No dependencies

5.2 Minimum strength of function claim

The minimum strength level claimed for the TOE is SOF-Basic.

5.3 TOE security assurance requirements

The evaluation assurance level claimed for the TOE is EAL3. The assurance components for the TOE are shown in Table 3. It is the set of components defined by the evaluation assurance level EAL3 and no other requirements have been augmented.

Table 3: TOE security assurance requirement (EAL3)

Assurance class	Assurance component	
ACM: Configuration management	ACM_CAP.3	Authorisation controls
	ACM_SCP.1	TOE CM coverage
ADO: Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security enforcing high-level design
	ADV_RCR.1	Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ALC: Life cycle support	ALC_DVS.1	Identification of security measures
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

5.4 Explicitly stated TOE security functional requirements

In this section, an explicitly stated TOE security functional requirement that achieves the security objective is described.

FDP_SIP.1	**Specified information protection**
Hierarchical to:	No other components.
FDP_SIP.1.1	The TSF shall ensure that any previous information content of a specified resource is made unavailable.
Dependencies:	No dependencies

5.5 Security requirements for the IT environment

There are no security requirements for the IT environment.

6 TOE summary specification

6.1 TOE security functions

SF.OVERWRITE

The TSF has two types of overwriting functionality, Auto Erase Memory and Erase All Memory.

(1) Auto Erase Memory

The TSF monitors management information of HDD RAW area recorded on the shared memory, and overwrite HDD area specified by the management information.

The TSF also overwrite HDD UNIX area specified by the MFP.

To overwrite the HDD, the after-mentioned methods are used.

(2) Erase All Memory

The TSF overwrites all data on the HDD. The TSF can cancel Erase All Memory by order of the MFP. To overwrite the HDD, the after-mentioned methods are used.

[Methods of overwriting]

Auto Erase Memory and Erase All Memory described above use one of the following three methods to overwrite the HDD.

- NSA method
- DoD method
- Random Numbers method

(a) NSA method

When NSA method is selected, the TSF overwrites data in following procedure.

- overwrite twice with random numbers,
- overwrite once with Null (0).

(b) DoD method

When DoD method is selected, the TSF overwrites data in following procedure.

- overwrite once with fixed numbers,
- overwrite once with complement of above fixed numbers,
- overwrite once with random numbers,
- carry out final verification.

(c) Random Numbers method

When Random Numbers method is selected, the TSF overwrites specified number of times (from one to nine times) with random numbers.

In Random Numbers method, number of times is specified in the range from one to nine.

6.2 Strength of function claim

There are no security functions realized by probabilistic or permutational mechanisms.

6.3 Assurance measures

In this section, assurance measures for the TOE are identified. The assurance measures listed in Table 4 cover security assurance requirements listed in the section 5.3.

Table 4: Assurance requirements for EAL3 and assurance measures

Assurance class	Assurance component	Assurance measure
ACM: Configuration Management	ACM_CAP.3	Configuration Management Plan for imagio Security Card Type C, DataOverwriteSecurity Unit Type D, imagio Security Card Type D, DataOverwriteSecurity Unit Type C
	ACM_SCP.1	
ADO: Delivery and operation	ADO_DEL.1	Delivery Procedure for imagio Security Card Type C, DataOverwriteSecurity Unit Type D, imagio Security Card Type D, DataOverwriteSecurity Unit Type C
	ADO_IGS.1	Production Procedure for imagio Security Card Type C, DataOverwriteSecurity Unit Type D, imagio Security Card Type D, DataOverwriteSecurity Unit Type C imagio Security Card Type C/Type D Service Manual DataOverwriteSecurity Unit Type C/Type D Service Manual
ADV:	ADV_FSP.1	Zoffy V3 system design

Assurance class	Assurance component	Assurance measure
Development	ADV_HLD.2	IMH design specification B0.HDD overwrite functional specification IMH design specification B0.HDD overwrite I/F: command specification LPUX specification 05 library HDD overwrite library I/F specification ZOFFY-V3 UNIX filesystem Auto Erase Memory system basic design ZOFFY-V2/V3 HDD Erase All Memory system basic design
	ADV_RCR.1	Correspondence Analysis for imagio Security Card Type C, DataOverwriteSecurity Unit Type D, imagio Security Card Type D, DataOverwriteSecurity Unit Type C
AGD: Guidance documents	AGD_ADM.1	imagio Security Card Type C imagio Security Card Type D Operating Instructions DataOverwriteSecurity Unit Type C DataOverwriteSecurity Unit Type D Operating Instructions
	AGD_USR.1	
ALC: Life cycle support	ALC_DVS.1	Development Security Plan for imagio Security Card Type C, DataOverwriteSecurity Unit Type D, imagio Security Card Type D, DataOverwriteSecurity Unit Type C
ATE: Tests	ATE_COV.2	Test Document for imagio Security Card Type C, DataOverwriteSecurity Unit Type D, imagio Security Card Type D, DataOverwriteSecurity Unit Type C
	ATE_COV.1	
	ATE_FUN.1	
	ATE_IND.2	TOE
AVA: Vulnerability assessment	AVA_MSU.1	Vulnerability Assessment for imagio Security Card Type C, DataOverwriteSecurity Unit Type D, imagio Security Card Type D, DataOverwriteSecurity Unit Type C
	AVA_SOF.1	
	AVA_VLA.1	

Notes: The documents listed in Table 4 are written in Japanese except for the "DataOverwriteSecurity Unit Type C DataOverwriteSecurity Unit Type D Operating Instructions" and the TOE.

7 PP claims

There are no Protection Profiles claimed to which this ST is conformant.

8 Rationale

8.1 Security objectives rationale

In this section, it is demonstrated that the security objectives stated in section 4 are appropriate and cover all aspects of the security environment stated in section 3.

Table 5 shows that each security objective addresses at least one threat or assumption, and that each threat and assumption is covered by at least one security objective.

Table 5: Relation between security needs and objectives

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

OSP.RESIDUAL is achieved by O.OVERWRITE, because O.OVERWRITE ensures that the information on the HDD area specified by the MFP becomes unreadable by overwriting.

A.BREAK is achieved by OE.POWER, because it is assured that overwriting of the TOE is not interrupted by waiting for finish of overwriting on shutting down the MFP.

A.CANCEL is achieved by OE.CANCEL, because it is prevented from cancelling Erase All Memory against user's intent to keep the MFP under watch.

8.2 Security requirements rationale

8.2.1 Rationale for functional requirements

In this section, it is demonstrated that security functional requirements stated in section 5 achieve security objectives for the TOE and IT environment identified in section 4.

Table 6 shows that TOE security functional requirements meet security objectives for the TOE and IT environment.

Table 6: Relation between security objective and functional requirements

	FDP_SIP.1	FPT_RVM.1
O.OVERWRITE	X	X

O.OVERWRITE is achieved by FDP_SIP.1, because this requirement ensures that the information specified by the MFP becomes unavailable, i.e. no one can retrieve the information specified by the MFP. Furthermore, it is ensured that the TSP cannot be bypassed with FPT_RVM.1.

8.2.2 Rationale for minimum strength of function

This TOE is the option of the MFP as products in the market. It is assumed that the MFP, which is operating environment of the TOE, is used in general offices. So, it is appropriate that minimum strength of function for the TOE is SOF-Basic.

8.2.3 Dependency of security functional requirements

Table 7 shows dependencies of TOE security functional requirements. The dependencies in this ST are satisfied for interdependence of CC requirements.

Table 7: Dependencies of TOE security functional requirements

TOE security functional requirement	Dependencies required by CC	Dependencies satisfied in this ST
FDP_SIP.1	None	None
FPT_RVM.1	None	None

As shown in Table 7 above, FDP_SIP.1 and FPT_RVM.1 have no dependencies required by CC. So, there are no dependencies to be satisfied by TOE security functional requirements.

8.2.4 Rationale for assurance requirements

This TOE is the option of the MFP as products in the market. It is assumed that the MFP which is operating environment of the TOE is used in general offices, and the attackers with moderate attack potential or over is not assumed for the TOE.

Furthermore, the TOE realizes the security function with simple mechanism such as overwriting data, which has no probabilistic or no permutational one. Implementation and analysis of developers test based on the functional specification and high-level design of the security functions, which means the high-level design evaluation (ADV_HLD.2), is sufficient to demonstrate the accuracy. Analysis of apparent vulnerability (AVA_VLA.1) is sufficient for general needs. It is also important to achieve security assurance from development security (ALC_DVS.1) by evaluating the development environment and management of developed deliverables.

Checking operation of the TOE security function and external interfaces with functional specification level test is appropriate to assure this security function. So, considering evaluation period and cost, EAL3 is appropriate for the TOE.

8.2.5 Mutual support of security requirements

Table 8 shows mutual support of security requirements.

Table 8: Mutual support of security requirement

Functional requirement	Bypass	Deactivate	Tamper
FDP_SIP.1	FPT_RVM.1	None	None

[Bypass]

Once the TOE is started, FDP_SIP.1 is certainly executed. So, there is no bypass for FDP_SIP.1.

[Deactivate]

Once the TOE is started, FDP_SIP.1 is certainly executed. So, there is no deactivation for FDP_SIP.1.

[Tamper]

There is no illegal subject for the TOE. So, the TSF is not tampered.

8.2.6 Rationale for explicitly stated security requirements

The functional requirement FDP_SIP.1 used for the TOE is an explicitly stated security requirement. The purpose of the TOE is to make residual information of the MFP unavailable in cooperation with the MFP. So, FDP_RIP.1 seems to meet the purpose. But the MFP performs the management of residual information, and the TOE overwrites the information according to the order of the MFP. Thereby, FDP_RIP.1 is not applicable. So, the security requirement extended for the TOE based on FDP_RIP.1 is applied. Also, the explicitly stated security requirement is stated in the same style as CC Part 2 security requirements and to a comparable level of detail.

The explicitly stated security requirement is stated as the security function separated off the part determining residual information from FDP_RIP.1.

FDP_RIP.1 basis of the requirement is not required any dependencies and particular assurance requirements. So, the explicitly stated functional requirement does not need any dependencies and assurance requirements.

Also, the assurance requirements of EAL3 package are sufficient to assure the explicitly stated security requirement, because it is obvious that the evidences by special documents for the requirement are not needed.

8.3 TOE summary specification rationale

8.3.1 Rationale for TOE security functions

In this section, it is demonstrated that the TOE security function described in section 6.1 realizes TOE security functional requirements stated in section 5.1.

Table 9 shows that the TOE security function meets TOE security functional requirements.

Table 9: Relation between TOE security functional requirements and TOE security function

	SF.OVERWRITE
FDP_SIP.1	X
FPT_RVM.1	X

SF.OVERWRITE ensures that information specified by the MFP is unavailable by overwriting. Therefore, FDP_SIP.1 is realized.

After executed, SF.OVERWRITE is surely performed. Therefore, FPT_RVM.1 is realized.

8.3.2 Rationale for Strength of function claim

As described in section 6.2, no security function has probabilistic or permutational mechanisms. So, SOF claim is not needed for this ST.

8.3.3 Rationale for combination of security functions

As described in section 8.3.1, the TOE has one security function. This shows that the ST has no mutual support of security functions. So, the security function performs to satisfy security functional requirements by itself.

8.3.4 Rationale for assurance measures

In section 6.3, documents as assurance measures and the TOE meet all security assurance requirements required for EAL3, and all evidences required for security assurance requirements are covered by those documents and the TOE. So, TOE security assurance requirements are satisfied.

8.4 PP claims rationale

There are no Protection Profiles claimed to which this ST is conformant.

9 Annex

9.1 References

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 Abbreviations

CC	Common Criteria
CE	Customer Engineer
HDD	Hard Disk Drive
MFP	Multi-functional printer
OS	Operating System
PP	Protection Profile
SF	Security Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function