Security Target for

imagio Security Card Type 9,

DataOverwriteSecurity Unit Type I

Author: Atsushi SATOH and Junko YAEGASHI, RICOH COMPANY, LTD.
Date: 2007-11-14
Version: 1.00

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

Revision history

Version	Date	Author	Description
1.00	2007-11-14	Junko YAEGASHI	Revised ST version 1.00 according to fixed the TOE version.

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 9,
DataOverwriteSecurity Unit Type I

ST version: 1.00

Date: 2007-11-14

Author: Atsushi SATOH and Junko YAEGASHI, RICOH COMPANY, LTD.

Product: imagio Security Card Type 9,
DataOverwriteSecurity Unit Type I

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

"imagio Security Card Type 9" is a name in Japan.

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

TOE identification: TOE name in Japan: imagio Security Card Type 9 Software
TOE name in other countries: DataOverwriteSecurity Unit Type I Software

TOE version: 1.01m

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

Keywords: Digital MFP, hard disk, overwrite, protection for residual information

1.2 ST overview

This ST describes the data overwrite module software (hereinafter: DOMS) installed in Multi Function Product (hereinafter: MFP) produced by Ricoh Co., Ltd. The MFP is an OA device consisting of copy function, printer function, scanner function and facsimile function. This TOE is an option kit of the MFP for safer use. This TOE is installed in the MFP, and its function is to overwrite designated areas of the HDD by the MFP for erasure.

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.

2 TOE description

2.1 TOE overview

2.1.1 Product type

The product classification of this TOE is a software product installed as an option of the MFP. This software product overwrites designated areas of the HDD by receiving instructions from the MFP in which the software is installed.

2.1.2 Positioning of the TOE

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

The HDD used by the MPF is divided into RAW area and UNIX area. The TOE monitors supervised information of RAW area on the HDD in shared memory of the MFP. If the TOE found an indicated area to be overwritten for erasure, the TOE executes overwriting for erasure that area. In addition, the TOE receives instructions from the MFP to overwrite information (UNIX data) of UNIX area and execute the instructions. Moreover, the TOE has a function to overwrite all information on the HDD mounted in the MFP in order to prevent leaking of confidential information from stored information on the HDD; for example, return due to termination of the lease/rental agreement, movement to another department or disposal of the MFP.

The MFP determines which information to be overwritten and designates HDD areas or data information to the TOE.

The MFP saves temporary image data on the HDD for working data. When copying, printing, scanning or facsimile processing have finished; the MFP deletes the above-mentioned temporarily working image data.

And, when a user indicates image data storage, the MFP stores the image data on the HDD. When a user indicates deletion of stored image data, the MFP deletes above-mentioned stored image data. “Deletion data” means “making unnecessary information apparently non-existent” for the copy, printer, scanner, facsimile and document box functions. In fact, although deleted image data can be no longer used by those functions of the MFP, their contents actually exist on the HDD. When stored information, as image data, is deleted, the MFP supervises those data as residual information. Depending on functions, the MFP stores the data into either RAW area or UNIX area. In order that the MFP can inform the TOE of the existence/non-existence of residual information in RAW area, the MFP records supervised information into shared memory. In addition, when residual information exists in UNIX area, the MFP indicates the TOE to overwrite.

2.1.3 The MFP in which the TOE can be installed

As for Ricoh MFP, the optional products’ list is prepared for each MFP model. The list contains description of the product information concerning optional products, which can be mounted in relevant

MFP. For an MFP in which the TOE can be installed, the TOE is mentioned as an optional product in that list. By reference to the optional products list of the MFP, an MFP user can distinguish which MFP can be installed with the TOE.

The MFP models in which the TOE can be installed are listed in Annex A.

2.1.4 Operational environment of MFP in which TOE is installed

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, but also several varieties of functions on its single unit, including facsimile, printer and scanner. It is assumed that this TOE is installed and used on an MFP working in a general office. The MFP is mounted with an internal HDD. The HDD is used for storing image data of the copy and printer. During business hours , the MFP is under the supervision of persons related to the office. However, at night or when on holidays, there is a possibility of an outsider intruding unwatched office and removing away the HDD.

Figure 1 shows an assumed operational environment of the MFP.

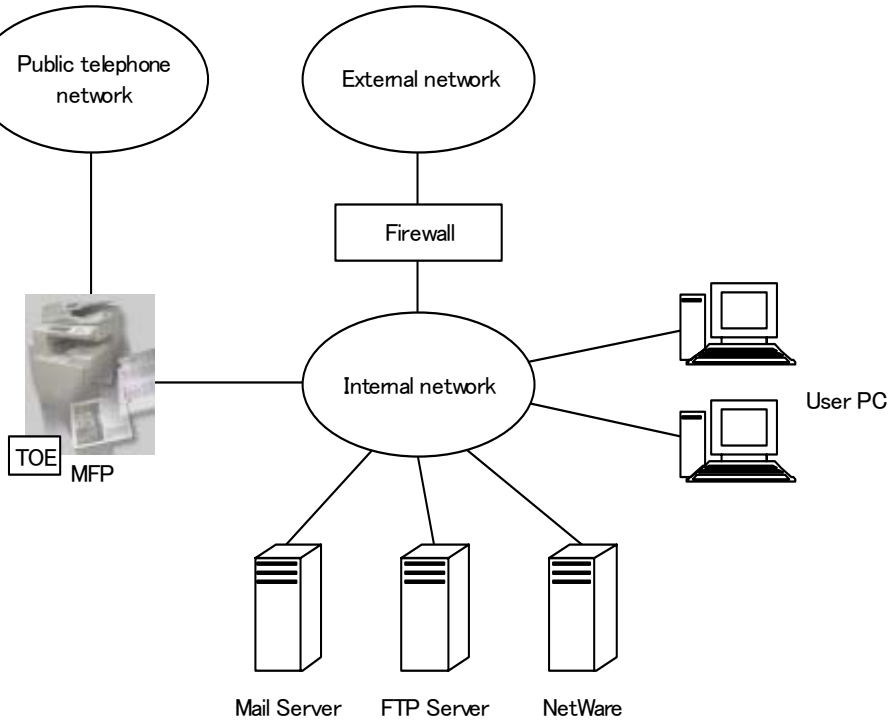

Figure 1: Operational environment of the MFP

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

- User PC:
  User PC requests printing documents and sending facsimile data to MFP. Also User PC can receive scanned data from MFP and stored image data into the MFP.

- Mail server, FTP server, NetWare server:
  MFP can send image data scanned by itself to Mail server, FTP server or NetWare server.
- Public telephone line:
  MFP uses Public telephone line to send and receive facsimile data.

A firewall should be installed between the internal and the external networks in order to protect the devices connected to the internal network. In addition, assume that public telephone line can be only used for sending and receiving facsimile data, but it is impossible to intrude into the MFP or the internal network through this line.

2.2 Physical boundary of the TOE

Ricoh's MFP is composed of hardware and software.

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

The printing engine prints out data from copy and printer functions and also received data through the facsimile unit in parallel controlling paper feed and paper eject.

The scanner unit gets in image data from paper documents. It is used for copy, scanner and facsimile sending functions to get in image data.

The facsimile unit operates sending and receiving of facsimile data.

The operation panel displays information to general users and administrator and also receives input command/data entered by general users and administrator. General users and administrator can make use of functions of the MFP with operating the operation panel.

Image data is stored on the HDD. During copying, printing, scanning or facsimile sending and receiving, the MFP temporarily stores image data for working. Accumulating image data with instruction of general users is also stored on the HDD.

The controller board controls whole of the MFP. The controller board is equipped with a processor and RAM to execute software in the MFP, ROM on which software such as operating system (OS) and various application modules are installed, NV-RAM on which setting information for MFP is stored, and Host interface connected to user PC and servers. And also SD memory card, in which software of additional function is stored, can be attached to the controller board. DOMS is stored on SD memory card, and SD memory card is mounted in the controller board.

Figure 2 shows the hardware structure of the MFP.

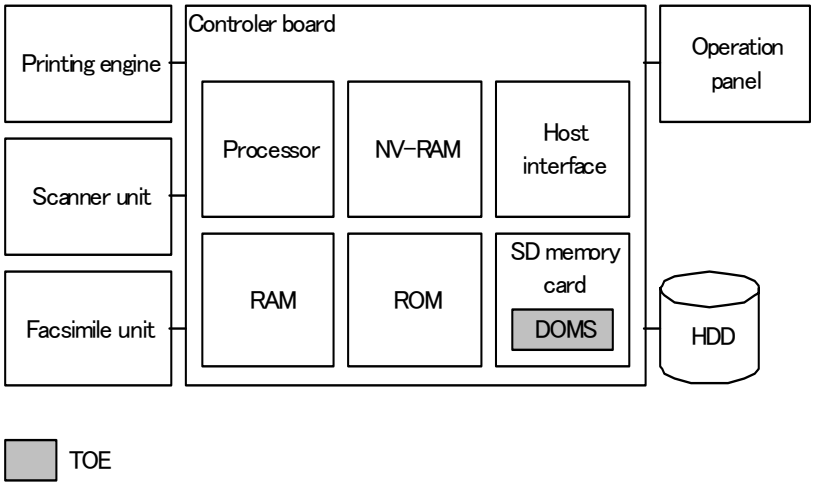

Figure 2: Hardware Structure of the MFP

The software is composed of OS, Common Service Module (CSM), and application modules.

The OS manages the hardware such as HDD and provides interfaces to operate these hardware resources. The OS is UNIX-like operating system ported by Ricoh.

The application modules provide functions such as copy, printing, scanning and facsimile to general users. These modules receive operational instructions from general users and request the required processes to CSM to realize each function.

CSM provides common functions that are used by the application modules. Also CSM provides such as a management function for the HDD areas on which image data and residual information exist, and display function for the status of residual information on the operation panel.

SCS is contained in CSM. SCS controls all applications running on the MFP and manages setting information. Moreover, SCS starts up Erase All Memory function of DOMS in case of request from administrator.

The HDD is divided into RAW area and UNIX area, and data is stored into each area according to MFP functions.

IMH is contained in CSM. IMH controls, through the OS, image data transfer between the printing engine, the scanner unit or the facsimile unit and the controller board. IMH also manages the existence or non-existence of image data and residual information in RAW area of the HDD, and records that management information into shared memory.

ZFSD is contained in CSM. ZFSD always monitors UNIX area of the HDD and informs DOMS that unnecessary files are found.

DOMS includes three software modules, HSM, ZFE and HDE. Those modules are extended functions for CSM.

HSM monitors management information recorded in shared memory, that information indicates status of RAW area of the HDD. When HSM finds a record that indicates a deleted area by the MFP, Through the OS, HSM overwrites that area of the HDD indicated by the record.

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

When HDE is called by SCS due to a request from administrator, HDE overwrites whole area on the HDD.

Figure 3 shows the software structure of the MFP.

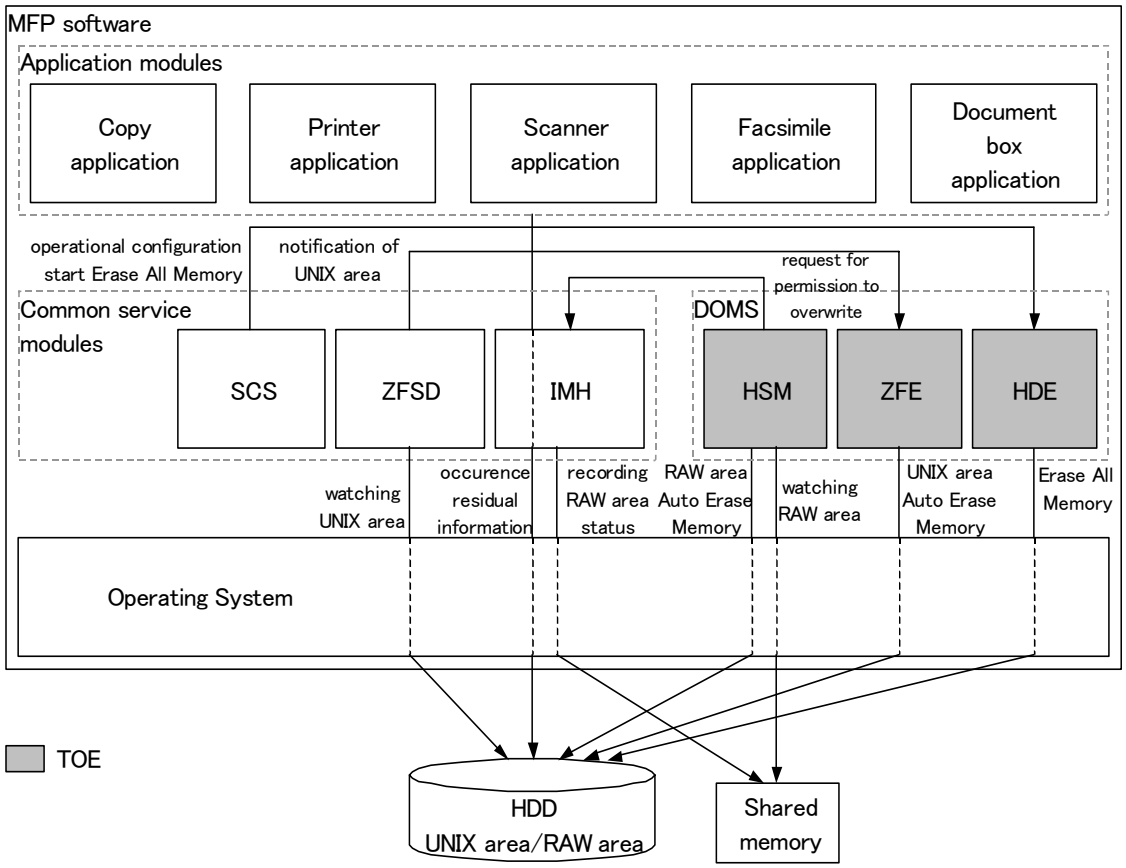

Figure 3: Software Structure of the MFP

2.3 Logical boundary of the TOE

[Logical boundary of the TOE]

The TOE provides Auto Erase Memory function for RAW area in order to overwrite designated RAW area of the HDD by the MFP. The TOE monitors RAW area management information in shared memory and finds an area indicated to be overwritten, then executes. Also, the TOE provides Auto Erase Memory function for UNIX area to overwrite indicated UNIX area in response to an order from the MFP. Furthermore, the TOE provides Erase All Memory function to make all information on the HDD irreversible.

[Logical boundary of the MFP]

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

The MFP also provides document box function. This function stores image data on the HDD by user's operation. When stored image data becomes no longer required, that image data is deleted by general user's operation, and remains as residual information.

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

Furthermore, the MFP provides sequential overwrite configuration function to control the behaviour of Auto Erase Memory of the TOE. Also, the MFP provides batch overwrite activation function to control the behaviour of Erase All Memory of the TOE. Furthermore, the MFP provides status indication function of residual information for users to be able to check residual information.

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

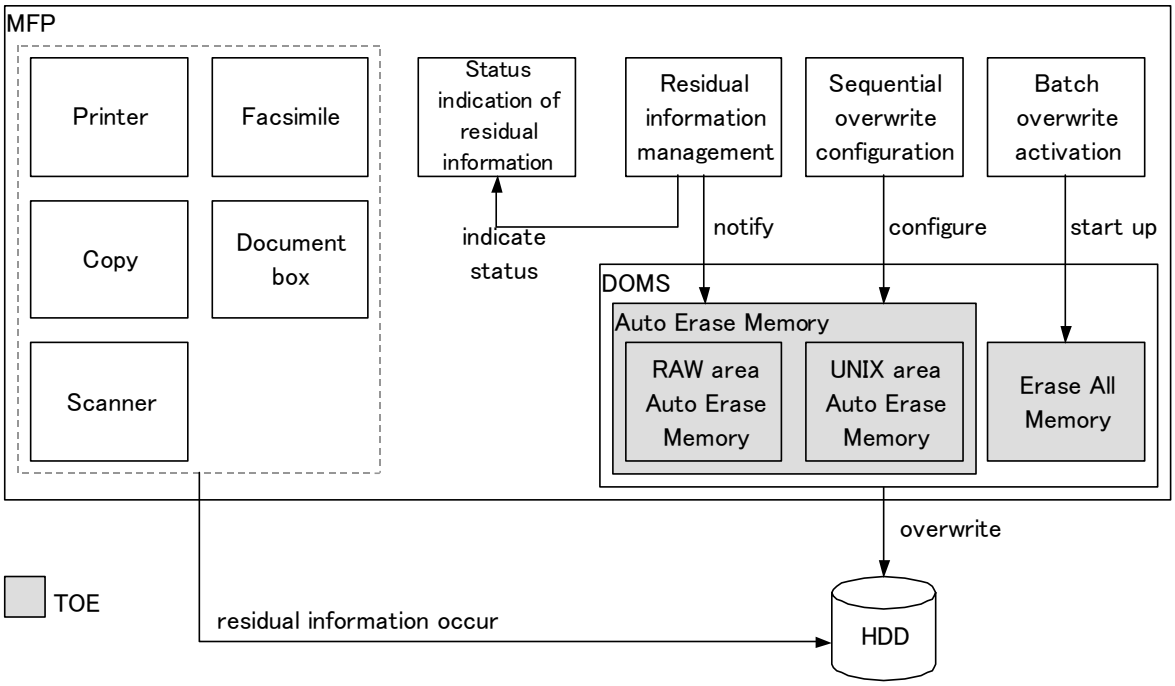

Figure 4: The MFP and the TOE functions and those relations

2.3.1 TOE functionality

Details of the functions provided by the TOE are described below.

[Auto Erase Memory]

HSM monitors management information of RAW area on the HDD, that information is recorded in shared memory. HSM requests IMH of permission to overwrite designated area of the HDD based on the management information in shared memory. When receiving IMH permission, HSM overwrites that area with specified method. When finished overwriting, HSM notifies IMH of completion of overwriting the area, and start again to monitor management information of RAW area on the HDD.

When received notice of existence of unnecessary file in UNIX area from ZFSD, ZFE overwrites the file area with specified method.

[Erase All Memory]

When called by the MFP, HDE overwrites all area of the HDD. Additionally Erase All Memory can be suspended by order of the MFP.

2.3.2 MFP functionality

Details of the MFP functions out of the TOE but related to the TOE are described below.

[Management of residual information]

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

[Configuration of Auto Erase Memory]

Only administrator can activate or deactivate Auto Erase Memory through the operation panel of the MFP.

[Start up / Suspend of Erase All Memory]

Only administrator can start up batch overwrite function, Erase All Memory of the TOE, through the operation panel of the MFP. The MFP resets configuration values recorded in NV-RAM to factory default values. Then, the MFP stops all jobs other than Erase All Memory, and starts up Erase All Memory.

Also, administrator can suspend Erase All Memory during overwriting. When the MFP is started again, then Erase All Memory restarts.

[Indicating status of residual information]

When DOMS is running, icon that indicates status of residual information is displayed don the operation panel of the MFP. When residual information exists on the HDD, an icon that indicates existence of residual information is displayed on the operation panel. During overwriting residual information, that icon blinks on and off. When residual information does not exist on the HDD, another icon that indicates non-existence of residual information is displayed. Thereby, general users and administrator can confirm existence or non-existence of residual information easily. Displaying icon, also, indicates that DOMS is installed correctly and overwrite function is activated.

[General functions of MFP]

The MFP has copy/printer/scanner/facsimile/document box functions. Those functions create working data or store image data in RAW area or UNIX area of the HDD. When those data become unnecessary, the MFP manages those data as residual information, and gives the TOE directions to overwrite them.

[Miscellaneous]

If the power is turned off during overwriting, the MFP can restart overwriting process of the TOE after the power is turned on.

The jobs of copy/printer/scanner/facsimile/document box have higher priority processes than the TOE. If overwriting process of the TOE and the other job are started simultaneously , the TOE waits for completion of the job and starts overwriting. If another job is started during overwriting of the TOE, the TOE is suspended and restarted after completion of the job.

2.4 Terminology

For realizing of this ST, the meanings of specific terminology are defined in Table 1.

Table 1: Terminology related to DOMS

Term	Definition
MFP	Multi Function Product; This is a printer that has multiple functions such as copy, printer in one machine. The TOE of this ST is used in the MFP that is produced by Ricoh.
DOMS	Data Overwrite Modules; This module has a function to overwrite an area of the HDD for preventing analysis of a footprint of data.
HSM	One of modules contained within DOMS; This module executes sequential overwriting the data in RAW area specified to overwrite by the MFP.
ZFE	One of modules contained within DOMS; This module executes sequential overwriting the data in UNIX area specified to overwrite by the MFP.
HDE	One of modules contained within DOMS; This module executes batch overwriting the whole HDD.
CSM	Common Service Modules; These modules provide general functions commonly used by applications such as copy or printer. The management function of image data is also included in CSM.
SCS	One of modules contained within CSM; This module supervises applications running on the MFP, and manages configuration information. Also, SCS activates butch overwrite function, Erase All Memory of DOMS, upon request of the administrator.
IMH	One of modules contained within CSM; . This module controls, through the OS, image data transfer between printing engine, scanner unit, or facsimile unit and controller board. IMH also manages existence or non-existence of image data and residual information in RAW area of the HDD, and records the management information in shared memory.
ZFSD	One of modules contained within CSM; .

	This module always monitors UNIX area of the HDD and notifies DOMS of occurrence of unnecessary files.
Residual information	The residual information means unnecessary information generated with deletion of image data by the MFP. Generally, “Delete” process removes image data logically, but traces of deleted data exist actually. Those traces are residual information.
UNIX area	HDD area managed by OS file system; The data that exists in this area can be accessed by normal file operation.
RAW area	HDD area not managed by OS file system; The data that exists on this area is managed by CSM in its own way without use of OS file operation.
Document box	It is a logical box in which electronic files of documents are stored. It can be used when document box option is installed.
SD memory card	SD memory card is secure digital memory card. It is a memory device with high functionality, as small as postal stamp. It is used to provide the TOE or other applications to the MFP.

3 TOE security environment

3.1 Assumptions

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

A.MODE.AUTOMATIC **It is assumed that the execution of Auto Erase Memory of the TOE is not aborted.**

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

A.MODE.MANUAL **It is assumed that the execution of Erase All Memory of the TOE is not suspended.**

The execution of Erase All Memory of the TOE is not suspended without user's intent by pressing the [Suspend] button or turning off the power of the MFP before the function finishes.

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.

P.UNREADABLE **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 objectives for the TOE are described. The security objectives for the TOE realize 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 designated information on the HDD 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 against assumptions or threats.

4.2.2 Security objectives for the non-IT environment

In this section, the security objectives for the environment except the IT environment are described. Those security objectives are countered against the assumptions or threats described in section 3.

OE.MODE.AUTOMATIC **User shall not turn off the power of the MFP before overwrite of Auto Erase Memory finishes.**

When turning off the power of the MFP, user shall confirm the icon shown on the operation panel and then turns off the power with the condition that the overwriting by Auto Erase Memory is finished.

OE.MODE.MANUAL **User shall manage the MFP to prevent the function of Erase All Memory from being suspended.**

When Erase All Memory executing, user manages the MFP to prevent the function from being suspended by pressing the [Suspend] button or turning off the power of the MFP without user's intent.

5 IT security requirements

5.1 TOE security functional requirements

In this section, the TOE security functional requirement to achieve the security objective that described in section 4.1 is identified and described. The parts of the assignment and selection operations defined in [CC] are implemented and 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 2. It is the set of components defined by the evaluation assurance level (EAL) 3 and no other requirements have been augmented.

Table 2: 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, explicitly stated TOE security functional requirements that achieve the security objective are 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 RAW area of the HDD recorded in shared memory, and overwrite HDD area specified by the management information.

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

(2) Erase All Memory

The TSF overwrites all data on the HDD. The TSF can suspend Erase All Memory by order of the MFP

Application notes:

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

(1) NSA method: the TSF overwrites data in following procedure.

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

(2) DoD method: the TSF overwrites data in following procedure.

- Overwriting once with fixed numbers,
- Overwriting once with complement of above fixed numbers,
- Overwriting once with random numbers,
- Carrying out final verification.

(3) Random Numbers method: the TSF overwrites specified number of times with random numbers.

When Random Numbers method is chosen, number of times is specified.

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 described. The assurance measures listed in Table 3 meet security assurance requirements listed in the section 5.3.

Table 3: Assurance requirements for EAL3 and assurance measures

Assurance class	Assurance component	Assurance measure
ACM: Configuration Management	ACM_CAP.3 ACM_SCP.1	Configuration Management Plan for imagio Security Card Type 7, DataOverwriteSecurity Unit Type H, imagio Security Card Type 9, DataOverwriteSecurity Unit Type I
ADO: Delivery and operation	ADO_DEL.1	Delivery Procedure for imagio Security Card Type 7, DataOverwriteSecurity Unit Type H, imagio Security Card Type 9, DataOverwriteSecurity Unit Type I
	ADO_IGS.1	Production Procedure for imagio Security Card Type 7, DataOverwriteSecurity Unit Type H, imagio Security Card Type 9, DataOverwriteSecurity Unit Type I Service Manual for imagio Security Card Type 7 imagio Security Card Type 9 Service Manual for DataOverwriteSecurity Unit Type H DataOverwriteSecurity Unit Type I
ADV: Development	ADV_FSP.1 ADV_HLD.2	Zoffy V3 system design 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 7, DataOverwriteSecurity Unit Type H, imagio Security Card Type 9, DataOverwriteSecurity Unit Type I

Assurance class	Assurance component	Assurance measure
AGD: Guidance documents	AGD_ADM.1 AGD_USR.1	"imagio Security Card Type 7 imagio Security Card Type 9 Operating Instructions" "DataOverwriteSecurity Unit Type H DataOverwriteSecurity Unit Type I Operating Instructions"
ALC: Life cycle support	ALC_DVS.1	Development Security Plan for imagio Security Card Type 7, DataOverwriteSecurity Unit Type H, imagio Security Card Type 9, DataOverwriteSecurity Unit Type I
ATE: Tests	ATE_COV.2 ATE_COV.1 ATE_FUN.1	Test Document for imagio Security Card Type 7, DataOverwriteSecurity Unit Type H, imagio Security Card Type 9, DataOverwriteSecurity Unit Type I Test Result for imagio Security Card Type 7, DataOverwriteSecurity Unit Type H, imagio Security Card Type 9, DataOverwriteSecurity Unit Type I
	ATE_IND.2	TOE
AVA: Vulnerability assessment	AVA_MSU.1 AVA_SOF.1 AVA_VLA.1	Vulnerability Assessment for imagio Security Card Type 7, DataOverwriteSecurity Unit Type H, imagio Security Card Type 9, DataOverwriteSecurity Unit Type I

Notes: The documents listed in Table 3 are written in Japanese except for the "DataOverwriteSecurity Unit Type H DataOverwriteSecurity Unit Type I Service Manual", "DataOverwriteSecurity Unit Type H DataOverwriteSecurity Unit Type I 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 4 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 4: Relation between security needs and objectives

	O.OVERWRITE	OE.MODE.AUTOMATIC	OE.MODE.MANUAL
P.UNREADABLE	X		
A.MODE.AUTOMATIC		X	
A.MODE.MANUAL			X

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

A.MODE.AUTOMATIC is achieved by OE.MODE.AUTOMATIC, because it is ensured that overwrite of the TOE is not interrupted by waiting for completion of overwrite when shutting down the MFP.

A.MODE.MANUAL is achieved by OE.MODE.MANUAL, because it is prevented from suspending 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 5 shows that TOE security functional requirements meet security objectives for the TOE and IT environment.

Table 5: 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 an 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 office. So, it is appropriate that minimum strength of function for the TOE is SOF-Basic.

8.2.3 Dependency of security functional requirements

Table 6 shows dependencies of TOE security functional requirements. The dependencies in this ST are satisfied for interdependence of CC requirements.

Table 6: 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 6 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 an 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.

In addition, the TOE realizes the security function with simple mechanism such as overwriting data, which has no probabilistic or no permutational mechanism, therefore the high-level design evaluation (ADV_HLD.2) is sufficient to demonstrate the validity of that mechanism. Furthermore, a high-level attack capability is needed for attacks such as bypassing or tampering TSF, but those are out of scope of this evaluation. That is to say, an analysis of apparent vulnerability (AVA_VLA.1) is sufficient for general needs.

On the other hand, for making it more difficult to attack, it is needed to keep pertinent information in security. So it is important to ensure that the development environment is in security, that is, development security (ALC_DVS.1).

So, considering evaluation period and cost, EAL3 is appropriate for the TOE.

8.2.5 Mutual support of security requirements

Table 7 shows mutual support of security requirements.

Table 7: 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 extended 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 of 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 8 shows that the TOE security function meets TOE security functional requirements.

Table 8: 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 activated the TOE, 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.

Annex A

The MFP models in which the TOE can be installed are listed in Table 9.

Table 9: The MFP models in which the TOE can be installed

Product names in Japan	Product names in other country
Ricoh imagio MP 2550 series Ricoh imagio MP 3350 series Ricoh imagio MP 4000 series Ricoh imagio MP 5000 series	Ricoh Aficio MP 2550 series Ricoh Aficio MP 3350 series Savin 9025/9033 series Lanier LD425/433 series Lanier MP 2550/3350 series Gestetner MP 2550/3350 series Nashuatec MP 2550/3350 series Rex-Rotary MP 2550/3350 series Infotec MP 2550/3350 series Ricoh Aficio MP 4000 series Ricoh Aficio MP 5000 series Savin 9040/9050 series Lanier LD040/050 series Lanier MP 4000/5000 series Gestetner MP 4000/5000 series Nashuatec MP 4000/5000 series Rex-Rotary MP 4000/5000 series Infotec MP 4000/5000 series

Notes: "series" means the product group, they have some different configurations which have no effect on the performance of the TOE.