KONICA MINOLTA

bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.1)

Control Software

Security Target

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

Version：1.10

Issued on：September 8, 2006

Created by：KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

＜Revision History＞

Date	Ver.	Division	Approved	Checked	Created	Revision
2005/09/12	1.00	Development Division 12	Tada	Hashimoto	Kato	Initial Version.
2006/04/04	1.01		Tada	Hashimoto	Kato	Change according to specification revision
2006/05/11	1.02	Development Division 12	Tada	Hashimoto	Kato	• Specify TOE Identification • Update version of TOE, and correct typos.
2006/06/02	1.03	Development Division 12	Tada	Hashimoto	Kato	• Delete all the related descriptions since Chapter 3 as all service functions unnecessary in security • Change the method of TOE Identification • Add the explanation of the Write authority of SNMPv1 prohibited with the Enhanced mode (Chapter2) • Change the position of Auto log-out function from the state of the security function（basic function）
2006/06/05	1.04	Development Division 12	Tada	Hashimoto	Kato	• Correct the details of remote diagnostic function(recovery of various service functions) • Correct typos
2006/06/13	1.05	Development Division 12	Tada	Hashimoto	Kato	• Correct identification incompleteness of guidance document as the Assurance Measures • Remove auto reset function from the subject of Security.
2006/06/28	1.06	Development Division 12	Tada	Hashimoto	Kato	• Correct the explanation of basic function（Capter2） • Correct the explanation of Enhanced security function（Capter2） • Correct the contents of measure for “Complete overwrite deletion” and Overwrite deletion of a file unit（Capter4） • Correct the role to cancel the Enhanced security function（Capter5）
2006/07/05	1.07	Development Division 12	Tada	Hashimoto	Kato	• Correct unnecessary mapping of FIA_SOS.1[1] and IT security function（Capter8） • Delete FIA_UAU.2[4] unnecessary dependency of FIA_UAU.7（Capter5, Capter8） • Correct typos of nonexistence FIA_UAU.2[5] • Correct expression of T.DISCARD-MFP and T.BRING-OUT-STORAGE • Add extra explanation of remaining image file（Capter3）
2006/07/18	1.08	Development Division 12	Tada	Hashimoto	Kato	・Add explanation of NVRAM • Add the explanation of Auto Reset function • Correct a part of the ST Introduction • Correct typos of Table12（Relation of FIA_SOS.1 requirement） • Add explanation of a case of no dependency applied (Reason for FMT_MSA.3 not applied in user box and secure print, Necessity of identification requirement in HDD lock functional requirement) • Explain in several paragraphs (TOE description, Rationale, etc.) that the operation of FIA_UAU.7, the security requirement for TOE, is applied only to the panel processing of MFP • Correct Table 9 (Incompleteness of rationale explanation concerning logoff operation) • Correct description incompleteness of select operation for FIA_AFL.1 requirement • Add the explanation of the Protective assets (Clarifies that the transmission address data and MFP address are different objects.) • Add the description of threat without HDD. • Delete the logoff operation measures of the service engineer because the unnecessity to express it intently on ST. Correct related part of it. • Add the proof rationale for a nonexistence of competitive requirement.

						• Correct typos, etc.
2006/09/02	1.09	Development Division 12	Tada	Hashimoto	Kato	• Change the dependencies of Static attribute initialization for secure print. (add FMT_MSA.3) • Correct the expression of denying the access to service mode, since it wasn’t correctly expressed that the service engineer is under authentication. • Correct typos - rationale of HDD lock password condition - rationale of Lock release condition for secure print - others
2006/09/08	1.10	Development Division 12	Tada	Hashimoto	Kato	• Add the audit and management item along with the extended requirement Part2 • Delete [Re-] for the authentication of user box • Add the description of the relation of Enhanced security function to all area deletion function

【 Contents 】

—【 List of Figures】—

—【 List of Tables 】—

1. ST Introduction

1.1. ST Identification

• ST Title	:	bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.1) Control Software Security Target
• ST version	:	1.10
• CC version	:	2.1, CCIMB Interpretations-0407
• Created on	:	September 8, 2006
• Created by	:	KONICA MINOLTA BUSINESS TECHNOLOGIES, INC. T. KATO

1.2. TOE Identification

• TOE Name	:	Japan：bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.1) Zentai Seigyo Software Overseas：bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.1) Control Software
• TOE version	:	4040-0100-G10-25-000
• TOE type	:	Software
• Created by	:	KONICA MINOLTA BUSINESS TECHONOLOGIES, INC

1.3. CC Conformance Claim

The TOE, which is the subject of this ST, conforms to the following.

- Security function requirement

  Part 2 Extended

- Security assurance requirement

  Part 3 Conformant

- Evaluation assurance level

  EAL3 Conformant (No additional assurance component)

- PP Reference

  This ST does not carry out a PP reference.

- Complement

  CCIMB Interpretations-0407 is applied.

- References
  - Common Criteria for Information Technology Security Evaluation Part 1:Introduction and general model Version 2.1 August 1999 CIMB-99-031
  - Common Criteria for Information Technology Security Evaluation Part 2:Security functional requirements Version 2.1 August 1999 CCIMB-99-032
  - Common Criteria for Information Technology Security Evaluation Part 3:Security assurance requirements Version2.1 August 1999 CCIMB-99-033
  - CCIMB Interpretations-0407

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model Version 2.1 August 1999 CCIMB-99-031 (January 2001 Translation Version 1.2, Information-technology Promotion Agency Japan, Security Center)
- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements Version 2.1 August 1999 CCIMB-99-032 (January 2001 Translation Version 1.2, Information-technology Promotion Agency Japan, Security Center)
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements Version 2.1 August 1999 CCIMB-99-033 (January 2001 Translation Version 1.2, Information-technology Promotion Agency Japan, Security Center)
- CCIMB Interpretations - 0210 Version 2 [1] (August 2004 Information-technology Promotion Agency Japan, Security Center, Information Security Certification Office)
- CCIMB Interpretations - 0407（August 2004 Information-technology Promotion Agency Japan, Security Center, Information Security Certification Office)

1.4. ST Overview

bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.1) is Konica Minolta Business Technologies, Inc. digital MFP comprised by selecting and combining copy, print, scan and FAX functions.（Hereafter, “MFP” as all these generic names）. The target of evaluation (TOE) of this Security Target (ST) is the “bizhub 350/ bizhub 250/ bizhub 200/ ineo 350/ ineo 250 (Ver.1),” that controls the entire operation of MFP, including the operation control processing and the image data management that are accepting from the panel of the main body of MFP or through the network. This ST explains the security functions that are realized by the TOE.

TOE offers the protection from exposure of the highly confidential document stored in the MFP. Moreover, HDD, the medium that stores the image data in MFP, owns the mechanism that can use the unauthorized access lock function (HDD lock function) and offers the protection to overwrite at once the data that became unnecessary, for the danger of taking HDD out illegally. Besides, TOE has the deletion method to follow various overwrite deletion standards, and it deletes all the data of HDD completely. This contributes to the prevention of the divulging information of the organization that uses MFP, by using this deletion at the time of discarding MFP or returning the lease MFP.

This ST is the documentation for describing the necessity and sufficiency of these TOE Security Functions.

[1] Translation of CCIMB Interpretations- 0407 is shown in supplementation 0407 and 0210 in the 2nd edition.

2. TOE Description

2.1. TOE Type

Bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.1) Control Software that is the TOE is embedded software that dominates the control of the entire MFP locating on the flash memory on the MFP Controller.

2.2. Environment for the usage of MFP

Figure 1 shows the expected general environment for the usage of MFP equipped with TOE. Moreover, the matters, assumed in the environment for the usage, show by a run of the item below.

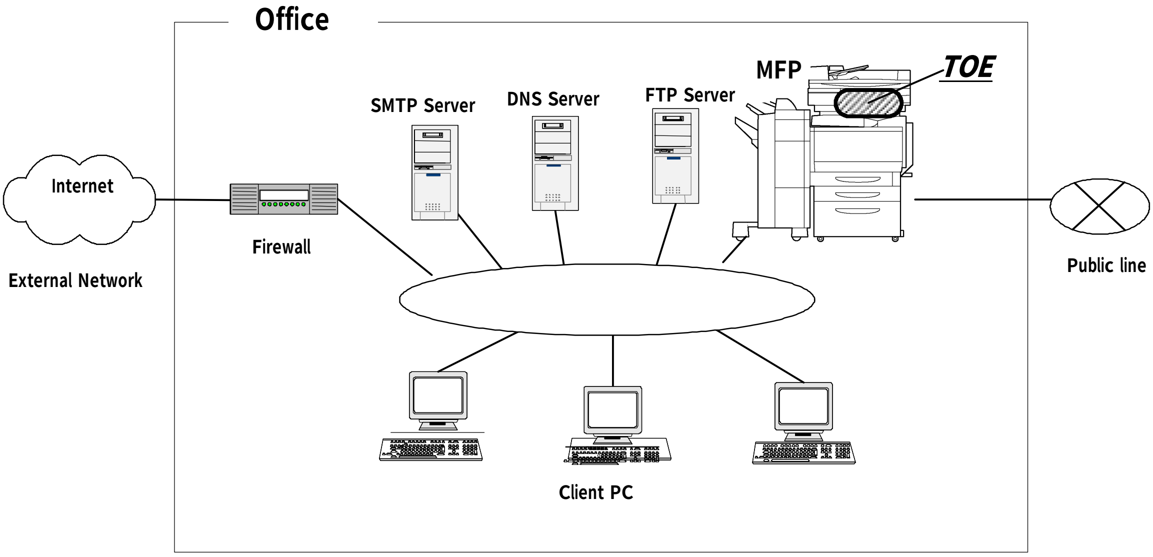

Figure1 An example of the expected environment for usage of the MFP

- An intra-office LAN exists as a network in the office.
- The MFP connects to the client PCs via the intra-office LAN, and has mutual data communication.
- When the SMTP server or FTP server are connected to the intra-office LAN, the MFP can carry out data communication with these. (Need the DNS Service when setting the Domain name of SMTP Server or FTP Server)
- When the intra-office LAN connects to an external network, measures such as connecting via a firewall are taken, and an appropriate setup to block access requests to the MFP from the external network is carried out.
- The intra-office LAN provides a network environment that cannot be intercepted by the office operation including using the switching hub and installing the wiretapping detector.
- The public line connected with MFP is used to communicate with the FAX and the remote support function.

2.3. Operation Environment of the TOE

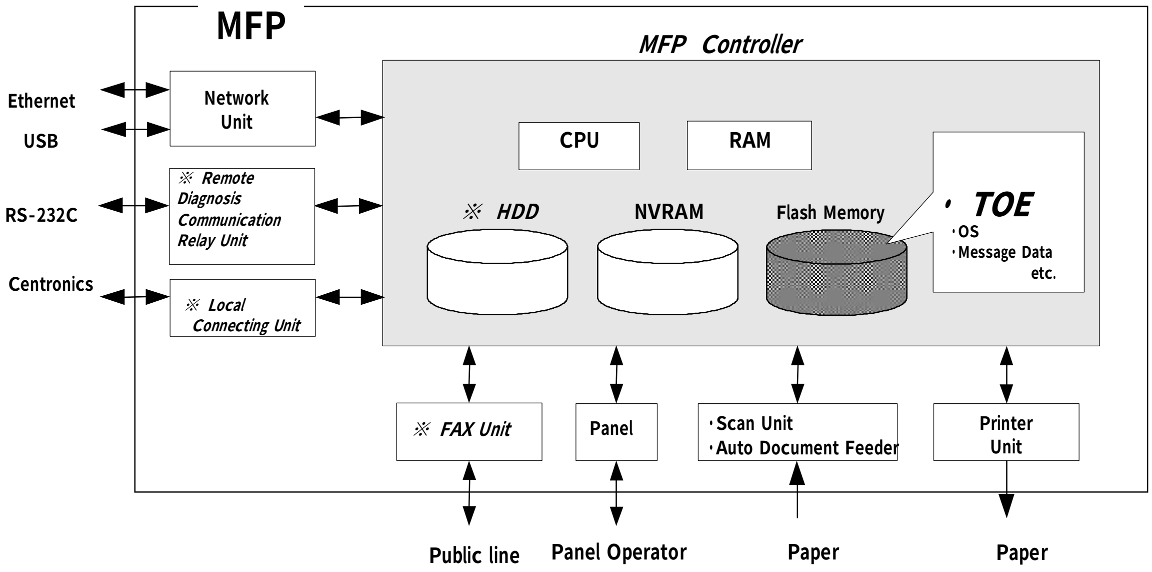

Figure 2 Hardware structure that relates to TOE

Figure2 shows the structure of the hardware environment on the MFP that TOE needs for the operation. TOE exists on the flash memory on the MFP controller, which built in the body of the MFP, and is loaded and run on the RAM.

The following explains about the characteristic hardware on the MFP controller, the hardware having the interface and the MFP controller, and the connection using RS-232C, shown in Figure 2.

- Flash memory
  Storage medium that stores the object code of the “MFP Control Software” that is the TOE. Additionally, it stores the message data of each country’s language to display the response accessed through the panel and network, OS (VxWorks), and so on.

- NVRAM
  Nonvolatile Memory. The memory medium that stores various setting values (administrator password, transmission address data, etc) needed for the operation of the MFP.

- Panel
  The exclusive control device for the operation of the MFP equipped with the touch panel of a liquid crystal monitor, ten-key, start key, stop key, screen switch key, etc.

- Network Unit
  The interface device to connect to the Ethernet. It supports 10BASE-T and 100BASE-TX. USB port is equipped as the port of the use of Print function via local connection with PC.

- Scan Unit／Auto Document Feeder
  The device that scans images and photos from a paper and converts them into the digital data.

- Printer Unit
  The device that actually prints the converted image data for printing when demanded to print by the MFP controller.

- HDD（※Option parts）
  Hard disk drive. It stores the image data as the file, and is also used for the storage area for swapping the image data which exceeds the capacity of RAM processing area.
  As a feature function, the security function (HDD lock function) is installed, that can set the password and does not permit to read from or write in HDD without password match. As for the prescribed number of failure to the password verification, it also has the function to lock the password verification function.
  According to the marketing circumstances in sales, it is sold as the option part and is not attached on the MFP. The function which needs HDD cannot be used without its option.

- FAX Unit（※Option parts）
  A device that is used for the communication for sending and receiving FAX and for the remote diagnosis function (described later) via public line. According to the circumstances in sales, it is sold as the option part and is not attached on the MFP.

- Local Connecting Unit（※Option parts）
  A unit that uses Print function with local connection by connecting using the client PC and Centronics interface (parallel mode). According to the circumstances in sales, it is sold as the option part and is not attached on the MFP.

- Remote diagnosis communication relay unit（※Option parts）
  It enables to connect serially via RS-232C. By connecting to the modem that is connected to the public line, the remote diagnosis function (described later) via this interface can be used when any troubles occurred. According to the circumstances in sales, it is sold as the option part and is not attached on the MFP.

2.4. Role of the TOE user

The roles of the personnel that relate to the use of the MFP with TOE are defined as follows.

- User
  A person who does copying, scanning, etc. with MFP.（In general, the employee in the office is assumed.）

- Administrator
  MFP's user who carries out the management of the operation of MFP. An administrator performs the operation management of MFP and the management of user box.（In general, it is assumed that the person elected from the employees in the office plays this role.）

- Service Engineer
  A user who performs management of maintenance for the MFP. Service Engineer performs the repair and adjustment of MFP. (In general, the person in charge at the sales companies that performs the maintenance service of MFP and is in cooperation with Konica Minolta Business

Technologies Inc. is assumed.)

- Person in charge at the Organization that uses the MFP
  A person in charge at the organization that manages the office where the MFP is installed. This person assigns an administrator who carries out the management of the operation of the MFP.

- Person in charge at the Organization that manages the Maintenance of the MFP
  A person in charge at the organization that carries out management of the maintenance for the MFP. This person assigns service engineers who perform the maintenance management for the MFP.

Besides this, though not a user of TOE, a person who goes in and out in the office are assumed as an accessible person to TOE.

2.5. Functions provided by the TOE

A User uses a variety of functions of the TOE from the panel and a client PC via the network. The following explains typical functions, such as the basic function, the user box function to manage the image files stored, the administrator function manipulated by administrator, the service engineer function manipulated by service engineer, and the function operated in the background without user's awareness.

2.5.1. Basic function

In MFP, a series of function for the office work concerning the image such as copy, print, scan, and fax exists as a basic function, and TOE performs the core control in the operation of these functions. It converts the raw data acquired from the external device of the MFP controller into the image file, and registered in RAM and HDD. (Several conversion processing is done for the print image file from PC.) The image file is converted as data for the printing or transmission and is forwarded to the target external device of the MFP controller.

Operations of copy, print, scan, and fax are managed by the unit of job, and can be cancelled the operation by the command from the panel.

The following is the functions related to the security in the basic function.

- Secure Print Function
  When the secure print password is received with the printing data, the image data is stored as the standby status. And the print command and password input from the panel allows printing.
  This function, in the printing operation by the PC, removes the possibility that other users stole a glance at the printing of high-leveled confidential data and lost it into the other printings.

2.5.2. User Choice Function

User can freely set it, which is chiefly needed to use the basic function, such as image quality adjustment (magnification and print density, etc.), a standard layout, the power saving shift time, and the auto reset time (function that the display of the operation panel returns to a basic screen if it doesn't operate it during the fixed time).

2.5.3. User Box Function

The directory named “user box” can be created as an area to store the image file in HDD. Two types of user box exist; one is the user box with the fixed name "Public" which all users can use, and the other is the user box used by setting password which can be used individually or among users with sharing password.

TOE processes the following required operation, against the image file in a user box and the user box, from the panel or the network unit. (Upon request via the network from the client PC.)

- Downloading the image files in a user box by the client PC
- Deletion of the image files in a user box
- Setting of the period to keep the image files in a user box (delete automatically by the fixed time passed)
- Change of user box name, change of the password, and deletion of user box etc.

If HDD is not equipped, a “user box” cannot be created.

2.5.4. Administrator Function

TOE provides the functions such as the management of user boxes and management of various settings of the network, image quality, etc in the administrator mode that only authenticated administrator can manipulate.

The following shows the function related to the security.

- Management of user box setting
  - Changing the user box password
- Management of network setting
  - IP Address, etc
- Overwrite Delete Function at the time of disposal
  - Perform the Overwrite Deletion for the whole data area of HDD
  - Initialize the various set values and the charging information in NVRAM that an administrator set.

The followings are the operation setting function related especially to the behavior of the security function.

- Setting of the password policy function
  - Select ON or OFF for the function to check the several conditions of the password, such as the valid number of digits for the various passwords, etc.
- Setting of the Prohibit Functions When Auth. Error
  - Function detecting the unsuccessful operation of each authentication function
  - Select the above operation mode

  - With the unsuccessful authentication detection mode, the user box password matching function works when downloading a user box file by the PC.
- Setting the method of the remaining information overwrite deletion function (described later)
  - Overwrite Data：Valid and invalid setting of the method of 0x00 ⇒ 0x00 ⇒ 0x00 exists.
  - Select the above operating method
- Setting the HDD lock function
  - Select ON or OFF
  - Register or change the HDD lock password when ON is selected.

2.5.5. Service Engineer Function

TOE provides a management function of administrator and a maintenance function, such as adjusting the device for Scan/Print etc, within the service mode that only a service engineer can operate. The following shows the functions related to the security.

- Initialization of the administrator mode password
- Settings for the Remote diagnosis function (described later)
- Total clear function
  - Initialize the various setting values that an administrator set
- Memory dump function
  - Function to confirm the NVRAM condition when troubles happened.
  - Possible to confirm the value of the administrator password by the dumping.

2.5.6. Other Functions

TOE provides the functions that run background without awareness of the user and the updating function of TOE. The following explains the major functions.

① Overwrite delete function of the remaining information
It performs the overwrite deletion of the unneeded image files made by the job termination, the deleting operation by the job management function, the deletion of image files saved in the user box, and the deletion after a lapse of the storage period of image file. Overwriting data is 0x00 ⇒ 0x00 ⇒ 0x00 and performs the overwriting in this order.

② HDD lock function
HDD has the HDD lock function as measure against the illegal taking out, when the password is set.
The administrator function does the operation setting of this function. As for the starting operation of MFP, the access to HDD is permitted by the matching of the HDD lock password set to the HDD and the one set on the MFP. (Even if HDD is taken out, it is impossible to use it excluding the MFP that the concerned HDD installed.)

③ Remote diagnosis function
This manages the operation status of MFP, setup information of the administrator password, and the device information like the number of prints by using the several methods for the connection, such as the modem connection via RS-232C, the FAX unit, the E-Mail, etc, and communicating with the support center run by the subsidiaries of the Konica Minolta

Business Technologies, Inc. Also, an appropriate service is provided if necessary. (Shipment of an additional toner, charging request, failure diagnosis, dispatch of a service engineer, etc.).

④ Updating function of TOE
TOE facilitated with the function to update itself. When it receives a command from the remote diagnosis function, it can upgrade itself by downloading from the FTP server via Ethernet. There is also another way of updating by connecting a compact flash memory.

2.5.7. Enhanced Security Function

Various setting functions related to the behavior of the security function for the Administrator function and the Service engineer function can be set collectively to the secure values by the operation settings of the "Enhanced Security Function". Each value set is prohibited changing itself into the vulnerable one individually. As the function that does not have a setting function of the operation individually, the setting of the secure print authentication function (The operation method that searching both the ID and a password at the same time and then allowing a matching file to be printed, and the operation method that inputting a password into after having chosen ID) exists, but it is the setting to enhance the security. (latter described method).

The following explains the series of the setting condition of being the enhanced security unction active. In order to activate the enhanced security function, the prerequisite is required that an administrator password and a service code should be set along with the password policy.

- Setting of the Password policy function :valid
- Modification function of the network setting of SNMPv1 :prohibit
- Setting of the secure print authentication method :password examination operation after the file ID specified
- Setting of the prohibition of the authentication operation :valid (account lock status (threshold of unsuccessful attempts: 3) Also, the user box authentication method becomes password examination function operating method when downloading)
- Setting of HDD lock function :valid
- Setting of overwrite delete function for the remaining information :valid
- Total clear function :valid
- Memory dump function :prohibit
- Administrator password initialize function :prohibit
- Remote diagnosis function [2] : - Prohibited to connect RS232C modem
  -Prohibit the receiving function by connecting FAX unit
  - Prohibit the receiving function by e-mail

[2] However, the fax unit connection transmission function and the transmission function by E-mail are effective.

3. TOE Security Environment

This chapter will describe the concept of protected assets, assumptions, threats, and organizational security policies.

3.1. Concept of Protected Assets

Security concept of TOE is "the protection of data that can be disclosed against the intention of the user". As MFP is generally used, the following image file in available situation becomes the protected assets.

- Secure Print File
  - Image file registered by the secure print
- User Box File
  - Image files stored in a user box except "Public"

In the case of printing the secure print file, in order to prepare for the threat that is thought when an unauthorized MFP was connected by any chance, it is necessary to be unable to change MFP settings (IP address, etc) illegally. Therefore, the settings (IP address, etc) of MFP are considered as subsidiary protected assets.

An image file of a job stored as standby state by the operation of several jobs, an image file of a job stored as standby state with the remainder of copies for printing for the confirmation of the finish, and so forth, other than the target image files as the above mentioned are not treated as protected assets because it is not intended to be protected in the general use of MFP.

On the other hand, when the stored data have physically been separated from the jurisdiction of a user, such as the use of MFP ended by the lease return or being disposed, or the case of an HDD theft, a user has concerns about leak possibility of every remaining data. Therefore, in this case, the following data files become protected assets.

- All User Box Files
  - The image files which are stored in all types of user boxes including "Public" user box
- Swap Data File
  - A file to constitute an image that is a big size that does not fit into an RAM area occurring by a copy and a PC print (including secure print file).
- Overlay Image File
  - A background image file
  - This registered image file can be set as wallpaper and used for copying, etc.
- HDD accumulation image file
  - A file stored in an HDD from a PC print, and printed by the operation from a panel
- Remaining Image file[3]
  - The file which remains in the HDD data area that is not deleted only by general deletion operation (deletion of a file management area)
- A transmission address data file

[3] This data is assets controlled by means of TOE installed so as not to be generated with the operation of the security function. The threat identification explains the treatment of these assets as an event that can happen when it is assumed that security objectives were unimplemented.

- The file included an address transmitting an image, such as an E-mail address, a phone number, etc.

3.2. Assumptions

The present section identifies and describes the assumptions for the environment for using the TOE.

A.ADMIN（Personnel conditions to be an administrator）

Administrators, in the role given to them, will not carry out a malicious act during the series of permitted operations given to them.

A.SERVICE（Personnel conditions to be a service engineer）

Service engineers, in the role given to them, will not carry out a malicious act during series of permitted operations given to them.

A.NETWORK（Network connection conditions for MFP）

- The intra-office LAN where the MFP with the TOE will be installed is not intercepted.
- When the intra-office LAN where the MFP with the TOE will be installed is connected to an external network, access from the external network to the MFP is not allowed.

A.SECRET（An operational condition about secret information）

Each password does not leak out from each user in the use of TOE.

A.SETTING（A operation setting condition of enhanced security function）

MFP with the TOE is used after enabling the enhanced security function.

3.3. Threats

In this section, threats that are expected during the use of the TOE and the environment for using the TOE are identified and described.

T.DISCARD-MFP（the lease return or disposal of the MFP）

- When the leaser returned or the discarded MFP were collected, all user box files, a swap data file, an overlay image file, an HDD accumulation image file, and a remaining image file can leak by the person with malicious intent taking out and analyzing an HDD in MFP.
- When lease returned or the discarded MFP were collected, the person with malicious intent operates MFP and may find out concealment information such as a transmission address data file, various set passwords, etc.

T.BRING-OUT-STORAGE（An unauthorized carrying out of HDD）

- All user box files, a swap data file, an overlay image file, an HDD accumulation image file, and a remaining image file leak by a person or a user with malicious intent illegally taking out and analyzing an HDD in MFP.
- A person or a user with malicious intent illegally replaces an HDD in MFP. In the replaced

HDD, new files of the “user box” file, a swap data file, an overlay image file, an HDD accumulation image file, and a remaining image file are accumulated. A person or a user with malicious intent takes out and analyzes the replaced HDD and image files leak.

T.ACCESS-BOX（Unauthorized access to the user box which used a user function）

Exposure of the user box file when malicious person or user accesses the unpermitted user box and downloads the user box file.

T.ACCESS-SECURE-PRINT（Unauthorized access to the secure print file which used a user function）

Exposure of secure print file when malicious person or user prints the file which is not permitted to use.

T.ACCESS-NET-SETTING（An unauthorized change of network setting）

Malicious person or user changes the network settings of MFP with TOE to identify MFP and uses the setting value of the original MFP with TOE (IP address etc.) into the entity for another illegal MFP. The secure print file becomes sent to unauthorized MFP and the data is exposed.

T.ACCESS-SETTING（An unauthorized change of a function setting condition related to security）

The possibility of leaking user box file and secure print file rises because malicious person or user changes the settings related to the enhanced security function.

＜※ Complement：When HDD unattached＞

It is not necessary to consider about the following threats.（no threats exists）

・T.BRING-OUT-STORAGE
・T.ACCESS-BOX

The following threats have to consider the transmission address data file and various passwords stored in NVRAM.

・T.DISCARD-MFP

The following threats have to consider only the secure print file which is an available function regardless of attachment of an HDD.

・T.ACCESS-SETTING

3.4. Organizational Security Policies

There is no organizational security policy assumed to be applied to this TOE.

4. Security Objectives

In this chapter, in relation to the assumptions, the threats, and the organizational security policy identified in Chapter 3, the required security objectives policy for the TOE and the environment for the usage of the TOE are described by being divided into the categories of the security objectives for the TOE and the security objectives for the environment, as follows.

When an HDD is not installed, unnecessary security objectives may exist, but hereafter, assuming that an HDD was installed, this chapter disserts about the security objectives and the security requirements thought to be the maximum necessity against the threat.

4.1. Security Objectives for the TOE

In this section, the security objectives for the TOE is identified and described.

O.BOX（User Box access control）

TOE permits the user function of a user box file in the user box only to users who are authorized to use the user box.

O.SECURE-PRINT（Secure print file access control）

TOE permits the print of the secure print file only to the users who are authorized to use the secure print file.

O.CONFIG（Access limitation to management function）

TOE permits only the administrator to operate the following functions.

•Setting function that relates to address of MFP

•Function that relates to setting of enhanced security function

O.OVERWRITE-ALL（Complete overwrite deletion）

•TOE overwrites all data regions of HDD in MFP by using the deletion data, and makes all the image data of restoration impossible.

• TOE offers the function to delete the transmission address data of the telephone number and the E-mail address, etc. that become a part of individual or corporate information that the user has set, and the function to restore default administrator password and HDD lock password.

O.OVERWRITE-FILE（Overwrite deletion of each file）

When an image file written in HDD within MFP becomes unnecessary, TOE overwrites by deletion data and makes the restoration of the image impossible.

O.CHECK-HDD（Validity confirmation of HDD）

TOE verifies that the correct HDD is set up.

4.2. Security objectives for the Environment

In this section, the security objectives for the environment, in the environment of the usage of the TOE, is identified and described being divided into the IT environment security objectives and the non-IT environment security objectives.

4.2.1. IT environment security objectives

OE.LOCK-HDD（Access control of HDD）

HDD installed in MFP permits reading of data only from the MFP it installed.

OE.FEED-BACK（Feedback of password）

The applications, such as a browser or a PC print driver used for accessing the MFP by client PC offer the appropriate feedback protected for user box password and administrator password to be input

4.2.2. Non-IT environment security objective

OE-N.ADMIN（Reliable administrator）

The person in charge in the organization who uses MFP will assign a person who can faithfully execute the given role during the operation of the MFP with TOE as an administrator.

OE-N.SERVICE（Service engineer's guarantee）

- The person in charge in the organization that carries out the maintenance management of the MFP educates a service engineer in order to faithfully carry out the given role for the installation of the TOE, set up of TOE and the maintenance of the MFP with TOE.
- The administrator observes the maintenance work of MFP with TOE by a service engineer.

OE-N.NETWORK（Network Environment in which the MFP is connected）

- The person in charge in the organization who uses MFP carries out the tapping prevention measures by setting the cipher communications equipment and the tapping detection equipment to the LAN of the office where MFP with TOE is installed.
- The person in charge in the organization who uses MFP carries out the measures for the unauthorized access from the outside by setting up the equipment such as the firewall to intercept the access from an external network to MFP with TOE.

OE-N.SESSION（Termination of session after operation）

The administrator has the user implement the following operation.

- After the operation of the function to the secure print file ends, the logoff operation is performed.

The administrator executes the following operation.

- After the operation of the administrator mode function ends, the logoff operation is performed.

OE-N.SETTING-SECURITY（Operation setting of enhanced security function）

The administrator makes the setting of the enhanced security function effective for the operation of TOE.

OE-N.SECRET（Appropriate management of confidential information）

The administrator has the user implement the following operation.

- Keep the secure print password confidential.
- Keep the user box password confidential only among users who commonly use it.
- Should not set the value that can be guessed for the secure print password and the user box password.
- Change the user box password properly.
- Make the user box password change promptly when the administrator changes it.

The administrator executes the following operation.

- Should not set the value that can be guessed for the administrator password and the HDD lock password.
- Keep the administrator password and the HDD lock password confidential.
- Change the administrator password and the HDD lock password properly.

The service engineer executes the following operation.

- Should not set the value that can be guessed for the service code.
- Keep the service code confidential.
- Change the service code properly.

5. IT Security Requirements

In this chapter, the TOE security requirements and IT environment security requirements are described.

<Definition of Label>

The security function requirements required for the TOE and IT environment are described. Those regulated in CC Part 2 will be directly used for the functional requirements components, and the same labels will be used as well. The new additional requirement which is not described in CC part 2 is newly established and identified with the label that doesn't compete with CC part 2. In addition, [E] is added at the end of a label of a requirement needed in IT environment in order to state it clearly whether an object of each requirement is TOE or IT environment.

< Method of specifying security function requirement "Operation" >

In the following description, when items are indicated in "italic" and "bold," it means that they are assigned or selected. When items are indicated in "italic" and "bold" with parenthesis right after the underlined original sentences, it means that the underlined sentences are refined. A number in the parentheses after a label means that the functional requirement is used repeatedly. (The number to indicate the repetition is added with separating respectively by TOE requirement and IT environmental requirement.)

<Method of clear indication of dependency>

The label in the parentheses "( )" in the dependent section indicates a label for the security functional requirements used in this ST. When it is a dependency that is not required to be used in this ST, it is described as "N/A" in the same parentheses.

5.1. TOE Security Requirements

5.1.1. TOE Security Function Requirements

5.1.1.1. User data protection

FDP_ACC.1[1]	**Subset access control**
FDP_ACC.1.1[1]	
The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].	
[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]： ***Listed in 「Table 1 User Box Access Control Operational List」***	
[assignment: *access control SFP*]： ***User Box access control***	
Hierarchical to ： No other components Dependencies ： FDP_ACF.1（FDP_ACF.1[1]）	

Table 1 User Box Access Control Operational List

Subject	Object	Operational list
A task that substitutes for a user	***User Box file***	***Download***

FDP_ACC.1[2]　　Subset access control

FDP_ACC.1.1[2]

The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]：

Listed in 「Table 2 secure print file access control　Operational List

[assignment: *access control SFP*]：

Secure Print file access control

Hierarchical to　：　No other components
Dependencies　：　FDP_ACF.1（FDP_ACF.1[2]）

Table 2　Secure Print File Access Control　Operational List

Subject	Object	Operational list
A task that substitutes for a user	***Secure print file***	***Print***

FDP_ACC.1[3]　　Subset access control

FDP_ACC.1.1[3]

The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]：

Listed in 「Table 3　Administrator mode access control　operational list」

[assignment: *access control SFP*]：

Administrator mode access control

Hierarchical to　：　No other components
Dependencies　：　FDP_ACF.1（FDP_ACF.1[3]）

Table 3　Administrator Mode Access Control　Operational List

Subject	Object	Operational list
A task that　substitutes for a user	***• HDD lock password object*** ***• MFP address group object***	***Setting***

FDP_ACF.1[1]　　Security attribute based access control

FDP_ACF.1.1[1]

The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].

[assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]：

＜Subject＞　　　　　＜Subject attributes＞
• A task that substitutes for a user　⇒　• User Box attributes（User Box ID）

＜Object＞　　　　　＜Object attributes＞
• User Box File　⇒　• User Box attributes（User Box ID）

[assignment: *access control SFP*]：

User Box access control

FDP_ACF.1.2[1]

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*] ：

The task that substitutes a user who is related to the User Box attributes（Box ID）is allowed the download operation to the user box files that have the matched user box attributes with the user box attributes of the subject attributes.

FDP_ACF.1.3[1]

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]：

None

FDP_ACF.1.4[1]

The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects] ：

None

Hierarchical to ： No other components
Dependencies ： FDP_ACC.1（FDP_ACC.1[1]）, FMT_MSA.3（N/A）

FDP_ACF.1[2] Security attribute based access control

FDP_ACF.1.1[2]

The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].

[assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*] ：

＜Subject＞ ＜Subject attributes＞
• a task that substitutes for the user ⇒ • File attributes（secure print internal control ID）

＜Object＞ ＜Object attributes＞
• secure print file ⇒ • File attributes（secure print internal control ID）

[assignment: *access control SFP*] ：

secure print file access control

FDP_ACF.1.2[2]

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*] ：

A task that substitutes a user who has file attributes (secure print internal control ID) is permitted the printing operation to the secure print file that has a matching file attribute (secure print internal control ID) with the file attribute (secure print internal control ID).

FDP_ACF.1.3[2]

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects] ：

None

FDP_ACF.1.4[2]

The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects] ：

None

Hierarchical to ： No other components

Dependencies	：	FDP_ACC.1（FDP_ACC.1[2]）, FMT_MSA.3（N/A）

FDP_ACF.1[3] Security attribute based access control

FDP_ACF.1.1[3]

The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].

[assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*] ：

＜Subject＞		***＜Subject attributes＞***
・task that substitutes for a user	⇒	***・Administrator attributes***

＜Object＞

・HDD Lock Password Object

・MFP Address Group Object [4]

[assignment: *access control SFP*] ：

Administrator mode access control

FDP_ACF.1.2[3]

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*] ：

The task that substitutes the user who has the administrator attribute is permitted the setting operation of the HDD lock password object and the MFP address group object.

FDP_ACF.1.3[3]

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects] ：

None

FDP_ACF.1.4[3]

The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects] ：

None

Hierarchical to	：	No other components
Dependencies	：	FDP_ACC.1（FDP_ACC.1[3]）, FMT_MSA.3（N/A）

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: [assignment: *list of objects*].

[selection: *allocation of the resource to, deallocation of the resource from*] ：

deallocation of the resource from

[assignment: *list of objects*] ：

・All user box file

・Swap data file

・Overlay image file

・HDD accumulation image file

[4] The MFP address group object is a series of data concerning the address of the MFP body such as IP address and the Appletalk printer name.

Hierarchical to	：	No other components
Dependencies	：	No dependencies

5.1.1.2. Identification and Authentication

FIA_AFL.1[1]	**Authentication failure handling**	
FIA_AFL.1.1[1]		
The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].		
[assignment: *list of authentication events*] ： ***•Authentication in the case of accessing the service mode*** ***•Re-authentication in the case of modifying the service code***		
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] ***[assignment: positive integer number] ：3***		
FIA_AFL.1.2[1]		
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].		
[assignment: *list of actions*] ： ***＜An action when it is detected＞*** ***・ Log off from the authentication status of the service mode if it is, and lock the authentication function which uses the service code*** ***・ If it's not under the authentication status, lock the authentication function which uses the service code*** ***＜Operation for recovering the normal condition＞*** ***Perform the boot process of the TOE.***		
Hierarchical to	：	No other components
Dependencies	：	FIA_UAU.1（FIA_UAU.2[1]）

FIA_AFL.1[2]	**Authentication failure handling**
FIA_AFL.1.1[2]	
The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].	
[assignment: *list of authentication events*] ： ***•Authentication in the case of accessing administrator mode*** ***•Re-authentication in the case of modifying the administrator password***	
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] ***[assignment: positive integer number] ：3***	
FIA_AFL.1.2[2]	
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].	
[assignment: *list of actions*] ： ***＜An action when it is detected＞*** ***・ Log off from the authentication status of the administrator mode if it is, and lock the authentication function which uses the administrator password.*** ***・ If it's not under the authentication status, lock the authentication function which uses the administrator password.*** ***＜Operation for recovering the normal condition＞*** ***Perform the boot process of the TOE.***	

Hierarchical to	：	No other components
Dependencies	：	FIA_UAU.1（FIA_UAU.2[2]）

FIA_AFL.1[3] Authentication failure handling

FIA_AFL.1.1[3]
The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].
[assignment: *list of authentication events*] ： ***Authentication in the case of accessing the secure print file.***
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] ***[assignment: positive integer number] ：3***
FIA_AFL.1.2[3]
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].
[assignment: *list of actions*] ： ***＜An action when it is detected＞*** ***Refuse the access to the secure print file, and lock the authentication function to the secure print file*** ***＜Operation for recovering the normal condition＞*** ***Perform Lock release function offered in administrator mode.***
Hierarchical to ： No other components
Dependencies ： FIA_UAU.1（FIA_UAU.2[3]）

FIA_AFL.1[4] Authentication failure handling

FIA_AFL.1.1[4]
The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].
[assignment: *list of authentication events*]： ***Authentication in the case of accessing the user box.***
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] ***[assignment: positive integer number] ：3***
FIA_AFL.1.2[4]
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].
[assignment: *list of actions*] ： ***＜An action when it is detected＞*** ***Refuse the access to the user box and the user box file in it, and lock the authentication function to the appropriate user box*** ***＜Operation for recovering the normal condition＞*** ・ ***Perform the Lock release function offered in administrator mode.*** ・ ***Perform the boot process of the TOE.***
Hierarchical to ： No other components
Dependencies ： FIA_UAU.1（FIA_UAU.2[4]）

FIA_ATD.1 User attribute definition

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].	
[assignment: *list of security attributes*] ： ***• User Box attributes （User Box ID）*** ***• File attributes （secure print internal control ID）***	
Hierarchical to ：	No other components
Dependencies ：	No dependencies

FIA_SOS.1[1] Verification of secrets

FIA_SOS.1.1[1]	
The TSF shall provide a mechanism to verify that secrets ***(Administrator Password)*** meet [assignment: *a defined quality metric*].	
[assignment: *a defined quality metric*]： ***•Number of digits: 8- digits*** ***•Character type: Numeric*** ***•Rule: It is not composed of the same kind of character string alone.***	
Hierarchical to ：	No other components
Dependencies ：	No dependencies

FIA_SOS.1[2] Verification of secrets

FIA_SOS.1.1[2]	
The TSF shall provide a mechanism to verify that secrets ***（Secure Print Password, User Box Password）*** meet [assignment: *a defined quality metric*].	
[assignment: *a defined quality metric*] ： ***•Number of digits: 8- digits*** ***•Character type: ASCII code （0x20 - 0x7E except 0x22, 0x2B and 0x5E）*** ***•Rule: It is not composed of the same kind of character string alone.***	
Hierarchical to ：	No other components
Dependencies ：	No dependencies

FIA_SOS.1[3] Verification of secrets

FIA_SOS.1.1[3]	
The TSF shall provide a mechanism to verify that secrets ***（HDD Lock Password）*** meet [assignment: *a defined quality metric*].	
[assignment: *a defined quality metric*] ： ***•Number of digits: 20- digits*** ***•Character type: ASCII code （0x20 - 0x7E except 0x20, 0x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3C, 0x3E, 0x5B, 0x5C, 0x5D and 0x5E）*** ***•Rule: It is not composed of the same kind of character string alone.***	
Hierarchical to ：	No other components
Dependencies ：	No dependencies

FIA_SOS.1[4] Verification of secrets

FIA_SOS.1.1[4]
The TSF shall provide a mechanism to verify that secrets ***（Service Code）*** meet [assignment: *a defined quality metric*].
[assignment: *a defined quality metric*] ：

•Number of digits: 8- digits ***•Character type: Numeric, #, **** ***•Rule: It is not composed of the same kind of character string alone.***	
Hierarchical to ：	No other components
Dependencies ：	No dependencies

FIA_UAU.2[1] User authentication before any action

FIA_UAU.2.1[1]	
The TSF shall require each user ***（Service Engineer）*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user ***（Service Engineer）***.	
Hierarchical to ：	FIA_UAU.1
Dependencies ：	FIA_UID.1（FIA_UID.2[1]）

FIA_UAU.2[2] User authentication before any action

FIA_UAU.2.1[2]	
The TSF shall require each user ***（Administrator）*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user ***（Administrator）***.	
Hierarchical to ：	FIA_UAU.1
Dependencies ：	FIA_UID.1（FIA_UID.2[2]）

FIA_UAU.2[3] User authentication before any action

FIA_UAU.2.1[3]	
The TSF shall require each user ***（User who is permitted to use the secure print file）*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user ***（User who is permitted to use the secure print file）.***	
Hierarchical to ：	FIA_UAU.1
Dependencies ：	FIA_UID.1（FIA_UID.2[3]）

FIA_UAU.2[4] User authentication before any action

FIA_UAU.2.1[4]	
The TSF shall require each user ***（User who is permitted to use the user box）*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user ***（User who is permitted to use the user box）.***	
Hierarchical to ：	FIA_UAU.1
Dependencies ：	FIA_UID.1（FIA_UID.2[4]）

FIA_UAU.6 Re-authenticating

FIA_UAU.6.1
The TSF shall re-authenticate the use under the conditions [assignment: *list of conditions under which re-authentication is required*].
[assignment: *list of conditions under which re-authentication is required*] ***•When the administrator modifies the administrator password*** ***•When the service engineer modifies the service code*** ***•When the administrator changes the setting of the HDD lock function***

Hierarchical to ： No other components
Dependencies ： No dependencies

FIA_UAU.7 Protected authentication feedback
FIA_UAU.7.1
The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.
[assignment: *list of feedback*]： ***Display “*" every character data input.***
Hierarchical to ： No other components
Dependencies ： FIA_UAU.1（FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3]）

FIA_UID.2[1] User identification before any action
FIA_UID.2.1[1]
The TSF shall require each user ***（Service Engineer）*** to identify itself before allowing any other TSF-mediated actions on behalf of that user ***（Service Engineer）.***
Hierarchical to ： FIA_UID.1
Dependencies ： No dependencies

FIA_UID.2[2] User identification before any action
FIA_UID.2.1[2]
The TSF shall require each user ***（Administrator）*** to identify itself before allowing any other TSF-mediated actions on behalf of that user ***（Administrator）.***
Hierarchical to ： FIA_UID.1
Dependencies ： No dependencies

FIA_UID.2[3] User identification before any action
FIA_UID.2.1[3]
The TSF shall require each user ***（User who is permitted to use the secure print file）*** to identify itself before allowing any other TSF-mediated actions on behalf of that user ***（User who is permitted to use the secure print file）.***
Hierarchical to ： FIA_UID.1
Dependencies ： No dependencies

FIA_UID.2[4] User identification before any action
FIA_UID.2.1[4]
The TSF shall require each user ***（User who is permitted to use the user box）*** to identify itself before allowing any other TSF-mediated actions on behalf of that user ***（User who is permitted to use the user box）.***
Hierarchical to ： FIA_UID.1
Dependencies ： No dependencies

FIA_USB.1	**User-subject binding**
FIA_USB.1.1	
The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.	
Hierarchical to ：	No other components
Dependencies ：	FIA_ATD.1

5.1.1.3. Security management

FMT_MOF.1	**Management of security functions behaviour**
FMT_MOF.1.1	
The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].	
[assignment: *list of functions*] ： ***Enhanced Security Setting***	
[selection: *determine the behaviour of, disable, enable, modify the behaviour of*] ： ***disable***	
[assignment: *the authorised identified roles*] ： ***Administrator***	
Hierarchical to ：	No other components
Dependencies ：	FMT_SMF.1（FMT_SMF.1）, FMT_SMR.1（FMT_SMR.1[2]）

FMT_MSA.3	**Static attribute initialisation**
FMT_MSA.3.1	
The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes ***(secure print internal control ID)*** that are used to enforce the SFP.	
[selection, choose one of: *restrictive, permissive, [assignment: other property]*] ： ***[assignment: other property]: Identified uniquely***	
[assignment: *access control SFP, information flow control SFP*]： ***Secure print file access control***	
FMT_MSA.3.2	
The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.	
[assignment: *the authorised identified roles*]： ***None***	
Hierarchical to ：	No other components
Dependencies ：	FMT_MSA.1（N/A）, FMT_SMR.1（N/A）

FMT_MTD.1[1]	**Management of TSF data**
FMT_MTD.1.1[1]	
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].	
[assignment: *list of TSF data*] ： ***"User Box password" of the concerned user box***	
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]：	

modify	
[assignment: *the authorised identified roles*]： ***• User who is permitted to use that user box*** ***• Administrator***	
Hierarchical to ：	No other components
Dependencies ：	FMT_SMF.1（FMT_SMF.1）, FMT_SMR.1（FMT_SMR.1[2], FMT_SMR.1[3]）

FMT_MTD.1[2] Management of TSF data

FMT_MTD.1.1[2]	
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].	
[assignment: *list of TSF data*] ： ***Administrator Password***	
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] ： ***modify***	
[assignment: *the authorised identified roles*] ： ***Administrator***	
Hierarchical to ：	No other components
Dependencies ：	FMT_SMF.1（FMT_SMF.1）, FMT_SMR.1（FMT_SMR.1[2]）

FMT_MTD.1[3] Management of TSF data

FMT_MTD.1.1[3]	
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].	
[assignment: *list of TSF data*] ： ***Administrator Password***	
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] ： ***query***	
[assignment: *the authorised identified roles*] ： ***Service Engineer***	
Hierarchical to ：	No other components
Dependencies ：	FMT_SMF.1（FMT_SMF.1）, FMT_SMR.1（FMT_SMR.1[1]）

FMT_MTD.1[4] Management of TSF data

FMT_MTD.1.1[4]	
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].	
[assignment: *list of TSF data*] ： ***Service Code***	
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] ： ***modify***	
[assignment: *the authorised identified roles*] ： ***Service Engineer***	
Hierarchical to ：	No other components
Dependencies ：	FMT_SMF.1（FMT_SMF.1）, FMT_SMR.1（FMT_SMR.1[1]）

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [assignment: *list of security management functions to be provided by the TSF*].

[assignment: *list of security management functions to be provided by the TSF*]：

•Stop function of enhanced security function by administrator
•Deletion function of detected value of unauthorized access to secure print by administrator
•Deletion function of detected value of unauthorized access to user box by administrator
•Modification function of administrator password by administrator
•Modification function of user box password by administrator
•Modification function of service code by service engineer
•Inquiry function of administrator password by service engineer
•Modification function of user box password of appropriate user box by user who is permitted to use the user box

Hierarchical to	：	No other components
Dependencies	：	No dependencies

FMT_SMR.1[1] Security roles

FMT_SMR.1.1[1]

The TSF shall maintain the roles [assignment: *the authorised identified roles*].

[assignment: *the authorised identified roles*] ：

Service Engineer

FMT_SMR.1.2[1]

The TSF shall be able to associate users with roles.

Hierarchical to	：	No other components
Dependencies	：	FIA_UID.1 （FIA_UID.2[1]）

FMT_SMR.1[2] Security roles

FMT_SMR.1.1[2]

The TSF shall maintain the roles [assignment: *the authorised identified roles*].

[assignment: *the authorised identified roles*] ：

Administrator

FMT_SMR.1.2[2]

The TSF shall be able to associate users with roles.

Hierarchical to	：	No other components
Dependencies	：	FIA_UID.1 （FIA_UID.2[2]）

FMT_SMR.1[3] Security roles

FMT_SMR.1.1[3]

The TSF shall maintain the roles [assignment: *the authorised identified roles*].

[assignment: *the authorised identified roles*] ：

User who is permitted to use the user box

FMT_SMR.1.2[4]

The TSF shall be able to associate users with roles.

Hierarchical to	：	No other components
Dependencies	：	FIA_UID.1 （FIA_UID.2[4]）

5.1.1.4. Protection of the TSF

FPT_RVM.1	**Non-bypassability of the TSP**
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.	
Hierarchical to	： No other components
Dependencies	： No dependencies

FPT_SEP.1	**TSF domain separation**
FPT_SEP.1.1	
The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.	
FPT_SEP.1.2	
The TSF shall enforce separation between the security domains of subjects in the TSC.	
Hierarchical to	： No other components
Dependencies	： No dependencies

5.1.1.5. Extended requirement: Identification and approval of access destination

FIA_NEW.1	**Identification and approval of a user becoming an access object from TOE**
FIA_NEW.1.1	
TSF shall demand to succeed in the user's identification before the action is taken to <u>user</u> ***(HDD)*** by TOE.	
FIA_NEW.1.2	
TSF shall stop the start of the action to <u>user</u> ***(HDD)*** by TOE if the user's identification is failed.	
Hierarchical to	： No other components
Dependencies	： No dependencies

Audit: FIA_NEW.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST. a) Minimal unsuccessful use of user identification mechanism including offered user identification information b) Basic Use all of user identification mechanism including offered user deification information
Management: FIA_NEW.1
The following actions could be considered for the management functions in FMT. a) management of user identification information

5.1.1.6. Extended requirement: Remaining information protection after explicit deletion operation

FNEW_RIP.1	**Protection of remaining information on the user data and TSF data after explicit deletion operation**
FNEW_RIP.1.1	

TSF shall guarantee not to be able to use the content of any information before having been assigned to the resource on the explicit deleting operation to the following objects and the TSF data : [assignment: *list of object and list of TSF data*].
[assignment: *list of object and list of TSF data*] : ***< object >*** ***•All user box file*** ***•Swap data file*** ***•Overlay image file*** ***•HDD accumulation image file*** ***•Transmission address data file*** ***•HDD lock password object*** ***< TSF data >*** ***•Administrator password*** ***•User Box password***
Hierarchical to : No other components Dependencies : No dependencies

Audit: FNEW_RIP.1
Use including the information of user identification performing the explicit deletion operation.
Management: FNEW_RIP.1
There is no foreseen management activity.

5.1.2. Minimum Security Strength of Function

The minimum strength of function level of the TOE is SOF-Basic. The required TOE security functions that use a probabilistic/permutational mechanism are FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3], FIA_UAU.2[4], FIA_UAU.6, FIA_SOS.1[1], FIA_SOS.1[2], FIA_SOS.1[3], FIA_SOS.1[4].

5.1.3. TOE Security Assurance Requirements

The TOE is a commercial office product that is used in a general office environment, and therefore a TOE security assurance requirement that is required for EAL3 conformance, which is a sufficient level as an assurance for commercial office products, is applied. The following table summarizes the applied TOE security assurance requirements.

Table 4 TOE Security Assurance Requirements

TOE Security Assurance Requirements		Component
Class ACM: Configuration management	CM capabilities	ACM_CAP.3
	CM scope	ACM_SCP.1
Class ADO: Delivery and Operation	Delivery	ADO_DEL.1
	Installation, generation and start-up	ADO_IGS.1
Class ADV: Development	Function specification	ADV_FSP.1
	High-level design	ADV_HLD.2
	Representation correspondence	ADV_RCR.1
Class AGD: Guidance Documents	Administrator guidance	AGD_ADM.1
	User guidance	AGD_USR.1

TOE Security Assurance Requirements		Component
Class ALC: Life Cycle Support	Development security	ALC_DVS.1
Class ATE: Tests	Coverage	ATE_COV.2
	Depth	ATE_DPT.1
	Functional tests	ATE_FUN.1
	Independent testing	ATE_IND.2
Class AVA: Vulnerability Assessment	Misuse	AVA_MSU.1
	Strength of TOE security functions	AVA_SOF.1
	Vulnerability analysis	AVA_VLA.1

5.2. Security Requirements for the IT environment

5.2.1.1. Identification and Authentication

FIA_AFL.1[E] Authentication failure handling

FIA_AFL.1.1[E]

The TSF *（HDD）* shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

[assignment: *list of authentication events*] ：

Authentication by HDD lock function when accessing HDD

[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]

[assignment: positive integer number] ：5

FIA_AFL.1.2[E]

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].

[assignment: *list of actions*] ：

＜Action when it is detected＞
Refuse reading and writing of data in HDD
＜Operation for recovering the normal condition＞
Energizing OFF to HDD (Power OFF)

Hierarchical to ： No other components

Dependencies ： FIA_UAU.1（FIA_UAU.2[E]）

FIA_UAU.2[E] User authentication before any action

FIA_UAU.2.1[E]

The TSF *（HDD）* shall require each user *（The main body of MFP where HDD installed）* to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user *（The main body of MFP where HDD installed）*.

Hierarchical to ： FIA_UAU.1

Dependencies ： FIA_UID.1（N/A）

FIA_UAU.7[E] Protected authentication feedback

FIA_UAU.7.1[E]

The TSF ***（PC application）*** shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.		
[assignment: *list of feedback*] ： ***display "*" in every character data input***		
Hierarchical to	：	No other components
Dependencies	：	FIA_UAU.1（FIA_UAU.2[2], FIA_UAU.2[4]）

6. TOE Summary Specification

6.1. TOE Security Functions

The list of the TOE security function led from the TOE security function requirement is shown in the following Tables 5. The detailed specification is explained in the paragraphs described below.

Table 5 The list of the name and identifier of TOE Security function

No.	Security function of TOE	
1	F.ADMIN	Administrator function
2	F.SERVICE	Service mode function
3	F.BOX	User Box function
4	F.PRINT	Secure Print function
5	F.OVERWRITE-FILE	Remaining information Overwrite Deletion function
6	F.OVERWRITE-ALL	All area Overwrite Deletion function
7	F.HDD	HDD verification function
8	F.RESET	Authentication failure frequency reset function

6.1.1. F.ADMIN（Administrator Function）

F.ADMIN is a series of security function that administrator operates, such as an administrator identification authentication function in an administrator mode accessing from a panel or through a network, and a security management function that includes a change of an administrator password and a lock cancellation of a locked user box. (Nevertheless, all functions are not feasible functions through both a panel and a network.)

6.1.1.1. Administrator identification authentication function

It identifies and authenticates the accessing user as the administrator in response to the access request to the administrator mode.

- ● Offers the administrator password authentication mechanism authenticating by the administrator password that consists of the character shown in Table 6.
- ● Return “*" for each character as feedback for the entered administrator password by the access from the panel.
- ● Resets the number of authentication failure when succeeding in the authentication.
- ● Locks all the authentication functions to use the administrator password when detecting the authentication failure that becomes the third times at total in each authentication function by using the administrator password. (Refuse the access to the administrator mode)
- ● Lock of Authentication function is released with F.RESET function operated.

Table 6 Character and number of digits used for password

Objectives	Number of digits	Character
Service code	8-digits	12 characters in total can be selected ・Number：0 ～ 9, # , *

Objectives	Number of digits	Character
Administrator password	8-digits	10 characters in total can be selected ・Number：0 ～ 9
User Box password	8-digits	92 characters in total can be selected ASCII code（0x20-0x7E except 0x22, 0x5E and 0x2B） ・Number：0 ～ 9 ・Alphabet：capital letter, small letter ・Symbol：! , # , $, % , & , ' , (,) , * , , , - , . , / , : , ; , < , = , > , ? , @ , [, ¥ ,] , _ , ` , { , | , } , ~ , *SPACE*
Secure Print password		
HDD lock password	20-digits	82 characters in total can be selected ASCII code（0x20-0x7E except 0x20, x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3C, 0x3E, 0x5B, 0x5C, 0x5D and 0x5E） ・Number：0 ～ 9 ・Alphabet：capital letter, small letter ・Symbol：! , # , $, % , & , ' , * , + , - ,. , / , = , ? , @ , _ , ` , { , | , } , ~

6.1.1.2. Function offered in Administrator Mode

When a user is identified and authenticated as an administrator by the administrator identification authentication function at the accessing request to the administrator mode, the administrator authority is associated with the task substituting the user. And the following operations and the use of the functions are permitted.

① Change of the administrator password

When a user is reauthenticated as an administrator, and the new password satisfies the quality, the password is changed.

- Offers the administrator password authentication mechanism that is authenticated by the administrator password which consists of the character shown in Table 6.
- Resets the number of authentication failure when succeeding in the re-authentication.
- Return "*" for each character as feedback for the entered administrator password in the re-authentication by the access from the panel.
- When the authentication failure that becomes the third times at total in each authentication function by using the administrator password is detected, it logoffs the administrator mode accessing from the panel, and locks all the authentication functions to use the administrator password. (The access to the administrator mode is refused.)
- Lock of Authentication function is released with F.RESET function operated.
- Verify the new administrator password if the following qualities are satisfied.
  - It is composed of the characters and by the number of digits, shown in the Table 6.
  - It shall not be composed of one kind of character.

② Change of User box password

A user box password other than the "Public" user box is changed. Verify that the new user box password satisfies the following qualities.

- It is composed of the characters and by the number of digits, shown in Table 6
- It shall not be composed of one kind of character.

③ Release of lock

Reset (0 clear) the number of authentication failure for all secure prints.

- If a secure print that access locked exists, the lock is released.

Reset (0 clear) the number of authentication failure of all user boxes.

- If a user box that access locked exists, the lock is released.

④ Setting and execution of all area overwrite deletion function

Perform the overwrite deletion of all area. (F.OVERWRITE-ALL is executed.)

⑤ Network setting

A setup operation of the following setting data is performed.

- A series of setup data that relates to MFP address (IP address, etc.)

⑥ Password setting function of HDD lock function

Change the HDD lock password. By using the HDD lock password currently set, when it is re-authenticated as an administrator, and the new password satisfies the quality, it is changed.

- Offers the HDD lock password verification mechanism that verified the HDD lock password that consists of the character shown in Table 6.
- Return, in verification, “*" for each character as feedback for the entered HDD lock password.
- Verify the HDD lock password newly set if the following qualities are satisfied.
  - It is composed of the characters and by the number of digits shown in Table 6.
  - It shall not be composed of one kind of character.

⑦ Operation setting of Enhanced security function

The function that influences the setting of the enhanced security function operated by the administrator is as follows.

- Operation setting of enhanced security function

  Function to set enhanced security function valid or invalid.
- Overwrite deletion function for all area

  The settings of enhanced security function are invalidated by executing the overwrite deletion of all area.

6.1.2. F.SERVICE（Service Mode Function）

F.SERVICE is a series of security function that the service engineer operates, such as the service engineer identification authentication function in service mode accessing from a panel, and a security management function that includes a change in the service code and the administrator password.

6.1.2.1. Service engineer identification authentication function

It is identified and authenticated the accessing user as the service engineer in response to the access request to the service mode from the panel.

- Offers the service code authentication mechanism that is authenticated by the service code that consists of the character shown in Table 6.
- Return "*" for each character as feedback for the entered service codes.
- Resets the number of the authentication failure when succeeding in the authentication.
- When the authentication failure that becomes the third times at total in each authentication function by using the service code is detected, it locks all the authentication functions to use the service code. (The access to the service mode is refused.)
- Lock of authentication function is released with F.RESET function operated.

6.1.2.2. Function offered in service mode

When a user is identified and authenticated as a service engineer by the service engineer identification authentication function at the access request to the service mode, the use of the following functions is permitted.

① Change of the service code

When a user is reauthenticated as a service engineer, and the new password satisfies the quality, it is changed.

- ➢ Offers the service code authentication mechanism that is reauthenticated by the service code that consists of the characters shown in Table 6.
- ➢ Resets the number of authentication failure when succeeding in the re-authentication.
- ➢ Return "*" for each character as feedback for the entered service codes in the re-authentication.
- ➢ When the authentication failure that becomes the third times at total in each authentication function by using the service code is detected, it logoffs the service mode accessing from the panel, and locks all the authentication functions to use the service code. (The access to the service mode is refused.)
- ➢ Lock of the authentication function is released with F.RESET function operated.
- ➢ Verify the new service code if the following qualities are satisfied.
  - It is composed of the characters and by the number of digits, shown in the Table 6.
  - It shall not be composed of one kind of character.

② Transmission of administrator password

The device information of MFP is transmitted to MFP support center via FAX unit or by E-mail.

- ➢ The device information sent includes the security information and administrator password with stealth. (Correspond to the inquiry function of the administrator password.)

6.1.3. F.BOX（User Box Function）

F.BOX is a security function that relates to the user box such as the user box access control function, which identifies and authenticates that a person is a permitted user to use the user box in the accessing to the user box from a PC and controls the operation to the user box file.

6.1.3.1. Registration function of user box

The user box registration operation is offered by the user operation. The user box specified is registered by the name and password of a user box appropriately identified.

- Verify that there is no user box name already registered.
- Verify the user box password satisfies the following requirements.
  - ➢ It is composed of the characters and by the number of digits shown in the Table 6.
  - ➢ It shall not be composed of one kind of character.

6.1.3.2. Identification authentication function in access to user box

It authenticates that the accessing user is a user to whom the use of a user box concerned is permitted respectively in response to the access request to each user box.

- Offers the user box password authentication mechanism that is authenticated by the user box password that consists of the character shown in Table 6.
- Resets the number of authentication failure when succeeding in the authentication.
- When the authentication failure is detected the third times at total for a user box concerned, it locks the authentication function to the user box.
- The lock of the authentication function executes the lock release function to the user box of F.ADMIN or operates F.RESET function and releases the lock of the user box.

The followings are the function that the user who is permitted the use of the user box is offered in the user box identification authentication domain of the user box, and to execute it authentication is required for all.

- Offers the user box password authentication mechanism that is authenticated by the user box password that consists of the character shown in Table 6.
- Resets the number of authentication failure of a user box concerned when succeeding in the authentication.
- When the authentication failure is detected the third times at total in each authentication function to use the user box password, it logs off the user box identification authentication domain, and locks all the authentication functions to use the user box password.(The access of a user box concerned to the user box identification authentication domain is refused.)
- The lock of the authentication function executes the lock release function to the user box of F.ADMIN, or operates F.RESET function and releases the lock of the user box.

① Access control to user box file in the user box

As for the task of substituting the user, "User Box name" of the user box is related to the task as a user box attribute. This task is permitted to perform the download operation to the user box file of which a user box attributes match to the user box attributes of the subject attributes.

② Change of user box password

It changes the user box password of the user box.

- ➢ Offers the user box password authentication mechanism that is re-authenticated by the user box password that consists of the character shown in Table 6.
- ➢ Resets the number of authentication failure of a user box concerned when succeeding in the re-authentication.
- ➢ When the authentication failure is detected the third times at total in each authentication function by using the user box password, it locks all the authentication functions to use the user box password. (The access of a user box concerned to the user box identification

authentication domain is refused.)

- ➢ The lock of the authentication function executes the lock release function to the user box of F.ADMIN, or operates F.RESET function and releases the lock of the user box.
- ➢ Verify that the new user box password satisfies the following quality.
  - It is composed of the characters and by the number of digits shown in Table 6.
  - It shall not be composed of one kind of character.

6.1.4. F.PRINT（Secure Print Function）

F.PRINT is a series of security function related to the secure print such as the access control function that allows the printing of the secure print file after authenticating if a user is the authorized user to use the secure print file for the access to the secure print file from the panel.

6.1.4.1. Authentication Function by secure print password

It authenticates that the accessing user is a user to whom the use of the secure print file concerned is permitted, in response to the access request to each secure print file.

- ● Offers the secure print password authentication mechanism that is authenticated by the secure print password that consists of the character shown in Table 6.
- ● Return “*" for each character as feedback for the entered secure print password.
- ● When the authentication failure is detected the third times at total for the secure print file concerned, it locks the authentication function to the concerned secure print file.
- ● The lock status is released by executing the lock release function of F.ADMIN against the secure print file.

6.1.4.2. Access control function to secure print file

The secure print file access control activates when it is authenticated.

- ● The task of substituting the user that is identified and authenticated has the secure print internal control ID of the secure print file authenticated as the file attribute.
- ● This task is permitted to print the secure print file with the file attribute which matches to this file attribute.

6.1.4.3. Registration function of secure print file

① Registration of secure print password

Verify that the registering secure print password satisfies the following condition in the registration request of secure print file.

- ➢ It is composed of the characters and by the number of digits, shown in the Table 6.
- ➢ It shall not be composed of one kind of character.

② Grant of secure print internal control ID

Secure print internal control ID that is identified uniquely sets to the concerned secure print file after verifying the secure print password in the registration request of secure print file.

6.1.5. F.OVERWRITE-FILE（Remaining information overwrite deletion function）

F.OVERWRITE is not only the general deletion (deletion the management area for the file access), but also the overwrite deletion function of the HDD data domain when deleting a file in the following cases.

＜Event that remaining information overwrite deletion starts＞

- Job completion of copy and print. [5]
  - Overwrite deletion object：Swap data file
- Deletion by user operation.
  - Overwrite deletion object：All user box files, overlay image file, and HDD accumulation image file
- Start of automatic deletion by time limit passage.
  - Overwrite deletion object：All user box file, swap data file（Only the swap data of the secure print file corresponds）
- When the power is turned on, after the power was turned off while the job is running.
  - Overwrite deletion object：Swap data file

The deletion method is "0x00⇒0x00⇒0x00" and overwrite the object area. As a result of the operation of this function, the remaining image file does not exist.

6.1.6. F.OVERWRITE-ALL（All area overwrite deletion function）

F.OVERWRITE-ALL executes the overwrite deletion at the HDD data area and deletes the transmission address data file installed in NVRAM as well. The object deleted or initialized is as follows.

＜deletion object：HDD＞

- All user box files
- Swap data file
- Overlay image file
- HDD accumulation image file
- User box password

＜deletion object：NVRAM＞

- Transmission address data file
- HDD lock password

＜initialization object：NVRAM＞

- Administrator password

The deletion method for the data and the frequency written in HDD executes "0x00⇒0xFF⇒ 0x00⇒0xFF⇒0x00⇒0xFF⇒0xAA⇒ verification".

In addition, by the execution of this function, the enhanced security function becomes invalid. (Refer to the description of operation setting of the enhanced security function in F.ADMIN)

[5] The job completion means that the job is finished successfully with ending the printing of copy or other operation of the operation is discontinued by the user interruption.

6.1.7. F.HDD（HDD Verification function）

F.HDD is the checking function to permit or not permit reading and writing to HDD. When the HDD lock password is set to HDD, it verifies the status of HDD, and if HDD lock password is not set, it does not permit the reading and the writing operations by assuming that the illegal HDD is set up.

6.1.8. F.RESET（Authentication Failure Frequency Reset Function）

F.RESET is a function to reset the number of authentication failure counted in each authentication function including the administrator authentication. (Do not relate to the lock is valid or not.)

This function operates by activating TOE such that the main power supply is turned on, it returns from the power failure and so forth. When it starts, the following numbers of authentication failure are reset.

- The number of failure to authentication of administrator
- The number of failure to authentication of a service engineer
- The number of failure that is kept for each user box to authentication of a user box

6.2. TOE Security Strength of Function

The TOE security functions having probabilistic/permutational mechanisms are as follows. The strength of each of the functions satisfies the SOF-Basic.

① <u>Administrator password authentication mechanism and HDD lock password verification mechanism</u> that F.ADMIN offers

② <u>Service code authentication mechanism</u> that A F.SERVICE offers

③ <u>Secure print password authentication mechanism</u> that B F.PRINT offers

④ <u>User Box password authentication mechanism</u> that F.BOX offers

6.3. Correspondence between TOE Security Functions and Function Requirements

The correspondence between TOE security function and TOE security function requirements shows in 8.3 Table 12. Table 12 shows that the TOE security function corresponds to at least one TOE security function requirement.

6.4. Assurance Measures

The following table shows the assurance measures to meet the component of the TOE security assurance requirements for EAL3 that are stipulated in Table 7.

Table 7 Correspondence between TOE Assurance Requirements and assurance measures

TOE Security Assurance Requirement		Component	Assurance Measures
Class ACM: Configuration management	CM capabilities	ACM_CAP.3	・Configuration management plan ・Configuration List ・CM record
	CM scope	ACM_SCP.1	
Class ADO:	Delivery	ADO_DEL.1	Delivery instructions

TOE Security Assurance Requirement		Component	Assurance Measures
Delivery and Operation	Installation, generation and start-up	ADO_IGS.1	・Service Manual bizhub 200 / 250 / 350 Service Manual [Security Function] 2006.09（Japanese）, bizhub 200 / 250 / 350 ineo 250 / 350 Service Manual [Security Function] 2006.09（English） ・Users Guide bizhub 200 / 250 / 350 Users Guide [Security Operations] 2006.09（Japanese）, bizhub 200 / 250 / 350 User's Guide [Security Operations] 2006.09(English), ineo 250 / 350 User's Guide [Security Operations] 2006.09（English）
Class ADV: Development	Functional specification	ADV_FSP.1	Security function specifications
	High-level design	ADV_HLD.2	Security high level design specifications
	Representation correspondence	ADV_RCR.1	Representation correspondence analysis report
Class AGD: Guidance Document	Administrator guidance	AGD_ADM.1	・Service Manual bizhub 200 / 250 / 350 Service Manual [Security Function] 2006.09（Japanese）, bizhub 200 / 250 / 350 ineo 250 / 350 Service Manual [Security Function] 2006.09（English） ・Users Guide bizhub 200 / 250 / 350 Users Guide [Security Operations] 2006.09（Japanese）, bizhub 200 / 250 / 350 User's Guide [Security Operations] 2006.09(English), ineo 250 / 350 User's Guide [Security Operations] 2006.09（English）
	User Guidance	AGD_USR.1	
Class ALC: Life Cycle Support	Development security	ALC_DVS.1	Development security instructions
Class ATE: Test	Coverage	ATE_COV.2	Coverage analysis report
	Depth	ATE_DPT.1	Depth analysis report
	Functional tests	ATE_FUN.1	Test specification and results report
	Independent testing	ATE_IND.2	MFP control software including TOE
Class AVA: Vulnerability Assessment	Misuse	AVA_MSU.1	※ no specific document （Reflected in the guidance documents）
	Strength of TOE security functions	AVA_SOF.1	Vulnerability analysis report
	Vulnerability analysis	AVA_VLA.1	

7. PP Claims

There is no conformance to a PP in this ST.

8. Rationale

8.1. Security Objectives Rationale

8.1.1. Necessity

The correspondence between the assumptions, threats and security objectives are shown in the following table. It shows that the security objectives correspond to at least one assumption or threat.

Table 8. Conformity of Security Objectives to assumptions and Threats

Assumption/Treat Security objectives	A.ADMIN	A.SERVICE	A.NETWORK	A.SECRET	A.SETTING	T.DISCARD-MFP	T.BRING-OUT-STORAGE	T.ACCESS-BOX	T.ACCESS-SECURE-PRINT	T.ACCESS-NET-SETTING	T.ACCESS-SETTING
O.BOX	▨	▨	▨	▨	▨			●			
O.SECURE-PRINT	▨	▨	▨	▨	▨				●		
O.CONFIG	▨	▨	▨	▨	▨					●	●
O.OVERWRITE-ALL	▨	▨	▨	▨	▨	●					
O.OVERWRITE-FILE	▨	▨	▨	▨	▨		●				
O.CHECK-HDD	▨	▨	▨	▨	▨		●				
OE.LOCK-HDD							●				
OE.FEED-BACK								●	●	●	●
OE-N.ADMIN	●										
OE-N.SERVICE		●									
OE-N.NETWORK			●								
OE-N.SECRET				●							
OE-N.SESSION									●	●	●
OE-N.SETTING-SECURITY					●						

8.1.2. Sufficiency of Assumptions

The security objectives for the assumptions are described as follows.

- **A.ADMIN（Personnel Conditions to be an Administrator）**

  This condition assumes that administrators are not malicious.

  With OE-N.ADMIN, the organization that uses the MFP assigns personnel who are reliable in the organization that uses the MFP, so the reliability of the administrator is realized.

- **A.SERVICE（Personnel Conditions to be a Service Engineer）**

This condition assumes that the service engineers are not malicious.
With OE-N.SERVICE, the organization that manages the maintenance of the MFP educates the service engineer. Also the service engineer needs to observe the maintenance of the MFP, so that the reliability of service engineers is assured.

- **A.NETWORK（Network Connection Conditions for the MFP）**
  This condition assumes that there are no wiretapping activities for the intra-office LAN and no access by an unspecified person from an external network.
  OE-N.NETWORK regulates the wiretapping prevention by the installation of devices such as a wiretapping detection device and device to perform the encryption communication on the intra-office LAN. It also regulates the unauthorized access prevention from external by the installation of devices such as firewall in order to block access to the MFP from the external networks, so that this condition is realized.

- **A.SECRET（Operating condition concerning confidential information）**
  This condition assumes each password using for the use of TOE should not be leaked by each user.
  OE-N.SECRET regulates that the administrator makes the user to execute the operation rule concerning the secure print password and the user box password, and that the administrator executes the operation rule concerning the administrator password and the HDD lock password. It also regulates that the service engineer executes the operation rule concerning the service code, so that this condition is realized.

- **A.SETTING（Enhanced Security Function Operational Settings Condition）**
  This condition assumes the enhanced security function operational settings condition is satisfied.
  OE-N.SETTING-SECURITY regulates that this is used after the administrator activates the enhanced security function, so that this condition is realized.

8.1.3. Sufficiency of Threats

The security objectives against threats are described as follows.

- **T.DISCARD-MFP（lease return and disposal of MFP）**
  This threat assumes the possibility of leaking information from the HDD in MFP collected from the user.
  O.OVERWRITE-ALL is that TOE offers the function to overwrite data for the deletion to all data area of HDD, so that the possibility of the threat is removed by executing this function before MFP is collected.
  Accordingly, this threat is countered sufficiently.

- **T.BRING-OUT-STORAGE（Unauthorised taking out of HDD）**
  This threat assumes the possibility that the image data in HDD leaks by being stolen from the operational environment under MFP used or by installing the unauthorised HDD and taking away with the data accumulated in it.
  O.OVERWRITE-FILE is that TOE overwrites the deletion data when the image file written in HDD becomes unnecessary, and so the data available of the minimum requirement exist on

HDD. Therefore, the threat is reduced greatly.

OE.LOCK-HDD, as a function of HDD, doesn't permit to read data from other than MFP with HDD that is installed in MFP and the possibility of the threat is removed.

In the above-mentioned, if HDD is replaced and a HDD which doesn't have the function that assumes this measure is installed, the significant risk which leaks the data accumulated in the replaced HDD by taking it out exists. For this, O.CHECK-HDD verifies the validity of HDD set up by TOE and so no data is written in HDD replaced secretly.

Therefore, the possibility of the threat is removed.

Accordingly, this threat is countered sufficiently.

- **T.ACCESS-BOX（Unauthorised access to user box using user function）**

This threat assumes the possibility that an unauthorised operation is done by using the user function to the user box which stores the image file.

The operation of the user box file in a user box is limited only for the authorized user by O.BOX, and so the possibility of the threat is removed.

OE.FEED-BACK regulates to return the protected feedback for the entered password in the authentication of the user box password, so that O.BOX is supported sufficiently.

Accordingly, this threat is countered sufficiently.

- **T.ACCESS-SECURE-PRINT（Unauthorised access to secure print file）**

This threat assumes the possibility that an unauthorised operation is done to the secure print. The operation of the secure print is limited only to the authorized user by O.SECURE-PRINT, so that the possibility of the threat is removed.

OE.FEED-BACK regulates to return the protected feedback for the entered password in the access authentication to the secure print, and OE-N.SESSION also requires the logoff after the operation ends, so that O.SECURE-PRINT is supported sufficiently.

Accordingly, this threat is countered sufficiently.

- **T.ACCESS-NET-SETTING（Unauthorised change in network setting）**

This threat assumes the possibility that the user who uses the TOE with belief uses the print function from PC to an unauthorised entity when the network setting relating to the MFP address is illegally changed. Especially, it becomes a problem if secure print file required hiding secretly against the other users in the office is transmitted to the unauthorised entity.

On the other hand, O.CONFIG regulates that the role to operate the network setting relating to the transmission of TOE is limited to the administrator, and so the possibility of this threat is removed.

OE.FEED-BACK regulates that the feedback protected is returned for the entered password by the administrator's authentication and OE-N.SESSION requires to logoff after the operation ends, so that O.CONFIG is supported sufficiently.

Accordingly, this threat is countered sufficiently.

T.ACCESS-SETTING（Unauthorised change of function setting condition related to security）

This threat assumes the possibility of developing consequentially into the leakage of the user box file and the secure print file by having been changed the specific function setting which relates to security.

O.CONFIG regulates that only the administrator is permitted to perform the setting of the enhanced security function that controls all setting function related to a series of security, and so the possibility of the threat is removed.

OE.FEED-BACK regulates that the feedback protected is returned for the entered password by the administrator's authentication, and OE-N.SESSION is also requested to logoff respectively after the operations of the administrator mode ends, so that O.CONFIG is supported sufficiently.

Accordingly, this threat is countered sufficiently.

8.1.4. Sufficiency of Organizational Security Policies

The organizational security policy is not applied.

8.2. IT Security Requirements Rationale

8.2.1. Rationale for IT Security Functional Requirements

8.2.1.1. Necessity

The correspondence between the security objectives and the IT security functional requirements are shown in the following table. It shows that the IT security functional requirements correspond to at least one security objective.

Table 9 Conformity of IT Security Functional Requirements to Security Objectives

Security Objective Security Functional Requirements	O.BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE-ALL	O.OVERWRITE-FILE	O.CHECK-HDD	OE.LOCK-HDD	OE.FEED-BACK	※ set.admin	※ set.service
set.admin	●	●	●							
set.service	●	●	●							
FDP_ACC.1[1]	●									
FDP_ACC.1[2]		●								
FDP_ACC.1[3]			●							
FDP_ACF.1[1]	●									
FDP_ACF.1[2]		●								
FDP_ACF.1[3]			●							
FDP_RIP.1					●					
FIA_AFL.1[1]										●
FIA_AFL.1[2]									●	
FIA_AFL.1[3]		●								
FIA_AFL.1[4]	●									
FIA_ATD.1	●	●								
FIA_SOS.1[1]									●	

Security Objective Security Functional Requirements	O.BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE-ALL	O.OVERWRITE-FILE	O.CHECK-HDD	OE.LOCK-HDD	OE.FEED-BACK	※ set.admin	※ set.service
FIA_SOS.1[2]	●	●					▨	▨		
FIA_SOS.1[3]			●				▨	▨		
FIA_SOS.1[4]							▨	▨		●
FIA_UAU.2[1]							▨	▨		●
FIA_UAU.2[2]							▨	▨	●	
FIA_UAU.2[3]		●					▨	▨		
FIA_UAU.2[4]	●						▨	▨		
FIA_UAU.6			●				▨	▨	●	●
FIA_UAU.7		●					▨	▨	●	●
FIA_UID.2[1]							▨	▨		●
FIA_UID.2[2]							▨	▨	●	
FIA_UID.2[3]		●					▨	▨		
FIA_UID.2[4]	●						▨	▨		
FIA_USB.1	●	●					▨	▨		
FMT_MOF.1			●				▨	▨		
FMT_MSA.3		●					▨	▨		
FMT_MTD.1[1]	●						▨	▨		
FMT_MTD.1[2]							▨	▨	●	
FMT_MTD.1[3]							▨	▨	●	
FMT_MTD.1[4]							▨	▨		●
FMT_SMF.1	●		●				▨	▨	●	●
FMT_SMR.1[1]							▨	▨	●	●
FMT_SMR.1[2]	●		●				▨	▨	●	
FMT_SMR.1[3]	●						▨	▨		
FPT_RVM.1	●	●	●			●	▨	▨		
FPT_SEP.1	●	●	●				▨	▨		
FNEW_RIP.1				●			▨	▨		
FIA_NEW.1						●	▨	▨		
FIA_AFL.1[E]	▨	▨	▨	▨	▨	▨	●			
FIA_UAU.2[E]	▨	▨	▨	▨	▨	▨	●			
FIA_UAU.7[E]	▨	▨	▨	▨	▨	▨		●		

Note) ***set.admin*** and ***set.service*** indicates the set of the requirements. And the security objectives assumed to have the correspondence and presented by "●" also correspond to a series of requirement set associated by ※set.admin and ※set.service shown in columns.

8.2.1.2. Sufficiency

The IT security functional requirements for the security objectives are described as follows.

- **O.BOX（User Box Access Control）**

This security objective limits the user box setting and the operation of the user box file in the user box to only the user permitted to use the user box, and needs various requirements that relate to the access control.

＜User box access control＞

It should be a user permitted to use the user box to operate the user box file in the user box. FIA_UID.2[4] and FIA_UAU.2 [4] identifies and authenticates that a user is the authorised user to use the user box.

When the authentication failure reaches three times, FIA_AFL.1[4] locks the authentication function to the user box. This lock status is released by the TOE rebooting or the administrator's release operation.

The user box ID is correlated with the task of substituting the use by FIA_ATD.[1] and FIA_USB.[1]. And FDP_ACC.1[1] and FDP_ACF.1[1] allows the download operation to the user box file that has corresponding object attribute to the user box ID of the subject attribute.

＜Management of user box＞

FMT_MTD.1[1] permits the change in the user box password only to the administrator and the authorized user to use the user box. FIA_SOS.1 2 verifies the quality of the user box password.

＜Roles and controlling function for each management＞

As the role of doing these managements, FMT_SMR.1[2] maintains an administrator and FMT_SMR.1[3] maintains a user permitted the use of the user box. FMT_SMF.1 specifies these management functions.

＜Necessary requirement to keep the administrator secure＞

⇒ refer to set.admin

＜Necessary requirement to keep the service engineer secure＞

⇒ refer to set.service

This security objective is satisfied by the completion of these multiple functional requirements.

- **O.SECURE-PRINT（Secure Print File Access Control）**

This security objective limits the print of the secure print file only for the user, who is permitted the use of the secure print file, and requires various requirements that relate to the access control.

＜Secure print file access control＞

In order to print the secure print file, it should be a user who is permitted the use of the secure print file, and FIA_UID.2[3] and FIA_UAU.2[3] identify and authenticate if a user is a permitted user to use the secure print file.

FIA_AFL.1[3] locks the authentication function to the user box when the authentication failure reaches three times. This lock is released by the administrator's release operation.

FIA_UAU.7 returns “*" for each entered character as feedback protected by the panel and supports the authentication.

The internal control ID of the secure print is correlated with the task of substituting the use by FIA_ATD.1 and FIA_USB.1. And FDP_ACC.1[2] and FDP_ACF.1[2] allow the print operation to the secure print file that has corresponding object attribute to the secure print internal control ID of the subject attribute.

＜Secure print password＞
FIA_SOS.1[2] verifies the quality of the secure print password.

＜Necessary requirement to keep the administrator secure＞
⇒ refer to set.admin

＜Necessary requirement to keep the service engineer secure＞
⇒ refer to set.service

This security objective is satisfied by the completion of these multiple functional requirements.

- **O.CONFIG（Access limitation to management function）**

This security objective limits the setting of network and the setting related for the enhanced security function, to the administrator, and requires various requirements for limiting the access to a series of the setting function and the management function.

＜Management of network setting＞
When the administrator attribute is associated with the task of substituting the use, FDP_ACC.1[3] and FDP_ACF.1[3] permits the task of substituting the user to operate the settings for the MFP address group object.

＜Operation limitation of Enhanced security function＞
FMT_MOF.1 permits only the administrator to disable the setting for the enhanced security function.

＜Management of HDD lock password＞
When the administrator attribute is correlated to the task of substituting the use, FDP_ACC.1[3] and FDP_ACF.1[3] permits the task of substituting the user to operate the setting for the HDD lock password object. FIA_SOS.1[3] verifies the quality of the HDD lock password. In order to change the HDD lock password, FIA_UAU.6 reauthenticates that a user is an administrator by collating with the registered HDD lock password. When the authentication is succeeded, the HDD lock password is allowed to be changed.

＜Role and management function for each management＞
FMT_SMR.1[2] maintains the role to do these management as a administrator. Also, FMT_SMF.1 specifies these management functions.

＜Necessary requirement to keep the administrator secure＞
⇒ refer to set.admin

＜Necessary requirement to keep the service engineer secure＞
⇒ refer to set.service

This security objective is satisfied by the completion of these multiple functional requirements.

- O.OVERWRITE-ALL（Complete overwrite deletion）

  This security objective regulates that it deletes all data areas of HDD and initializes the administrator password of NVRAM, and requires various requirements that relate to the deletion.

  FNEW_RIP.1 guarantees not to be able to use the content of any previous information of the targeted information by the deletion operation.

  This security objective is satisfied by the completion of these multiple functional requirements.

- O.OVERWRITE-FILE（Overwrite Deletion of each file）

  This security objective regulates that it deletes the image file written in HDD, which became unnecessary, and needs various requirements that relate to the deletion.

  FDP_RIP.1 guarantees not to be able to use the content of any previous information when targeted information (all user box files, swap data file, overlay image file, and HDD accumulation picture file) is released from the allocation of the resource.

  This security objective is satisfied by the completion of these multiple functional requirements.

- O.CHECK-HDD（Validity confirmation of HDD）

  This security objective regulates that it verifies the validity of HDD in order to confirm the unauthorised HDD doesn't exist, and needs various requirements that relate to the verification of an external entity from TOE.

  FIA_NEW.1 identifies HDD before the action from TOE to HDD, and cancels the scheduled action when the identification fails.

  This security objective is satisfied by the completion of this function requirement.

- OE.LOCK-HDD（Access control of HDD）

  This security objective regulates that it refuses the unauthorized access from MFP other than the one that is set by the HDD which is the entity of a necessary IT environment for the TOE security maintenance, and needs various requirements that verify that it is right MFP where TOE is installed.

  By FIA_UAU.2[E], HDD authenticates that the entity accessing to HDD is MFP, which HDD is installed.

  When the failure authentication reaches five times, FIA_AFL.1[E] refuses all the accesses to HDD concerning reading and writing data.

  This security objective is satisfied by the combination of these multiple functional requirements.

- OE.FEED-BACK（Feedback of password）

  This security objective regulates that the application (used by client PC for accessing to MFP) that is the entity of a necessary IT environment for the TOE security maintenance offers the appropriate protected feedback for the entered user box password and the entered administrator password.

By FIA_UAU.7[E], the application displays "*" for each character as feedback for entered character data.

This security objective is satisfied by the completion of this function requirement.

The following is the compilation of set such as ①the set of necessary requirement to keep administrator secure (set.admin), ②the set of necessary requirement to keep service engineer secure (set.service).

- ***set.admin*** **(Set of necessary requirement to keep administrator secure)**

  ＜Identification and Authentication of administrator＞

  FIA_UID.2[2] and FIA_UAU.2[2] identifies and authenticates that the accessing user is a administrator.

  FIA_UAU.7 returns "*" for each character entered as feedback protected in the panel, and supports the authentication.

  FIA_AFL.1[2] locks all the authentication functions to use the administrator password when the authentication failure reaches three times. This lock is released by rebooting TOE such as turning the power OFF and ON.

  ＜Management of administrator's authentication information＞

  FIA_SOS.1[1] verifies the quality of the administrator password. FMT_MTD.1[2] limits to the administrator the change in the administrator password. FIA_UAU.6 reauthenticates the administrator password when the administrator changes the administrator password. In this the re-authentication, FIA_AFL.1[2] cancels the administrator authenticated state when the authentication failure reaches three times, and locks all the authentication functions to use the administrator password. This lock state is released by rebooting TOE such as turning power OFF and ON.

  Also, the inquiry of administrator's password is limited to the service engineer by FMT_MTD.1[3].

  ＜Role and management function for each administration＞

  FMT_SMR.1[1] have service engineer maintain the role to do these management, and FMT_SMR.1[2] have the administrator do the same. Additionally, FMT_SMF.1 specifies these management functions.

- ***set.service*** **(Set of necessary requirement to keep service engineer secure)**

  ＜Identification and Authentication of the service engineer＞

  FIA_UID.2[1] and FIA_UAU.2[1] identifies and authenticates that the accessing user is a service engineer.

  FIA_UAU.7 returns "*" for each character entered as feedback protected in the panel, and supports the authentication.

  FIA_AFL.1[1] locks all the authentication functions to use the service code when the authentication failure reaches three times. This lock is released by rebooting TOE such as turning the power OFF and ON.

  ＜Management of service engineer's authentication information＞

  FIA_SOS.1[4] verifies the quality of the service code. FMT_MTD.1[4] limits to the service engineer the change in the service code. FIA_UAU.6 reauthenticates the service engineer. In this the re-authentication, FIA_AFL.1[1] cancels the service engineer authenticated state when the authentication failure reaches three times, and locks all the authentication functions to use the service code. This lock state is released by rebooting TOE such as turning power OFF and ON.

＜Role and management function for each administration＞
FMT_SMR.1[1] maintains the role to do these management as a service engineer. FMT_SMF.1 specifies these management functions.

FPT_RVM.1 and FPT_SEP.1 are the security function requirements immediately not related to the security objective, though it is not included in the explanation of the sufficiency of the above-mentioned. But, it is shown in the mutual support described later to support the security function requirement that is included in the explanation of the sufficiency of the above-mentioned. Because these two security function requirements will relate to the security objective that corresponds to the security function requirement supported respectively by two security function requirements, the relation with the security objective is consequentially clear.

8.2.1.3. Necessity of specified IT security function requirement

In this ST, FNEW_RIP.1 and FIA_NEW.1 is stated as an extended requirement. The necessity that presents these requirements and the validity of the assurance requirement applied in guaranteeing requirements is described as follows.

● Extended requirement: Necessity of FNEW_RIP.1
Regarding FNEW_RIP.1, FDP_RIP.1 is the closest requirement in the viewpoint of remaining information protection, but the requirement needs to regulate the protection of not only user data, but also the TSF data. And so, it is improper in the function requirement concerned that exists in the class of the user data protection, and it requires the extended requirement.

＜Validity of requirement identification structure＞
Because this requirement doesn't have the corresponding class in the data protection class of integration of no division of the TSF data and the user data, a new class named FNEW was set up, the same family name as the RIP family of the FDP class that indicates the remaining information protection, and clarifies the identification.

● Extended requirement: Necessity of FIA_NEW.1
Regarding FIA_NEW.1, FIA_UID.1 or FIA_UID.2 Is the closest requirement in the viewpoint of identification. But the verification act of HDD doesn't approve the act accessed from an external entity by TOE, but approval the act that TOE itself assigns to an external entity. It is improper in the function requirement concerned, and the extended requirement is necessary.

＜Validity of requirement identification structure＞
Because this requirement is one of the identification requirements, the family named NEW is set as a family added to the FIA class, and clarifies the identification.
As an activity that is predicted on management, FIA_UID requirement and similar management items are assumed. Also, an activity that is predicted on audit, FIA_UID

requirement and similar audit item are assumed.

8.2.1.4. Assurance validity of specified IT security function requirement

Two specified function requirements (FNEW_RIP.1, FIA_NEW.1) are not the greatly extended concept of the function requirement provided by CC part 2, and high contents of novelty. This is not the one to assume the necessity of presenting the TSP model specially or the possibility of a potential hiding channel in order to evaluate this function requirement accurately,

Therefore, it is possible to assure sufficiently the validity of the function that these functional requirements show by the set of the assurance requirement of EAL3, and a special assurance requirement and the assurance requirement required at EAL4 or higher are not required.

8.2.1.5. Dependencies of the IT Security Functional Requirements

The dependencies of the IT security functional requirements components are shown in the following table. When a dependency regulated in CC Part 2 is not satisfied, the reason is provided in the section for the “Dependencies Relation in this ST.”

Table 10　Dependencies of IT Security Functional Requirements Components

N/A：Not Applicable

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FDP_ACC.1[1]	FDP_ACF.1	FDP_ACF.1[1]
FDP_ACC.1[2]	FDP_ACF.1	FDP_ACF.1[2]
FDP_ACC.1[3]	FDP_ACF.1	FDP_ACF.1[3]
FDP_ACF.1[1]	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1[1], <Reason for not applying FMT_MSA.3> The user box file, the generated object, has no security attribute to be managed other than user box ID as the identifier, therefore, there is no necessity to regulate the event to provide the default value with any characteristics as an object attribute. User box ID that is related to the user box file, is a value specified by the user operation and doesn't correspond to the event assumed with FMT_MSA.3. (because the structure of limiting the selectable user box to the specified user at the time of generating the user box file is not necessary.)
FDP_ACF.1[2]	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1[2] FMT_MSA.3
FDP_ACF.1[3]	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1[3] <Reason for not applying FMT_MSA.3> This requirement is not necessary to be applied because the object attribute doesn't exist.
FDP_RIP.1	None	N/A
FIA_AFL.1[1]	FIA_UAU.1	FIA_UAU.2[1]

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FIA_AFL.1[2]	FIA_UAU.1	FIA_UAU.2[2]
FIA_AFL.1[3]	FIA_UAU.1	FIA_UAU.2[3]
FIA_AFL.1[4]	FIA_UAU.1	FIA_UAU.2[4]
FIA_ATD.1	None	N/A
FIA_SOS.1[1]	None	N/A
FIA_SOS.1[2]	None	N/A
FIA_SOS.1[3]	None	N/A
FIA_SOS.1[4]	None	N/A
FIA_UAU.2[1]	FIA_UID.1	FIA_UID.2[1]
FIA_UAU.2[2]	FIA_UID.1	FIA_UID.2[2]
FIA_UAU.2[3]	FIA_UID.1	FIA_UID.2[3]
FIA_UAU.2[4]	FIA_UID.1	FIA_UID.2[4]
FIA_UAU.6	None	N/A
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3]
FIA_UID.2[1]	None	N/A
FIA_UID.2[2]	None	N/A
FIA_UID.2[3]	None	N/A
FIA_UID.2[4]	None	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Both do not apply. ＜Reason for not applying FMT_MSA.1＞ This is the internal control ID that is identified uniquely, and this does not require the management such as change or deletion, after this is assigned once. ＜FMT_SMR.1＞ The assignment of FMT_MSA.3.2 is not applicable. FMT_SMR.1 is the dependency that is set relating to the following and so there is no necessity of application.
FMT_MTD.1[1]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2], FMT_SMR.1[3]
FMT_MTD.1[2]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2]
FMT_MTD.1[3]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[1]
FMT_MTD.1[4]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[1]
FMT_SMF.1	None	N/A
FMT_SMR.1[1]	FIA_UID.1	FIA_UID.2[1]
FMT_SMR.1[2]	FIA_UID.1	FIA_UID.2[2]
FMT_SMR.1[3]	FIA_UID.1	FIA_UID.2[4]
FPT_RVM.1	None	N/A
FPT_SEP.1	None	N/A
FNEW_RIP.1	None	N/A
FIA_NEW.1	None	N/A

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FIA_AFL.1[E]	FIA_UAU.1	FIA_UAU.2[E]
FIA_UAU.2[E]	FIA_UID.1	N/A ＜Reason for not applying FIA_UID.1＞ This regulates the access to HDD that is set up in MFP. There are no multiple access routes because the access to HDD is the one performed through a general IDE interface. Authentication information corresponding to the user needed when multiple users' access is unnecessary in this process, and there is no necessity of the identification of the accessed entity.
FIA_UAU.7[E]	FIA_UAU.1	FIA_UAU.2[2], FIA_UAU.2[4]

8.2.1.6. Mutual Support Correlations of IT Security Functional Requirements

The IT security functional requirements to operate effectively the other security functional requirements which are not specified in the analysis of the dependencies relation of the functional requirement are shown in the table below.

Table 11 Mutual Support Correlations of IT Security Functional Requirements

N/A：Not Applicable

IT Security Functional Requirement	Functional requirement component that operates other security functional requirements validly			
	①Bypass Prevention	②Interference/ Destruction Prevention	③Deactivation Prevention	④Disabling Detection
FDP_ACC.1[1]	N/A	N/A	N/A	N/A
FDP_ACC.1[2]	N/A	N/A	FMT_MOF.1	N/A
FDP_ACC.1[3]	N/A	N/A	N/A	N/A
FDP_ACF.1[1]	FIA_UAU.2[4]	FPT_SEP.1	N/A	N/A
FDP_ACF.1[2]	FIA_UAU.2[3]	FPT_SEP.1	FMT_MOF.1	N/A
FDP_ACF.1[3]	FIA_UAU.2[2]	FPT_SEP.1	N/A	N/A
FDP_RIP.1	N/A	N/A	FMT_MOF.1	N/A
FIA_AFL.1[1]	N/A	N/A	FMT_MOF.1	N/A
FIA_AFL.1[2]	N/A	N/A	FMT_MOF.1	N/A
FIA_AFL.1[3]	N/A	N/A	FMT_MOF.1	N/A
FIA_AFL.1[4]	N/A	N/A	FMT_MOF.1	N/A
FIA_ATD.1	N/A	N/A	FMT_MOF.1	N/A
FIA_SOS.1[1]	N/A	N/A	FMT_MOF.1	N/A
FIA_SOS.1[2]	N/A	N/A	FMT_MOF.1	N/A
FIA_SOS.1[3]	N/A	N/A	FMT_MOF.1	N/A
FIA_SOS.1[4]	N/A	N/A	FMT_MOF.1	N/A
FIA_UAU.2[1]	FPT_RVM.1	FMT_MTD.1[4]	N/A	N/A
FIA_UAU.2[2]	FPT_RVM.1	FMT_MTD.1[2]	N/A	N/A

IT Security Functional Requirement	Functional requirement component that operates other security functional requirements validly			
	①Bypass Prevention	②Interference/ Destruction Prevention	③Deactivation Prevention	④Disabling Detection
		FMT_MTD.1[3]		
FIA_UAU.2[3]	FPT_RVM.1	N/A	FMT_MOF.1	N/A
FIA_UAU.2[4]	FPT_RVM.1	FMT_MTD.1[1]	FMT_MOF.1	N/A
FIA_UAU.6	N/A	N/A	N/A	N/A
FIA_UAU.7	N/A	N/A	N/A	N/A
FIA_UID.2[1]	N/A	N/A	N/A	N/A
FIA_UID.2[2]	N/A	N/A	N/A	N/A
FIA_UID.2[3]	N/A	N/A	FMT_MOF.1	N/A
FIA_UID.2[4]	N/A	N/A	FMT_MOF.1	N/A
FIA_USB.1	N/A	N/A	FMT_MOF.1	N/A
FMT_MOF.1	N/A	N/A	N/A	N/A
FMT_MSA.3	N/A	N/A	N/A	N/A
FMT_MTD.1[1]	N/A	N/A	N/A	N/A
FMT_MTD.1[2]	N/A	N/A	N/A	N/A
FMT_MTD.1[3]	N/A	N/A	N/A	N/A
FMT_MTD.1[4]	N/A	N/A	N/A	N/A
FMT_SMF.1	N/A	N/A	N/A	N/A
FMT_SMR.1[1]	N/A	N/A	N/A	N/A
FMT_SMR.1[2]	N/A	N/A	N/A	N/A
FMT_SMR.1[3]	N/A	N/A	N/A	N/A
FPT_RVM.1	N/A	N/A	N/A	N/A
FPT_SEP.1	N/A	N/A	N/A	N/A
FIA_NEW.1	FPT_RVM.1	N/A	FMT_MOF.1	N/A
FNEW_RIP.1	N/A	N/A	N/A	N/A
FIA_AFL.1[E]	N/A	N/A	N/A	N/A
FIA_UAU.2[E]	N/A	N/A	N/A	N/A
FIA_UAU.7[E]	N/A	N/A	N/A	N/A

① Bypass Prevention

＜By-pass prevention of functional requirement that relates to service engineer＞
FIA_UAU.2[1] that regulates the service engineer's authentication is called by FPT_RVM.1 without fail, so that the by-pass prevention is supported.

＜By-pass prevention of functional requirement that relates to administrator＞
As for FDP_ACF.1[3] that regulates the administrator mode access control, the by-pass prevention is supported by FIA_UAU.2[2] that regulates the administrator's identification and authentication.
In addition, because FIA_UAU.2[2] is called by FPT_RVM.1 without fail, the by-pass prevention is supported.

＜By-pass prevention of functional requirement that relates to user box＞
As for FDP_ACF.1[1] that regulates the user box access control, the by-pass prevention is supported by FIA_UAU.2[4] that regulates the authentication of the authorized user to use

the user box.
In addition, FIA_UAU.2[4] that regulates the authentication of the authorized user to use the user box is called by FPT_RVM.1 without fail, so that the by-pass prevention is supported.

＜By-pass prevention of functional requirement that relates to secure print＞
As for FDP_ACF.1[2] that regulates the secure print file access control, the by-pass prevention is supported by FIA_UAU.2[3] that authenticates the authorized user to use the secure print file.
In addition, FIA_UAU.2[3] that regulates the authentication of the authorised user to use the secure print file is called by FPT_RVM.1 without fail, so that the by-pass prevention is supported.

＜By-pass prevention of validity verification of HDD＞
FIA_NEW.1 that verifies the validity of HDD is called by FPT_RVM.1 without fail, so that the by-pass prevention is supported.

② Interference and Destruction Prevention
＜Maintenance of user box access control＞
By FPT_SEP.1, only the authorized user to use the user box that is authenticated to be assumed by the user box access control can operate the user box file, so that the prevention of interference and destruction by other unauthorised subject is supported as for FDP_ACF.1[1].

＜Maintenance of secure print file access control＞
By FPT_SEP.1, only the authorized user to use the secure print file that is authenticated to be assumed by the secure print file access control can operate the secure print file, so that the prevention of interference and destruction by other unauthorised subject is supported as for FDP_ACF.1[2].

＜Maintenance of administrator mode access control＞
By FPT_SEP.1, only subject that substitutes the administrator authenticated to be assumed by the administrator mode access control can operate the object regulated by the administrator mode access control, so that the prevention of unauthorized interference and destruction by other unauthorised subject is supported as for FDP_ACF.1[3].

＜Management of service code＞
The modification operation of the service code has been permitted only to the service engineer by FMT_MTD.1[4]. This supports the prevention of unauthorised interference and destruction of FIA_UAU.2[1].

＜Management of administrator password＞
The modification operation of the administrator password is limited to the administrator by FMT_MTD.1[2]. The inquiry operation has been permitted only to the service engineer by FMT_MTD.1[3]. This supports the prevention of unauthorised interference and destruction of FIA_UAU.2 [2].

＜Management of user box password＞

The modification operation of the user box password has been permitted only to the user and the administrator, who are permitted the use of the user box by FMT_MTD.1[1]. This supports the prevention of unauthorised interference and destruction of FIA_UAU.2[4].

③ Deactivation Prevention

＜Maintenance of enhanced security function＞

The operation setting of the enhanced security function has been permitted only to the administrator by FMT_MOF.1. The enhanced security function is a function to make it compel for the execution of security function of TOE, such as Password rule function (FIA_SOS.1[1], FIA_SOS.1[2], FIA_SOS.1[3], FIA_SOS.1[4]), Authentication method of secure print (FIA_UAU.2[3], FIA_UID.2[3], FDP_ACC.1[2], FDP_ACF.1[2], FIA_ATD.1, FIA_USB.1), Identification and authentication in user box access (FIA_UAU.2[4], FIA_UID.2[4]), Authentication operation prohibition function(FIA_AFL.1[1], FIA_AFL.1[2], FIA_AFL.1[3], FIA_AFL.1[4]), Remaining information overwrite deletion function (FDP_RIP.1), so that the deactivation prevention is supported.

④ Disabling Detection

The requirement that supports the disabling detection doesn't exist.[6]

8.2.2. Rationale for Minimum Strength of Function

The MFP that is loaded with this TOE is connected to an intra-office LAN with appropriately controlled connections with external networks. Therefore, there is no possibility that it is directly attacked by unspecified people via the Internet. As long as it has a strength level that can counter the threat by users who are users of the TOE and a person who can enter the office and not user of the TOE as an agent, it is acceptable, as explicitly described in section 3.3. Therefore, this TOE regulates security objectives by assuming an unskilled attacker and thus, the selection of the SOF-Basic as the minimum strength of function is reasonable.

8.2.3. Rationale for IT Security Assurance Requirements

This TOE is installed and used in an environment where adequate security is maintained in terms of the physical, personnel, and connectivity. Nonetheless, adequate effectiveness in the environment where the TOE is used must be assured. As a general commercial office product, the execution of tests based on function specifications and high level design, and analysis of the strength of function and a search for vulnerabilities are required. In addition, it is desirable that it has a development environment control, a configuration management for the TOE and a secure distribution procedure. And therefore the selection of EAL3, which provides an adequate assurance level is reasonable.

The assurance requirement dependency analysis is assumed to be appropriate because the package EAL has been selected, therefore details are not discussed.

[6] Though this is not shown in the mutual support analysis, the FIA_AFL.1 requirement supports respectively against the attack that aims at the disabling of each authentication function. This is sufficient to maintain the security objective of this TOE. (This content is specified by the dependency analysis.)

8.2.3.1. Consistency rationale for the set of IT security functional requirement

The followings show the rationale in which the IT security requirement with a possibility to compete does not exist.

＜IT security functional requirement＞

- Though several access control policies are set up by repeating the access control requirement (FDP_ACC.1 etc.), it regulates the access control related to the followings, such as ①user box ②secure print ③HDD lock password and the MFP address. These do not cover each other the same controlled object by several policies, and so they do not compete each other.
- FDP_RIP.1 regulating the deletion of protective assets applies FNEW_RIP.1 as an extended requirement, but the threat concerning the possibility of an unauthorised deletion is not targeted in this case because of the concept of emphasis on confidentiality. Therefore, the requirement for the competing data deletion protection has not been selected at all.
- The structure, that a competition possibility is suggested, doesn't exist from the relations between requirements by dependency, correlation by mutual support, and the various analysis of validity of security functional requirement to TOE security objectives.

＜IT security assurance requirement＞

- EAL being the assurance package is used. That is, regardless of this ST, the possibility of that the security assurance requirement competes, is confirmed the nonexistence.

8.3. Rationale for TOE Summary Specifications

8.3.1. Rationale for the TOE Security Functions

8.3.1.1. Necessity

The conformity of the TOE security functions and the TOE security functional requirements are shown in the following table. It shows that the TOE security functions correspond to at least one TOE security functional requirement.

Table12 Conformity of TOE Security Functions to TOE Security Functional Requirements

TOE Security Function TOE Security Functional Requirement	F.ADMIN	F.SERVICE	F.BOX	F.PRINT	F.OVERWRITE-FILE	F.OVERWRITE-ALL	F.HDD	F.RESET
FDP_ACC.1[1]			●					
FDP_ACC.1[2]				●				
FDP_ACC.1[3]	●							
FDP_ACF.1[1]			●					
FDP_ACF.1[2]				●				
FDP_ACF.1[3]	●							
FDP_RIP.1					●			
FIA_AFL.1[1]		●						●
FIA_AFL.1[2]	●							●
FIA_AFL.1[3]	●			●				
FIA_AFL.1[4]	●		●					●
FIA_ATD.1			●	●				
FIA_SOS.1[1]	●							
FIA_SOS.1[2]	●		●	●				
FIA_SOS.1[3]	●							
FIA_SOS.1[4]		●						
FIA_UAU.2[1]		●						
FIA_UAU.2[2]	●							
FIA_UAU.2[3]				●				
FIA_UAU.2[4]			●					
FIA_UAU.6	●	●						
FIA_UAU.7	●	●		●				
FIA_UID.2[1]		●						
FIA_UID.2[2]	●							
FIA_UID.2[3]				●				
FIA_UID.2[4]			●					
FIA_USB.1			●	●				
FMT_MOF.1	●							

TOE Security Function TOE Security Functional Requirement	F.ADMIN	F.SERVICE	F.BOX	F.PRINT	F.OVERWRITE-FILE	F.OVERWRITE-ALL	F.HDD	F.RESET
FMT_MSA.3				●				
FMT_MTD.1[1]	●		●					
FMT_MTD.1[2]	●							
FMT_MTD.1[3]		●						
FMT_MTD.1[4]		●						
FMT_SMF.1	●	●	●					
FMT_SMR.1[1]		●						
FMT_SMR.1[2]	●							
FMT_SMR.1[3]			●					
FPT_RVM.1	●	●	●	●			●	
FPT_SEP.1	●	●	●	●				
FNEW_RIP.1						●		
FIA_NEW.1							●	

8.3.1.2. Sufficiency

The TOE security functions for the TOE security functional requirements are described.

- **FDP_ACC.1[1]**

  FDP_ACC.1[1] regulates the relationship between the controlled subject to the object: user box and user box file and the operation.
  F.BOX performs the user box access control for the task of substituting the user to download a user box file.
  Accordingly, this functional requirement is satisfied.

- **FDP_ACC.1[2]**

  FDP_ACC.1[2] regulates the relationship between the controlled subject to the object: secure print file and the operation.
  F.PRINT performs the secure print file control for the task of substituting the user to print secure print file.
  Accordingly, this functional requirement is satisfied.

- **FDP_ACC.1[3]**

  FDP_ACC.1[3] regulates the relationship between the controlled subject to the object: HDD lock password object and MFP address group object and the operation.
  F.ADMIN performs the administrator mode access control for the task of substituting the user to set the HDD lock password object and the MFP address group object.
  Accordingly, this functional requirement is satisfied.

- **FDP_ACF.1[1]**

FDP_ACF.1[1] regulates the regulation of relationship between the controlled subject to the object: user box and the user box file and the operation.

F.BOX performs the user box access control to which the following rules are applied.

➢ The download operation of the user box file in the selected public user box is permitted to the authorized user who can use the user box.

Accordingly, this functional requirement is satisfied.

- **FDP_ACF.1[2]**

FDP_ACF.1[2] regulates the regulation of the relationship between the controlled subject to the object: secure print file and the operation..

F.PRINT performs the secure print file access control to which the following rules are applied.

➢ The print operation of the selected secure print file is permitted to the authorized user who can use the secure print file.

Accordingly, this functional requirement is satisfied.

- **FDP_ACF.1[3]**

FDP_ACF.1[3] regulates the regulation of the relationship between the controlled subject to the object: HDD lock password object and MFP address group object and the operation.

F.ADMIN performs the administrator mode access control to which the following rules are applied.

➢ The setting operation of the HDD lock password object and the MFP address group object is permitted to the administrator.

Accordingly, this functional requirement is satisfied.

- **FDP_RIP.1**

FDP_RIP.1 regulates the protection of files that are released the assignment from HDD, such as all user box files, swap data files, overlay image files and HDD accumulation image files.

F.OVERWRITE-FILE performs the process of overwriting operation based on the deletion method, when the job is ended or the deletion operation is performed, to all user box files, the swap data files, the overlay image files, and the HDD accumulation image files.

Accordingly, this functional requirement is satisfied.

- **FIA_AFL.1[1]**

FIA_AFL.1[1] regulates the action of the authentication failure to the service engineer authentication. In the service engineer authentication for accessing the service mode or changing the service code, when the authentication failure of three times is detected, F.SERVICE logs off from the authentication status to the service mode and locks the authentication function, if it's under authentication.

If it's not under authentication, it locks the authentication function.

F.RESET releases the lock status by the reboot of TOE by the power supply OFF/ON that clears the times of failure in each authentication function.

Accordingly, this functional requirement is satisfied.

- **FIA_AFL.1[2]**

FIA_AFL.1[2] regulates the action of authentication failure to the administrator authentication. In the administrator authentication for accessing the administrator mode or changing the administrator password, when the authentication failure of three times is detected, F.ADMIN logs off from the authentication status to the administrator mode and locks the authentication function, if it's under authentication.

If it's not under authentication, it locks the authentication function.

F.RESET releases the lock status by the reboot of TOE by the power supply OFF/ON that clears the times of failure in each authentication function.

Accordingly, this functional requirement is satisfied.

- **FIA_AFL.1[3]**

FIA_AFL.1[3] regulates the action of the authentication failure to the authentication of that the user is an authorized user who can use the secure print file.

In the authentication of that the user is an authorized user who can use the secure print file, when the authentication failure of three times is detected, F.PRINT refuses the access to the secure print file and locks the authentication function.

F.ADMIN releases this lock status by the lock release function offered in the administrator mode.

Accordingly, this functional requirement is satisfied.

- **FIA_AFL.1[4]**

FIA_AFL.1[4] regulates the action of the authentication failure to the authentication of that the user is an authorized user who can use the user box.

In the authentication for accessing the user box or changing password of user box, when the authentication failure of three times is detected, F.BOX refuses the access to the concerned user box and locks the authentication function.

F.RESET releases the lock status by the reboot of TOE by the power supply OFF/ON that clears the times of failure in each authentication function.

Also, F.ADMIN releases this lock status by the lock release function offered in the administrator mode.

Accordingly, this functional requirement is satisfied.

- **FIA_ATD.1**

FIA_ATD.1 regulates the security attribute related by the user.

F.BOX assigns user box ID to the task of substituting the user.

F.PRINT assigns the internal control ID of the secure print to the task of substituting the user.

Accordingly, this functional requirement is satisfied.

- **FIA_SOS.1[1]**

FIA_SOS.1[1] regulates the quality of the administrator password.

F.ADMIN verifies the quality of the administrator password that is not composed of the same character of the eight digits by numbers.

Accordingly, this functional requirement is satisfied.

- **FIA_SOS.1[2]**

FIA_SOS.1[2] regulates the quality of the secure print password and the user box password.

F.ADMIN verifies the quality of the user box password that is not composed of the same characters by the eight digits ASCII code with a total of 92 characters (0x20-0x7E, except 0x22, 0x2B, and 0x5E).

F.BOX verifies the quality of the user box password that is not composed of the same characters by the eight digits ASCII code with a total of 92 characters (0x20-0x7E except0x22, 0x2B, and 0x5E).

F.PRINT verifies the quality of the secure print password that is not composed of the same characters by the eight digits ASCII code with a total of 92 characters (0x20-0x7E except, 0x22, 0x2B, and 0x5E) .

Accordingly, this functional requirement is satisfied.

- **FIA_SOS.1[3]**

FIA_SOS.1[3] regulates the quality of the HDD lock password.

F.ADMIN verifies the quality of the HDD lock password that is not composed of the same characters by the 20 digits ASCII code with a total of 82 characters (0x20-0x7E except, 0x20, 0x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3C, 0x3E, 0x5B, 0x5C, 0x5D, and 0x5E).

Accordingly, this functional requirement is satisfied.

- **FIA_SOS.1[4]**

FIA_SOS.1[4] regulates the quality of the service code.

F.SERVICE verifies the quality of the service code that is not composed of the same characters by the eight digits numbers, #, and *.

Accordingly, this functional requirement is satisfied.

- **FIA_UAU.2[1]**

FIA_UAU.2[1] regulates the service engineer's authentication.

F.SERVICE authenticates that the user who accesses the service mode by using the service code is the service engineer.

Accordingly, this functional requirement is satisfied.

- **FIA_UAU.2[2]**

FIA_UAU.2[2] regulates the administrator's authentication.

F.ADMIN authenticates the user who accesses the administrator mode by using the administrator password is the administrator.

Accordingly, this functional requirement is satisfied.

- **FIA_UAU.2[3]**

FIA_UAU.2[3] regulates the authentication of the authorized user who can use the secure print file.

F.PRINT authenticates that a user is the authorized user who can use the secure print file by using the secure print password that is set to each file.

Accordingly, this functional requirement is satisfied.

- **FIA_UAU.2[4]**

FIA_UAU.2[4] regulates the authentication of the authorized user who can use the user box.

F.BOX authenticates that a user is the authorized user who can use the user box by using the user box password that is set to each user box.

Accordingly, this functional requirement is satisfied.

- **FIA_UAU.6**

  FIA_UAU.6 regulates the re-authentication at an important operation such as changing the password.

  F.ADMIN reauthenticates the administrator at the operation for the change of the administrator password. Along with the change operation of the HDD lock password, by collating the registered HDD lock password, it reauthenticates the administrator who has known each of confidential information.

  F.SERVICE reauthenticates the service engineer at the operation of the change of the service code.

  Accordingly, this functional requirement is satisfied.

- **FIA_UAU.7**

  FIA_UAU.7 regulates the return of “*" as the feedback under the authentication.

  F.ADMIN returns “*" for each character as the feedback for entered administrator password from the panel in the authentication and re-authentication of administrator, and prevents a direct display of the administrator password.

  F.SERVICE returns “*" for each character as the feedback for the entered service code from the panel in the authentication and re-authentication of the service engineer, and prevents a direct display of the service code.

  F.PRINT returns “*" for each character as the feedback for the entered secure print password from the panel in the authentication of the authorized user who can use the secure print file, and prevents the direct display of the secure print password.

  Accordingly, this functional requirement is satisfied.

- **FIA_UID.2[1]**

  FIA_UID.2[1] regulates the service engineer's identification.

  F.SERVICE identifies that the user who accesses the service mode is a service engineer.

  Accordingly, this functional requirement is satisfied.

- **FIA_UID.2[2]**

  FIA_UID.2[1] regulates the administrator's identification.

  F.SERVICE identifies the user who accesses the administrator mode is an administrator.

  Accordingly, this functional requirement is satisfied.

- **FIA_UID.2[3]**

  FIA_UID.2[3] regulates the identification of the user who is permitted the use of the secure print file.

  F.PRINT identifies a user who is permitted the use of the secure print file by selecting the secure print file as an operation target.

  Accordingly, this functional requirement is satisfied.

- **FIA_UID.2[4]**

  FIA_UID.2[4] regulates the identification of the user who is permitted the use of the user box.

  F.BOX identifies a user who is permitted the use of the user box by selecting the user box as an operation target.

  Accordingly, this functional requirement is satisfied.

- **FIA_USB.1**

  FIA_USB.1 regulates the security attribute association to subject that substitutes the user.
  F.PRINT associates the "secure pint internal control ID" to the task of substituting the user.
  F.BOX associates the "User Box ID" to the task of substituting the user.
  Accordingly, this functional requirement is satisfied.

- **FMT_MOF.1**

  FMT_MOF.1 regulates the behavior management of the enhanced security function.
  F.ADMIN provides the settings of the enhanced security function in the administrator mode and manages the stop operation of the concerned function. Although the execution of the "all data area overwrite deletion function" invalidates the enhanced security setting, F.ADMIN permits this operation only to the administrator.
  Accordingly, this functional requirement is satisfied.

- **FMT_MSA.3**

  FMT_MSA.3 regulates the secure print internal control ID that is set at the time of registration of secure print file.
  F_PRINT grants the secure print internal control ID that is identified uniquely to the concerned secure print file at the time of registration of secure print file
  Accordingly, this functional requirement is satisfied.

- **FMT_MTD.1[1]**

  FMT_MTD.1[1] regulates the management of the user box password.
  F.ADMIN permits the change operation of the user box password that is set to the user box in the administrator mode.
  F.BOX permits the change operation of the user box password of the concerned user box to the authorized user who can use the user box.
  Accordingly, this functional requirement is satisfied.

- **FMT_MTD.1[2]**

  FMT_MTD.1[2] regulates the management of the administrator password.
  F.ADMIN permits the change operation of the administrator password in the administrator mode.
  Accordingly, this functional requirement is satisfied.

- **FMT_MTD.1[3]**

  FMT_MTD.1[3] regulates the management of the administrator password.
  F.SERVICE permits the function to transmit the administrator password through the fax unit or with E-mail in the service mode. (Correspond to the inquiry of the administrator password).
  Accordingly, this functional requirement is satisfied.

- **FMT_MTD.1[4]**

  FMT_MTD.1[4] regulates the management of the service code.
  F.SERVICE permits the change operation of the service code in the service mode.
  Accordingly, this functional requirement is satisfied.

- **FMT_SMF.1**

  FMT_SMF.1 specifies the security management function.

  F.ADMIN provides the following security management functions.

  - ➢ Function to stop the enhanced security function
  - ➢ Function to change the administrator password
  - ➢ Function to change the user box password
  - ➢ Lock release function

    Providing to the following authentication functions.

    •Authentication function in the access to a user box

    •Authentication function in the access to secure print

  F.SERVICE provides the following security management functions.

  - ➢ Function to change the service code
  - ➢ Function to inquiry administrator password

  F.BOX provides the following security management functions.

  - ➢ Function to change user box password

  Accordingly, this functional requirement is satisfied.

- **FMT_SMR.1[1]**

  FMT_SMR.1[1] regulates the role as the service engineer.

  F.SERVICE recognizes the user who is authenticated by the service code as a service engineer.

  Accordingly, this functional requirement is satisfied.

- **FMT_SMR.1[2]**

  FMT_SMR.1[2] regulates the role as the administrator.

  F.ADMIN recognizes the user who is authenticated by the administrator password as an administrator.

  Accordingly, this functional requirement is satisfied.

- **FMT_SMR.1[3]**

  FMT_SMR.1[3] regulates the role as the authorized user who can use the user box.

  F.BOX recognizes the user who is authenticated by the user box password as the authorized user who can use the user box.

  Accordingly, this functional requirement is satisfied.

- **FPT_RVM.1**

  FPT_RVM.1 regulates support so that the TSP enforcement functions are always invoked before each security function within the TOE is allowed to proceed.

  F.ADMIN definitely activates "Administrator authentication function" of which performance is indispensable, before the use of various functions that can be performed only by administrator is permitted.

  F.SERVICE definitely activates "Service engineer authentication function" of which performance is indispensable, before the use of various functions that can be performed only by the service engineer is permitted.

  F.BOX definitely activates "Authentication function by the user box password" of which performance is indispensable, before the use of various functions that can be performed only by the authorized user who can use the user box is permitted.

F.PRINT definitely activates "Authentication function by the secure print password" of which performance is indispensable, before the use of various functions that can be performed only by the authorized user who can use the secure print is permitted.

F.HDD definitely activates "Validity verification function of HDD" of which performance is indispensable, before writing HDD is permitted when HDD lock function is activated.

Accordingly, this functional requirement is satisfied.

- **FPT_SEP.1**

FPT_SEP.1 regulates maintaining of security domains for protecting against interference and tampering by subjects who cannot be trusted and regulates separating of security domains of subjects.

F.ADMIN maintains the administrator authentication domain that is provided various functions permitted to operate only by administrator, and it does not permit the interference by the unauthorized subjects.

F.BOX maintains the user box authentication domain that is provided various functions permitted to operate only by the authorized user who can use the user box by the authentication of the user box password, and it doesn't allow the interference by the unauthorized subject.

F.PRINT maintains the secure print file authentication domain that is provided various functions permitted to operate only by a user who is permitted to use the secure print file by the authentication of the secure print password, and it doesn't allow the interference by the unauthorized subject.

F.SERVICE maintains the service engineer authentication domain that is provided various functions permitted to operate only by the service engineer, and it doesn't allow the interference by the unauthorized subject

- **FNEW_RIP.1**

FNEW_RIP.1 regulates that the object and the TSF data, that are targeted in the explicit deletion operation can not be restored.

F.OVERWRITE-ALL deletes all user box files, the swap data files, the overlay image files, the HDD accumulation image files and the user box password by performing the overwrite deletion to all data areas of HDD. It also initializes the administrator password of NVRAM, and deletes the transmission address data file and the HDD lock password.

Accordingly, this functional requirement is satisfied.

- **FIA_NEW.1**

FIA_NEW.1 regulates the user's identification before the action to the user from TSF.

F.HDD provides the function to check the HDD status if HDD lock password is set, and if the HDD lock password is not set, it doesn't perform the process of writing and reading to HDD. Only when it is confirmed that the HDD lock password is certainly set in HDD, it permits the reading and the writing to HDD.

Accordingly, this functional requirement is satisfied.

8.3.2. Rationale for TOE Security Strength of Function

The TOE security functions having a probabilistic / permutational mechanism are as follows.

① Administrator password authentication mechanism offered by F.ADMIN
② Service code authentication mechanism offered by F.SERVICE
③ Secure print password authentication mechanism offered by F.PRINT
④ User box password authentication mechanism offered by F.BOX
⑤ HDD lock password collation mechanism offered by F.ADMIN

It used the secret composed from ①an 8-digit and 10kinds of character, ②an 8-digit and 12 kinds of character, ③&④an 8-digit and 92 kinds of character, and ⑤20-digit and 82 kinds of character. Among these, ①～④ locks the authentication function by the continuous three times of authentication failure by operating the authentication operation prohibition function.

Accordingly, as claimed in Section 6.2, the strength of function of mechanisms adequately satisfies the SOF-Basic, and it is consistent with the minimum strength of function: SOF-Basic that is claimed for the TOE security functional requirement for the security strength of function, stipulated in item 5.1.2.

8.3.3. Mutually Supported TOE Security Functions

The TOE security functional requirements that are satisfied by a combination of IT security functions that are identifies in the TOE summary specifications, are as shown in the text regarding the rationale in the section of 8.3.1.

8.3.4. Rationale for Assurance Measures

The required document for the evaluation assurance level EAL3 is covered by the reference document shown in the assurance measures described in Section 6.4. The TOE security assurance requirements are satisfied through development, test condition, vulnerability analysis, the development environment control, configuration management, life cycle management, and delivery procedures in accordance with the document provided as the assurance measures, as well as the preparation of a proper guidance document.

8.4. PP claims rationale

There is no PP that is referenced by this ST.