Multi functional printer
(digital copier)
bizhub PRO C5500/ineo+5500 Series
Security Target
Version 2

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

August 10, 2007
Konica Minolta Business Technologies, Inc.

Revision History

Version	Description	Approved by	Checked by	Created by
1	Initial Version	June 25, 2007 Tetsuya Niitsuma	June 25, 2007 Kazuo Yasuda	June 25, 2007 Tomoo Kudoh
2	Correction made on requests.	Aug 10, 2007 Tetsuya Niitsuma	Aug 10, 2007 Kazuo Yasuda	Aug 10, 2007 Tomoo Kudoh

Table of Contents

List of Figures

List of Tables

1. ST Introduction

1.1. ST Identification

1.1.1. ST Identification and Management

Title: Multi functional printer (digital copier) bizhub PRO C5500/ineo+5500 Series Security Target

Version: 2

Created on: August 10, 2007

Created by: Konica Minolta Business Technologies, Inc.

1.1.2. TOE Identification and Management

Title: Japan : bizhub PRO C5500/ineo+5500 Gazou Seigyo Program

Overseas : bizhub PRO C5500/ineo+5500 Image Control Program

*1) "Gazou Seigyo Program" in Japanese and "Image Control Program" in English are the same product with different calling name.

*2) It is identified as "Gazou Seigyo I1" in Japanese and "Image Control I1" in English on the operation panel of bizhub PRO C5500.

*3) According to the sales type, ineo+5500 is used as another product name for bizhub PRO C5500. ineo+5500 Image Control Program is identical to bizhub PRO C5500 Image Control Program.

Version: A0E70Y0-00I1-G00-10

Created on: June 21, 2007

Created by: Konica Minolta Business Technologies, Inc.

1.1.3. Used CC Version

CC Version 2.3, ISO/IEC 15408:2005

* The following references are used for Japanese version.

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005, CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005, CCMB-2005-002
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005, CCMB-2005-003

1.2. ST Overview

This Security Target (ST) describes “bizhub PRO C5500/ineo+5500 Image Control Program” installed on digital MFP “bizhub PRO C5500/ineo+5500” (Hereinafter referred to as “bizhub PRO C5500 Series”, and as “bizhub PRO C5500 Image Control Program” representing “Image Control Program”.) manufactured by Konica Minolta Business Technologies, Inc.

bizhub PRO C5500 Image Control Program prevents the document data in bizhub PRO C5500 Series from disclosing during the use of functions such as copier and printer. TOE offers the protective function with password lock system against the risk of reading data out illegally from HDD (Hard Disk Drive) that is a medium for storing temporarily document data. This contributes to the protection of information leak in the organization that uses bizhub PRO C5500 Series.

1.3. CC Conformance

Part 2 Conformant

Part 3 Conformant

EAL3 Conformant

1.4. Reference

- Common Criteria for Information Technology Security Evaluation
  Part 1: Introduction and general model
  August 2005 Version 2.3 CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation
  Part 2: Security functional requirements
  August 2005 Version 2.3 CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation
  Part 3: Security assurance requirements
  August 2005 Version 2.3 CCMB-2005-003-003
- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part1, 2005/12
- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part2, 2005/12
- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part3, 2005/12

2. TOE Description

2.1. TOE Type

The TOE is a software product with digital MFP that is installed network functions.

2.2. Terminology

No.	Term	Description
1	Document data	Digitized information data such as characters and figures.
2	Paper document	Paper-based document with information such as characters and figures.
3	Temporary storage	Input document data is stored temporarily into DRAM/HDD until it is printed as paper document.
4	Operation panel	Touch panel display and operation buttons integrated into main frame of bizhub PRO C5500 Series.
5	Internal network	LAN in an organization that introduces bizhub PRO C5500 Series. Connected to the client PC and several servers such as Mail server and FTP server.
6	External network	Network (e.g. Internet and so on) except the internal network (Refer to the above No.5).

2.3. TOE Overview

The TOE is the bizhub PRO C5500 Image Control Program. bizhub PRO C5500 Series installed this TOE is digital MFP with network functions. It offers functions for the use of copier and printer etc, the operation management of bizhub PRO C5500 Series, and the maintenance management of bizhub PRO C5500 Series. Figure 2.1 shows the excepted operating environment with bizhub PRO C5500 Series in office.

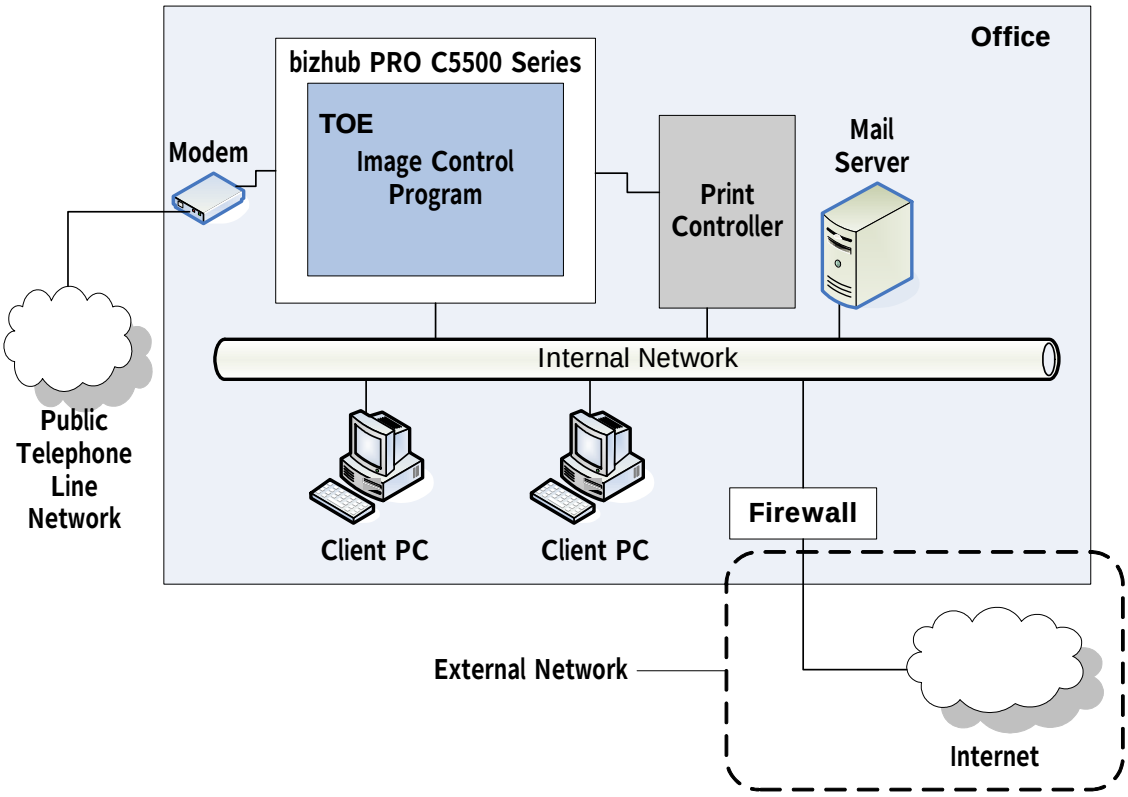

Figure 2.1 Operating Environment of bizhub PRO C5500 Series

bizhub PRO C5500 Series including the TOE is connected with an internal network and a public telephone line network as shown in Figure 2.1. The internal network is connected with general user client PCs and a mail server, to which bizhub PRO C5500 Series sends data. The TOE does not have sending/receiving function for the client PCs and the mail server. In addition, the TOE has not have an external network interface. When the external network is connected, it is connected through a firewall in order to protect each of equipments in the internal network.

2.4. bizhub PRO C5500 Series Participants and Roles

The following shows bizhub PRO C5500 Series related persons and their roles.

- General user

  General user uses the user functions such as copying and printing provided by the TOE. He/She has basic IT knowledge and can attack the TOE using opened information, however, it is not assumed for him/her to create any new attack by using unopened information.

- Administrator

  Administrator belongs to the organization that introduces bizhub PRO C5500 Series, and performs the operational management of bizhub PRO C5500 Series. He/She uses the

operational management functions provided by the TOE.

- Responsible person

  Responsible person belongs to the organization that introduces bizhub PRO C5500 Series, and appoints the administrator.

- CE

  CE belongs to the company undertaken to maintain bizhub PRO C5500 Series. He/She performs maintenance of bizhub PRO C5500 Series by using the maintenance management functions provided by the TOE. He/She makes bizhub PRO C5500 Series maintenance contract with responsible person or administrator.

The general user, administrator, and CE are called as product-related persons.

2.5. TOE Structure

Figure 2.2 shows the structure of this TOE.

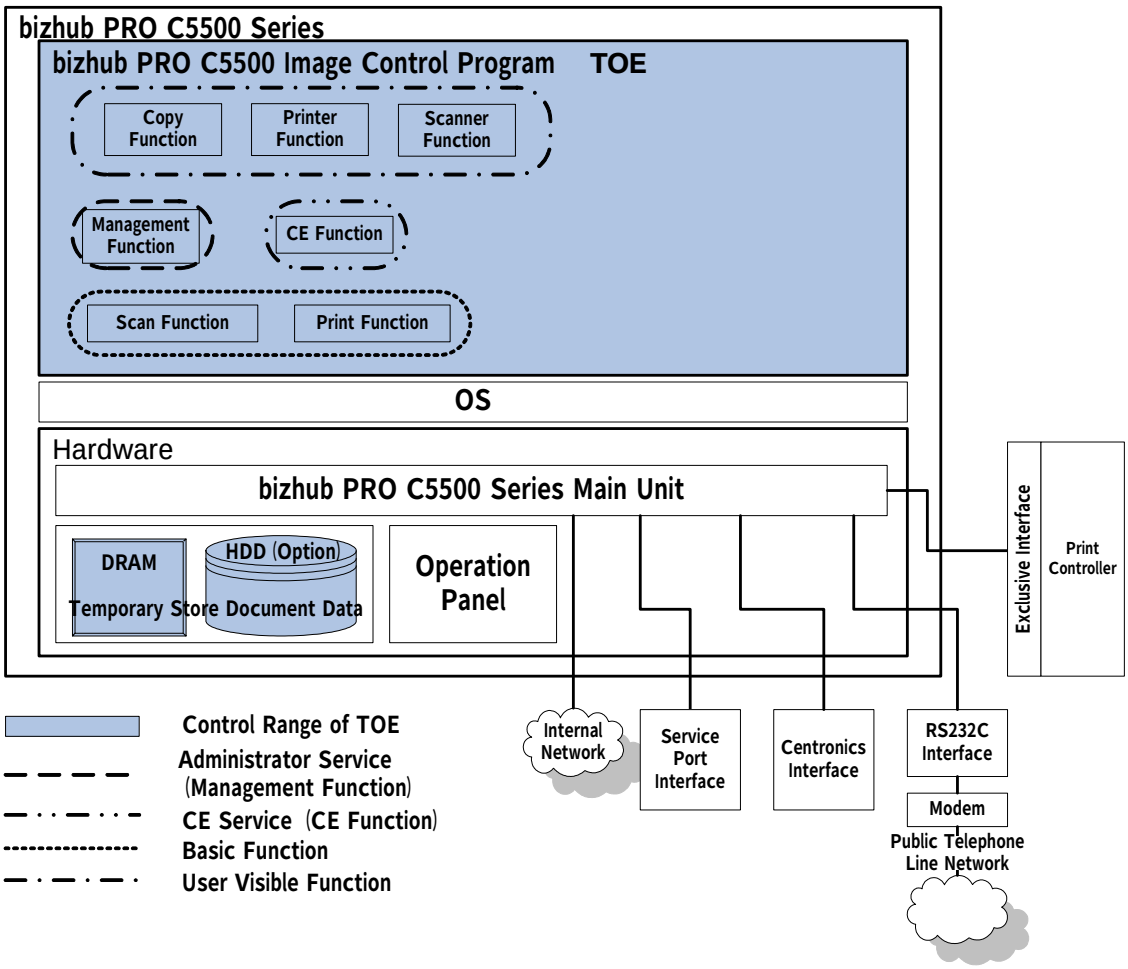

Figure 2.2 TOE Structure

bizhub PRO C5500 Series consists of hardware and bizhub PRO C5500 Image Control Program. The hardware includes bizhub PRO C5500 Series main unit, DRAM/HDD section, operation panel, network card, and various interfaces. The optional HDD (not equipped as standard) mounts four pieces of HDD that are allocated to each of yellow/magenta/cyan/black color image units. It is called "HDD" as all four HDDs, hereafter. The bizhub PRO C5500 Series main unit includes scan function that digitizes paper document and print function that prints characters and figures on printer paper. The print controller converts the received data from PC to print characters and figures on printer paper. The main unit is connected to the print controller by an exclusive interface. The service port interface and the Centronics interface are to connect with maintenance computer when setting and creating the TOE. They cannot be accessed document data. The DRAM/HDD section stores temporarily document data. bizhub PRO C5500 Image Control Program operates on OS that controls input/output of document data to hardware and bizhub PRO C5500 Image Control Program. The image control program controls management function, CE function, user function (copy function, printer function, scanner function, as shown in Table 2.1) and basic function (scan function and print function, as shown in Table 2.1).

bizhub PRO C5500 Series receives processing request from product-related person through the operation panel or network, then the TOE executes the task.

2.6. Functional Structure of bizhub PRO C5500 Image Control Program

bizhub PRO C5500 Image Control Program has the following functions.

The security functions are administrator identification/authentication function, security strengthen mode, CE identification/authentication function, and service setting mode.

2.6.1. Basic Function

In copy function, the document data (digitized data) scanned from paper document is once stored into the temporary storage area of DRAM/HDD and then printing is performed after reading out from there. In printer function, the document data from client PC is converted by the external print controller and is entered to bizhub PRO C5500 Series. It is once stored into the temporary storage area of DRAM/HDD and then printing is performed after reading out from there. The document data stored into the temporary storage DRAM is deleted by turning the power off. In scanner function, the digitized data scanned from paper document is transmitted to the external print controller without temporarily storing.

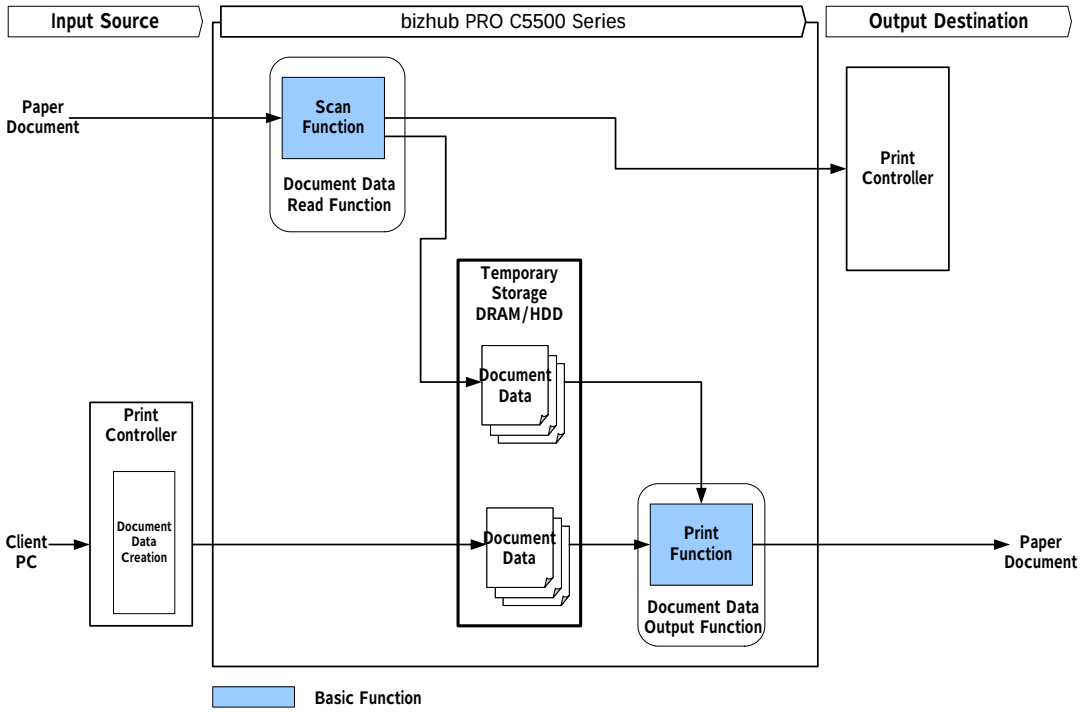

Figure 2.3 Processing Architecture of Basic Function

As shown in Table 2.1, the user functions are enabled by performing the basic functions. The following explains the basic functions.

Table 2.1 User Functions and Basic Functions

No	User function	Basic function
1	Copy function	Scan function and Print function
2	Printer function	Print function
3	Scanner function	Scan function

The functions shown in Figure 2.3 are described below.

(1) Scan function

The information of paper document that is requested through the operation panel by general user, is scanned and converted to digitized data. It is stored on the temporary storage area in copy function, and is directly transmitted to the external print controller in scan function.

(2) Print function

The document data stored on the temporary storage DRAM/HDD is printed out.

2.6.2. Management Function

The management function can be used by the administrator only when the identification and authentication have been successful. This function can be operated through the operation panel only. The administrator uses this function to conduct administrator password change, security strengthen mode (security function) setting, TOE network information setting and operation setting of functions provided by the TOE. Moreover, it controls information related to operation of digital MFP, such as printing audit information, controlling the number of prints, troubleshooting, and checking toner shortage.

- Security strengthen mode (Security function)

  The administrator enables security strengthen mode so as to make functions provided by the TOE more secure condition. Only the authenticated and identified administrator can be set security strengthen mode. In a state of effective security strengthen mode, when an optional HDD is installed, HDD lock password is set not to be read/written the data. Accordingly, the locked HDD blocks outside access (reading/writing is not available.) in bizhub PRO C5500 Series power off. At the time of bizhub PRO C5500 Series power on, the TOE commands HDD to authenticate and unlock by using the lock password. The HDD confirms to be the valid TOE and unlocks so as to make reading/writing data possible. Regardless of whether HDD is installed, the internal network functions other than CSRC function as described later are deactivated. In addition, for the setting operation related to security matter, the date and the result on operation are internally recorded and only the administrator can view it.

  The administrator needs to change the HDD lock password because bizhub PRO C5500 Series memorizes a unique HDD lock password at the time of installation. (It is not set in HDD.)

2.6.3. CE Function

The CE function can be used for the following functions by the CE only when the identification and authentication have been successful.

- Service setting mode (Security function)

  The CE registers and changes the administrator password by operating service setting mode functions through the operation panel. Only the identified and authenticated CE can use the function for registering administrator password. Only the identified and authenticated CE and the administrator permitted in management function can use the function for changing administrator password. Their functions are operated through the operation panel.

  Only the administrator is permitted to set security strengthen mode, thus, the administrator is assured by identifying and authenticating the CE who has the setting authority for the

administrator.

- CSRC (CS Remote Care)

The CE gets information for the hardware maintenance such as the number of prints, jam frequency, and toner shortage, by accessing bizhub PRO C5500 Series from a computer connected through public line network or internet. CSRC is executed by RS232C interface or E-mail interface. The transmission rule with RS232C interface or modem uses an original communication protocol. E-mail uses an original message communication protocol. Therefore, CSRC does not have interface to the document data.

2.7. Protected Asset

The asset protected by the TOE is the document data in temporary storage HDD.

The document data stored in DRAM is not accessed from outside. There is no the threat of data leakage because the temporary stored data in DRAM is deleted by turning the power off.

2.8. Function Not Provided by the TOE

The TOE does not prevent the deletion of document data because the user owns its original data in client PC or on paper.

3. TOE Security Environment

3.1. Assumptions

ASM.SECMOD Operation setting condition for the security strengthen mode

The administrator enables the security strengthen mode.

bizhub PRO C5500 Series mounts an optional HDD.

ASM.NET Setting condition of the internal network

When the internal network that sets bizhub PRO C5500 Series including the TOE is connected with the external network, bizhub PRO C5500 Series cannot be accessed by the external network.

ASM.ADMIN Reliable administrator

The administrator shall not carry out an illegal act.

ASM.CE Personal condition for the CE

The CE shall not carry out an illegal act.

ASM.SECRET Operational condition on the confidential information

When the TOE is used, the administrator password and HDD lock password shall not be disclosed by the administrator, and the CE password shall not be disclosed by the CE.

3.2. Threats

T.HDDACCESS Unauthorized access to the HDD

When a general user changes the setting on security strengthen mode and connects the HDD with an illegal device, the document data is read out.

3.3. Organizational Security Policies

Organizational security policies are not provided.

4. Security Objectives

4.1. Security Objectives for the TOE

O.IA Identification and authentication when using the management function or CE function

The TOE identifies and authenticates the administrator and the CE who try access the TOE.

O.MANAGE Provision of the management function

The TOE enables the security strengthen mode to provide function (manage and set the HDD lock password) to control securely the HDD provided by OE.HDD. Only the administrator is permitted to manage the security strengthen mode.

4.2. Security Objectives for the Environment

OE.SECMOD Operation setting for the security strengthen mode

The administrator shall attach an optional HDD to bizhub PRO C5500 Series, then enable the setting of security strengthen mode.

OE.NET Management of the network

The administrator shall connect the TOE to the internal network protected by a firewall.

OE.ADMIN Personal condition for the administrator

The responsible person shall select a person as administrator who does not carry out an illegal act.

OE.HDD Protection of the HDD

The HDD protected by the lock password shall be used.

OE.CE Assurance of the CE

The responsible person or administrator shall make the maintenance contract with the CE. The contract shall be specified a statement that CE will not carry out an illegal act.

OE.SECRET Appropriate management of confidential information

The administrator shall execute the following operations.

- A guessable value shall not be set for the administrator password or HDD lock password.
- The administrator password or HDD lock password shall be kept confidential.

The CE shall execute the following operations.

- A guessable value shall not be set for the CE password.
- The CE password shall be kept confidential.

- When the CE changed the administrator password, the administrator shall be requested promptly to change.

5. IT Security Requirements

5.1. TOE Security Requirements

5.1.1. TOE Security Functional Requirements

FIA_UID.2	User identification before any action

Hierarchical to : FIA_UID.1

FIA_UID.2.1

The TSF shall require each user to identify itself before allowing any other TSF- mediated actions on behalf of that user.

Refinement : “User” → Administrator, CE

Dependencies : No dependencies

FIA_UAU.2 User authentication before any action

Hierarchical to : FIA_UAU.1

FIA_UAU.2.1

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Refinement : “User” → Administrator, CE

Dependencies : FIA_UID.1 Timing of identification

FIA_UAU.7 Protected authentication feedback

Hierarchical to : No other components

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]

- Password characters entered by operator are shown as multiple dummy characters (*).

Dependencies : FIA_UAU.1 Timing of authentication

FIA_AFL.1 Authentication failure handling

Hierarchical : No other components

FIA_AFL.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]

- Unsuccessful authentication to the administrator or CE

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

- 1

FIA_AFL.1.2

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

[assignment: list of actions]

- For the administrator or CE authenticated unsuccessfully, the next authentication attempt is not executed until after five seconds.

Dependencies : FIA_UAU.1 Timing of authentication

FIA_SOS.1[1] Verification of secrets

Hierarchical to : No other components

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [assignment: a defined quality metric].

[assignment: a defined quality metric]

- The quality metric of password is defined as below.

Length of password:	8 characters
Characters types:	Alphabetic capital letters, small letters, and numerals (All is one-byte characters.)
Permitted condition:	Password cannot be identical to the previous password used.

Refinement : “Secret” → “Administrator password”, “CE password”

Dependencies : No dependencies

FIA_SOS.1[2] Verification of secrets

Hierarchical to: No other components

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [assignment: a defined quality metric].

[assignment: a defined quality metric]

- The quality metric of password is defined as below.

Length of password:	8 to 32 characters
Characters types:	Alphabetic capital letters, small letters, and numerals (All is one-byte characters.)
Permitted condition:	None

Refinement : “Secret” → “HDD lock password”

Dependencies : No dependencies

FMT_MTD.1[1]　Management of TSF data

Hierarchical to : No other components

FMT_MTD.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 authorized identified roles].

[assignment: list of TSF data]

- Administrator password

[selection: change_default, query, modify, delete, clear, [assignment: other operations]]

Other operations

[assignment: other operations]

- Registration

[assignment: the authorized identified roles]

- CE

Dependencies : FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1[2]　Management of TSF

Hierarchical to : No other components

FMT_MTD.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 authorized identified roles].

[assignment: list of TSF data]

- CE password

[selection: change_default, query, modify, delete, clear, [assignment: other operations]]

Modify

[assignment: the authorized identified roles]

- CE

Dependencies : FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1[3]　Management of TSF data

Hierarchical to : No other components

FMT_MTD.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 authorized identified roles].

[assignment: list of TSF data]

- Administrator password

[selection: change_default, query, modify, delete, clear, [assignment: other operations]]

Modify

[assignment: the authorized identified roles]

- Administrator, CE

Dependencies : FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_SMR.1[1] Security roles

Hierarchical to : No other components

FMT_SMR.1.1

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

[assignment: the authorized identified roles]

- Administrator

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies : FIA_UID.1 Timing of identification

FMT_SMR.1[2] Security roles

Hierarchical to : No other components

FMT_SMR.1.1

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

[assignment: the authorized identified roles]

- CE

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies : FIA_UID.1 Timing of identification

FMT_MOF.1 Management of security functions behavior

Hierarchical to : No other components

FMT_MOF.1.1

The TSF shall restrict the ability to [selection: determine the behavior of, disable, enable, modify the behavior of] the functions [assignment: list of functions] to [assignment: the authorized identified roles].

[assignment: list of functions]

- Function 1

  Function 1 : Security strengthen mode

[selection: determine the behavior of, disable, enable, modify the behavior of]

Disable, Enable

[assignment: the authorized identified roles]

- Administrator

Dependencies : FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

Hierarchical to : No other components

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]

- Registration of administrator password by CE
- Change of administrator password by CE
- Change of CE password by CE
- Change of administrator password by administrator
- Setting of security strengthen mode by administrator

Dependencies : No dependencies

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to : No other components

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies : No dependencies

FPT_SEP.1 TSF domain separation

Hierarchical to : No other components

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.

Dependencies : No dependencies

FDP_ACC.1 Subset access control

Hierarchical to : No other components

FDP_ACC.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]

Management function access control: Operational List

Subject	Object	Operation
A task that substitutes for a user	HDD lock password object	Modify

[assignment: access control SFP]

Management function access control

Dependencies : FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to : No other components

FDP_ACF.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 attribute>
- A task that substitutes for a user	=>	- Administrator attribute

<Object>

- HDD lock password object

[assignment: access control SFP]

Management function access control

FDP_ACF.1.2

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 for a user who has administrator attribute is allowed the operation to modify HDD lock password object.

FDP_ACF.1.3

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 authorize access of subjects to objects].

- None

FDP_ACF.1.4

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

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

5.1.2. TOE Security Assurance Requirements

This TOE asserts EAL3 that is a sufficient level as quality assurance for commercial office products. Table 5.1 summarizes the applied TOE security assurance requirements to EAL3.

Table 5.1 List of TOE Security Assurance Requirements

Assurance class	Assurance requirement
Configuration management	ACM_CAP.3 Authentication management
	ACM_SCP.1 TOE CM coverage
Distribution and operation	ADO_DEL.1 Distribution procedures
	ADO_IGS.1 Installation, creation, startup procedures
Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.2 Security enforcing high-level design
	ADV_RCR.1 Informal correspondence demonstration
Guidance document	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life cycle support	ALC_DVS.1 Identification of security measures
Test	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing : High-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment	AVA_MSU.1 Examination of guidance
	AVA_SOF.1 Evaluation of TOE security function strength
	AVA_VLA.1 Developer vulnerability analysis

FIA_UAU.2[E] User authentication before any action

Hierarchical to : FIA_UAU.1

FIA_UAU.2.1[E]

The TSF shall require each user to be successfully authenticated before allowing any otherTSF-mediated actions on behalf of that user.

Refinement : “TSF” → “HDD”

Dependencies : No dependencies

5.3. Strength of Security Functions

The following two password mechanisms are targeted for the claim of TOE function strength, and the subsequence six components of TOE functions are targeted for this ST.

Password mechanisms and corresponding TOE function components

1. Administrator password/CE password authentication function
   FIA_UID.2, FIA_UAU.2, FIA_UAU.7, FIA_AFL.1, FIA_SOS.1[1]
2. HDD lock password authentication function
   FIA_SOS.1[2]

TOE component functions

FIA_UID.2 (User identification)
FIA_UAU.2 (User authentication)
FIA_UAU.7 (Protected authentication feedback)
FIA_SOS.1[1] (Verification of secrets)
FIA_SOS.1[2] (Verification of secrets)
FIA_AFL.1 (Authentication failure handling)

The SOF-Basic is claimed for the above six TOE function requirements and the minimum TOE function strength.

6. TOE Summary Specification

6.1. TOE Security Functions

6.1.1. Identification Authentication Function

The identification authentication functions provide the following a group of security functions.

Function title	Specification of security function	TOE security functional requirement
IA.ADM_ADD Administrator registration	IA.ADM_ADD registers the administrator in the TOE. Only the CE operates IA.ADM_ADD. The CE registers the administrator password. IA.ADM_ADD provides an interface for administrator registration. The administrator registration interface requests password entry for registering the administrator. For the password entered by the administrator, the permitted value is verified according to the following rules. - A password shall be 8 characters. - A password shall be composed of alphabetic capital letters, small letters, and numerals. (All is one-byte characters.) - A password shall not be identical to the previous password used. In the verification of permitted value, the administrator is registered if the rules are obeyed, and it is rejected if not so.	FIA_SOS.1[1] FMT_MTD.1[1] FMT_SMF.1 FPT_RVM.1 FPT_SEP.1
IA.ADM_AUTH Administrator identification and authentication	Before the operator can use the TOE, IA.ADM_AUTH identifies that he/she is the registered administrator in the TOE and authenticates that he/she is the administrator. IA.ADM_AUTH does not permit any operation of the management functions before identification and authentication of the administrator. The interface for administrator identification and authentication requests to	FIA_UID.2 FIA_UAU.2 FIA_UAU.7 FIA_AFL.1 FPT_RVM.1 FPT_SEP.1 FMT_SMR.1[1]

	enter the password registered by IA.ADM_ADD and changed by IA_PASS. IA.ADM_AUTH identifies that he/she is the administrator through the interface display for administrator identification and authentication, and it authenticates that he/she is the administrator by the entered password. When the administrator enters the password, dummy characters (*) are displayed in stead of the entered password. When the authentication is unsuccessful, the interface for administrator identification and authentication is provided after five seconds.	
IA.CE_AUTH CE identification and authentica-tion	Before the operator can use the TOE, IA.CE_AUTH identifies that he/she is the registered CE in the TOE and authenticates that he/she is the CE. IA.CE_AUTH does not permit any operate of the CE functions before identification and authentication of the CE. It requests to enter the password changed by IA_PASS. IA.CE_AUTH identifies that he/she is the CE through the interface display for CE identification and authentication, and it authenticates that he/she is the CE by the entered password. When the CE enters the password, dummy characters (*) are displayed in stead of the entered password. When the authentication is unsuccessful, the interface for CE identification and authentication is provided after five seconds.	FIA_UID.2 FIA_UAU.2 FIA_UAU.7 FIA_AFL.1 FPT_RVM.1 FPT_SEP.1 FMT_SMR.1[2]
IA.PASS Password change	IA.PASS changes the administrator password or CE password that is the authentication information for administrator or CE. IA.PASS provides an interface for password change and requests to enter a new password. The following shows the password available to change depending on the type of user. CE : CE password, Administrator password	FIA_SOS.1[1] FMT_MTD.1[2] FMT_MTD.1[3] FMT_SMF.1 FPT_RVM.1 FPT_SEP.1

	Administrator : Administrator password For the password entered by the product-related persons, the permitted value is verified according to the following rules. - A password shall be 8 characters. - A password shall be composed of alphabetic capital letters, small letters, and numerals. (All is one-byte characters.) - A password shall not be identical to the previous password used. In the verification of permitted value, the password is changed if the rules are obeyed.	

6.1.2. Management Support Function

The management support functions provide the following a group of security functions.

Function title	Specification of security function	TOE security functional requirement
MNG.MODE Setting of security strengthen mode	MNG.MODE permits and executes only for the administrator to enable or disable the security strengthen mode.	FMT_MOF.1 FPT_RVM.1 FPT_SEP.1 FMT_SMF.1
MNG.HDD HDD lock password function	MNG.HDD permits and executes only for the administrator the following processing. - Change of HDD lock password For the HDD lock password entered by the administrator, the permitted value is verified according to the following rules. - A password shall be 8 to 32 characters. - A password shall be composed of alphabetic capital letters, small letters, and numerals. (All is one-byte characters.) In the verification of permitted value, the HDD lock password is set or changed in the HDD device if the rules are obeyed, and the change is rejected if not so.	FIA_SOS.1[2] FDP_ACC.1 FDP_ACF.1 FPT_RVM.1 FPT_SEP.1

6.2. Strength of Security Functions

This TOE claims the strength of security function of SOF-Basic for the password mechanism. The applicable password mechanisms are Identification Authentication Function (IA.ADM_AUTH, IA.CE_AUTH, IA.ADM_ADD and IA.PASS) and Management Support Function (MNG.HDD).

6.3. Assurance Measures

The developer shall develop according to the security assurance requirements and the development rules regulated by the development organization. Table 6.1 shows the related documents for security requirements and the components of security assurance requirements that fulfill EAL3.

Table 6.1 Assurance Requirements and Related Documents for EAL3

Assurance requirements item	Component	Related document
Configuration management	ACM_CAP.3	bizhub PRO C5500/ineo+5500 Configuration Management Plan bizhub PRO C5500/ineo+5500 List of Design Documents bizhub PRO C5500/ineo+5500 List of Source Codes
	ACM_SCP.1	bizhub PRO C5500/ineo+5500 Configuration Management Plan bizhub PRO C5500/ineo+5500 List of Design Documents bizhub PRO C5500/ineo+5500 List of Source Codes
Distribution and operation	ADO_DEL.1	bizhub PRO C5500/ineo+5500 Distribution Regulations (Japanese) bizhub PRO C5500 Installation Manual (Japanese) bizhub PRO C5500 User's Guide Copier (Japanese) bizhub PRO C5500 User's Guide POD Administrator's Reference (Japanese) bizhub PRO C5500 User's Guide Security (Japanese) bizhub PRO C6500/C6500P/C5500 Service Manual Field Service (Japanese) bizhub PRO C5500 User's Guide Copier (English) bizhub PRO C5500 User's Guide POD Administrator's Reference (English) bizhub PRO C5500 User's Guide Security (English) bizhub PRO C6500/C6500P/C5500 SERVICE MANUAL Field Service (English) bizhub PRO C5500 INSTALLATION MANUAL (English) ineo+5500 User's Guide [Copier] (English) ineo+5500 User's Guide [POD Administrator's Reference] (English) ineo+5500 User's Guide [Security] (English) COLOR MFP 55ppm INSTALLATION MANUAL (English)

	ADO_IGS.1	bizhub PRO C5500/ineo+5500 Introduction and Operation Regulations (Japanese) bizhub PRO C5500 Installation Manual (Japanese) bizhub PRO C5500 User's Guide Copier (Japanese) bizhub PRO C5500 User's Guide POD Administrator's Reference (Japanese) bizhub PRO C5500 User's Guide Security (Japanese) bizhub PRO C6500/C6500P/C5500 Service Manual Field Service (Japanese) bizhub PRO C5500 User's Guide Copier (English) bizhub PRO C5500 User's Guide POD Administrator's Reference (English) bizhub PRO C5500 User's Guide Security (English) bizhub PRO C6500/C6500P/C5500 SERVICE MANUAL Field Service (English) bizhub PRO C5500 INSTALLATION MANUAL (English) ineo+5500 User's Guide [Copier] (English) ineo+5500 User's Guide [POD Administrator's Reference] (English) ineo+5500 User's Guide [Security] (English) COLOR MFP 55ppm INSTALLATION MANUAL (English)
Development	ADV_FSP.1	bizhub PRO C5500/ineo+5500 Functional Specifications
	ADV_HLD.2	bizhub PRO C5500/ineo+5500 Functional Specifications
	ADV_RCR.1	bizhub PRO C5500/ineo+5500 Functional Correspondence Report

Guidance document	AGD_ADM.1	bizhub PRO C5500 Installation Manual (Japanese) bizhub PRO C5500 User's Guide Copier (Japanese) bizhub PRO C5500 User's Guide POD Administrator's Reference (Japanese) bizhub PRO C5500 User's Guide Security (Japanese) bizhub PRO C6500/C6500P/C5500 Service Manual Field Service (Japanese) bizhub PRO C5500 User's Guide Copier (English) bizhub PRO C5500 User's Guide POD Administrator's Reference (English) bizhub PRO C5500 User's Guide Security (English) bizhub PRO C6500/C6500P/C5500 SERVICE MANUAL Field Service (English) bizhub PRO C5500 INSTALLATION MANUAL (English) ineo+5500 User's Guide [Copier] (English) ineo+5500 User's Guide [POD Administrator's Reference] (English) ineo+5500 User's Guide [Security] (English) COLOR MFP 55ppm INSTALLATION MANUAL (English)
	AGD_USR.1	bizhub PRO C5500 User's Guide Copier (Japanese) bizhub PRO C5500 User's Guide POD Administrator's Reference (Japanese) bizhub PRO C5500 User's Guide Security (Japanese) bizhub PRO C5500 User's Guide Copier (English) bizhub PRO C5500 User's Guide POD Administrator's Reference (English) bizhub PRO C5500 User's Guide Security (English) ineo+5500 User's Guide [Copier] (English) ineo+5500 User's Guide [POD Administrator's Reference] (English) ineo+5500 User's Guide [Security] (English)
Life cycle support	ALC_DVS.1	bizhub PRO C5500/ineo+5500 Development Security Regulations
Test	ATE_COV.2	bizhub PRO C5500/ineo+5500 Functional Analysis Report
	ATE_DPT.1	bizhub PRO C5500/ineo+5500 Functional Analysis Report
	ATE_FUN.1	bizhub PRO C5500/ineo+5500 Functional Test Report
	ATE_IND.2	None (bizhub PRO C5500 Test Set)

Vulnerability assessment	AVA_MSU.1	bizhub PRO C5500/ineo+5500 Introduction and Operation Regulations (Japanese) bizhub PRO C5500 Installation Manual (Japanese) bizhub PRO C5500 User's Guide Copier (Japanese) bizhub PRO C5500 User's Guide POD Administrator's Reference (Japanese) bizhub PRO C5500 User's Guide Security (Japanese) bizhub PRO C6500/C6500P/C5500 Service Manual Field Service (Japanese) bizhub PRO C5500 User's Guide Copier (English) bizhub PRO C5500 User's Guide POD Administrator's Reference (English) bizhub PRO C5500 User's Guide Security (English) bizhub PRO C6500/C6500P/C5500 SERVICE MANUAL Field Service (English) bizhub PRO C5500 INSTALLATION MANUAL ineo+5500 User's Guide [Copier] (English) ineo+5500 User's Guide [POD Administrator's Reference] (English) ineo+5500 User's Guide [Security] (English) COLOR MFP 55ppm INSTALLATION MANUAL (English)
	AVA_SOF.1	bizhub PRO C5500/ineo+5500 Vulnerability Analysis Report
	AVA_VLA.1	bizhub PRO C5500/ineo+5500 Vulnerability Analysis Report

7. PP Claim

There is no applicable PP in this ST.

8. Rationale

8.1. Security Objectives Rationale

Table 8.1 shows the relationship of the security objectives to the threats and assumptions.

Table 8.1 Mapping between Threats, Assumptions, and Security Objectives

Threats/Assumptions / Security objectives	T.HDDACCESS	A.SMM-SECCMOD	A.SMM-NET	A.SMM-ADMIN	A.SMM-CE	A.SMM-SECRET
O.IA (Identification and authentication when using)	✔					
O.MANAGE (Provision of the management function)	✔					
OE.SECMOD (Operating setting for the security strengthen mode)		✔				
OE.NET (Management of the network)			✔			
OE.ADMIN (Personal condition for the administrator)				✔		
OE.CE (Assurance of the CE)					✔	
OE.HDD (Protection of the HDD)		✔				
OE.SECRET (Appropriate management of confidential information)						✔

The following shows the rationale for Table 8.1.

T.HDDACCESS : Unauthorized access to the HDD

The TSF identifies the administrator by O.IA, who sets and changes the HDD lock password by the management function of O.MANAGE. Only the administrator is permitted to set the security strengthen mode, thus the administrator is assured by identifying and authenticating the CE who has the setting authority for administrator by O.IA. Accordingly, it is prevented for the HDD lock

password to be changed by any attacker because the setting function for security strengthen mode is permitted only for the identified and authenticated administrator.
As mentioned above, the threat T.HDDACCESS can be resisted by O.IA and O.MANAGE of the security objects.

ASM.SECMOD : Operating setting condition for the security strengthen mode
The TOE makes the administrator install the optional HDD to bizhub PRO C5500 Series and enable the setting of security strengthen mode by OE.SECMOD. Therefore, the general user can use bizhub PRO C5500 Series with the TOE in the condition of attaching HDD and available security strengthen mode.
Also the optional HDD installed to bizhub PRO C5500 Series has the password lock function by OE.HDD.
As mentioned above, the assumption ASM.SECMOD can be realized by OE.SECMOD and OE.HDD of the security objectives.

ASM.NET : Setting condition for the internal network
In OE.NET, the administrator installs the TOE in the internal network that is protected by a firewall, thus TOE cannot be accessed by the external network when the internal network connects with the external network.
As mentioned above, the assumption ASM.NET can be realized by OE.NET of the security objectives.

ASM.ADMIN : Reliable administrator
OE.ADMIN regulates the condition of administrator. The responsible person selects a person who does not carry out an illegal act as administrator.
As mentioned above, the assumption ASM.ADMIN can be realized by OE.ADMIN of the security objectives.

ASM.CE : Maintenance contract
For the organization that introduces the TOE, OE.CE regulates to close the maintenance contract specified a statement that the organization and CE in charge of the maintenance of TOE shall not carry out an illegal act.
As mentioned above, the assumption ASM.CE can be realized by OE.CE of the security objectives.

ASM.SECRET : Operational condition on the confidential information

OE.SECRET regulates that the administrator implements the operation regulations related to administrator password and HDD lock password, and the CE implements the operation regulations related to CE password. Therefore, this condition can be realized.

8.2. Security Requirements Rationale

8.2.1. Rationale for Security Functional Requirements

Table 8.2 shows the relationship of the security functional requirements to the security objectives.

Table 8.2 Mapping between Security Objectives and IT Security Functional Requirements

IT security functional requirements \ Security objectives		O・IA	O・MANAGE	OE・HDD
TOE security functional requirements	FIA_UID.2	✔		
	FIA_UAU.2	✔		
	FIA_UAU.7	✔		
	FIA_AFL.1	✔		
	FIA_SOS.1[1]	✔		
	FIA_SOS.1[2]		✔	
	FMT_MTD.1[1]	✔		
	FMT_MTD.1[2]	✔		
	FMT_MTD.1[3]	✔		
	FMT_SMR.1[1]	✔	✔	
	FMT_SMR.1[2]	✔		
	FMT_MOF.1		✔	
	FPT_RVM.1	✔	✔	
	FPT_SEP.1	✔	✔	
	FMT_SMF.1	✔	✔	
	FDP_ACC.1		✔	

	FDP_ACF.1		✔	
Security functional requirements for IT environment	FIA.UAU.2[E]			✔

The following shows the rationale for Table 8.2.

O.IA : Identification and authentication when using management function or CE function

FIA_UID.2 and FIA_UAU.2 identifies and authenticates respectively that he/she is the CE, thus it is confirmed that the operation is made by the valid CE.

FIA_UID.2 and FIA_UAU.2 identifies and authenticates respectively that he/she is the administrator, thus it is confirmed that the operation is made by the valid administrator.

In case that the administrator or CE authentication is unsuccessful, FIA_AFL.1 keeps the administrator or CE waiting until after five seconds the next authentication attempt, in order to delay the time when the invalid user is successfully identified and authenticated as administrator or CE. To conceal the password, multiple dummy characters (*) are displayed corresponding to the password characters entered in the password entry area by FIA_UAU.7.

The CE can register the administrator password by FMT_MTD.1[1]. By registering the administrator password, the administrator is registered in the TOE and can start the operation. The CE can change his/her own password by FMT_MTD.1[2], thus the CE becomes possible to change it every a suitable period. Also FMT_MTD.1[3] permits the administrator or CE to change the administrator password, thus it can be changed every a suitable period. When the CE registers the administrator password, the administrator or CE changes the administrator password, or the CE changes the CE password, the password is verified to obey the password rules specified by FIA_SOS.1[1]. Changing password makes lower the possibility that it is identical with the administrator or CE password entered by general user.

With FPT_SEP.1, only the subject that substitutes for the authenticated CE, that is assumed by CE function control, can operate the object regulated by CE password change control and administrator password registration/change control. And only the subject that substitutes for the authenticated administrator, that is assumed by management function control, can operate the object regulated by administrator password change control.

The administrator and CE are maintained by FMT_SMR.1[1] and FMT_SMR.1[2] respectively. FMT_SMF.1 specifies the management of password. Their functions are not bypassed by FPT_RVM.1.

Therefore, O.IA can be realized by the correspondent security functional requirements.

O.MANAGE : Provision of the management function

FDP_ACC.1 and FDP_ACF.1 provide the function to change and manage the HDD lock password for the administrator. This prevents the unauthorized access to HDD. The password is verified to obey the specified rules by FIA_SOS.1[2].

The administrator is maintained by FMT_SMR.1[1]. Their functions are not bypassed by FPT_RVM.1. Also FMT_MOF.1 permits the administrator to activate or stop the security strengthen mode, and that encourages the HDD authentication function to activate or stop.

With FPT_SEP.1, only the subject that substitutes for the authenticated administrator, that is assumed by management function control, can operate the object regulated by HDD lock password change control and security strengthen mode start-and-stop control. FMT_SMF.1 specifies the management of security strengthen mode.

Therefore, O.MANAGE can be realized by the correspondent security functional requirements.

OE.HDD : Protection of the HDD

FIA_UAU.2[E] permits to access for only the TOE that the HDD is successfully authenticated.

Therefore, OE.HDD can be realized by the correspondent security functional requirements.

As mentioned above, the selected requirements are administrator/CE identification and authentication, their based access control (TOE security functional requirements), user authentication requirements before any action (security functional requirements for IT environment), thus there is no any requirement with which may conflict. Therefore, a set of IT security requirements ensures internal consistency.

8.2.2. Dependency of TOE Security Functional Requirements

The dependencies of TOE security functional requirements are satisfied all but No.17 as shown in Table 8.3.

Table 8.3 Dependencies of TOE Security Functional Requirements

No	TOE Security Functional Requirement	Lower level	Dependency	Reference No	Notes
1	FIA_UID.2	FIA_UID.1	None		
2	FIA_UAU.2	FIA_UAU.1	FIA_UID.1	1	
3	FIA_UAU.7	None	FIA_UAU.1	2	
4	FIA_AFL.1	None	FIA_UAU.1	2	
5	FIA_SOS.1[1]	None	None		

6	FIA_SOS.1[2]	None	None		
7	FMT_MTD.1[1]	None	FMT_SMR.1 FMT_SMF.1	12 11	
8	FMT_MTD.1[2]	None	FMT_SMR.1 FMT_SMF.1	13 11	
9	FMT_MTD.1[3]	None	FMT_SMR.1 FMT_SMF.1	12 11	
10	FMT_MOF.1	None	FMT_SMR.1 FMT_SMF.1	12 11	
11	FMT_SMF.1	None	None		
12	FMT_SMR.1[1]	None	FIA_UID.1	1	
13	FMT_SMR.1[2]	None	FIA_UID.1	1	
14	FPT_RVM.1	None	None		
15	FPT_SEP.1	None	None		
16	FDP_ACC.1	None	FDP_ACF.1	17	
17	FDP_ACF.1	None	FDP_ACC.1 FMT_MSA.3	16 (*)	
18	FIA_UAU.2[E]	FIA_UAU.1	FIA_UID.1	1	

(*) Reason that is not apply FMT_MSA.3 : It is not needed because there is no the event corresponding to the creation of object.

8.2.3. Interaction between TOE Security Functional Requirements

No	TOE security functional requirement	Function offering defense		
		Detour	Deactivation	Falsification
1	FIA_UID.2	FPT_RVM.1	FMT_MOF.1	
2	FIA_UAU.2	FPT_RVM.1	FMT_MOF.1	
3	FIA_UAU.7	FPT_RVM.1	FMT_MOF.1	
4	FIA_AFL.1	FPT_RVM.1	FMT_MOF.1	
5	FIA_SOS.1[1]	None	FMT_MOF.1	
6	FIA_SOS.1[2]	None	FMT_MOF.1	
7	FMT_MTD.1[1]	None	FMT_MOF.1	
8	FMT_MTD.1[2]	None	FMT_MOF.1	

9	FMT_MTD.1[3]	None	FMT_MOF.1	
10	FMT_MOF.1	FPT_RVM.1		
11	FMT_SMF.1	None	FMT_MOF.1	
12	FMT_SMR.1[1]	None	FMT_MOF.1	
13	FMT_SMR.1[2]	None	FMT_MOF.1	
14	FPT_RVM.1		FMT_MOF.1	
15	FPT_SEP.1		FMT_MOF.1	
16	FDP_ACC.1	None	FMT_MOF.1	
17	FDP_ACF.1	FIA_UAU.2	FMT_MOF.1	FPT_SEP.1

【Detour】 FPT_RVM.1

Upon using the TOE management function and CE function, the administrator and CE execute identification and authentication (FIA_UID.2, FIA_UAU.2, FIA_UAU.7, FIA_AFL.1).
Only the administrator is permitted the setting operation for security strengthen mode (FMT_ MOF.1).
The detour is prevented because the above mentioned matters are certainly executed by FPT_ RVM.1.

【Detour】 FIA_UAU.2

FDP_ACF.1 that regulates the management function access control is supported to prevent detour by FIA_UAU.2 that regulates the administrator identification and authentication. In addition, FIA_UAU.2 is supported to prevent detour because it is always invoked by FPT_RVM.1.

【Deactivation】 FMT_MOF.1

FMT_MOF.1 permits only the administrator to execute operating setting for security strengthen mode. The security strengthen mode influences all of the TOE security structure, therefore the prevention of deactivation is supported for all security functions that is realized by the TOE security requirements.

【Falsification】

With FPT_SEP.1, only the subject substituted for the authenticated administrator, that is assumed by management function access control, can operate the object regulated by management function access control. And only the subject substituted for the authenticated CE, that is assumed by CE unction access control can operate the object regulated by CE function access control. FDP_ACF.1 is supported to prevent unauthorized interference and destruction by other unauthorized subject.

8.2.4. Consistency of Security Function Strength for Security Objectives

This TOE assumes the attack capability of general user to be low level in “2. TOE Description”, and “3. TOE Security Environment” describes that “When a general user changes the setting on the security strengthen mode and connects the HDD with an illegal device, the document data is read out”. Accordingly the especially highly skilled attacker is not assumed. Moreover it assumes to be operated under the secured condition in terms of the physical and human aspect. Therefore in “5.3 Strength of Security Functions”, the security strength satisfies SOF-Basic which is able to resist sufficiently the attacks from the threat agent with low level attack capability.

The following shows the operational measures to make the TOE operate in safety.

- The administrator shall enable the setting of security strengthen mode.
- The administrator shall connect the TOE to the environment of internal network protected by a firewall.
- The responsible person shall appoint a person who does not carry out an illegal act as administrator.
- The responsible person or administrator shall close the maintenance contract with the CE. It shall be specified a statement that the CE will not carry out an illegal act.
- A guessable value shall not be set for the administrator password or HDD lock password.
- The administrator password or HDD lock password shall be kept confidential.
- A guessable value shall not be set for the CE password.
- The CE password shall be kept confidential.
- When the CE changed the administrator password, the administrator shall be requested promptly to change.

Therefore, the following person is specified as the threat agent.

Attack capability : Low level

As mentioned above, SOF-Basic is proper and consistent as the minimum function strength to security objectives because the sufficient resistance is taken for the threat agent with the attack capability listed above.

8.2.5. Rationale for Assurance Requirements

This TOE, a commercially available product, has to resist the threat by low level attack capability, thus requires the TOE functions, external interface specification, result of developer test, analysis of developer for obvious vulnerability, analysis of function strength, and so on. Therefore, EAL3 is an appropriate evaluation assurance level for the TOE.

8.3. TOE Summary Specification Rationale

8.3.1. Conformity of Security Functional Requirements to TOE Summary Specification

Table 8.4 shows the appropriateness between the security functional requirements and the TOE summary specification.

Table 8.4 Mapping between IT Security Functions and Security Functional Requirements

IT security function / TOE security functional requirement	IA・ADM_ADD	IA・ADM_AUTH	IA・CE_AUTH	IA・PASS	MNG・MODE	MNG・HDD
FIA_UID.2		✔	✔			
FIA_UAU.2		✔	✔			
FIA_UAU.7		✔	✔			
FIA_AFL.1		✔	✔			
FIA_SOS.1[1]	✔			✔		
FIA_SOS.1[2]						✔
FMT_MTD.1[1]	✔					
FMT_MTD.1[2]				✔		
FMT_MTD.1[3]				✔		
FMT_MOF.1					✔	
FMT_SMF.1	✔			✔	✔	
FMT_SMR.1[1]		✔				
FMT_SMR.1[2]			✔			
FPT_RVM.1	✔	✔	✔	✔	✔	✔
FPT_SEP.1	✔	✔	✔	✔	✔	✔
FDP_ACC.1						✔
FDP_ACF.1						✔

The following shows the rationale for Table 8.4.

FIA_UID.2

IA.ADM_AUTH identifies the administrator. IA.CE_AUTH identifies the CE.
As mentioned above, FIA_UID.2 can be realized by implementing IA.ADM_AUTH and IA.CE_ AUTH.

FIA_UAU.2

IA.ADM_AUTH authenticates the administrator. IA.CE_AUTH authenticates the CE.
As mentioned above, FIA_UAU.2 can be realized by implementing IA.ADM_AUTH and IA.CE_ AUTH.

FIA_UAU.7

The input characters are displayed as dummy characters (*), by IA.ADM_AUTH at password entry for the administrator authentication, by IA.CE_AUTH at password entry for the CE authentication.
As mentioned above, FIA_UAU.7 can be realized by implementing IA.ADM_AUTH and IA.CE_ AUTH.

FIA_SOS.1[1]

The input password is verified that it is within the permitted value along the password rules, by IA.ADM_ADD for the registration of administrator password, by IA.PASS for the change of administrator or CE password.
As mentioned above, FIA_SOS.1[1] can be realized by implementing IA.ADM_ADD and IA.PASS.

FIA_SOS.1[2]

The input password is verified that it is within the permitted value along the password rules, by MNG_HDD for the setting or change of HDD lock password, and HDD lock password is set or changed in the HDD device only when the rules are obeyed.
As mentioned above, FIA_SOS.1[2] can be realized by implementing MNG_HDD.

FIA_AFL.1

The next authentication attempt is not executed until after five seconds when the authentication is unsuccessful, by IA.ADM_AUTH for the administrator, by IA.CE_ AUTH for the CE.
As mentioned above, FIA_AFL.1 can be realized by implementing IA.ADM_AUTH and IA.CE_ AUTH.

FMT_MTD.1[1]

IA.ADM_ADD permits and executes only the CE to register the administrator password.

As mentioned above, FMT_MTD.1[1] can be realized by implementing IA.ADM_ADD.

FMT_MTD.1[2]

IA.PASS permits and executes only the CE to change the CE password.

As mentioned above, FMT_MTD.1[2] is realized by implementing IA.PASS.

FMT_MTD.1[3]

IA.PASS permits and executes the administrator or CE to change the administrator password.

As mentioned above, FMT_MTD.1[3] is realized by implementing IA.PASS.

FMT_MOF.1

MNG.MODE permits and executes the administrator to enable security functions regulated by this ST.

As mentioned above, FMT_MOF.1 can be realized by implementing MNG.MODE.

FMT_SMF.1

IA.ADM_ADD implements administrator password registration by the CE. IA.PASS implements administrator password change by the CE, CE password change by the CE, and administrator password change by the administrator. MNG.MODE implements the security strengthen mode by the administrator.

As mentioned above, FMT_SMF.1 can be realized by implementing IA.ADM_ADD, IA.PASS, and MNG.MODE.

FMT_SMR.1[1]

IA.ADM_AUTH authenticates the administrator. By keeping the role, FMT_SMR.1[1] can be realized.

FMT_SMR.1[2]

IA.CE_AUTH authenticates the CE. By keeping the role, FMT_SMR.1[2] can be realized.

FDP_ACC.1

FDP_ACC.1 regulates the relationship between the controlled subject to the object: HDD lock password object and the operation.

MNG_HDD performs the management function access control for the task of substituting the user

to modify the HDD lock password object.
Therefore, this functional requirement is satisfied.

FDP_ACF.1

FDP_ACF.1 regulates the relationship between the controlled subject to the object: HDD lock password object and the operation.
MNG.HDD performs the management function access control to which the following rules are applied.

- The operation to modify the HDD lock password object is permitted to the administrator.

Therefore, 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.
IA.ADM_ADD definitely activates IA.CE_AUTH of which performance is indispensable, before the CE registers the administrator.
IA.PASS definitely activates IA.CE_AUTH of which performance is indispensable, before the CE changes the CE password or administrator password.
IA.PASS definitely activates IA.ADM_AUTH of which performance is indispensable, before the administrator changes the administrator password.
MNG.MODE definitely activates IA.ADM_AUTH of which performance is indispensable, before the administrator sets the security strengthen mode.
MNG.HDD definitely activates IA.ADM_AUTH of which performance is indispensable, before the administrator changes the HDD lock password.
Therefore, this functional requirement is satisfied.

FPT_SEP.1

FPT_SEP.1 regulates to maintain the security domains for protecting against interference and falsification by subjects who cannot be trusted and regulates to separate the security domains of subjects.
IA.ADM_ADD maintains the CE authentication domain that is provided the function to register the administrator by only the CE who is authenticated by IA.CE_AUTH, and it does not permit the interference by the unauthorized subject.
IA.PASS maintains the CE authentication domain that is provided the function to change the CE password or administrator password by only the CE who is authenticated by IA. CE_AUTH, and it does not permit the interference by the unauthorized subject.

IA.PASS maintains the administrator domain that is provided the function to change the administrator password by only the administrator who is authenticated by IA.ADM_AUTH, and it does not permit the interference by the unauthorized subject.
MNG.MODE maintains the administrator authentication domain that is provided the function to set the security strengthen mode by only the administrator who is authenticated by IA.ADM_AUTH, and it does not permit the interference by the unauthorized subject.
MNG.HDD maintains the administrator authentication domain that is provided the function to change the HDD lock password by only the administrator who is authenticated by IA.ADM_AUTH, and it does not permit the interference by the unauthorized subject.

8.3.2. Rationale for Strength of Security Functions

As described in "6.2 Strength of Security Functions", SOF-Basic is claimed for the password mechanism of the identification authentication function (IA.ADM_AUTH, IA_CE_AUTH, IA_ADM_ADD, and IA.PASS) and the management support function (MNG_HDD). As described in "5.3 Strength of Security Functions", the minimum strength of function claims SOF-Basic for the security functional requirements and it is consistent with SOF-Basic that is claimed in "6.2 Strength of Security Functions".

8.3.3. Rationale for Assurance Measures

In section "6.3 Assurance Measures", the assurance measures are corresponded to all the TOE security assurance requirements required by EAL3. In addition, it covers all evidences required by TOE security assurance requirements regulated by this ST, by the related rules shown in the assurance measures.

Therefore, TOE security assurance requirements in EAL3 are realized.

8.4. PP Claim Rationale

There is no applicable PP in this ST.