Panasonic

Data Security Kit
DA-SC03

Security Target

Version 1.03 July 27, 2006

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

Panasonic Communications Co., Ltd.

Revision History

Version	Date	Page	Description	Revised By
1.00	2006.3.31	All pages	First version	Inohara
1.01	2006.5.29	—	Responded to ASE002-006, etc.	Inohara
1.02	2006.6.28	—	Responded to ASE007-009, ADV001, etc.	Inohara
1.03	2006.7.27	—	Responded to ASE010	Inohara

Contents

1. ST Introduction

1.1. ST Identification

1.1.1. ST Identification and Management

Title:	Data Security Kit DA-SC03 Security Target
Version:	1.03
Date:	July 27,2006
Creator:	Panasonic Communications Co., Ltd.

1.1.2. TOE Identification and Management

Title:	Japan:	Data Security Kit DA-SC03 (in Japanese)
	Overseas:	Data Security Kit DA-SC03
Version:	V1.01	
Creator:	Panasonic Communications Co., Ltd.	

The Data Security Kit DA-SC03 (in Japanese) for Japan and the Data Security Kit DA-SC03 for Overseas are the identical contents, with only different names.

1.1.3. Used CC Version

Common Criteria for Information Technology Security Evaluation,Version2.3,August 2005
Common Criteria for Information Technology Security Evaluation, Version2.3 (Translation Version 1.0)
Interpretation-0512(in Japanese)

1.2. ST Overview

1.2.1. Function Overview

This Security Target describes the security-related specifications of Data Security Kit DA-SC03, which is an optional product of Digital Imaging System DP-2330 / 3030 manufactured by Panasonic Communications Co., Ltd.
Data Security Kit DA-SC03 is a software product to protect the used document data which had been already stored on the hard disk drive after being processed by Digital Imaging System from being disclosed illicitly.

1.2.2. Evaluation Assurance Level

EAL2 conformant

1.2.3. Applicable PP

There is no applicable Protection Profile.

1.2.4. Related Security Target

There is no related Security Target.

1.3. CC Conformance

This TOE conforms to the following CCs.

- CC Version 2.3 Part 2 extension
- CC Version 2.3 Part 3 conformant

1.4. Terminology

The terminology used in this document is described in Table 1.

Table 1 Terminology

Terminology	Description
Internal Network	The LAN used in the organization where the Digital Imaging System DP-2330 / 3030 is introduced.
External Network	The networks other than the Internal Network, such as internet.
USB	A data transmission standard which connects peripherals to a personal computer.
Tandem Copy	A printing function whereby half of the specified number of copies for the data captured from the scanner are printed by the Digital Imaging System DP-2330 / 3030 that captured the data, and the other half are printed on the other Digital Imaging System DP-2330 / 3030 that is connected in the Internal Network.
Remote Copy	A printing function whereby all the data captured from the scanner are printed on some other Digital Imaging System DP-2330 / 3030.
General User	One who uses copy, printer, scanner or facsimile functions of Digital Imaging System DP-2330 / 3030.
Key operator	One who manages a Digital Imaging System DP-2330 / 3030.
Service Technician	A technician who belongs to the service provider company to provide installation, maintenance and repair services of Digital Imaging System DP-2330 / 3030.
Service Mode	A set of maintenance functions that the service technician uses for installation, maintenance and repair services of Digital Imaging System DP-2330 / 3030.
Service Mode Setting Procedure	The setting procedure that a service technician uses to switch the mode to Service Mode.
Initialization	Operation to go back to the initial setting activated by a Maintenance Management function "System Initialization".
Control Panel	Operation Panel with keys, LEDs and a touch panel display required for operating the functions of Digital Imaging System DP-2330 / 3030.
SPC	PCB to control the mechanical function of scanner and printer unit.
FROM	Nonvolatile memory allowing electrical block erasure and reprogramming of arbitrary portion.
Document Data	Collective name for all digitized image data handled inside digital imaging system when copy, print, scanner or facsimile functions are used in Digital Imaging System DP-2330 / 3030. - Image data captured from scanner unit. - Image data that can be printed on printer unit. - Image data that have been transformed from the raw data by image processing technology. - Image data received from client PCs or the received data to be transformed to image data.
Used Document Data	Document Data that is stored on the hard disk drive of the Digital Imaging System DP-2330 / 3030 and had already been used.
Job	A unit of operations comprising of a series of functions in copy, printer, scanner or facsimile functions of Digital Imaging System DP-2330 / 3030.
Job Cancellation	Canceling function issued from Control Panel to cancel some of the jobs that have not been started with printing yet on the printer unit, after multiple jobs have been assigned to Digital Imaging System DP-2330 / 3030 that is being used for copying or printing.
Accepting Sound	Panel touch tone peep sounding notifying that the input characters or operations from control panel have been accepted correctly in Digital Imaging System DP-2330 / 3030.
Alert Sound	Panel touch tone peep sounding three times notifying that the input characters or operations from control panel of Digital Imaging System DP-2330 / 3030 have been found to be incorrect.

1.5. Reference

- Common Criteria for Information Technology Security Evaluation
  Part1: Introduction and general model August 2005 Version 2.3 CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation
  Part2: Security functional requirements August 2005 Version 2.3 CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation
  Part3: Security assurance requirements August 2005 Version 2.3 CCMB-2005-08-003
- Interpretations-0512 (in Japanese)
- ISO/IEC 15408:2005 Information Technology –Security techniques-Evaluation criteria for IT Security –Part1
- ISO/IEC 15408:2005 Information Technology –Security techniques-Evaluation criteria for IT Security –Part2
- ISO/IEC 15408:2005 Information Technology –Security techniques-Evaluation criteria for IT Security –Part3

2. TOE Description

2.1. Type of TOE

TOE is a software product, Data Security Kit DA-SC03 installed in the digital imaging system, to protect the used document data which had been already stored on the hard disk drive after being processed by the digital imaging system from being disclosed illicitly.

TOE is offered as an optional product of Panasonic Communications Co., Ltd. Digital Imaging System DP-2330 / 3030, and provides the security functions by replacing with the standard bundled software of the digital imaging system.

2.2. Usage Environment of TOE

Digital Imaging System DP-2330 / 3030 is a digital imaging system with network function, offering not only copy, printer, scanner and facsimile functions, but also the functions to manage the operations as well as the maintenance for the machine.

Digital Imaging System DP-2330 / 3030 is assumed to be used, as shown in the Fig.1 Assumed Usage Environment, in the condition where the system is connected to internal network of offices or public facilities, public telephone line network, or locally to the client PC.

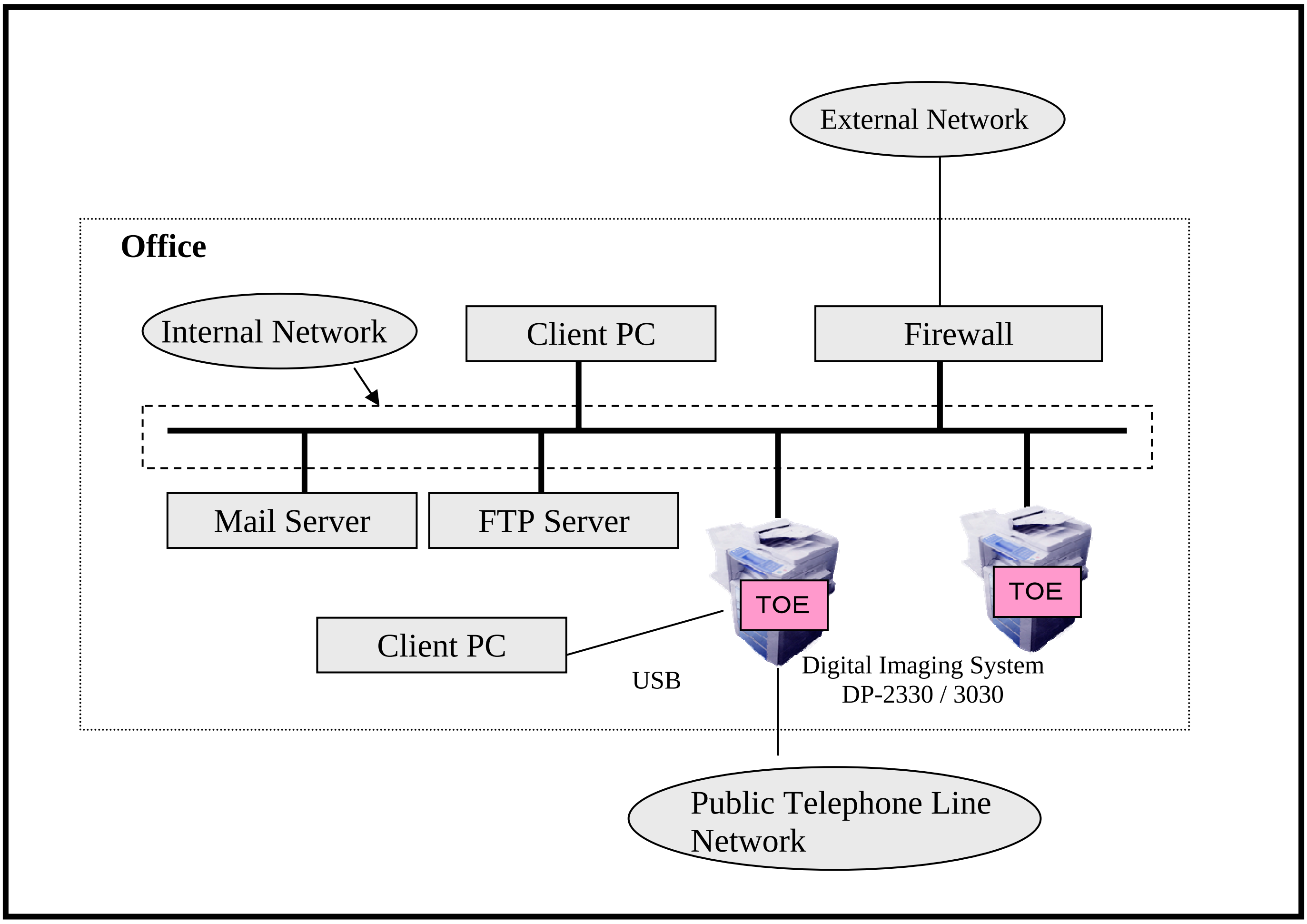

Fig. 1 Assumed Usage Environment

Digital Imaging System DP-2330 / 3030 is connected to general user's client PCs, FTP servers and Mail servers by Internal Network, and performs such operations as printing the document data received from Client PCs or Mail servers, and sending the document data captured from scanner to Client PCs, FTP servers and Mail servers.

Digital Imaging System DP-2330 / 3030 can also be connected to other Digital Imaging System DP-2330 / 3030 by Internal Network, and is used for tandem copy as well as remote copy whereby the document data captured from a scanner of one digital imaging system is printed by the other digital imaging system.

The system can also be connected locally to a general user's client PC (through USB) and used as a printer.

When connected to External Network, the connection is done via firewall to protect the various machines connected to Internal Network.

TOE is a software product installed on the Digital Imaging System DP-2330 / 3030 to protect the used document data which had been already stored on the hard disk drive after being processed by digital imaging systems from being disclosed illicitly.

2.3. Persons Related to TOE

Following are the persons related to Digital Imaging System DP-2330 / 3030 with TOE installed.

(1) General User

General users are the ones who use the general functions of Digital Imaging System DP-2330 / 3030, such as copy, printer, scanner and facsimile.

(2) Key operator

The machine administrator called key operator is to perform operating management using the operating management functions offered by Digital Imaging System DP-2330 / 3030.

Key operator is appointed by the person in charge of Digital Imaging System DP-2330 / 3030.

(3) Person in charge

Person in charge is the one who is in charge of introducing Digital Imaging System DP-2330 / 3030, and appoints and manages the Key operator.

(4) Service technician

The service technician provides installation, maintenance and repair services, using the maintenance and management functions offered by Digital Imaging System DP-2330 / 3030.

Service technicians belong to the company which undertakes the maintenance of Digital Imaging SystemDP-2330 / 3030.

2.4. Configuration of TOE

2.4.1. Physical Configuration

The physical configuration of Digital Imaging System DP-2330 / 3030 with TOE installed is shown in Fig. 2.

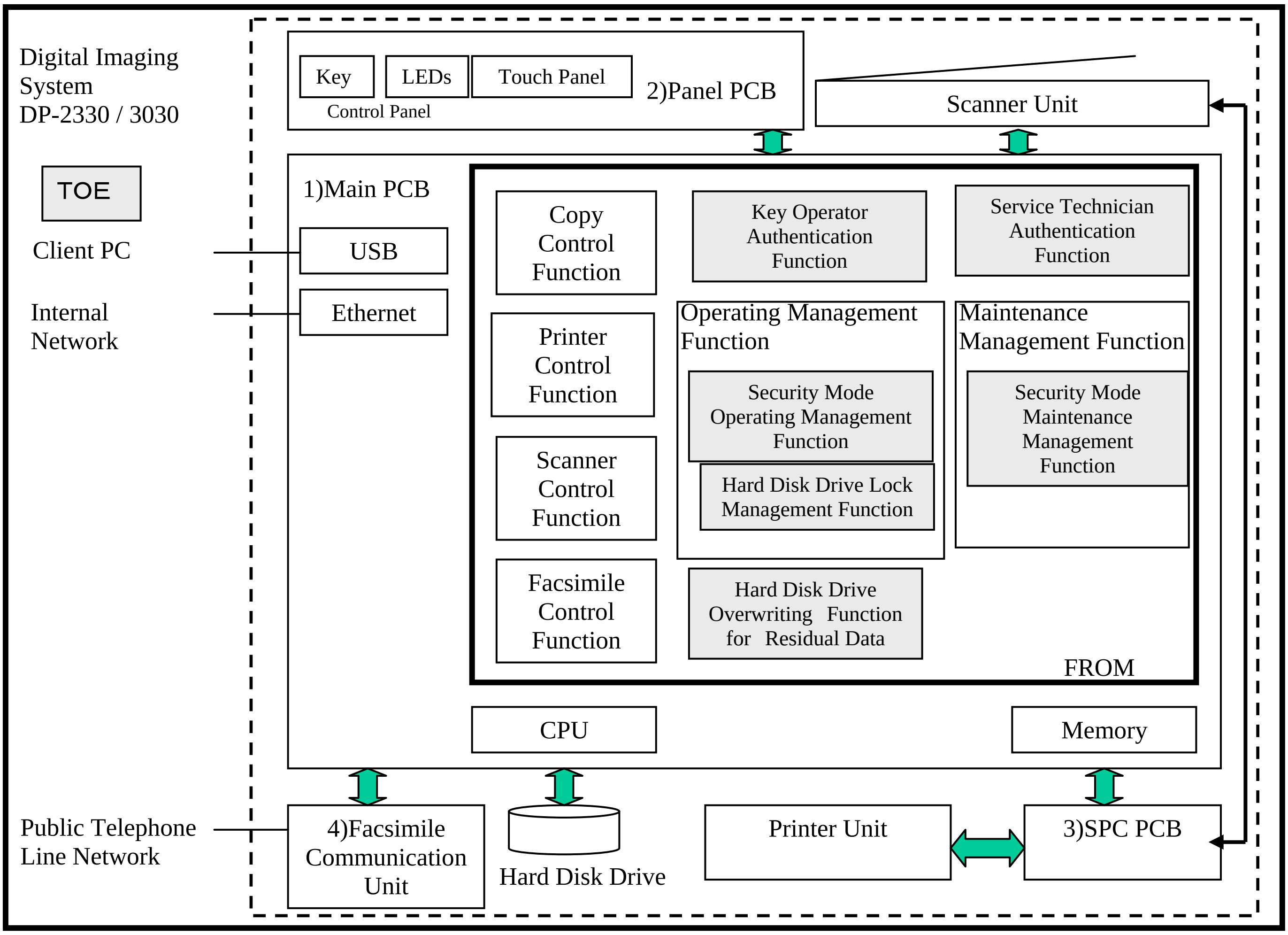
Digital Imaging System DP-2330 / 3030
TOE
Client PC
Internal Network
Public Telephone Line Network
Key
LEDs
Touch Panel
Control Panel
2)Panel PCB
Scanner Unit
1)Main PCB
USB
Ethernet
Copy Control Function
Key Operator Authentication Function
Service Technician Authentication Function
Printer Control Function
Operating Management Function
Security Mode Operating Management Function
Hard Disk Drive Lock Management Function
Maintenance Management Function
Security Mode Maintenance Management Function
Scanner Control Function
Facsimile Control Function
Hard Disk Drive Overwriting Function for Residual Data
FROM
CPU
Memory
4)Facsimile Communication Unit
Hard Disk Drive
Printer Unit
3)SPC PCB

Fig. 2 Physical Configuration of Digital Imaging System DP-2330 / 3030 and TOE

Digital Imaging System DP-2330 / 3030 comprises of four PCBs, which are: 1) Main PCB to control the entire digital imaging system, 2) Panel control PCB that controls the control panel where all the necessary keys, LEDs and a touch panel for operations of digital imaging system are laid out, 3) SPC PCB that controls the mechanical operations of scanner unit and printer unit, and 4) PCB for facsimile communication unit.

1) Main PCB and 2) Panel PCB are connected by Internal Interface for communicating the control data.

1) Main PCB and 3) SPC PCB are connected by Internal Interface for communicating the control data and the document data.

3) SPC PCB performs the communication of control data with scanner unit to control the mechanical motion of scanner. The document data captured from the scanner are sent directly to 1) Main PCB. Also 3) SPC PCB exchanges the control data and

document data with printer unit, and prints document data while executing the mechanical controls of the printer.

1) Main PCB and 4) Facsimile Communication Unit are connected to each other by Internal Interface, and 4) Facsimile Communication Unit is further connected to Public Telephone Line Network to send/receive facsimile data.

Furthermore, 1) Main PCB has the Ethernet and USB interface to connect to Client PCs and Mail/FTP servers. Also, the hard disk drive unit to store the document data is connected to 1) Main PCB.

1) Main PCB comprises of CPU, FROM that stores software, Memory that stores data and other electronic circuits to control the entire digital imaging system.

TOE is a group of software recorded on FROM that is mounted on Main PCB and is shown in the shaded portion of Fig. 2, namely:

- Key Operator Authentication Function
- Service Technician Authentication Function
- Security Mode Operating Management Function
- Security Mode Maintenance Management Function
- Hard Disk Drive Lock Management Function
- Hard Disk Drive Overwriting Function for Residual Data

TOE is to protect the used document data which had been already stored on the hard disk drive after being processed by copy, printer, scanner functions, from being disclosed illicitly.

2.4.2. Functions of Digital Imaging System

Digital Imaging System DP-2330 / 3030 provides general users with copy, printer, scanner and facsimile functions.

(1) Copy Function

The function is to capture the document data from scanner and to print the data on printer unit.

There are several copy functions depending upon how the document data are stored temporarily on the hard disk drive, as shown below.

- Non-sort Copy Function:

  Non-sort copy refers to the manner of output of, for example, 2 copies of a 3 page document in the printing order of P1, P1, P2, P2, P3, P3. The document data captured from the scanner is stored on the hard disk drive, and then read out from the hard disk to be printed in the non-sort order.
- Sort Copy Function:

  Sort copy refers to the manner of output of, for example, 2 copies of a 3 page document in the printing order of P1, P2, P3, P1, P2, P3. The document data captured from the scanner is stored on the hard disk drive, and then read out from the hard disk drive to be printed in the sort order.
- Tandem Copy Function:

  A printing function whereby document data are captured from the scanner to be stored on the hard disk drive and a half of the specified number of copies are printed by the Digital Imaging System DP-2330 / 3030 that captured the data, and the other half are printed on the other Digital Imaging System DP-2330 / 3030 that is connected in the Internal Network. The document data received from the Internal Network is also stored on the hard disk drive, and then read out from the hard disk drive to be printed so as to harmonize the printing speed.
- Remote Copy Function:

  A printing function whereby the document data are captured from the scanner to be stored on the hard disk drive, and then all the data are printed on some other Digital Imaging System DP-2330 / 3030 connected in the Internal Network. The document data received from the Internal Network is also stored on the hard disk drive, and then read out from the hard disk drive to be printed so as to harmonize the printing speed.
- Overlay Function:

  A printing function whereby the first page of the document data captured from the scanner is stored on the hard disk drive, and is printed with the second page and all other pages captured thereafter from the scanner, as the overlay manner.
- File Editing Function:

  The function allows the document captured from the scanner to be stored on the hard disk drive, registered with a document name called image title, and the document name be changed or deleted. The function is used when the registered document data and the document data captured from the scanner are overlay printed.

(2) Printer Function

The function is to print the document data received from a Client PC of a general user, on the printer unit.

On the Client PC of the general user, the dedicated printer driver software for the Digital Imaging System DP-2330 / 3030 is need to be installed.

Under the printer function, the received document data are temporarily stored on the hard disk drive. While in the usual printer function, the received document data are printed as soon as the internal processing within the imaging system is completed, following functions allow the document data to be preserved on the hard disk drive until the printing instructed from the control panel by the general user is completed.

- Mailbox Function:

  The received document data is stored on the hard disk drive, and is printed only when the user ID is input from the control panel of Digital Imaging System DP-2330 / 3030.
- Securitybox Function:

  The received document data is stored on the hard disk drive, and is printed only when the user ID and the correct password are input from the control panel of Digital Imaging System DP-2330 / 3030.

(3) Scanner Function

The document data captured from the scanner is temporarily stored on the hard disk drive, and then sent to a Client PC or an FTP server.

To be able to send the data to a Client PC, the accessory software Panasonic Communication Utility of Panasonic Document Management System must be installed and running on the Client PC.

(4) Facsimile Function

Facsimile Function is the collective name for the entire G3 communication, Internet FAX and E-mail functions.
G3 communication is to send the document data captured from the scanner unit to facsimile terminals over the public telephone line network, and receive the document data from facsimile terminals over the public telephone line network and print on the printer unit.
Internet FAX function is to send the document data captured from the scanner unit to a Mail server to be further sent to internet FAX terminals connected to internet, and receive the document data from internet FAX terminals via a Mail server and print it.
E-mail function is to send the document data captured from the scanner to the specified E-mail address with an E-mail attached, via a Mail server.
With the Facsimile Function, there is no document data temporarily stored on the hard disk drive.

The functions to control Digital Imaging System DP-2330 / 3030 to achieve above copy, printer, scanner and facsimile functions are called copy control function, printer control function, scanner control function and facsimile control function respectively.

(5)Maintenance Management Function

This function is also called service mode which is only operable by the service technicians, and can direct such works as installation, maintenance and repair of Digital Imaging System DP-2330 / 3030 from the control panel. The major functions include self testing function of all LEDs lighting up on the control panel, operating test function such as single copy and serial copy, parameter setting such as switching of power frequency, and software update function.
Although Maintenance Management Function itself does not have the function to access to the document data stored on hard disk drive, it has the function called “System initialization” which resets the setting of TOE data described in 2.4.3. Logical Configuration (6) Security Mode Maintenance Management Function, to the initial values.

(6)Operating Management Function

This function is only operable by the key operator, and can change the setting regarding the operations of Digital Imaging System DP-2330 / 3030 from the control panel. The major functions include setting of low power mode, date and time setting, and network settings, and can also set the "Mailbox Data Holding" for the Mailbox and Securitybox described in (2) Printer Function, or direct "Delete Mailbox Data"
Although the Operating Management Function does not have the function to access to the document data stored on the hard disk drive, it has the formatting function to create management information to make the hard disk drive usable. The (3) Hard Disk Drive Lock Management Function and (4) Security Mode Operating Management Function described in 2.4.3. Logical Configuration are also part of the Operating Management Function.

(7) Hard Disk Drive Function

The hard disk drive unit of Digital Imaging System DP-2330 / 3030 has the drive lock function attached whereby the password can directly be assigned to the hard disk drive so that the hard disk drive cannot be recognized unless the correct password is entered. Once the hard disk drive receives the setting command of "Hard Disk Drive Lock Password" using the (3) Hard disk drive lock management function described in 2.4.3. Logical Configuration, it accepts the access from the Digital Imaging System DP-2330 / 3030 only when the password matches with the one that is retained in the drive unit. Also the hard disk drive unit has the function to reset the password that was set in the hard disk drive to "unsetup" condition, when the lock password matches.

2.4.3. Logical Configuration

The logical configuration of Digital Imaging System DP-2330 / 3030 with TOE installed is shown in Fig. 3.

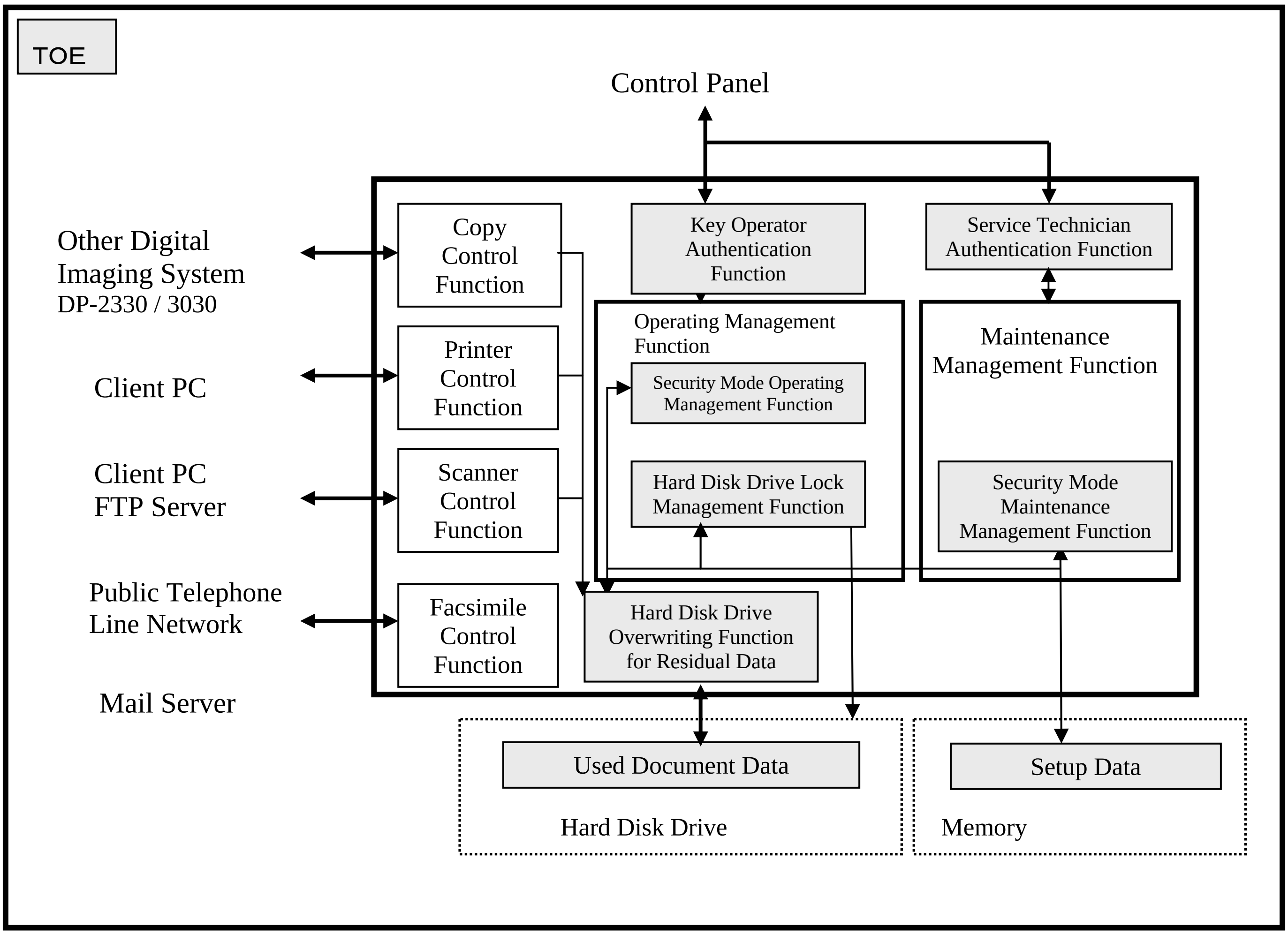
TOE
Control Panel
Other Digital Imaging System DP-2330 / 3030
Client PC
Client PC FTP Server
Public Telephone Line Network
Mail Server
Copy Control Function
Printer Control Function
Scanner Control Function
Facsimile Control Function
Key Operator Authentication Function
Service Technician Authentication Function
Operating Management Function
Security Mode Operating Management Function
Hard Disk Drive Lock Management Function
Maintenance Management Function
Security Mode Maintenance Management Function
Hard Disk Drive Overwriting Function for Residual Data
Used Document Data
Hard Disk Drive
Setup Data
Memory

Fig. 3 Logical Configuration of Digital Imaging System DP-2330 / 3030 and TOE

Digital Imaging System DP-2330 / 3030, with the TOE installed, stores document data temporarily on the hard disk drive to perform copy, printer or scanner function. This temporary document data becomes a set of used document data as shown in Table 2 “Patterns of Used Document Data Development”, and will be erased as soon as they are finished with usage.
Usually in the electronic equipments using hard disk drive, the deletion of data in the hard disk drive means to delete the data management information only, and the entire data area of the corresponding data is not erased.
Therefore when the hard disk drive are stolen, replaced or discarded, the used document data of general users are still remaining, and it is possible to retrieve the used document data from the hard disk drive using a PC or some other tools.
To deal with this problem, The TOE provides the following security functions to protect the used document data which had been already stored on the hard disk drive.

(1) Hard Disk Drive Overwriting Function for Residual Data

When the document data is processed by copy control function, printer control function or scanner control function, and becomes used document data, this function immediately and automatically overwrites and erases the entire area of the document data.
There are following three overwriting and erasing methods.

- Basic: Only the management information for the document data is deleted.
- Medium: Over the entire area of the document data, the data of all 0's are overwritten three times for erasure.
- High: Over the entire area of the document data, random values are overwritten twice and then all 0's are overwritten once for erasure.

This overwriting and erasing method is specified in the "Hard Disk Data Erasure Level" described in (4) Security Mode Operating Management Function.
Since "Basic: Only the management information for the document data is deleted" is the initial setting, the key operator normally selects Medium or High to operate the Digital Imaging System DP-2330 / 3030.
Note that only the key operator can use the "Hard Disk Initialization" function which is described in (4) Security Mode Operating Management Function, to overwrite and erase the residual document data on the hard disk drive by either Medium or High, in such cases as the drives are discarded.

(2) Key Operator Authentication Function

This function is key operator identification and authentication, by means of the input to the control panel and the entered dedicated password for key operator (hereinafter called key operator password). Only the key operator can perform operations described in (3) Hard Disk Drive Lock Management Function and (4) Security Mode Operating Management Function.

(3)Hard Disk Drive Lock Management Function

The hard disk drive unit has the drive lock function attached whereby the password can directly be assigned to the hard disk drive so that the hard disk drive cannot be recognized unless the correct password is entered. Only the key operator can set up and change the password for the memory inside the digital imaging system controlling the "Hard Disk Drive Lock Password" and the hard disk drive, and also reset the drive lock setting the password to "unsetup" condition. At its startup time, the digital imaging system sends the password stored in the memory inside the system to the hard disk drive, requesting the data access to it.

(4) Security Mode Operating Management Function

Only the key operator can direct following setup and change of setting data and processing regarding the security.

- "Hard Disk Data Erasure Level"
  This function specifies the erasing mode of overwriting data for residual data stored on the hard disk drive, which is automatically executed at the instant when the copy control function, printer control function or scanner control function is completed and the used document data develops.
  It can set up three types of overwriting and erasing, Basic (initial setting), Medium and High.
- "Hard Disk Initialization"
  Upon the direction from key operator, this function overwrites and erases all document data stored on the hard disk drive. As the ways to overwrite and erase, there are two types, Medium and High.
- "Key Operator Password"
  This function is to set up and change the key operator password.

(5) Service Technician Authentication Function

This function is service technician identification and authentication by the operations of service mode setup procedure from the control panel as well as the entered password. Only the service technician is allowed for operations described in (6) Security Mode Maintenance Management Function.

(6) Security Mode Maintenance Management Function

Only the service technician can direct the setup, change and initialization (returning to the initial setting) for the following setup data regarding the security.

- "Service Technician Password"
  Sets up and changes the service technician password.
- "System Initialization"
  Under the direction from the service technician, this function is to initialize such setup data as "Hard Disk Drive Lock Password" described in (3) Hard Disk Drive Lock Management Function, "Hard Disk Data Erasure Level" and "Key Operator Password" described in (4) Security Mode Operating Management Function, "Service Technician Password" described in (6) Security Mode Maintenance Management Function, to the initial setting.

The security related setting data, "Hard Disk Drive Lock Password", "Hard Disk Data Erasure Level", “Key Operator Password” and "Service Technician Password" are stored in the memory.
"System Initialization" is to initialize the contents set up in the memory mounted on the Main PCB, which is usable at the time of repair or disposal of Digital Imaging System DP-2330 / 3030, to the initial setting, the condition of shipment from the factory. Since the initial setting of "Hard Disk Data Erasure Level" is "Basic", the data area of residual used document data stored on the hard disk drive cannot be overwritten and erased. Since “System initialization” only initialize the setup data of "Hard Disk Drive Lock Password", and will not send the setup command to the hard disk drive, "System initialization" only will not allow reading the residual data stored on the hard disk drive. Since the setup data of "Key Operator Password" and "Service Technician Password" are also initialized, reconfiguring the setup for these data will be necessary at the time of "System initialization."

At the time of installing a Digital Imaging System DP-2330 / 3030 with TOE installed, when the "System initialization" Is executed:

A service technician, after entering the initial setting data of service technician Password and being authenticated, will

- change the "Service Technician Password"

A key operator, after entering the initial setting data of key operator Password from the control panel and being authenticated, will

- set up the "Hard Disk Data Erasure Level" to Medium or High
- at the installation time, set up the "Hard Disk Drive Lock Password"
  at the execution time of "System Initialization", set up again the "Hard Disk Drive Lock Password" that was set up in the hard disk drive
- change "Key Operator Password"

before using TOE and operating it.

Table 2 Patterns of Used Document Data Development

Function Name	Development Pattern
Copy Function(*)	When a general user is using the non-sort copy (e.g. printing 2 copies of a 3 page document in the order of P1, P1, P2, P2, P3, P3) by directing from the control panel, the used document data develops at the point when each page is finished with printing.
	When a general user is using the sort copy (e.g. printing 2 copies of a 3 page document in the order of P1, P2, P3, P1, P2, P3) by directing from the control panel, the used document data develops at the point when the entire printing is finished.
	When a general user uses the remote copy directing from the control panel, the captured document data becomes the used document data at the point when all data is finished with being transferred to the other digital imaging system.
	During the above sort copy and non-sort copy operations, the data becomes the used document data at the point when the general user directs cancel printing from the control panel.
	During the above sort copy and non-sort copy operations, the data becomes the used document data at the point when the general user directs job cancellation from the control panel.
	During file editing, a document data becomes used data at the time when a general user directs erasure of the registered document data from the control panel.
Printer Function	During the print function being initiated by a general user from a Client PC, the document data becomes used data when each page is finished with printing for the non-sort copying, and when the entire printing is finished for the sort copying.
	The document data received from a Client PC where a general user directed Mailbox transaction becomes used data at the point when the receiving user(s) complete all printings after entering the user IDs from the control panel.
	The document data received from a Client PC where a general user directed Securitybox transaction becomes used data at the point when the receiving user(s) complete all printings after entering the user IDs and password(s) from the control panel.
	During printing operations using printing functions, the data becomes the used document data at the point when the general user directs cancel printing from the control panel.
	During printing operations using printing functions, the data becomes the used document data at the point when the general user directs job cancellation from the control panel.
	The document data preserved in the Mailbox or Securitybox becomes used document data at the point when the "Mailbox Data Holding" set up by the key operator using Operating Management Function expires.
	The document data preserved in the Mailbox or Securitybox becomes used document data at the point when the "Delete Mailbox Data" is directed by the key operator using Operating Management Function.
Copy/ Printer Function	In the copy operation directed from the control panel by a general user, or in the printing operation directed from a Client PC by a general user, if the printing is suspended by such events as paper jam, the document data temporarily stored on the hard disk drive becomes used data at the point when each page is finished with printing for the non-sort mode, and entire printing is finished for the sort mode, after recovering from the suspension.
Scanner Function	When a general user uses the scanner function directing from the control panel, the captured document data becomes the used document data at the point when all data is finished with being transferred to the Client PC or FTP server.
	When a general user uses the scanner function directing from the control panel, the captured document data becomes the used document data at the point when the data transfer to the Client PC or FTP server fails by some error.
	The document data captured from the scanner becomes used data at the point when the general user directs canceling from the control panel during the capturing operation.

(*) With regards to the tandem copy, remote copy and overlay copy, the same patterns of used document data development as non-sort copy and sort copy are included in the non-sort copy and sort copy respectively in this table.

2.5. Assets Protected by TOE

The assets protected by TOE are the used document data which had been already stored on the hard disk drive of Digital Imaging System DP-2330 / 3030 after being processed by the digital imaging system.

3. TOE Security Environment

3.1. Assumptions

The assumptions of performance, operations and uses for this TOE are shown in Table 3.

Table 3 Assumptions

Assumptions	Description
A.SETSEC	- Security Mode setting Key operator enables following TOE functions before operations. "Hard Disk Drive Lock Password" is set up.
A.ADMIN	- Credibility of key operator Key operator is a person who commits no illicit acts.
A.SE	- Credibility of service technician Service technician is a person who commits no illicit acts.

3.2. Threats

The threats that this TOE should counter are shown in Table 4.

Attacker is assumed to have general knowledge of IT and Digital Imaging Systems, and have the low level of attacking ability using the information and tools that are easily available.

Table 4 Threats

Threats	Description
T.RECOVER	- Illicit recovery of used document data General users or the non-related persons to TOE having malicious intention may attempt to recover the used document data by connecting PC or other tools to hard disk drive.

3.3. Organizational Security Policies

The organizational security policies that this TOE is requested to follow are shown in Table 5.

Table 5 Organizational Security Policies

Organizational Security Policies	Description
P.OWMETHOD	- The used document data remaining on the hard disk drive to be overwritten and erased. The data area of used document data remaining on the hard disk drive must be overwritten and erased.

4. Security Objectives

4.1. Security Objectives of TOE

The security objectives of TOE are shown in Table 6.

Table 6 Security Objectives of TOE

Security Objectives	Description
O.HDLMNG	TOE must disable the recovery of any used document remaining on the hard disk drive, by allowing only the authenticated key operator to set up the "Hard Disk Drive Lock Password" on the hard disk drive.
O.RESIDUAL	TOE must provide, in addition to the Basic level that has no overwriting and erasing operations, two types of hard disk drive overwriting function for residual data, the Medium and the High of "Hard Disk Data Erasure Level".

4.2. Security Objectives for IT Environment

The security objectives for TOE IT Environment are shown in Table 7.

Table 7 Security Objectives of TOE IT Environment

Security Objectives	Description
OE.AUTH	At all times other than maintenance services, key operator must use the Operating Management Function of Digital Imaging System DP-2330 / 3030, and set up and use Medium or High of "Hard Disk Data Erasure Level", and also "Hard Disk Drive Lock Password".
OE.ADMIN	To assure that the key operator performs no illicit acts, the person in charge must appoint the right person for the key operator, and also provide adequate administrations and educations so that the key operator can execute the required jobs and acquire necessary knowledge.
OE.SE	When a service technician is to be engaged with maintenance works for Digital Imaging System DP-2330 / 3030, person in charge or key operator must confirm that the technician is the employee of the company which undertakes the maintenance of the Digital Imaging System.
OE.HDD	Hard disk drive protects the used residual document data stored on the hard disk drive from illicit accesses by Hard Disk Drive Lock Password.

5. IT Security Requirements

5.1. TOE Security Functional Requirements

The requirements here specify the security functional requirements provided by TOE.

5.1.1. Class FDP: User Data Protection

FDP_RIP.1 **Subset Residual Information Protection**

Hierarchical to: No other components.

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]
-Hard disk drive on which used document data are stored

Dependencies: No dependencies.

5.1.2. Class FIA: Identification and Authentication

FIA_AFL.1(1) **Authentication failure handling**

Hierarchical to: No other components.

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]. (Note)

[assignment: list of authentication events]
-Key Operator Authentication Function
[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]](Note)
-1

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]
-Withholding authentications for more than one second.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1(2) **Authentication failure handling**

Hierarchical to: No other components.

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]. (Note)

[assignment: list of authentication events]
-Service Technician Authentication Function
[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]] (Note)
-1

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]
-Withholding authentications for more than one second.

Dependencies: FIA_UAU.1 Timing of authentication

(Note) The relationship among [, ", "and] is different from the Common Criteria Version 2.3 (Translation Version 1.0) for IT Security Evaluation.

FIA_SOS.1(1) Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1(1) The TSF shall provide a mechanism to verify that secrets meet[assignment: a defined quality metric] .

Refinement: Secret -> Key operator password

[assignment: a defined quality metric]

The quality metric of key operator password is defined as follows.

- Character length fixed to 8
- Upper case alphabets, lower case alphabets, numerals, symbols
- A string of same 8 characters is prohibited.

Dependencies: No dependencies.

FIA_SOS.1(2) Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1(2) The TSF shall provide a mechanism to verify that secrets meet [assignment: a defined quality metric] .

Refinement: Secret -> Service technician password

[assignment: a defined quality metric]

The quality metric of service technician password is defined as follows.

- Character length fixed to 8
- Upper case alphabets, lower case alphabets, numerals, symbols
- A string of same 8 characters is prohibited.

Dependencies: No dependencies.

FIA_UID.2(1) User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1(1) The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Refinement: User -> Key operator

Dependencies: No dependencies.

FIA_UID.2(2) User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1(2) The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Refinement: User -> Service technician

Dependencies: No dependencies.

FIA_UAU.2(1) User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1(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 -> Key operator

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2(2) User authentication before any action

Hierachical to : FIA_UAU.1

FIA_UAU.2.1(2) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Refinement: User -> Service technician

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.7(1) Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1(1) The TSF shall provide only [assignment: list of feedback] to the user while the authentication is in progress.

[assignment: list of feedback]

-For every entered character as the key operator password, one * is displayed at a time.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7(2) **Protected authentication feedback**
Hierarchical to: No other components.
FIA_UAU.7.1(2) The TSF shall provide only [assignment: list of feedback] to the user while the authentication is in progress.

[assignment: list of feedback]
-For every entered character as the service technician password, one * is displayed at a time.
Dependencies: FIA_UAU.1 Timing of authentication

5.1.3. Class FMT: Security Management

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 authorised identified roles].

[assignment: list of functions]
- Hard Disk Drive Overwriting Function for Residual Data

[selection: determine the behavior of, disable, enable, modify the behavior of]
- Determine the behavior of
- Disable
- Enable

[assignment: the authorised identified roles]
-Key operator, Service technician

The relationship between the roles and the selectable abilities of Hard Disk Drive Overwriting Functions for Residual Data is shown in Table 8.

Table 8 Relationship between the roles and the selectable abilities of Hard Disk Drive Overwriting Functions for Residual Data

Roles \ Abilities	Hard Disk Drive Overwriting Function for Residual Data
Key operator	Determines the behavior of the functions Disables the functions Enables the functions
Service technician	Disables the functions

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MTD.1(1) **Management of TSF data**
Hierarchical to: No other components.
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]
- "Hard Disk Data Erasure Level"
Basic: Only the management information for the document data is deleted (initial setting).
Medium: Over the entire area of the document data, the data of all 0's are overwritten three times for erasure.
High: Over the entire area of the document data, random data are overwritten twice and then all 0's are overwritten once for erasure.

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

[assignment: the authorised identified roles]
-Key operator, Service technician

The relationship between the roles and the selectable abilities of "Hard Disk Data Erasure Level" is shown in Table 9.

Table 9 Relationship between the roles and the selectable abilities of "Hard Disk Data Erasure Level"

Ability / Role	"Hard Disk Data Erasure Level"			
	Query	Modify		
		Basic	Medium	High
Key operator	○	○	○	○
Service technician	×	○	×	×

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MTD.1(2) **Management of TSF data**

Hierarchical to: No other components.

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]
- "Key Operator Password"

[selection: change_default, query, modify, delete, clear, [assignment: other operations]]
- modify, other operations: initialization (operation to return to the initial setting)

[assignment: the authorised identified roles]
-Key operator, Service technician

The relationship between the roles and the selectable abilities of "Key Operator Password" is shown in Table 10.

Table 10 Relationship between the roles and the selectable abilities of "Key Operator Password"

Ability / Role	"Key Operator Password"	
	Modify	Other operations : Initialization
Key operator	○	×
Service technician	×	○

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(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]
- "Service Technician Password"

[selection: change_default, query, modify, delete, clear, [assignment: other operations]]
- modify, other operations: initialization (operation to return to the initial setting)

[assignment: the authorised identified roles]
-Service technician

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]
Functions to manage the management items described in Table 11.

Dependencies: No dependencies.

Table 11 Functions to Manage Management Items

Functional requirement	Management requirement	Management item and management function
FDP_RIP.1	Management of when to perform residual information protection	Since the timing to perform residual information protection is fixed to deallocation, there is no management item.
FIA_AFL.1(1)	Management of the threshold value for unsuccessful authentication attempt, and management of actions to be taken in the event of authentication failure	Since threshold value is fixed, and action is also fixed, there is no management item.
FIA_AFL.1(2)	Management of the threshold value for unsuccessful authentication attempt, and management of actions to be taken in the event of authentication failure	Since threshold value is fixed, and action is also fixed, there is no management item.
FIA_SOS.1(1)	Management of the metric used to verify the secrets	Since the metric is fixed, there is no management item.
FIA_SOS.1(2)	Management of the metric used to verify the secrets	Since the metric is fixed, there is no management item.
FIA_UID.2(1)	Management of user identification information	Since the user identification information is fixed, there is no management item.
FIA_UID.2(2)	Management of user identification information	Since the user identification information is fixed, there is no management item.
FIA_UAU.2(1)	Management of authentication data by key operator	Key operator password
FIA_UAU.2(2)	Management of authentication data by service technician	Service technician password
FIA_UAU.7(1)	No management requirements	—
FIA_UAU.7(2)	No management requirements	—
FMT_MOF.1	Management of the group of roles that can interact with the functions in the TSF	Since the roles of key operator and service technician are fixed, there is no management item.
FMT_MTD.1(1)	Management of the group of roles that can interact with the TSF data	Since the roles of key operator and service technician are fixed, there is no management item.
FMT_MTD.1(2)	Management of the group of roles that can interact with the TSF data	Since the roles of key operator and service technician are fixed, there is no management item.
FMT_MTD.1(3)	Management of the group of roles that can interact with the TSF data	Since the role of service technician is fixed to one person, there is no management item described here.
FMT_SMF.1	No management requirements	—
FMT_SMR.1	Management of the user group that is a part of the roles	Since the roles of key operator and service technician are fixed, there is no management item.
FPT_RVM.1	No management requirements	—
FIT_SOS.1	Management of the metric used to verify the secrets of IT environment	Since the metric is fixed, there is no management item.
FIT_MTD.1	Management of the group of roles that can interact with the Administrator data	Since the roles of key operator and service technician are fixed, there is no management item.

FMT_SMR.1 **Security roles**
Hierarchical to: No other components.
FMT_SMR.1.1 The TSF shall maintain the roles [assignment: the authorised identified roles].

[assignment: the authorised identified roles]
-Key operator, Service technician
FMT_SMR.1.2 The TSF shall be able to associate users with roles.
Dependencies : FIA_UID.1 Timing of identification

5.1.4. Class FPT: Protection of the TSF

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

5.1.5. New Security Functional Requirements

In this ST, new TOE Security Functional Requirements (FIT_SOS.1 Verification of secrets of IT Environment, FIT_MTD.1 Management of Administrator Data) are defined and used.

Administrator Data are the control data for IT environment security functions that can be accessed only by the key operator and the service technician.

FIT_SOS.1 Verification of secrets of IT Environment requires the TSF to verify that secrets of IT environment meet defined quality metrics.

Management: FIT_SOS.1
The following actions could be considered for the management functions in FMT:
a) the management of the metric used to verify the secrets of IT environment.

Audit: FIT_SOS.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.
a) Minimal: Rejection by the TSF of any tested secret of IT environment;
b) Basic: Rejection or acceptance by the TSF of any tested secret of IT environment;
c) Detailed: Identification of any changes to the defined quality metrics.

FIT_SOS.1 **Verification of secrets of IT Environment**
Hierarchical to: No other components.
FIT_SOS.1.1 The TSF shall provide a mechanism to verify that secrets of IT environment meet [assignment: a defined quality metric].

Refinement: secrets of IT environment -> "Hard Disk Drive Lock Password"
[assignment: a defined quality metric]
The quality metric of "Hard Disk Drive Lock Password" is defined as follows.
- Character string from 8 to 32 characters
- Upper case alphabets, lower case alphabets, numerals, symbols

Dependencies: No dependencies.

FIT_MTD.1 Management of Administrator Data allows authorised users to manage Administrator Data.

Management: FIT_MTD.1
The following actions could be considered for the management functions in FMT:
a) managing the group of roles that can interact with the Administrator Data.

Audit: FIT_MTD.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.
a) Basic: Basic: All modifications to the values of Administrator Data.

FIT_MTD.1 **Management of Administrator Data**
Hierarchical to: No other components.
FIT_MTD.1.1 The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of Administrator Data] to [assignment: authorised identified roles].

[assignment: list of Administrator Data]
- "Hard Disk Drive Lock Password"

[selection: change default, query, modify, delete, clear, [assignment: other operations]]
- modify, delete, other operations: initialization (operation to return to the initial setting)

[assignment: authorised identified roles]
-Key operator, Service technician

The relationship between the roles and the selectable abilities of "Hard Disk Drive Lock Password" is shown in Table 12.

Table 12 Relationship between the roles and the selectable abilities of "Hard Disk Drive Lock Password"

Roles Abilities	"Hard Disk Drive Lock Password"
Key operator	modify, delete
Service technician	Other operations : Initialization

"delete" refers to releasing the "Hard Disk Drive Lock Password."

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

5.2. TOE Security Assurance Requirements

The evaluation assurance level of TOE is EAL2.

The EAL2 assurance requirements are shown in Table 13.

Table 13 EAL2 Assurance Requirements

Assurance class	Assurance component ID	Assurance components	Dependencies
Configuration management	ACM_CAP.2	Configuration items	None
Delivery and operation	ADO_DEL.1	Delivery procedures	None
	ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1
Development	ADV_FSP.1	Informal functional specification	ADV_RCR.1
	ADV_HLD.1	Descriptive high-level design	ADV_FSP.1 ADV_RCR.1
	ADV_RCR.1	Informal correspondence demonstration	None
Guidance documents	AGD_ADM.1	Administrator guidance	ADV_FSP.1
	AGD_USR.1	User guidance	ADV_FSP.1
Tests	ATE_COV.1	Evidence of coverage	ADV_FSP.1 ATE_FUN.1
	ATE_FUN.1	Functional testing	None
	ATE_IND.2	Independent testing-sample	ADV_FSP.1 AGD_ADM.1 AGD_USR.1 ATE_FUN.1
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1 ADV_HLD.1
	AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1 ADV_HLD.1 AGD_ADM.1 AGD_USR.1

5.3. Security Functional Requirements for IT Environment

FIA_UID.2(IT) User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1(IT) The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Refinement: TSF -> Hard disk drive

Dependencies: No dependencies.

FIA_UAU.2(IT) User authentication before any action

Hierarchical to : FIA_UAU.1

FIA_UAU.2.1(IT) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Refinement: TSF -> Hard disk drive

Dependencies: FIA_UID.1 Timing of identification

5.4. TOE Security Function Strength

The minimum security functional strength of this TOE is SOF - Basic.

The functional requirements using probabilistic or permutational mechanism are:

- FIA_UID.2(1), FIA_UAU.2(1), FIA_UAU.7(1), FIA_AFL.1(1), FIA_SOS.1(1)
- FIA_UID.2(2), FIA_UAU.2(2), FIA_UAU.7(2), FIA_AFL.1(2), FIA_SOS.1(2)

And the strength of these indicated functional strength is SOF - Basic.

6. TOE Summary Specification

6.1. TOE Security Functions

TOE has following security functions.

- Hard Disk Drive Overwriting Function for Residual Data (SF.OVWRT)
- Key Operator Authentication Function (SF.ADM_IA)
- Hard Disk Drive Lock Management Function (SF.HDMNG)
- Security Mode Operating Management Function (SF.ADMMNG)
- Service Technician Authentication Function (SF.SE_IA)
- Security Mode Maintenance Management Function (SF.SEMNG)

The relationship between each TOE security and security functional requirements is shown in Table 14.

Table 14 Relationship between TOE Security Functions and Security Functional Requirements

*	SF.OVWRT	SF.ADM_IA	SF.HDMNG	SF.ADMMNG	SF.SE_IA	SF.SEMNG
FDP_RIP.1	○					
FIA_AFL.1(1)		○				
FIA_AFL.1(2)					○	
FIA_SOS.1(1)				○		
FIA_SOS.1(2)						○
FIA_UID.2(1)		○				
FIA_UID.2(2)					○	
FIA_UAU.2(1)		○				
FIA_UAU.2(2)					○	
FIA_UAU.7(1)		○				
FIA_UAU.7(2)					○	
FMT_MOF.1				○		○
FMT_MTD.1(1)				○		○
FMT_MTD.1(2)				○		○
FMT_MTD.1(3)						○
FMT_SMF.1				○		○
FMT_SMR.1				○		○
FPT_RVM.1	○	○	○	○	○	○
FIT_SOS.1			○			
FIT_MTD.1			○			○

* TOE security functions are shown horizontally, and security functional requirements are shown vertically.

6.1.1. Hard Disk Drive Overwriting Function for Residual Data (SF.OVWRT)

The purpose of this function is to overwrite and erase the data area of the residual document data stored on the hard disk drive.

There are following methods to overwrite and erase:

- Basic: Only the management information for the document data is deleted.
- Medium: Over the entire area of the document data, the data of all 0's are overwritten three times and erased.
- High: Over the entire area of the document data, random values are overwritten twice and then all 0's are overwritten once for erasing.

This function is executed in the following cases.

- General users are not required to be aware of this function, and the key operator will overwrite and erase the used document data that develops at the points shown in Table 2, according to the "Hard Disk Data Erasure Level", Basic, Medium or High which are set up by the Security Mode Operating Management Function.
- The key operator performs the overwriting and erasing from control panel, according to the method of Medium or High instructed by "Hard Disk Initialization" in Security Mode Operating Management Function.

6.1.2. Key Operator Authentication Function (SF.ADM_IA)

This function restricts such operations as the setting data of "Hard Disk Drive Lock Password", "Key Operator Password", "Hard Disk Data Erasure Level" that are provided by Hard Disk Drive Lock Management Function (SF.HDMNG) as well as Security Mode Operating Management Function (SF.ADMMNG), and also the instruction of "Hard Disk Initialization" to be performed only by the key operator.

Before allowing any operation or instruction, it checks the key operator password entered from the control panel and identifies and authenticates that the operator is the key operator.

SF.ADM_IA authorizes no single operation or instruction of above mentioned operating management functions before identifying and authenticating the key operator. When the key operator enters the password, each entered character is displayed as the dummy character "*" at a time.

When the key operator enters the password correctly causing the authentication of key operator successful, the operation or instruction of setting data will be authorized.

When the entered key operator password is incorrect causing the key operator authentication to fail, the result is notified by the alert sound. When a failure of authentication happens once, the successive authentication will be withheld for one second, and after the one second the next round of authentication interface will be reopened.

6.1.3. Hard Disk Drive Lock Management Function (SF.HDMNG)

This function is for the key operator to manage the hard disk drive lock, and it authorizes and executes the setup and modification of "Hard Disk Drive Lock Password" and the release of drive lock, only when the key operator is identified and authorized by SF.ADM_IA.

The setup and modification function of "Hard Disk Drive Lock Password" verifies if the "Hard Disk Drive Lock Password" entered by the key operator is within the limit of following rule.

- Character string from 8 to 32 characters
- Upper case alphabets, lower case alphabets, numerals, symbols

Upon the verification of permissible limit, if the password is conformant to the rule, the drive lock password in the Digital Imaging System and the hard disk drive will be set up or modified.

If not conformant to the rule, the result is notified by the alert sound and the setup/modification is rejected.

The release of drive lock of "Hard Disk Drive Lock Password" is initiated by the key operator's action from the control panel to select and instruct the lock release, and if the hard disk drive already had the "Hard Disk Drive Lock Password" set up, the password in the Digital Imaging System's memory and hard disk drive will be released and take the "unsetup" condition.

At the startup time, Digital Imaging System sends the "Hard Disk Drive Lock Password" to the hard disk drive, requesting to identify and authenticate itself.

6.1.4. Security Mode Operating Management Function (SF.ADMMNG)

This function is the management function for key operator to conduct operations, and it authorizes and executes the setup/modification of "Key Operator Password", the setup/modification of "Hard Disk Data Erasure Level" and the instruction of "Hard Disk Initialization" only when the key operator is identified and authenticated by SF.ADM_IA.

The setup and modification function of "Key Operator Password" verifies if the "Key Operator Password" entered by the key operator is within the limit of following rule.

- Character length fixed to 8
- Upper case alphabets, lower case alphabets, numerals, symbols
- A string of same 8 characters is prohibited.

Upon the verification of the limit, if the password is conformant to the rule, the key operator password is set up or modified.

If not conformant to the rule, the result is notified by the alert sound and the setup/modification is rejected.

The setup and modification of the "Hard Disk Data Erasure Level" is carried out in such a manner that the currently selected overwriting and erasing method is shown on the control panel first, the new method is selected from the control panel, and finally the newly selected overwriting and erasing method is displayed for confirmation.

For the setup and modification of "Hard Disk Data Erasure Level", one from following methods can be selected.

- Basic: Only the management information for the document data is deleted.
- Medium: Over the entire area of the document data, the data of all 0's are overwritten three times for erasure.
- High: Over the entire area of the document data, random values are overwritten twice and then all 0's are overwritten once for erasure.

The key operator can determine the behavior of Hard Disk Drive Overwriting for Residual Data as mentioned above, and also stop the Hard Disk Drive Overwriting Function for Residual Data by setting "Hard Disk Data Erasure Level" to Basic.

"Hard Disk Initialization" enables the key operator to select and instruct the overwriting method from the control panel, have the selected method displayed, initiate the Hard Disk Drive Overwriting Function for Residual Data, and complete the overwriting for erasure.

To instruct "Hard Disk Initialization", one from following methods can be selected.

- Medium: Over the entire area of the document data, the data of all 0's are overwritten three times for erasure.
- High: Over the entire area of the document data, random values are overwritten twice and then all 0's are overwritten once for erasure.

6.1.5. Service Technician Authentication Function (SF.SE_IA)

This function enables only the authenticated service technician to manipulate the setup data of "Service Technician Password" that is offered by Security Mode Maintenance Management Function (SF.SEMNG) and also to instruct "System Initialization".

Before allowing any operation or instruction, it checks the service mode setup procedure entered from the control panel as well as the service technician password, and identifies and authenticates that the operator is a service technician.

SF.SE_IA authorizes no single operation or instruction of security mode maintenance management functions (SF.SEMNG) before identifying and authenticating the service technician.

When the service technician enters the password, each entered character is displayed as the dummy character "*" at a time.

When the service technician enters the password correctly causing the authentication of service technician successful, the operation or instruction of setting data will be authorized.

When the entered service technician password is incorrect causing the key operator authentication to fail, the result is notified by the alert sound.

When a failure of authentication happens once, the successive authentication will be withheld for one second, and after the one second the next round of authentication interface will be reopened.

6.1.6. Security Mode Maintenance Management Function (SF.SEMNG)

This function is for service technician to carry out the management functions for maintenance works, and it authorizes and executes the setup/modification of "Service Technician Password" as well as the instruction of "System Initialization" only when an operator is identified and authenticated as service technician by SF.SE_IA.

The setup and modification function of "Service Technician Password" verifies if the password entered by the service technician is within the limit of following rule.

- Character length fixed to 8
- Upper case alphabets, lower case alphabets, numerals, symbols
- A string of same 8 characters is prohibited.

Upon the verification of the limit, if the password is conformant to the rule, the service technician password is set up or modified.

If not conformant to the rule, the result is notified by the alert sound and the setup/modification is rejected.

"System Initialization" is executed by instructing "System Initialization" displayed on the control panel, and initializes such settings as "Hard Disk Drive Lock Password", "Hard Disk Data Erasure Level", "Key Operator Password" and "Service Technician Password," returning each setting to the initial setting.

By "System Initialization", "Hard Disk Data Erasure Level" returns to Basic, stopping the Hard Disk Drive Overwriting Function for Residual Data.

6.2. Security Function Strength

Probabilistic or permutational mechanism is being used in Key Operator Authentication Function (SF.ADM_IA) and Service Technician Authentication Function (SF.SE_IA).

The security function strength of this TOE claims SOF-basic.

6.3. Assurance Measures

The documents that give the assurance measures to each component of the security assurance requirements in this ST are shown in Table 15.

Table 15 Assurance Measures

Assurance component ID	Assurance components	Assurance measures
ACM_CAP.2	Configuration items	Data Security Kit DA-SC03 Configuration Management Plan
		Data Security Kit DA-SC03 Configuration List
ADO_DEL.1	Delivery procedure	Data Security Kit DA-SC03 Delivery Procedures
ADO_IGS.1	Installation, generation and start-up procedures	- Operating Instructions Data Security Kit DA-SC03(in Japanese) - Installation Instructions for service technicians Data Security Kit DA-SC03(in Japanese) - Service Manual Digital Imaging Systems DP-3030 / 2330(in Japanese) - Operating Instructions Data Security Kit DA-SC03 - Installation Instructions for service technicians Data Security Kit DA-SC03 - Service Manual Digital Imaging Systems DP-3030 / 2330
ADV_FSP.1	Informal functional specification	Data Security Kit DA-SC03 Functional Specification
ADV_HLD.1	Descriptive high-level design	Data Security Kit DA-SC03 Design Specification
ADV_RCR.1	Informal correspondence demonstration	Data Security Kit DA-SC03 Functional Correspondence Description
AGD_ADM.1	Administrator guidance	- Operating Instructions(For Basic Operations) Digital Imaging Systems DP-3030P / 2330P DP-3030V / 2330V DP-3030VA / 2330VA DA-NS601 / NS600(in Japanese) - Operating Instructions Data Security Kit DA-SC03(in Japanese) - Installation Instructions for Service Technicians Data Security Kit DA-SC03(in Japanese) - Service Manual Digital Imaging Systems DP-3030 / 2330 (in Japanese) - Operating Instructions(For Copy & Network Scan Functions) Digital Imaging Systems DP-3030 / 2330 - Operating Instructions Data Security Kit DA-SC03 - Installation Instructions for Service Technicians Data Security Kit DA-SC03 - Service Manual Digital Imaging Systems DP-3030 / 2330

AGD_USR.1	User guidance	- Operating Instructions(For Basic Operations) Digital Imaging Systems DP-3030P / 2330P DP-3030V / 2330V DP-3030VA / 2330VA DA-NS601 / NS600(in Japanese) - Operating Instructions Data Security Kit DA-SC03(in Japanese) - Operating Instructions(For Copy & Network Scan Functions) Digital Imaging Systems DP-3030 / 2330 - Operating Instructions Data Security Kit DA-SC03
ATE_COV.1	Evidence of coverage	Data Security Kit DA-SC03 Test Plan and Report
ATE_FUN.1	Functional testing	
ATE_IND.2	Independent testing-sample	TOE
AVA_SOF.1	Strength of TOE security function evaluation	Data Security Kit DA-SC03 Security Function Strength Analysis
AVA_VLA.1	Developer vulnerability analysis	Data Security Kit DA-SC03 Vulnerability Analysis

7. PP Claims

This TOE does not conform to PP.

8. Rationale

8.1. Rationale for Security Objectives

Correspondence between security objectives and threats, organizational security policies and assumptions are described in Table 16.

Table 16 Correspondence between security objectives and threats, organizational security policies and assumptions

*	T.RECOVER	P.OWMETHOD	A.SETSEC	A.ADMIN	A.SE
O.HDLMNG	○				
O.RESIDUAL		○			
OE.AUTH		○	○		
OE.ADMIN				○	
OE.SE					○
OE.HDD	○				

*: Threats, organizational security policies and assumptions are shown horizontally, and security objectives are shown vertically.
○: Indicates the threats and assumptions that the corresponding security objectives counter or support.

As shown in Table 16, every security objective supports/counters one or more threats, organizational policies and/or assumptions. Table 16 also shows that all threats, organizational policies and assumptions are supported or countered by some security objective.
By satisfying the corresponding security objectives, the threats are countered, the organizational security policies are achieved, and the assumptions are assured.
The rationale showing that the measures against threats, organizational security policies and assumptions are taken is shown below.

T.RECOVER

To counter the threat T.RECOVER, recovery of the used document data which had been already stored on the hard disk drive must be made impossible. To achieve this, only the authenticated key operator is allowed to set up the "Hard Disk Drive Lock Password" on the hard disk drive, and to operate the TOE.
The hard disk drive model must have the function to prohibit any access to the document data inside the drive unless the correct "Hard Disk Drive Lock Password" is entered using OE.HDD, and only the key operator authenticated by O.HDLMNG can set up the "Hard Disk Drive Lock Password" on the hard disk drive, the mechanism of which makes the access to the used document data impossible.
Therefore, any attempt to access to the used document data using PCs or tools will not recover the used document data unless exactly the same password is entered as the hard disk drive lock password set up on the hard disk drive.
Above counter measures will assure that the residual document data which had been already stored on the hard disk drive is protected against any illicit attempt to recover it.

P.OWMETHOD

To achieve the organizational security policy P.OWMETHOD, it is necessary to operate the TOE with the "Hard Disk Data Erasure Level" set at Medium or High, which overwrites and erases the data area of the hard disk drive where the used document data is stored. Furthermore, O.RESIDUAL provides, not only the Basic level that does not overwrite to erase, but also Medium and High of "Hard Disk Data Erasure Level" for overwriting and erasing residual document data stored on the hard disk drive, and by the key operator setting up the "Hard Disk Data Erasure Level" to Medium or High under OE.AUTH at all times except for maintenance time, the data area of residual document data stored on the hard disk drive is overwritten and erased always in the operation mode.
By above security objectives, P.OWMETHOD can be realized.

A.SETSEC

The assumption A.SETSEC assumes that key operator enables TOE security functions and sets up "Hard Disk Drive Lock Password" for operation. Therefore key operator uses operating management function by OE.AUTH and sets up "Hard Disk Drive Lock Password" to operate, except for maintenance time. By this setup, A.SETSEC can be realized.

A.ADMIN

Assumption A.ADMIN assumes that key operator is a credible person. For this reason, under OE.ADMIN, the person in charge needs to understand the role of key operator, take prudent step for appointment of the key operator, and provide adequate education so that the key operator can learn how to manage to execute the tasks and learn the necessary knowledge. By this setup, A.ADMIN can be realized.

A.SE

The assumption A.SE assumes that the service technician (an employee of the company which undertakes the maintenance of Digital Imaging System DP-2330 / 3030) is a credible person. Therefore when a service technician performs the maintenance of Digital Imaging System DP-2330 / 3030, the person in charge or the key operator needs under OE.SE to confirm the service technician is the employee of the company which undertakes the maintenance of Digital Imaging System DP-2330 / 3030. By this setup, A.SE can be realized.

8.2. Rationale for Security Requirements

8.2.1. Rationale for Security Function Requirements

8.2.1.1. Reason to Introduce Security Function Requirement FIT_SOS.1 and FIT_MTD.1

Reason to Introduce FIT_SOS.1: Verification of secrets of IT Environment and FIT_MTD.1: Management of Administrator Data is shown below.

Administrator Data are the control data for IT environment security functions that can be accessed only by the key operator and the service technician.

The control for the verification of secrets of IT environment and IT environment security function are performed under the TOE security function requirements.

In order for OE.HDD to be able to execute authentication correctly, it is necessary to protect Hard Disk Drive Lock Password from being illicitly modified or erased, which requires TOE security function requirements.

Hard Disk Drive Lock Password is not only the TSF data of hard disk drive in IT environment but also the secret of IT environment, and is at the same time the user data from the view of TOE. It also has the character of TSF data that only key operator or service technician can operate.

This kind of data can neither be handled by FIA/FMT class of TOE, nor is the object of access control from the general users.

Also, since such data would always be authorized by FDP_ACC/FDP_ACF, these cannot handle such data.

Therefore it is necessary to define the new function requirements that have the administrative characteristics.

FIT_SOS.1 and FIT_MTD.1 have been introduced using FIA_SOS.1 and FMT_MTD.1 as the reference respectively.

8.2.1.2. Relationship between Security Function Requirements and Security Objectives

Table 17 shows the relationship between security function requirements and security objectives.

Table 17 Relationship between Security Function Requirements and Security Objectives

*1	O.HDLMNG	O.RESIDUAL	OE.HDD
FDP_RIP.1		○	
FIA_AFL.1(1)	○	○	
FIA_AFL.1(2)	○	○	
FIA_SOS.1(1)	○	○	
FIA_SOS.1(2)	○	○	
FIA_UID.2(1)	○	○	
FIA_UID.2(2)	○	○	
FIA_UAU.2(1)	○	○	
FIA_UAU.2(2)	○	○	
FIA_UAU.7(1)	○	○	
FIA_UAU.7(2)	○	○	
FMT_MOF.1		○	
FMT_MTD.1(1)		○	
FMT_MTD.1(2)	○	○	
FMT_MTD.1(3)	○	○	
FMT_SMF.1	○	○	
FMT_SMR.1	○	○	
FPT_RVM.1	○	○	
FIT_SOS.1	○		
FIT_MTD.1	○		
FIA_UID.2(IT)*2			○
FIA_UAU.2(IT)*2			○

*1: Security objectives are shown horizontally, and security function requirements are shown vertically.
*2: Indicates security function requirements of IT environment, others indicate TOE security function requirements.
○: Indicates the security objective that the corresponding security function requirement supports.

As shown in Table 17, every security function requirement is supported by some security objectives.
Also, as shown in Table 17, every security objective corresponds to some of the security function requirements.
Following shows the rationale that all security objectives are assured for counter measures by functional requirements.

O.HDLMNG

By identifying and authenticating key operator using FIA_UID.2(1) and FIA_UAU.2(1), the operation to follow can be assured to come from the legitimate key operator. Under FIA_AFL.1(1) when the key operator fails the authentication once, the consecutive authentication will be withheld for more than one second, which can reduce the possible number of consecutive attacks. By FIA_UAU.7(1), each time the password is entered, each entered character will be displayed by "*" to hide the password. By FMT_MTD.1(2), only key operator is allowed to modify "Key Operator Password", reducing the possibility of matching the password by illicit attacks. Also by FIA_SOS.1(1), when the key operator password is set up or modified, the entered password is verified if it agrees with the defined rule.
FMT_SMF.1 provides the security management function to manage the key operator password described above.
By FIT_MTD.1, modification and erasure of Hard Disk Drive Lock Password is restricted to key operator, and when the Hard Disk Drive Lock Password is set up or modified, FIT_SOS.1 verifies if the entered password conforms to the defined rule of password.
To prohibit the illicit initialization (i.e. returning to the initial setting) of key operator password, service technician password and Hard Disk Drive Lock Password, the initialization of "key operator password" in FMT_MTD.1(2), the initialization of "Service Technician Password" in FMT_MTD.1(3), and the initialization of "Hard Disk Drive Lock Password" in FIT_MTD.1 restrict the operations to service technician only.
To ensure the secure initializations above, the service technician at work is identified and authenticated. By identifying and authenticating the service technician using FIA_UID.2(2) and FIA_UAU.2(2), the operation to follow can be assured to come from the legitimate service technician. Under FIA_AFL.1(2) when the service technician fails the authentication once, the consecutive authentication will be withheld for more than one second, which can reduce the possible number of consecutive attacks.
By FIA_UAU.7(2), each time the password is entered, each entered character will be displayed by "*" to hide the password.
By FMT_MTD.1(3), only service technician is allowed to modify or initialize "Service Technician Password", reducing the possibility of matching the password by illicit attacks. Also by FIA_SOS.1(2), when the service technician password is set up or modified, the entered password is verified if it agrees with the defined rule.
FMT_SMF.1 provides the security management function to manage the service technician password described above.
By FMT_SMR.1, the roles of key operator and service technician are maintained.
By FPT_RVM.1, TOE security functions are assuredly invoked, and will never be bypassed.
By above security functional requirements, TOE allows only the key operator to set up the "Hard Disk Drive Lock Password" on the hard disk drive, realizing the security objective O.HDLMNG to disable the recovery of the used document data which had been already stored on the hard disk drive.

O.RESIDUAL

By FMT_MTD.1(1), query and modification of "Hard Disk Data Erasure Level" are restricted to key operator, who is enabled to set up Basic, Medium and High of "Hard Disk Data Erasure Level."
(Note, however, that modifying "Hard Disk Data Erasure Level" to Basic using "System Initialization" function only can also be done by service technician.)
To ensure the modification above assuredly, the key operator at work is identified and authenticated. By identifying and authenticating key operator using FIA_UID.2(1) and FIA_UAU.2(1), the operation to follow can be assured to come from the legitimate key operator. Under FIA_AFL.1(1) when the key operator fails the authentication once, the consecutive authentication will be withheld for more than one second, which can reduce the possible number of consecutive attacks. By FIA_UAU.7(1), each time the password is entered, each entered character will be displayed by "*" to hide the password.
By FMT_MTD.1(2), only key operator is allowed to modify "Key Operator Password", reducing the possibility of matching the password by illicit attacks. Also by FIA_SOS.1(1), when the key operator password is set up or modified, the entered password is verified if it agrees with the defined rule.
FMT_SMF.1 provides the security management function to manage the key operator password described above.
To prohibit the illicit initialization of "Key Operator Password", "Service Technician Password" and "Hard Disk Data Erasure Level", the initialization of "key operator password" in FMT_MTD.1(2), the initialization of "Service Technician Password" in FMT_MTD.1(3), and the initialization of "Hard Disk Data Erasure Level"(i.e. modification to Basic by "System Initialization") in FMT_MTD.1(1) restrict the operations to service technician only.
To ensure the secure initializations above, the service technician at work is identified and authenticated. By identifying and authenticating the service technician using FIA_UID.2(2) and FIA_UAU.2(2), the operation to follow can be assured to come from the legitimate service technician. Under FIA_AFL.1(2) when the service technician fails the authentication once, the consecutive authentication will be withheld for more than one second, which can reduce the possible number of consecutive attacks.
By FIA_UAU.7(2), each time the password is entered, each entered character will be displayed by "*" to hide the password.
By FMT_MTD.1(3), only service technician is allowed to modify or initialize "Service Technician Password", reducing the possibility of matching the password by illicit attacks. Also by FIA_SOS.1(2), when the service technician password is set up or modified, the entered password is verified if it agrees with the defined rule.
FMT_SMF.1 provides the security management function to manage the service technician password described above.
Since FMT_MOF.1 restricts the operation of Hard Disk Drive Overwriting Function for Residual Data as it is one of the security functions to key operator and service technician, only key operator and service technician can set up or instruct the Hard Disk Drive Overwriting Function for Residual Data.
By FMT_SMR.1, the roles of key operator and service technician are maintained.
By FDP_RIP.1, any contents of information in the residual document data stored on the hard disk drive are made unusable.
By FPT_RVM.1, TOE security functions are assuredly invoked, and will never be bypassed.
By above security functional requirements, TOE provides not only the Basic level that does not overwrite and erase, but also two types of overwriting and erasing functions, Medium and High, for Hard Disk Drive Overwriting Function for Residual Data, realizing the security objectives O.RESIDUAL.

OE.HDD

By FIA_UID.2(IT) and FIA_UAU.2(IT), hard disk drive allow the access only from the TOE which succeeds identification and authentication.
This realizes OE.HDD that prohibits illicit accesses to hard disk drive.

8.2.1.3. Appropriateness of Security Requirements by Adding Security Functional Requirement FIT_SOS.1 and FIT_MTD.1

FIT_SOS.1 has essentially the same meaning as FIA_SOS.1 except that "secrets" of FIA_SOS.1 is changed to "secrets of IT environment "; likewise FIT_MTD.1 has essentially the same meaning as FMT_MTD.1 except that "TSF data" in FMT_MTD.1 is changed to "Administrator Data." Therefore adding FIT_SOS.1 and FIT_MTD.1 will not require specific functional requirements and the same security requirements as FIA_SOS.1 and FMT_MTD.1 can hold.

8.2.2. Dependencies of Security Functional Requirements

Table 18 shows the dependency relationship of security functional requirements. When the dependency defined by CC Part 2 is not satisfied, the reason is described in the column of "Dependency in this ST."

Table 18 Dependency of Functional Requirements

Functional requirement	Dependency required by CC	Dependency in this ST
FDP_RIP.1	None	None
FIA_AFL.1(1)	FIA_UAU.1	FIA_UAU.2(1) Description: Since FIA_UAU.2 is the security functional requirement that is an upper hierarchy of FIA_UAU.1, the dependency to FIA_UAU.1 is satisfied.
FIA_AFL.1(2)	FIA_UAU.1	FIA_UAU.2(2) Description: Since FIA_UAU.2 is the security functional requirement that is an upper hierarchy of FIA_UAU.1, the dependency to FIA_UAU.1 is satisfied.
FIA_SOS.1(1)	None	None
FIA_SOS.1(2)	None	None
FIA_UID.2(1)	None	None
FIA_UID.2(2)	None	None
FIA_UAU.2(1)	FIA_UID.1	FIA_UID.2(1) Description: Since FIA_UID.2 is the security functional requirement that is an upper hierarchy of FIA_UID.1, the dependency to FIA_UID.1 is satisfied.
FIA_UAU.2(2)	FIA_UID.1	FIA_UID.2(2) Description: Since FIA_UID.2 is the security functional requirement that is an upper hierarchy of FIA_UID.1, the dependency to FIA_UID.1 is satisfied.
FIA_UAU.7(1)	FIA_UAU.1	FIA_UAU.2(1) Description: Since FIA_UAU.2 is the security functional requirement that is an upper hierarchy of FIA_UAU.1, the dependency to FIA_UAU.1 is satisfied.
FIA_UAU.7(2)	FIA_UAU.1	FIA_UAU.2(2) Description: Since FIA_UAU.2 is the security functional requirement that is an upper hierarchy of FIA_UAU.1, the dependency to FIA_UAU.1 is satisfied.
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1(1)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1(2)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1(3)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2(1), FIA_UID.2(2) Description: Since FIA_UID.2 is the security functional requirement that is an upper hierarchy of FIA_UID.1, the dependency to FIA_UID.1 is satisfied.
FPT_RVM.1	None	None
FIT_SOS.1	None	None
FIT_MTD.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FIA_UID.2(IT) *	None	None
FIA_UAU.2(IT) *	FIA_UID.1(IT)	FIA_UID.2(IT) Description: Since FIA_UID.2 is the security functional requirement that is an upper hierarchy of FIA_UID.1, the dependency to FIA_UID.1 is satisfied.

*: Indicates security functional requirements of IT environment, others indicate TOE security functional requirements.

8.2.3. Interactions among Security Functional Requirements

Table 19 shows the interaction relationship among security functional requirements.

Table 19 Interactions among Security Functional Requirements

Security functional requirements	Circumvention	Deactivation
FDP_RIP.1	FPT_RVM.1	FMT_MOF.1
FIA_AFL.1(1)	FPT_RVM.1	—
FIA_AFL.1(2)	FPT_RVM.1	—
FIA_SOS.1(1)	FPT_RVM.1	—
FIA_SOS.1(2)	FPT_RVM.1	—
FIA_UID.2(1)	FPT_RVM.1	—
FIA_UID.2(2)	FPT_RVM.1	—
FIA_UAU.2(1)	FPT_RVM.1	—
FIA_UAU.2(2)	FPT_RVM.1	—
FIA_UAU.7(1)	FPT_RVM.1	—
FIA_UAU.7(2)	FPT_RVM.1	—
FMT_MOF.1	FPT_RVM.1	—
FMT_MTD.1(1)	FPT_RVM.1	—
FMT_MTD.1(2)	FPT_RVM.1	—
FMT_MTD.1(3)	FPT_RVM.1	—
FMT_SMF.1	—	—
FMT_SMR.1	—	—
FPT_RVM.1	—	—
FIT_SOS.1	FPT_RVM.1	—
FIT_MTD.1	FPT_RVM.1	—

8.2.3.1. Circumvention

FPT_RVM.1

Since FIA_UID.2(1), FIA_UAU.2(1) and FIA_UAU.7(1) controlling key operator identification and authentication mandates the execution of key operator identification and authentication before key operator uses any security related operating management function, user identification before action, user authentication before action or protected authentication feedback can never be circumvented. FIA_AFL.1(1) controlling the handling for failed authentication is always invoked at such failure, and therefore can never be circumvented.

Since FIA_UID.2(2), FIA_UAU.2(2) and FIA_UAU.7(2) controlling service technician identification and authentication mandates the execution of service technician identification and authentication before service technician uses any security related maintenance management function, user identification before action, user authentication before action or protected authentication feedback can never be circumvented. FIA_AFL.1(2) controlling the handling for failed authentication is always invoked at such failure, and therefore can never be circumvented.

FDP_RIP.1 controlling residual data protection is invoked every time the used document data develops and "Hard Disk Initialization" is executed by the instruction from key operator, and can never be circumvented.

FIA_SOS.1(1) and FIA_SOS.1(2) controlling the verification of secrets can never be circumvented because the former is invoked every time "Key Operator Password" is set up or modified, and the latter is invoked every time "Service Technician Password" is set up or modified. FMT_MTD.1(1) and FMT_MTD.1(2) can never be circumvented because they are invoked every time "Hard Disk Data Erasure Level" and "Key Operator Password" are modified or initialized. Likewise, FMT_MTD.1(3) controlling the management of TSF data can never be circumvented because it is invoked every time "Service Technician Password" is modified or initialized.

FMT_MOF.1 controlling the security function behavior can never be circumvented because it is invoked every time "Hard Disk Data Erasure Level" is set up or modified after key operator identification and authentication, "Hard Disk Drive Initialization" is instructed, and "Hard Disk Data Erasure Level" is initialized by service technician.

FIT_SOS.1 the verification of secrets of IT environment can never be circumvented because it is invoked every time "Hard Disk Drive Lock Password" is set up or modified after key operator is identified and authenticated. FIT_MTD.1 controlling the management of administrator data also can never be circumvented because it is invoked every time "Hard Disk Drive Lock Password" is set up or modified after key operator is identified and authenticated, and "Hard Disk Drive Lock Password" is initialized after service technician is identified and authenticated.

8.2.3.2. Deactivation

FMT_MOF.1

FMT_MOF.1 restricts the deactivation role of Hard Disk Drive Overwriting Function for Residual Data (FDP_RIP.1) to key operator and service technician.

8.2.3.3. Corruption

This TOE authorizes only key operator and service technician to management of security functions behaviors. Therefore there can be no illicit subjects, and there is no needs to perform the access control either. Accordingly TSF cannot be corrupted by illicit subjects.

8.2.3.4. Detection of Attacks Aiming at Defeasance

Since this TOE uses FPT_RVM.1 to limit the use of operating management functions to the licit key operator, and the use of maintenance management functions to the licit service technician, requirements of FAU class concerning audit are not necessary.

8.2.4. Validity of Security Function Strength Level

Attack capability of the attackers assumed for this TOE is low level. Therefore, "SOF-basic" being the security function strength level is appropriate.

The security function strength is satisfied because all the probabilistic and permutational mechanisms are SOF-basic.

8.2.5. Rationale for Security Assurance Requirements

This TOE is assumed to be used in offices and public facilities, and used by limited users. Also the capabilities of attackers are assumed to be low. Therefore evaluation assurance level of EAL2 is appropriate.

8.3. Rationale for TOE Summary Specification

8.3.1. Rationale for Function Summary Specification

Correspondence between TOE security functions and security functional requirements is shown in Table 20.

Table 20 Correspondence between TOE Security Functions and Security Functional Requirements

*	SF.OVWRT	SF.ADM_IA	SF.HDMNG	SF.ADMMNG	SF.SE_IA	SF.SEMNG
FDP_RIP.1	○					
FIA_AFL.1(1)		○				
FIA_AFL.1(2)					○	
FIA_SOS.1(1)				○		
FIA_SOS.1(2)						○
FIA_UID.2(1)		○				
FIA_UID.2(2)					○	
FIA_UAU.2(1)		○				
FIA_UAU.2(2)					○	
FIA_UAU.7(1)		○				
FIA_UAU.7(2)					○	
FMT_MOF.1				○		○
FMT_MTD.1(1)				○		○
FMT_MTD.1(2)				○		○
FMT_MTD.1(3)						○
FMT_SMF.1				○		○
FMT_SMR.1				○		○
FPT_RVM.1	○	○	○	○	○	○
FIT_SOS.1			○			
FIT_MTD.1			○			○

*: TOE security functions are shown horizontally, and security functional requirements are shown vertically.
○: Indicates the TOE security function that the corresponding security function requirement supports.

Following shows the rationale for correspondences between TOE security functions and security functional requirements.

FDP_RIP.1

At the time when used document data develops as shown in Table 2, SF.OVWRT automatically overwrites and erases the data area of used document data stored on the hard disk drive three times, and when the key operator instructs "Hard Disk Initialization" to be executed, it overwrites and erases the entire data area of document data three times.
By above setup, FDP_RIP.1 is satisfied.

FIA_AFL.1(1)

When key operator fails in authentication once, SF.ADM_IA denies the next authentication from the key operator for one second, which satisfies FIA_AFL.1(1).

FIA_AFL.1(2)

When service technician fails in authentication once, SF.SE_IA denies the next authentication from the service technician for one second, which satisfies FIA_AFL.1(2).

FIA_SOS.1(1)
When key operator sets up or modifies the password, SF.ADMMNG verifies if the operation conforms to the defined rule of password, which satisfies FIA_SOS.1(1).

FIA_SOS.1(2)
When service technician sets up or modifies the password, SF.SEMNG verifies if the operation conforms to the defined rule of password, which satisfies FIA_SOS.1(2).

FIA_UID.2(1)
SF.ADM_IA satisfies FIA_UID.2(1) by executing the identification of key operator.

FIA_UID.2(2)
SF.SE_IA satisfies FIA_UID.2(2) by executing the identification of service technician.

FIA_UAU.2(1)
SF.ADM_IA satisfies FIA_UAU.2(1) by executing the authentication of key operator.

FIA_UAU.2(2)
SF.SE_IA satisfies FIA_UAU.2(2) by executing the authentication of service technician.

FIA_UAU.7(1)
SF.ADM_IA satisfies FIA_UAU.7(1) by displaying "*" each time one character of password is entered at the time of key operator authentication.

FIA_UAU.7(2)
SF.SE_IA satisfies FIA_UAU.7(2) by displaying "*" each time one character of password is entered at the time of service technician authentication.

FMT_MOF.1
SF.ADMMNG and SF.SEMNG satisfy FMT_MOF.1 by the fact that the former authorizes identified and authenticated key operator only to determine the behavior, disable and enable of Hard Disk Drive Overwriting Function for Residual Data, and the latter authorizes identified and authenticated service technician only to disable of Hard Disk Drive Overwriting Function for Residual Data.

FMT_MTD.1(1)
SF.ADMMNG and SF.SEMNG satisfy FMT_MTD.1(1) by the fact that the former authorizes the identified and authenticated key operator only to query or modify "Hard Disk Data Erasure Level" and the latter authorizes the identified and authenticated service technician only to initialize "Hard Disk Data Erasure Level."

FMT_MTD.1(2)
SF.ADMMNG and SF.SEMNG satisfy FMT_MTD.1(2) by the fact that the former authorizes the identified and authenticated key operator only to modify "Key Operator Password" and the latter authorizes the identified and authenticated service technician only to initialize "Key Operator Password."

FMT_MTD.1(3)
SF.SEMNG satisfies FMT_MTD.1(3) by authorizing the identified and authenticated service technician only to modify and initialize "Service Technician Password."

FMT_SMF.1
SF.ADMMNG and SF.SEMNG satisfy FMT_SMF.1 by the fact that the former provides security management function to manage "Key Operator Password" and the latter provides the security management function to manage "Service Technician Password."

FMT_SMR.1
SF.ADMMNG and SF.SEMNG satisfy FMT_SMR.1 by the former maintaining the role of key operator and the latter maintaining the role of service technician.

FPT_RVM.1
SF.OVWRT, SF.ADM_IA, SF.HDMNG, SF.ADMMNG, SF.SE_IA and SF.SEMNG satisfy FPT_RVM.1 by being executed always without any circumvention.

FIT_SOS.1
SF.HDMNG satisfies FIT_SOS.1 by the fact that when "Hard Disk Drive Lock Password" is set up or modified, it verifies if the operation conforms to the defined rule of password.

FIT_MTD.1
SF.HDMNG and SF.SEMNG satisfy FIT_MTD.1 by the fact that the former authorizes the identified and authenticated key operator only to modify or delete "Hard Disk Drive Lock Password" and the latter authorizes the identified and authenticated service technician only to initialize "Hard Disk Drive Lock Password."

8.3.2. Rationale for TOE Security Function Strength

As described in 6.2. Security Function Strength, probabilistic or permutational mechanism is being used in Key Operator Authentication Function (SF.ADM_IA) and Service Technician Authentication Function (SF.SE_IA).

The security function strength of this TOE is SOF-basic, and it satisfies SOF-basic claimed in 5.4. TOE Security Function Strength.

8.3.3. Rationale for Assurance Measures

Correspondences between Assurance Measures and Assurance Components of EAL2 are shown in Table 21.

Table 21 Correspondences between Assurance Measures and Assurance Components of EAL2

Assurance measures	ACM_CAP.2	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVA_VLA.1
Data Security Kit DA-SC03 Configuration Management Plan	○												
Data Security Kit DA-SC03 Configuration List	○												
Data Security Kit DA-SC03 Delivery Procedures		○											
- Operating Instructions Data Security Kit DA-SC03(in Japanese) - Installation Instructions for service technicians Data Security Kit DA-SC03(in Japanese) - Service Manual Digital Imaging Systems DP-3030 / 2330(in Japanese) - Operating Instructions Data Security Kit DA-SC03 - Installation Instructions for service technicians Data Security Kit DA-SC03 - Service Manual Digital Imaging Systems DP-3030 / 2330			○										
Data Security Kit DA-SC03 Functional Specification				○									
Data Security Kit DA-SC03 Design Specification					○								

Data Security Kit DA-SC03 Functional Correspondence Description						○							
- Operating Instructions(For Basic Operations) Digital Imaging Systems DP-3030P / 2330P DP-3030V / 2330V DP-3030VA / 2330VA DA-NS601 / NS600(in Japanese) - Operating Instructions Data Security Kit DA-SC03(in Japanese) - Installation Instructions for Service Technicians Data Security Kit DA-SC03(in Japanese) - Service Manual Digital Imaging Systems DP-3030 / 2330 (in Japanese) - Operating Instructions(For Copy & Network Scan Functions) Digital Imaging Systems DP-3030 / 2330 - Operating Instructions Data Security Kit DA-SC03 - Installation Instructions for Service Technicians Data Security Kit DA-SC03 - Service Manual Digital Imaging Systems DP-3030 / 2330							○						
- Operating Instructions(For Basic Operations) Digital Imaging Systems DP-3030P / 2330P DP-3030V / 2330V DP-3030VA / 2330VA DA-NS601 / NS600(in Japanese) - Operating Instructions Data Security Kit DA-SC03(in Japanese) - Operating Instructions(For Copy & Network Scan Functions) Digital Imaging Systems DP-3030 / 2330 - Operating Instructions Data Security Kit DA-SC03								○					
Data Security Kit DA-SC03 Test Plan and Report									○	○			
TOE											○		
Data Security Kit DA-SC03 Security Function Strength Analysis												○	
Data Security Kit DA-SC03 Vulnerability Analysis													○

ACM_CAP.2

Data Security Kit DA-SC03 Configuration Management Plan and Configuration List satisfy the requirements because they clearly identify the TOE configuration items.

ADO_DEL.1

Data Security Kit DA-SC03 Delivery Procedures satisfies the requirements because they describe the necessary procedures to maintain the security at delivery of TOE.

ADO_IGS.1

- Operating Instructions Data Security Kit DA-SC03(in Japanese)
- Installation Instructions for service technicians Data Security Kit DA-SC03(in Japanese)
- Service Manual Digital Imaging Systems DP-3030 / 2330(in Japanese)
- Operating Instructions Data Security Kit DA-SC03
- Installation Instructions for service technicians Data Security Kit DA-SC03
-Service Manual Digital Imaging Systems DP-3030 / 2330

All above documents satisfy the requirements because they describe the procedures of secure installation, generation and start-up of TOE.

ADV_FSP.1

Data Security Kit DA-SC03 Functional Specification satisfies the requirements because it describes the informal functional specification of TOE.

ADV_HLD.1

Data Security Kit DA-SC03 Design Specification satisfies the requirements because it describes the descriptive high-level design of TOE.

ADV_RCR.1

Data Security Kit DA-SC03 Functional Correspondence Description satisfies the requirements because it describes the informal correspondence demonstration of TOE.

AGD_ADM.1

- Operating Instructions(For Basic Operations) Digital Imaging Systems DP-3030P / 2330P DP-3030V / 2330V DP-3030VA / 2330VA DA-NS601 / NS600(in Japanese)
- Operating Instructions Data Security Kit DA-SC03(in Japanese)
- Installation Instructions for Service Technicians Data Security Kit DA-SC03(in Japanese)

- Service Manual Digital Imaging Systems DP-3030 / 2330 (in Japanese)
- Operating Instructions(For Copy & Network Scan Functions) Digital Imaging Systems DP-3030 / 2330
- Operating Instructions Data Security Kit DA-SC03
- Installation Instructions for Service Technicians Data Security Kit DA-SC03
- Service Manual Digital Imaging Systems DP-3030 / 2330

All above satisfy the requirements because they describe the guidance for TOE administrators.

AGD_USR.1

- Operating Instructions(For Basic Operations) Digital Imaging Systems DP-3030P / 2330P DP-3030V / 2330V DP-3030VA / 2330VA DA-NS601 / NS600(in Japanese)
- Operating Instructions Data Security Kit DA-SC03(in Japanese)
- Operating Instructions(For Copy & Network Scan Functions) Digital Imaging Systems DP-3030 / 2330
- Operating Instructions Data Security Kit DA-SC03

All above satisfy the requirements because they describe the guidance for TOE users.

ATE_COV

Data Security Kit DA-SC03 Test Plan and Report satisfies the requirements because it describes the correspondence between the identified tests and TSF described in functional specification.

ATE_FUN.1

Data Security Kit DA-SC03 Test Plan and Report satisfies the requirements because it describes the test plan, test procedure, anticipated test results and the actual test results.

ATE_IND.2

Assurance Measures TOE satisfies the requirements because it is necessary for the evaluator to execute the independent tests.

AVA_SOF.1

Data Security Kit DA-SC03 Security Function Strength Analysis satisfies the requirements because it describes the security function strength of TOE.

AVA_VLA.1

Data Security Kit DA-SC03 Vulnerability Analysis satisfies the requirements because it describes the obvious vulnerabilities and identified vulnerabilities.

8.4. Rationale for PP Claims

There is no applicable PP.