Certification Report

TOMITA Tatsuo, Chairman
Information-technology Promotion Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku, Tokyo

IT Product (TOE)

Reception Date of Application (Reception Number)	2020-07-31 (ITC-0766)
Certification Identification	JISEC-C0719
Product Name	RICOH Pro C5300S/C5310S, SAVIN Pro C5300S/C5310S, LANIER Pro C5300S/C5310S, nashuatec Pro C5300S/C5310S, Rex Rotary Pro C5300S/C5310S, Gestetner Pro C5300S/C5310S, infotec Pro C5300S/C5310S
Version and Release Numbers	E-1.00
Product Manufacturer	RICOH COMPANY, LTD.
Conformance of Functionality	PP conformant functionality, CC Part 2 Extended
Protection Profile Conformance	U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)
Assurance Package	EAL2 Augmented by ALC_FLR.2
Name of IT Security Evaluation Facility	ECSEC Laboratory Inc., Evaluation Center

This is to report that the evaluation result for the above TOE has been certified as follows.
2021-04-14

YANO Tatsuro, Technical Manager
IT Security Technology Evaluation Department
IT Security Center

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following standards prescribed in the "IT Security Evaluation and Certification Scheme Document."

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 5

- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 5

Evaluation Result: Pass

"RICOH Pro C5300S/C5310S, SAVIN Pro C5300S/C5310S, LANIER Pro C5300S/C5310S, nashuatec Pro C5300S/C5310S, Rex Rotary Pro C5300S/C5310S, Gestetner Pro C5300S/C5310S, infotec Pro C5300S/C5310S version E-1.00" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "RICOH Pro C5300S/C5310S, SAVIN Pro C5300S/C5310S, LANIER Pro C5300S/C5310S, nashuatec Pro C5300S/C5310S, Rex Rotary Pro C5300S/C5310S, Gestetner Pro C5300S/C5310S, infotec Pro C5300S/C5310S version E-1.00" (hereinafter referred to as the "TOE") developed by RICOH COMPANY, LTD., and the evaluation of the TOE was finished on 2021-03-30 by ECSEC Laboratory Inc., Evaluation Center (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, RICOH COMPANY, LTD., and provide security information to procurement entities and consumers who are interested in the TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") described in Chapter 10. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

This Certification Report assumes "general consumers and procurement entities who purchase the TOE that is commercially available" to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee an individual IT product itself.

1.1 Product Overview

An overview of the TOE functions and operational conditions is described as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Protection Profile or Assurance Package

The TOE conforms to the following protection profile [14] [15] (hereinafter referred to as the "conformance PP").

U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)

Assurance Package of the TOE is EAL2 augmented by ALC_FLR.2.

1.1.2 TOE and Security Functionality

The TOE is a digital Multi-Function Product (hereinafter referred to as "MFP") made by RICOH COMPANY, LTD., which provides the functions of copy, scanner, printer, and fax for digitising paper-based documents, document management, and printing.

This MFP is an IT product which incorporates each function of scanner, printer, and fax with Copy Function, and is generally connected to an office LAN and used for inputting, storing, and outputting documents.

The TOE provides the Security Functions required for the conformance PP, and also provides the Security Functions to accomplish the necessary security policy for an organisation which manages the TOE.

For these security functionalities, the evaluation for the validity of the design policy and the

correctness of the implementation is conducted in the scope of the assurance package. The next clause describes the assumed threats and assumptions in the TOE.

1.1.2.1 Threats and Security Objectives

The TOE assumes the following threats and provides the Security Functions to counter them.

For protected assets such as the documents that the TOE handles and the setting information relevant to the Security Functions, there are threats of disclosure and tampering caused by unauthorised access to both the TOE and the communication data on the network.

The TOE provides the Security Functions to prevent those protected assets from unauthorised disclosure and tampering.

1.1.2.2 Configuration and Assumptions

The evaluated product is assumed to be operated in the following assumptions.

It is assumed that the TOE is located in an environment where physical components and interfaces of the TOE are protected from the unauthorised access. For the operation, the TOE shall be properly configured, maintained, and managed according to the guidance documents.

1.1.3 Disclaimers

The TOE is assumed to be operated while the following functions are deactivated. The case that the TOE is operated with these settings changed is not included in the assurance provided by this evaluation:

- Maintenance Function
- IP-Fax and Internet Fax Function
- Authentication methods except for Basic Authentication (for Internal Authentication)

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed in 2021-03, based on functional requirements and assurance requirements of the TOE according to the publicised documents "IT Security Evaluation and Certification Scheme Document"[1], "Requirements for IT Security Certification"[2], and "Requirements for Approval of IT Security Evaluation Facility"[3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [13] prepared by the Evaluation Facility as well as evaluation documentation, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The certification oversight reviews were also prepared for those concerns found in the certification process. The Certification Body confirmed that all the concerns were fully resolved, and that the

TOE evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

TOE Name:	RICOH Pro C5300S/C5310S, SAVIN Pro C5300S/C5310S, LANIER Pro C5300S/C5310S, nashuatec Pro C5300S/C5310S, Rex Rotary Pro C5300S/C5310S, Gestetner Pro C5300S/C5310S, infotec Pro C5300S/C5310S
TOE Version:	E-1.00
Developer:	RICOH COMPANY, LTD.

Users can verify that a product is the TOE, which is evaluated and certified, by the following means.

- Confirm that the name displayed on the product exterior matches “Pro C5300S” or “Pro C5310S”.
- Confirm that the name described on the label sticker of the packing box for a fax option matches “Fax Option Type M42”.
- Operate as described in the product guidance, and confirm that the name, the version and the part number (some items have no part number) displayed on the Operation Panel of the product match the ones shown in Table 2-1, Table 2-2, or Table 2-3.

Table 2-1 Identification Information of the Software for the MFP

Name	Version	Part Number
System/Copy	1.04	D0CQ5760H
Network Support	19.21	D0CQ5769D
Web Support	1.03	D0CQ5765G
OSS Info	1.00	D0CQ5789A
Fax	01.00.00	D0CQ5762B
RemoteFax	01.00.00	D0CQ5763B
Scanner	01.01	D0CQ5764D
Web Uapl	1.00	D0CQ5766D
NetworkDocBox	1.01.1	D0CQ5770B
animation	1.00	D0CQ5767C
Printer	1.01	D0CQ5772D
RPCS	3.24.6	D0CN5774B
Font EXP	1.00	D2415581
PCL	1.00	D0CN5775C

Name	Version	Part Number
IRIPS PS3	1.00	D0CN5781B
IRIPS PDF	1.02	D0CN5778C
IRIPS Font	1.20	D0CN5783
GraphicData	1.01	D0CQ5784D
MovieData	1.01	D0CQ5785C
MovieData2	1.01	D0CQ5786C
MovieData3	1.01	D0CQ5787C
HelpData	0.03	D0CQ5788A
Data Erase Onb	1.05	D2625244
GWFCU3.8-25(WW)	01.00.00	D0CN5755A
PowerSaving Sys	F.L3.25	D0CN5761
MediaLibrary	0.03	D0CQ5776A
CheetahSystem	1.04	D0CN1537E
appsite	3.02.01	D0CN1576A
bleservice	1.02	D0CN1568A
camelsl	1.00	D0CN1597A
cispluginble	4.0.1	D0CN1548
cispluginkeystr	3.03.02	D0CN1547A
cispluginnfc	3.03.02	D0CN1546A
decolet	3.00.02	D0CN1541A
ecoinfo	1.00	D0CN1564A
faxinfo	1.00	D0CN1562A
helpservice	1.00	D0CN1596A
iccd	3.08.02	D0CN1578A
introductionset	0.41G25	D0CN1584B
iwnnimelanguage	2.8.2	D0BQ1456A
iwnnimelanguage	2.8.2	D0BQ1454A
iwnnimelanguage	2.8.2	D0BQ1455A
iwnnimeml	2.8.201	D0BQ1453C
kerberos	1.07.03	D0CN1595A
langswitcher	1.00	D0CN1560A
mediaappappui	1.00	D0CN1574A
mlpsmartdevicec	4.1.0	D0CN1542
multidevicehub	2.01	D0BM1472A
optimorurcmf	1.1	D0BQ1499B
pptop	1.00	D0CQ1439A
programinfoserv	1.00	D0CN1569A

Name	Version	Part Number
remotesupport	1.00	D0CN1598A
simpleauth	3.05.03	D0CN1540A
simpledirectcon	1.18	D0CN1549
simpleprinter	1.00	D0CN1570A
smartcopy	1.01	D0CN1571B
smartfax	1.00	D0CN1573A
smartprtstoredj	1.00	D0CN1575A
smartscanner	1.00	D0CN1572A
smartscannerex	2.03	D0CN1593A
stopwidget	1.00	D0CN1543A
tonerstate	1.00	D0CN1561A
voicecontrolser	1.00	D0CN1513A
Engine	1.04:02	D0CN5520G
ADF	01.040:02	D3HA5260C
TDCU	0.07.1:05	D0CN5530

Table 2-2 Identification information of the Hardware for the MFP

Name	Version	Part Number
Ic Ctlr	03	(none)
Ic Key	01024704	(none)

Table 2-3 Identification Information of the Software for the Operation Panel Unit

Name	Version	Part Number
Firmware	1.04	D0CN1537E
Keymicon	9.10	(none)
Application Site	3.02.01	D0CN1576A
Bluetooth Authentication Plugin	4.0.1	D0CN1548
BluetoothService	1.02	D0CN1568A
ChangeLanguages	1.00	D0CN1560A
Copy	1.01	D0CN1571B
CSPF	3.00.02	D0CN1541A
Direct Connection	1.18	D0CN1549
Eco-friendly	1.00	D0CN1564A
Fax	1.00	D0CN1573A
FaxRXFile	1.00	D0CN1562A

Name	Version	Part Number
GraphicData	1.01	D0CQ5784D
ICCardDispatcher	3.08.02	D0CN1578A
Installation Settings	0.41G25	D0CN1584B
iWnn IME	2.8.201	D0BQ1453C
iWnn IME Korean Pack	2.8.2	D0BQ1456A
iWnn IME SimplifiedChinesePack	2.8.2	D0BQ1454A
iWnn IME TraditionalChinesePack	2.8.2	D0BQ1455A
KerberosService	1.07.03	D0CN1595A
LegacyUIData	1.00	D0CQ5767C
MachineStatus	1.00	D0CQ1439A
MultiDevice Hub	2.01	D0BM1472A
Print/Scan (Memory Storage Device)	1.00	D0CN1574A
Printer	1.00	D0CN1570A
ProgramInfoService	1.00	D0CN1569A
Proximity Card Reader Support Plugin	3.03.02	D0CN1547A
Quick Card Authentication Config.	3.05.03	D0CN1540A
Quick PrintRelease	1.00	D0CN1575A
Remote Panel Operation	1.00	D0CN1597A
RemoteConnect Support	1.1	D0BQ1499B
RemoteSupportService	1.00	D0CN1598A
RicohScanGUIService	2.03	D0CN1593A
Scanner	1.00	D0CN1572A
Smart Device Connector	4.1.0	D0CN1542
Standard IC Card Plugin	3.03.02	D0CN1546A
Stop	1.00	D0CN1543A
Supply Information	1.00	D0CN1561A
Support Settings	1.00	D0CN1596A
VoiceControlService	1.00	D0CN1513A

3. Security Policy

This chapter describes security function policies that the TOE adopts to counter threats, and organisational security policies.

The TOE provides the Security Functions to counter the unauthorised access to the stored documents in the MFP, and to protect the communication data on the network.

For meeting the organisational security policies, the TOE provides the functions to overwrite the internal stored data, to encrypt the stored data in an HDD, and to prevent the unauthorised access through telephone lines via fax I/F.

For each setting that is relevant to the above mentioned Security Functions, only administrators are permitted to set configurations in order to prevent the deactivation and unauthorised use of the Security Functions.

Tables 3-1 and 3-2 show the protected assets for the Security Functions of the TOE.

Table 3-1 TOE Protected Assets (user data)

Type	Asset
Document information	Digitised documents, deleted documents, temporary documents and their fragments under the TOE control.
Function information	Active Job executed by users. (Hereinafter referred to as "user job.")

Table 3-2 TOE Protected Assets (TSF data)

Type	Asset
Protected data	The information that shall be protected from changes by users without edit permission; it includes Login user name, Number of Attempts before Lockout, year/month/day setting, time setting, and Minimum Character No. of password, etc. (Hereinafter referred to as "TSF protected data.")
Confidential data	The information that shall be protected from changes by users without edit permission, and also shall be protected from reading by users without viewing permission; it includes Login password, audit log, and HDD cryptographic key. (Hereinafter referred to as "TSF confidential data.")

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Section 3.1.1 and to satisfy the organisational security policies shown in Section 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE presumes the threats shown in Table 3-3 and provides the security functions to counter them. Although threats are expressed differently from the conformance PP, the evaluation process confirmed the equivalence of both threats.

Table 3-3 Assumed Threats

Identifier	Threat
T.DOC.DIS (Document disclosure)	Documents under the TOE management may be disclosed to persons without a login user name, or to persons with a login user name but without an access permission to the document.
T.DOC.ALT (Document alteration)	Documents under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the document.
T.FUNC.ALT (User job alteration)	User jobs under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the user job.
T.PROT.ALT (Alteration of TSF protected data)	TSF Protected Data under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the TSF Protected Data.
T.CONF.DIS (Disclosure of TSF confidential data)	TSF Confidential Data under the TOE management may be disclosed to persons without a login user name, or to persons with a login user name but without an access permission to the TSF Confidential Data.
T.CONF.ALT (Alteration of TSF confidential data)	TSF Confidential Data under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the TSF Confidential Data.

* "Persons with a login user name" mean persons who are permitted to use the TOE.

3.1.1.2 Security Function Policies against Threats

All threats shown in Table 3-3 describe breaches (viewing or alteration) of user data and TSF data caused by persons who are not permitted users for the TOE, or by persons who do not have any valid authorities.
These threats are countered by the following Security Functions:

(1) User identification and authentication

The TOE requires a user to enter the login user name and login password. By confirming that the entered data are identical to the user authentication data managed internally by the TOE, the TOE verifies that the person who attempts to use the TOE is an authorised TOE user. The entry means are the input from Operation Panel of the TOE itself, the input on a Web browser of client computers, the input via drivers when using Printer Function and LAN-Fax Transmission.

As a means to ensure the necessary functional strength, the following functions are provided:

- If users fail to be authenticated consecutively until reaching the specified number of times set by the MFP administrator, the user accounts are forced to be locked out. (The user accounts cannot be used until the lockout time elapses or the lockout is released.)
- The login passwords are required, when they are set, to be composed of more than the level of quality that has been established in terms of the length (number of characters) and the character types.

When the login password is validated and a user is confirmed as an authorized TOE user, the user receives the user privilege that is set in advance in accordance with the role assigned to the user. Accordingly, the user is allowed to use the TOE. As shown in "Table 4-2 TOE Users," the roles specified by the TOE include normal user, MFP administrator, and supervisor.

As a means to support the Identification and Authentication Function, the following functions are provided:

- Display dummy characters in place of the entered login password on the input screen.
- After once logged in, if at any time the TOE is not operated by the user or anyone in a certain period of time, the user account will be automatically logged out.

(2) Access control (Access control against the user data)

For processing request by users, access control to the document information and the user jobs is performed, based on the login user names and permissions of each user role of the users. Stored documents are associated with specific information (a document user list) that stipulates which user is allowed to perform the operation (deletion, printing, and downloading, etc.). Access control to allow or deny the operation request by normal user is performed, according to the login user names and the information in the document user list. The MFP administrator is permitted to delete any stored documents, but is not permitted to perform any other operation on stored documents.

User jobs are associated with the login user names of the users that create the jobs, and the normal user who is associated with the login user name is allowed to delete the applicable job. The MFP administrator is allowed to delete all the user jobs. The supervisor is forbidden to perform any operations on the user data.

(3) Overwrite residual data

In order to protect from unauthorised access to documents that have been deleted but remain residually stored in the HDD, temporary documents and their fragments in the HDD, the residual data shall be overwritten by specified data when deleting the documents.

(4) Network protection

In order to prevent information leakage by being monitored via communication paths, TLS encrypted communication is used for communications between the TOE and client computers for the operations via a Web browser and communications using Printer Function and LAN-Fax Transmission. IPsec communication and S/MIME communication are also used for the communications between the TOE and the clients.

(5) Security management

In order to protect the TSF data from unauthorised access beyond the user permissions, access control is performed on actions, such as viewing or altering TOE setting information, and newly creating or altering user data in accordance with the TOE user roles. As a permission policy of information alteration (modification), normal users are only authorised to alter their login passwords, and supervisor is only authorised to alter the login passwords of the supervisor and the MFP administrators. Only MFP administrators are allowed to alter the TSF data, except for the above mentioned permissions.

3.1.2 Organisational Security Policies and Security Function Policies

3.1.2.1 Organisational Security Policies

Organisational security policies required in use of the TOE are shown in Table 3-4. The evaluation process has confirmed that the security policies except for P.STORAGE.ENCRYPTION are identical to the security policies in the conformance PP. P.STORAGE.ENCRYPTION is the security policy that assumes writing data into the HDD not in a directly readable format.

Table 3-4 Organisational Security Policies

Identifier	Organisational Security Policy
P.USER.AUTHORIZATION (User identification and authentication)	Only users with operation permission of the TOE shall be authorised to use the TOE.
P.SOFTWARE.VERIFICATION (Software verification)	Procedures shall exist to self-verify executable code in the TSF.
P.AUDIT.LOGGING (Management of audit log records)	The TOE shall create and maintain a log of TOE use and security-relevant events. The audit log shall be protected from unauthorised disclosure or alteration, and shall be reviewed by authorised persons.
P.INTERFACE.MANAGEMENT (Management of external interfaces)	To prevent unauthorised use of the external interfaces of the TOE, operations of those interfaces shall be controlled by the TOE and its IT environment.
P.STORAGE.ENCRYPTION (Encryption of storage devices)	The data stored on the HDD inside the TOE shall be encrypted.

3.1.2.2 Security Function Policies to Organisational Security Policies

The TOE provides the security functions to satisfy the organisational security policies shown in Table 3-4.

(1) Means to support Organisational Security Policy, "P.USER.AUTHORIZATION"

This security policy requires that only officially registered TOE users be allowed to use the TOE.
The TOE implements this policy by the following Security Function:

(a) User identification and authentication

Based on the user identification and authentication described in Section 3.1.1.2, whether a person who attempts to use the TOE is an authorised user will be verified with reference to the identification and authentication information obtained from the user. A person is provided with the user privileges that are set in advance in accordance with the role assigned to the user, so that the authorised person is allowed to use the TOE only if the person is confirmed as an authorised user.

(2) Means to support Organisational Security Policy, "P.SOFTWARE.VERIFICATION"

This security policy requires the validity of the TOE executable code to be self-verified.
The TOE implements this policy by the following Security Function:

(a) Self test

The TOE (configuration items except for FCU) runs a self test during the initialisation start-up after turning on the power, and it checks the integrity and the validity of executable codes in the MFP control software and the Operation Panel control software. The self test verifies the hash values of firmware and confirms the integrity of the executable code. The test verifies each application on the basis of a signature key and confirms the validity of the executable code.

If something abnormal is recognised in the MFP control software during the self test, an error message is displayed on the Operation Panel, and the TOE stops the operations so that normal users cannot use the TOE. If something abnormal is recognised in the Operation Panel control software, normal users cannot use the TOE through the Operation Panel. If no abnormal operations are recognised during the self test, the TOE continues the start-up processing and makes itself usable for the users.

As for the FCU, the TOE provides the verification information to perform integrity verification in a way that the users can confirm it. The users need to confirm the FCU based on this information, and can use the TOE when there is no problem.

(3) Means to support Organisational Security Policy, "P.AUDIT.LOGGING"

This security policy requires audit logs for the security events of the TOE to be acquired, and the audit logs to be appropriately managed.
The TOE implements this policy by the following Security Function:

(a) Security audit

When auditable security events occur, the TOE generates the audit logs that consist of such items as event type, user identification, occurrence date and time, and

outcome, etc., to add and save to the audit logging file. Only successfully authenticated MFP administrators are allowed to read and delete the generated audit logging file. Reading the audit logging file is executed by text format through a Web browser of client computers.
In addition, in order to record the occurrence date and time of the audit event log, the date and time information are acquired from the system clock of the TOE.

(4) Means to support Organisational Security Policy, "P.INTERFACE.MANAGEMENT"

This security policy requires that external interfaces (Operation Panel, LAN interface, USB interface, and telephone lines) of the TOE are appropriately managed without being used by unauthorised persons.
The TOE implements this policy by the following Security Functions:

(a) User identification and authentication

Based on the user identification and authentication described in Section 3.1.1.2, whether a person who attempts to use the TOE is an authorised user will be verified with reference to the identification and authentication information obtained from the user. A person is provided with the user privileges that are set in advance in accordance with the role assigned to the user, so that the authorised person is allowed to use the TOE only if the person is confirmed as an authorised user.

(b) Restricted forwarding of data to external interfaces

This function is not an implementation for active mechanism, but is addressed as architectural design of external interfaces. By its architecture, any information received from an external interface is processed by the TSF, and any information sent to an external interface is controlled by the TSF. Thus, unauthorised forwarding of data between the different external interfaces is prevented.
As for USB interfaces, unauthorised forwarding of data by using this interface is prevented by deactivating the use of USB interfaces.

(5) Means to support Organisational Security Policy, "P.STORAGE.ENCRYPTION"

This security policy requires that the TOE encrypts the stored contents on the HDD inside the TOE.
The TOE implements this policy by the following Security Functions:

(a) Stored data protection function

The encryption and decryption by AES are performed for all data written into or reading out to the HDD. When encrypting and decrypting the data, the key of 256-bits length is used. The key is created from the administrator setting an initial value and stored in the TOE.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate the TOE as useful information for the assumed readers to determine whether to use the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE. Although the assumptions in Table 4-1 are expressed differently from the conformance PP, the evaluation process confirmed the equivalence of both assumptions.
The effective performances of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.ACCESS.MANAGED (Access management)	According to the guidance document, the TOE is placed in a restricted or monitored area that provides protection from physical access by unauthorised persons.
A.USER.TRAINING (User training)	The responsible manager of MFP trains users according to the guidance document so that users are aware of the security policies and procedures of their organisation and are competent to follow those policies and procedures.
A.ADMIN.TRAINING (Administrator training)	Administrators are aware of the security policies and procedures of their organisation, and are competent to correctly configure and operate the TOE in accordance with the guidance document following those policies and procedures.
A.ADMIN.TRUST (Trusted administrator)	The responsible manager of MFP selects administrators who do not use their privileged access rights for malicious purposes according to the guidance document.

4.2 Environmental Assumptions

The TOE is installed in a general office and connected to a local area network (hereinafter referred to as "LAN"), and it is used through the Operation Panel of the TOE itself and client computers that are also connected to the LAN. Figure 4-1 shows the general operational environment as assumptions of the TOE.

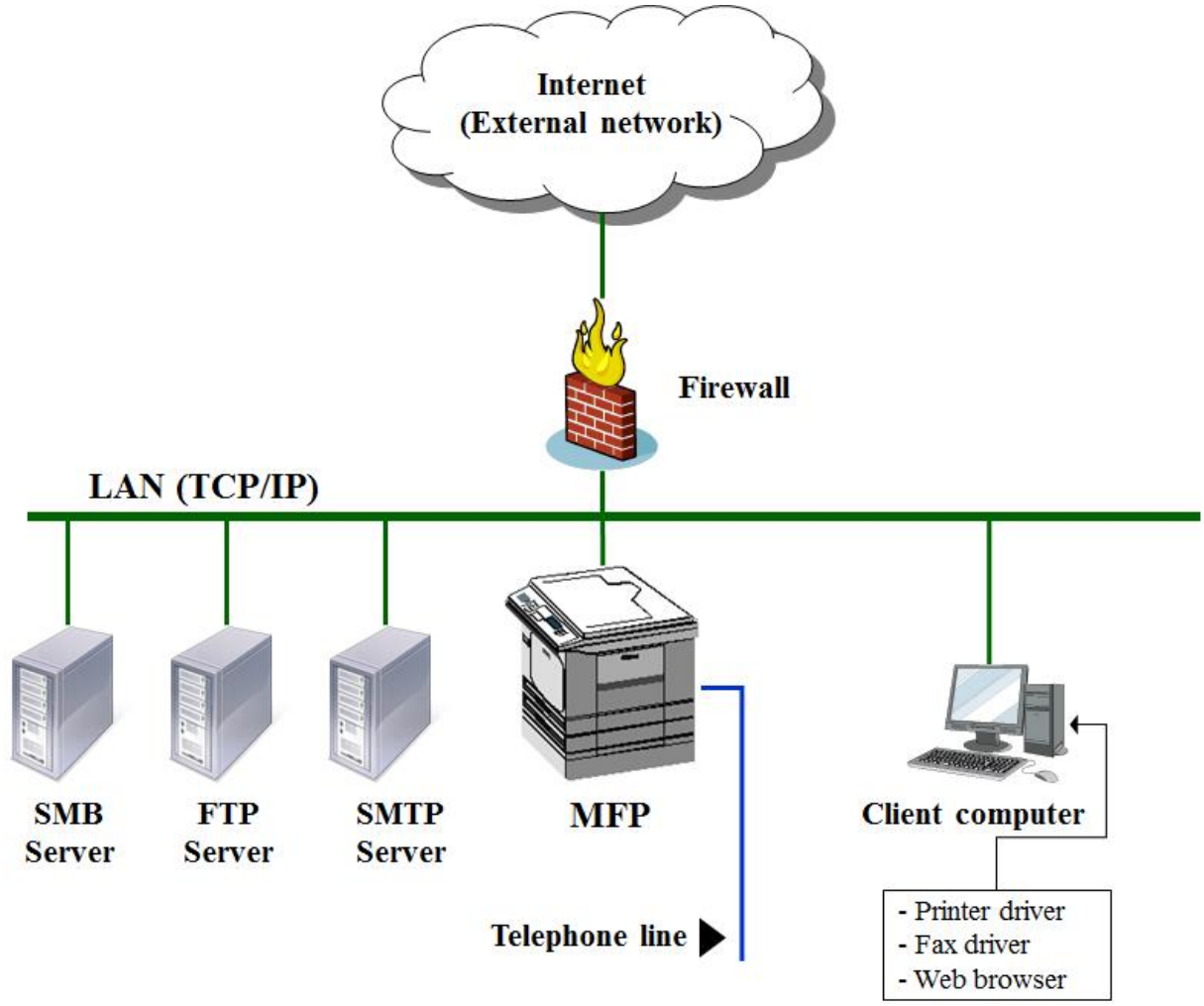

Figure 4-1 Operational Environment of the TOE

Figure 4-1 gives an example environment to handle office documents in general offices where the TOE is assumed to be used. The TOE is connected to the LAN and telephone lines.

When the TOE is connected to the LAN that is connected to an external network such as the Internet, firewalls are installed at the boundaries between the external network and the LAN to protect the LAN and the TOE from attacks that originate from the external network. The LAN is connected to server computers such as an FTP server, an SMB server, and an SMTP server, and is connected to client computers. The LAN performs the communication for the TOE to gather data such as documents and a variety of information.

The operation of the TOE includes both cases of using the Operation Panel of the TOE and using client computers. Installing the printer drivers or the fax drivers in client computers enables to process printing via the local area network from the client computers.

The following devices are assumed to be used on the operational environment:

- Client PC
  > OS: Windows 8.1/10
  > Web browser: Internet Explorer11, or Microsoft Edge 44

> Printer driver (for North America and Asia Pacific): PCL6 Driver 1.0.0.0
> Printer driver (for Europe): PCL6 Driver 1.4.0.0
> Fax driver: LAN Fax Driver 9.5.0.0

- SMTP server: Windows Server 2012 P-Mail Server Manager

- FTP server: Windows Server 2012 (IIS8), Linux (Fedora20) vsftpd

- SMB server: Windows Server 2012

Although the reliability of hardware and software shown in this configuration is outside the scope of this evaluation, it is assumed to be trustworthy.

Table 4-2 shows the associated users to use of the TOE in this environment.

Table 4-2 TOE Users

User Definition		Explanation
Normal user		A user who is allowed to use the TOE. A normal user is provided with a login user name and can use normal functions of MFP.
Administrator	Supervisor	A user who is authorised to modify the login password of the MFP administrator.
	MFP administrator	A user who is allowed to manage the TOE and performs the management operations such as normal user management, device management, file management, and network management.

As shown in Table 4-2, the TOE users are classified into normal user and administrator. According to the roles, administrators shall be identified as supervisor and MFP administrator. The users shown in Table 4-2 are direct users of the TOE. There is also a responsible manager of the MFP who, as an indirect TOE user, is authorised to select the MFP administrator and supervisor. The responsible manager of the MFP is assumed to be an organisational manager in the operational environment.

4.3 Clarification of Scope

To protect data on communication paths between client computers/each server and the TOE, it is necessary that communication protocols on client computers and each server are operated securely to work properly.
To operate client computers and each server securely is the responsibility of the operator.

5. Architectural Information

This chapter explains the scope and the main components of the TOE.

5.1 TOE Boundary and Components

Figure 5-1 shows the composition of the TOE. The TOE is the entire MFP product.

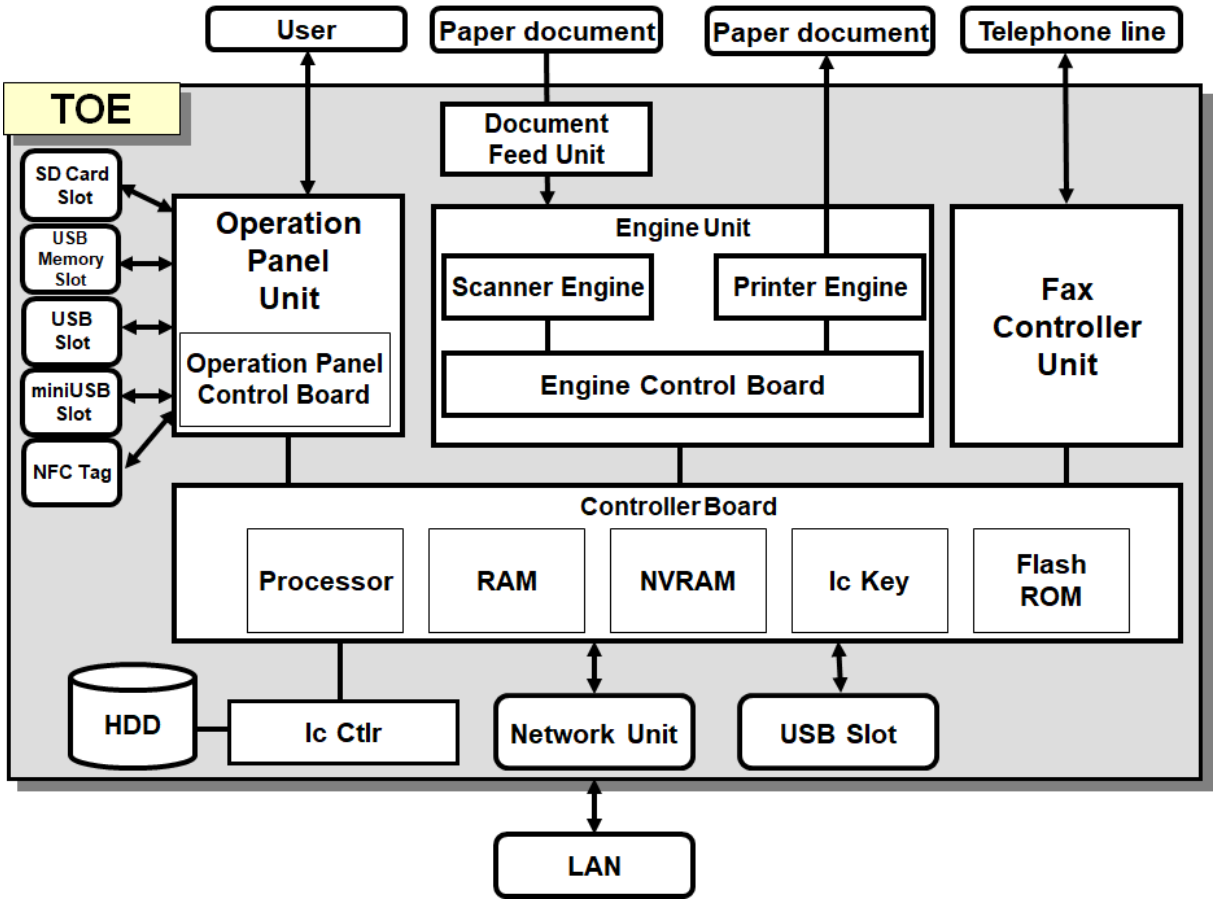

Figure 5-1 TOE Boundary

The general description of each configuration item is described as follows:

[Operation Panel Unit (hereinafter referred to as "Operation Panel")]
The Operation Panel is attached to the TOE and is an interface device that the TOE users use for the TOE operation. It features the following devices: key switches, LED indicators, an LCD touch screen, and Operation Panel Control Board. The Operation Panel control software is installed on the Operation Panel Control Board.

[Engine Unit]
The Engine Unit contains a Scanner Engine that is an input device to read paper documents, Printer Engine that is an output device to print and eject paper documents, and Engine Control Board that controls each engine.

[Document Feed Unit]
The Document Feed Unit is Auto Document Feeder (ADF) (one-pass duplex scanning ADF).

[Fax Controller Unit (FCU)]
The Fax Controller Unit is a unit that has a modem function and sends or receives fax data to and from other fax devices with G3 standard when connected to a telephone line.

[Controller Board]
The Controller Board is a device that contains Processors, RAM, NVRAM, Ic Key and FlashROM. The following describes the components of the Controller Board:

- Processor
  A semiconductor chip which carries out the basic arithmetic processing of MFP operations.
- RAM
  A volatile memory medium which is used as the image data.
- NVRAM
  A non-volatile memory medium which stores the MFP control data to configure the MFP operation.
- Ic Key
  A security chip which has the function of a random number generation and cryptographic key generation. It is used to detect alteration of the MFP Control Software.
- FlashROM
  A non-volatile memory medium in which the MFP Control Software is installed.

[HDD]
The HDD is a hard disk drive which image data as well as login user names and login passwords to be used for identification and authentication are written into.

[Ic Ctlr]
The Ic Ctlr is a security chip that has the functions to encrypt the information stored into the HDD and decrypt the information read from the HDD.

[Network Unit]
The Network Unit is an external interface to support an Ethernet LAN.

The following components are not used in normal operation.
- USB Slot (Controller Board)
- SD Card Slot (Operation Panel Unit)
- USB Memory Slot (Operation Panel Unit)
- USB Slot (Operation Panel Unit)
- miniUSB Slot (Operation Panel Unit)
- NFC Tag

5.2 IT Environment

The TOE is connected to the LAN and communicates with server computers, such as an FTP server, an SMB server, and an SMTP server, as well as with client computers. The TOE communicates with fax devices via telephone lines.

The client computer connected via the LAN uses the TOE through the printer driver, the fax driver, and the Web browser. The client computer performs not only communication of document data to the TOE, but also an operation of some management functions and status checking of the TOE via the Web browser.

6. Documentation

The identification of documents attached to the TOE is listed below. There are three sets of the guidance documents of the TOE, depending on the sales area in which the TOE is sold. There are differences between the document sets in English notations, organisation of the documents, regulation depending on a country or area, etc. However, the equivalency of the contents between them is confirmed through the evaluation process.

TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

[English version] Product-attached documents for North America

Document Name	Version
Safe Use of This Machine	D0CM-7062
Notes for Users	D0CM-7066
For Users of This Product	D0CM-7068
SOFTWARE LICENSE AGREEMENT	D0CM-7070
For Users of This Product	D181-2597
Notes to Users in the United States of America	D219-7457
Note to users in Canada	D219-7460
Safety Information	D0CP-7475
Operating Instructions Paper Fundamentals	D0CP-7477
Operator's Guide	D0CP-7478
Security Reference	D0CP-7493
Introduction and Basic Operations	D0CP-7479
Setup/System Settings	D0CP-7480
Copy	D0CP-7481
Document Server	D0CP-7482
Fax	D0CP-7483
Scan	D0CP-7484
Printer	D0CP-7485
Maintenance	D0CP-7486
Troubleshooting	D0CP-7487
Application Settings	D0CP-7488
Paper Settings	D0CP-7489
Specifications	D0CP-7490
Security	D0CP-7491
Copy (Classic)	D0CP-7494
Fax (Classic)	D0CP-7495
Scan (Classic)	D0CP-7496
Printer (Classic)	D0CP-7497
Driver Installation Guide	D0CP-7492

Document Name	Version
Notes for Administrators: Using This Machine in a Network Environment Compliant with IEEE Std 2600.2™-2009	D0CP-7087
Notes on Security Functions	D0CP-7085
Help	83NHELENZ 1.00 v251

[English version] Product-attached documents for Europe

Document Name	Version
Safe Use of This Machine	D0CM-7062
Notes for Users	D0CM-7064
Notes for Users	D0CM-7065
For Users of This Product	D0CM-7068
SOFTWARE LICENSE AGREEMENT	D0CM-7070
Note to users EU Countries	D150-1468A
Safety Information	D0CP-7474
Operating Instructions Paper Fundamentals	D0CP-7477
Operator's Guide	D0CP-7478
Security Reference	D0CP-7493
Introduction and Basic Operations	D0CP-7479
Setup/System Settings	D0CP-7480
Copy	D0CP-7481
Document Server	D0CP-7482
Fax	D0CP-7483
Scan	D0CP-7484
Printer	D0CP-7485
Maintenance	D0CP-7486
Troubleshooting	D0CP-7487
Application Settings	D0CP-7488
Paper Settings	D0CP-7489
Specifications	D0CP-7490
Security	D0CP-7491
Copy (Classic)	D0CP-7494
Fax (Classic)	D0CP-7495
Scan (Classic)	D0CP-7496
Printer (Classic)	D0CP-7497
Driver Installation Guide	D0CP-7492
Notes for Administrators: Using This Machine in a Network Environment Compliant with IEEE Std 2600.2™-2009	D0CP-7087
Notes on Security Functions	D0CP-7085
Help	83NHELENZ 1.00 v251

[English version] Product-attached documents for Asia Pacific

Document Name	Version
Safe Use of This Machine	D0CM-7062
Notes for Users	D0CM-7067
For Users of This Product	D0CM-7068
SOFTWARE LICENSE AGREEMENT	D0CM-7070
Safety Information	D0CP-7476
Operating Instructions Paper Fundamentals	D0CP-7477
Operator's Guide	D0CP-7478
Security Reference	D0CP-7493
Introduction and Basic Operations	D0CP-7479
Setup/System Settings	D0CP-7480
Copy	D0CP-7481
Document Server	D0CP-7482
Fax	D0CP-7483
Scan	D0CP-7484
Printer	D0CP-7485
Maintenance	D0CP-7486
Troubleshooting	D0CP-7487
Application Settings	D0CP-7488
Paper Settings	D0CP-7489
Specifications	D0CP-7490
Security	D0CP-7491
Copy (Classic)	D0CP-7494
Fax (Classic)	D0CP-7495
Scan (Classic)	D0CP-7496
Printer (Classic)	D0CP-7497
Driver Installation Guide	D0CP-7492
Notes for Administrators: Using This Machine in a Network Environment Compliant with IEEE Std 2600.2™-2009	D0CP-7087
Notes on Security Functions	D0CP-7085
Help	83NHELENZ 1.00 v251

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Facility

ECSEC Laboratory Inc., Evaluation Center that conducted the evaluation as the Evaluation Facility is approved under JISEC and is accredited by NITE (National Institute of Technology and Evaluation), the Accreditation Body, which joins Mutual Recognition Arrangement of ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

7.2 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance requirements in the CC Part 3. Details for evaluation activities were reported in the Evaluation Technical Report. The Evaluation Technical Report explains the summary of the TOE as well as the content of the evaluation and the verdict of each work unit in the CEM.

7.3 Overview of Evaluation Activity

The history of the evaluation conducted is described in the Evaluation Technical Report as follows.

The evaluation started in 2020-07 and concluded upon completion of the Evaluation Technical Report dated 2021-03. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted. For the development sites, site visits have been omitted, and the Evaluation Facility determined with its responsibility that the examination details on those of the past CC-certified products could be reused.

Furthermore, the evaluator conducted the sampling check of the developer testing and the evaluator testing by using the developer testing environment at the Evaluation Facility or the developer site in 2021-01.

Concerns in the evaluation process that the Certification Body found were described as the certification oversight reviews, and they were sent to the Evaluation Facility. After the Evaluation Facility and the developer examined them, those were reflected in the Evaluation Technical Report.

7.4 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had performed. As the verification results of the evidence shown in the evaluation process and the testing performed by the developer, the evaluator performed the reproducibility testing, additional testing and penetration testing based on vulnerability assessments judged to be necessary.

7.4.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer had performed and the documentation of actual test results. The content of the developer testing evaluated by the evaluator is explained as follows.

1) Developer Testing Environment

Figure 7-1 shows the testing configuration performed by the developer, and Table 7-1 shows the main configuration items.

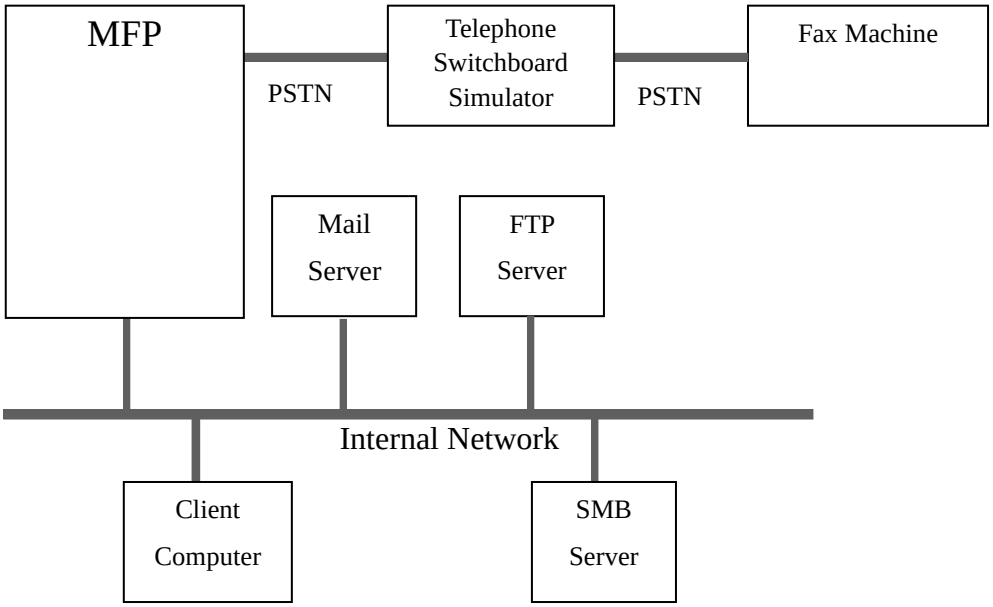

Figure 7-1 Configuration of the Developer Testing

Table 7-1 Test Configurations

Configuration Item	Detail
TOE	Configuration when the name of the MFP is Pro C5300S (For Europe) Configuration when the name of the MFP is Pro C5300S (For North America) Configuration when the name of the MFP is Pro C5310S (For Asia Pacific) (Refer to Chapter 2 for the specific contents of the configuration)

Configuration Item	Detail
Client Computer	OS: Windows 8.1/10 Web browser: Internet Explorer 11, Microsoft Edge 44 Printer driver (for North America and Asia Pacific): PCL6 Driver 1.0.0.0 Printer driver (for Europe): PCL6 Driver 1.4.0.0 FAX driver: LAN Fax Driver 9.5.0.0
Mail Server (SMTP Server)	Windows Server 2012 P-Mail Server Manager version 1.91
FTP Server	Windows Server 2012 IIS8 V8.0.9200.16384 Linux (Fedora20) vsftpd 3.0.2
SMB Server	Windows Server 2012
Telephone Switchboard Simulator	XF-A150 (Panasonic Corporation)
Fax Machine	MP C6503

Multiple MFP models are identified as the TOE in the ST. The differences between the models are printing speed and display depending on destination.

The TOE used in the developer testing is only a part of the identified models, however, these models cover all the required printing speeds and displays depending on destination.

Therefore, the evaluator judged that the developer testing was performed in the TOE testing environment consistent with the TOE configuration identified in the ST.

2) Summary of the Developer Testing

A summary of the developer testing is as follows.

a. Developer Testing Outline

An outline of the developer testing is as follows.

<Developer Testing Approach>

The testing approaches consisted of:

- stimulating the assumed external interfaces (Operation Panel, Web browser, and so on) in normal use of the TOE, and visually observing the results;
- analysing the generated audit log and the logging data for debug;
- checking the communication protocols between client computers/each server and the TOE with packet capture; and
- executing anomaly simulation tests to generate abnormal events by altering a part of the TSF implementation, and so on.

<Developer Testing Tool>

Table 7-2 shows the tool used for the developer testing.

Table 7-2 Developer Testing Tool

Name (Version)	Outline
Wireshark (2.2.5,3.0.6,3.0.11)	Packet capture tool

<Content of the Performed Developer Testing>

The expected values of testing results described in testing specifications which are provided in advance by the developer were compared to the values of the actual developer testing results described in the testing result reports which are also provided by the developer. As a result, it was found that the values of the actual testing results are in conformity to those of the expected testing results.

b. Scope of the Performed Developer Testing

The developer testing was performed on about 500 items by the developer.

By the coverage analysis, it was verified that all security functions and external interfaces described in the functional specification had been tested.

c. Result

The evaluator confirmed the approach of the performed developer testing and the validity of tested items, and confirmed consistencies between the testing approach described in the testing plan and the actual testing approach.

The evaluator confirmed consistencies between the expected test results by the developer and the actual test results performed by the developer.

7.4.2 Evaluator Independent Testing

The evaluator performed the sample testing to reconfirm the implementation of security functions using the test items extracted from the developer testing. In addition, the evaluator performed the evaluator independent testing (hereinafter referred to as the "independent testing") to gain further confidence that security functions are certainly implemented, based on the evidence shown in the process of the evaluation.

The independent testing performed by the evaluator is explained as follows.

1) Independent Testing Environment

The configuration of the independent testing performed by the evaluator was the same as the configuration of the developer testing as shown in Figure 7-1.

2) Summary of the Independent Testing

A summary of the independent testing is as follows.

a. Viewpoints of the Independent Testing

Viewpoints of the independent testing are shown below, which are devised by the evaluator based on the analysis of developer testing and the evaluation documentation provided.

<Independent Testing Viewpoints>

1. For TSFI that has many types of input parameters and to which the developer testing is insufficient in terms of completeness, the testing items such as parameter scheme, boundary values, and abnormal values are added.

2. For execution timing of several TSFs and combination of execution, the testing items to which conditions are added are performed.

3. The testing items to which the different variation from the developer testing is added are performed in regard to procedures of exception and cancellation.

4. The testing items are selected in the sampling testing from the following viewpoints:
   - The testing items are selected to include all of TSFs and TSFIs in terms of completeness.
   - The testing items are selected to cover the different testing approaches and testing environments.
   - The testing items involving TSFI that meet many of the SFRs are mainly selected in order to conduct tests efficiently.

b. Independent Testing Outline

An outline of the independent testing that the evaluator performed is as follows.

<Independent Testing Approach>

In setting the different initialisation and the different parameters from the developer testing, the independent testing approaches consisted of:
- stimulating the assumed external interfaces (Operation Panel, Web browser, and so on) in normal use of the TOE, and visually observing the results;
- analysing the generated audit log; and
- checking the communication protocols between client computers/each server and the TOE with packet capture, and so on.

<Content of the Performed Independent Testing>

Based on the viewpoints of the independent testing, 23 items for the independent testing and 19 items for the sampling testing were performed.

The outline of the main independent testing performed and corresponding viewpoints are shown in Table 7-3.

Table 7-3 Viewpoints for the Independent Testing

Viewpoints for the Independent Testing	Outline of the Independent Testing
1	- Confirm that the behaviours concerning the user account lock are as specified by changing conditions, etc. - Confirm that the access control of the stored document is as specified for the combination with the access means. - Confirm that the access control of the stored document is as specified for the combination with editing of the stored document. - Confirm that the customisation of the operation panel display does not affect the security function.
2	- Confirm that the auto logout process is performed as specified while the same user simultaneously logged on. - Confirm that the behavior when changing the auto logout time during login is as specified. - Confirm that access control is performed as specified when the change of access authority to the internally stored document and the operation of the internally stored document is performed from a different interface. - Confirm that normal users cannot change the settings relevant to the security from several interfaces.

Viewpoints for the Independent Testing	Outline of the Independent Testing
3	- Confirm that the IPsec procedure is performed as specified when using the expired certificates. - Confirm that the exception procedures are performed as specified when entering unauthorised inputs from the printer driver. - Confirm that the fax function is performed as specified when an error occurs and transmission standby queue is full. - Confirm that the procedures are performed as specified even when performing unexpected operations or entering unexpected parameters on the Operation Panel. - Confirm that the access control is still performed as specified even when an abnormal parameter specification or an interruption occurs at editing of the stored document. - Confirm that the deactivated features are actually deactivated.

c. Result

All the independent testing performed by the evaluator was correctly completed, and the evaluator confirmed the behaviour of the TOE. The evaluator confirmed consistencies between the expected behaviour and all the test results.

7.4.3 Evaluator Penetration Testing

The evaluator devised and performed the necessary evaluator penetration testing (hereinafter referred to as the "penetration testing") on the potentially exploitable vulnerabilities of concern under the assumed environment of use and attack level from the evidence shown in the process of the evaluation.

The penetration testing performed by the evaluator is explained as follows.

1) Summary of the Penetration Testing

A summary of the penetration testing performed by the evaluator is as follows.

a. Vulnerability of Concern

The evaluator searched into the provided documentation and the publicly available information for the potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing.

1. Unauthorised access to the TOE may be caused by unexpected interfaces.

2. Security Functions may be bypassed in case of entering data, for interfaces, which have the values and formats that are unintended by the TOE.
3. There may be some vulnerabilities when implementing secure channels, and consequently the Security Functions of the TOE may be bypassed.
4. Security Functions may be bypassed by maintaining the TOE overloaded.

b. Penetration Testing Outline

The evaluator performed the following penetration testing to identify potentially exploitable vulnerabilities.

<Penetration Testing Environment>

The penetration testing configuration is identical with those of the developer testing shown in Figure 7-1, and evaluator independent testing.

Table 7-4 shows key tools used in the penetration testing.

Table 7-4 Penetration Testing Tools

Name (Version)	Outline
ZAP (2.7.0)	Inspection tool of Web vulnerabilities with Proxy traffic
nmap (7.70)	Port Scanning Tool
Netcat (1.12)	Packet Communication Tool
Nessus (8.8.0) Plugin 202101132029	Vulnerability Scanning Tool
Burp Suite Professional (1.7.37)	Inspection tool of Web vulnerabilities with Proxy traffic
Wireshark (2.2.5, 3.0.6, 3.0.11)	Packet Capture Tool
OpenSSL 1.0.1j	Software library that provides the SSL/TLS protocol
PRET (0.40)	PJL and PostScript test tools
Android Debug Bridge (1.0.41)	Debugging tool for Android OS devices. (Used for the TOE components operated by Android OS.)

<Content of the Performed Penetration Testing>

Table 7-5 shows vulnerabilities concerned and the content of the related penetration testing. The evaluator performed 15 test cases in the following penetration testing to identify possibly exploitable vulnerabilities:

Table 7-5 Outline of the Performed Penetration Testing

Vulnerability	Outline of the Penetration Testing
1	Confirmed that the unexpected available interfaces were not exist by using the port scanning tool, the vulnerability scanning tool, and debug tool.

Vulnerability	Outline of the Penetration Testing
2	Checked no publicly-known vulnerabilities on Web interfaces to access the TOE. Confirmed that the Security Functions may not be bypassed by the specified URL at the time of connecting to the TOE via a Web browser. Checked no implementation-specific vulnerabilities regarding PJL, PostScript, and SQL.
3	Checked no implementation-specific vulnerabilities regarding the encryption communication with TLS and IPsec. Confirmed that parameters were not easily predicted by verifying the randomness of numbers as parameters used in Web interfaces.
4	Confirmed that the TOE was not unsecured due to insufficient resources.

c. Result

In the penetration testing performed by the evaluator, the evaluator did not find any exploitable vulnerabilities that attackers who have the assumed attack potential could exploit.

7.5 Evaluated Configuration

The configuration conditions of the TOE, which are the prerequisites for this evaluation, are described in the guidance documents listed in Chapter 6. In order to enable the security functions of the TOE and use them securely, the TOE must be set as described in the guidance documents. Different settings from those described in the guidance documents are not subject to the assurance of this evaluation.

7.6 Evaluation Results

The evaluator had concluded that the TOE satisfies all work units prescribed in the CEM as per the Evaluation Technical Report.

In the evaluation, the following were confirmed.

- PP Conformance:

  U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)

  The TOE also conforms to the following SFR packages defined in the above PP.

  - 2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B
  - 2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B
  - 2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B
  - 2600.2-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment B
  - 2600.2-DSR, SFR Package for Hardcopy Document Storage and Retrieval Functions, Operational Environment B
  - 2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B

- Security functional requirements: Common Criteria Part 2 Extended

- Security assurance requirements: Common Criteria Part 3 Conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.

- All assurance components of EAL2 package

- Additional assurance component ALC_FLR.2

The result of the evaluation is only applied to those which are composed by the TOE corresponding to the identification described in Chapter 2.

7.7 Evaluator Comments/Recommendations

There is no evaluator recommendation to be addressed to procurement entities.

8. Certification

Based on the evidence submitted by the Evaluation Facility during the evaluation process, the Certification Body has performed certification by checking that the following requirements are satisfied:

1. The submitted documentation was sampled, the content was examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.

2. Rationale of the evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.

3. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in the certification process were prepared as the certification oversight reviews, and they were sent to the Evaluation Facility.
The Certification Body confirmed such concerns pointed out in the certification oversight reviews were solved in the ST and the Evaluation Technical Report and issued this Certification Report.

8.1 Certification Result

As a result of verification of the Evaluation Technical Report and related evaluation documentation submitted by the Evaluation Facility, the Certification Body determined that the TOE evaluation satisfies all assurance requirements for EAL2 augmented by ALC_FLR.2 in the CC Part 3.

8.2 Recommendations

Any influences on the security functions of the TOE in the operation, in the case the Maintenance Functions are activated, are out of the scope of the assurance provided by this evaluation. Therefore, it is advised to make a judgment at the administrator's responsibility about the acceptance of maintenance.

It should be noted that the TOE users need to refer to the description of "4.3 Clarification of Scope" and to see whether or not the evaluated scope of the TOE and the operational requirement items can be handled in the actual operating environment of the TOE.

To make sure of the TOE identification, checking the sticker on the surface of package as well as display of the TOE should be required, as described in Chapter 2. Be sure to keep the information described on this sticker to certainly identify the TOE.

9. Annexes

There is no annex.

10. Security Target

The Security Target [12] of the TOE is provided as a separate document from this Certification Report.

RICOH Pro C5300S/C5310S, SAVIN Pro C5300S/C5310S, LANIER Pro C5300S/C5310S, nashuatec Pro C5300S/C5310S, Rex Rotary Pro C5300S/C5310S, Gestetner Pro C5300S/C5310S, infotec Pro C5300S/C5310S Security Target, Version 1.00, March 16, 2021, RICOH COMPANY, LTD.

11. Glossary

The abbreviations relating to the CC used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

The abbreviations relating to the TOE used in this report are listed below.

FCU	An abbreviation of Fax Controller Unit.
HDD	An abbreviation of Hard Disk Drive; in this document, it indicates the HDD installed in the TOE if simply described as "HDD."
IPsec	Security Architecture for Internet Protocol; a protocol that provides the functions of data tampering prevention and data confidentiality with IP packets traffic using cryptographic technology.
MFP	An abbreviation of a digital multifunctional product.
PSTN	An abbreviation of Public Switched Telephone Networks.
S/MIME	Secure / Multipurpose Internet Mail Extensions; a standard for e-mail encryption and digital signatures with a public key system.

The definitions of terms used in this report are listed below.

Administrative role	Pre-defined roles that enable administrators to be given. Although the following four types of administrative roles are defined and can be assigned to respective administrators, the TOE assumes the MFP administrator who is assigned to all the roles. (The access control for each subcategorised administrative role is excluded from this evaluation.) - Device administrator (executes device administration and audit) - User administrator (executes the management of normal users) - Network administrator (executes the network connection management of the TOE) - File administrator (executes the management of stored documents and document user list)

Documents	General term for paper documents and electronic documents operated by the TOE.
Internet Fax	A function to perform fax communications with the system of sending or receiving e-mails. It also uses the Internet lines.
IP-Fax	A generic term of Realtime-Internet Fax of RICOH, conformant with the International Standard ITU-T T.38. It assigns IP address to a fax that is connected to a telephone line, instead of Fax number.
LAN-Fax Transmission	One of the Fax Functions. A function that transmits fax data and stores documents using the fax driver on client computers.
Lockout	The state of making the user accounts unavailable.
Lockout time	The time from being locked out to automatically releasing the user accounts.
Login password	A password corresponding to each login user name.
Login user name	An identifier assigned to normal users, an MFP administrator, and a supervisor. The TOE identifies users by this identifier.
Maintenance Function	A function to perform maintenance service for machine malfunctions. In the operation of the TOE, the Service Mode Lock Function is set to "ON" for deactivating this function.
Number of Attempts before Lockout	The number of consecutive failed attempts to identify and authenticate users, which is allowable until locking out the user accounts. The MFP administrator can assign 1 to 5 as a setting value.
Stored Documents	Documents stored in the TOE so that they can be used with Document Server Function, Printer Function, Scanner Function, and Fax Function.
User job	A work, from beginning to end, for each of the following TOE functions: Copy, Document Server, Scanner, Printer, and Fax. A user job may be paused or cancelled during the process by a user. If a user job is cancelled, the user job will end.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme Document, July 2018, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, September 2018, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, September 2018, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001, (Japanese Version 1.0, July 2017)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-002, (Japanese Version 1.0, July 2017)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-003, (Japanese Version 1.0, July 2017)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 5, April 2017, CCMB-2017-04-004, (Japanese Version 1.0, July 2017)

[12] RICOH Pro C5300S/C5310S, SAVIN Pro C5300S/C5310S, LANIER Pro C5300S/C5310S, nashuatec Pro C5300S/C5310S, Rex Rotary Pro C5300S/C5310S, Gestetner Pro C5300S/C5310S, infotec Pro C5300S/C5310S Security Target, Version 1.00, March 16, 2021, RICOH COMPANY, LTD.

[13] RICOH Pro C5300S/C5310S, SAVIN Pro C5300S/C5310S, LANIER Pro C5300S/C5310S, nashuatec Pro C5300S/C5310S, Rex Rotary Pro C5300S/C5310S, Gestetner Pro C5300S/C5310S, infotec Pro C5300S/C5310S Evaluation Technical Report, Version 2.0, March 31, 2021, ECSEC Laboratory Inc., Evaluation Center

[14] U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)

[15] CCEVS Policy Letter #20, 15 November 2010, National Information Assurance Partnership