Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application Date/ID	2012-01-25 (ITC-2396)
Certification No.	C0394
Sponsor	Canon Inc.
TOE Name	Canon imageRUNNER ADVANCE C2200 Series 2600.1 model
TOE Version	1.1
PP Conformance	IEEE Std 2600.1™-2009
Assurance Package	EAL3 Augmented with ALC_FLR.2
Developer	Canon Inc.
Evaluation Facility	ECSEC Laboratory Inc. Evaluation Center

This is to report that the evaluation result for the above TOE is certified as follows.
2013-07-10

Takumi Yamasato, Technical Manager
Information Security Certification Office
IT Security Center
Technology Headquarters

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

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 3
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 3

Evaluation Result: Pass

"Canon imageRUNNER ADVANCE C2200 Series 2600.1 model" 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 1
1.1 Product Overview 1
1.1.1 Assurance Package 1
1.1.2 TOE and Security Functionality 1
1.1.2.1 Threats and Security Objectives 1
1.1.2.2 Configuration and Assumptions 2
1.1.3 Disclaimers 2
1.2 Conduct of Evaluation 2
1.3 Certification 2
2. Identification 3
3. Security Policy 4
3.1 Security Function Policies 5
3.1.1 Threats and Security Function Policies 5
3.1.1.1 Threats 5
3.1.1.2 Security Function Policies against Threats 5
3.1.2 Organizational Security Policies and Security Function Policies 6
3.1.2.1 Organizational Security Policies 6
3.1.2.2 Security Function Policies to Organizational Security Policies 7
4. Assumptions and Clarification of Scope 10
4.1 Usage Assumptions 10
4.2 Environmental Assumptions 10
4.3 Clarification of Scope 12
5. Architectural Information 13
5.1 TOE Boundary and Components 13
5.2 IT Environment 14
6. Documentation 15
7. Evaluation conducted by Evaluation Facility and Results 16
7.1 Evaluation Approach 16
7.2 Overview of Evaluation Activity 16
7.3 IT Product Testing 17
7.3.1 Developer Testing 17
7.3.2 Evaluator Independent Testing 19
7.3.3 Evaluator Penetration Testing 22
7.4 Evaluated Configuration 24
7.5 Evaluation Results 25
7.6 Evaluator Comments/Recommendations 25
8. Certification 26
8.1 Certification Result 26

8.2 Recommendations 27
9. Annexes 28
10. Security Target 28
11. Glossary 29
12. Bibliography 31

1. Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "Canon imageRUNNER ADVANCE C2200 Series 2600.1 model Version 1.1" (hereinafter referred to as the "TOE") developed by Canon Inc., and the evaluation of the TOE was finished on 2013-06-28 by ECSEC Laboratory Inc., Evaluation Center (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, Canon Inc., and provide security information to procurement personnel and consumers who are interested in this TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") that is the appendix of this report together. 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 "procurement personnel and general consumers who purchase this TOE" 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 Assurance Package

Assurance Package of the TOE is EAL3 augmented with ALC_FLR.2.

1.1.2 TOE and Security Functionality

The TOE is a multifunction printer (hereinafter referred to as "MFP") that offers Copy, Print, Universal Send, and I-fax capabilities. Additionally, the TOE supports connection of a Fax Board as an option to provide the telephone-based fax transmission.

The security functions provided by the TOE satisfy all security functional requirements, as required and defined in the Protection Profile for Hardcopy Devices, IEEE Std 2600.1™-2009 [14] (hereinafter referred to as the "PP").

About these security functionalities, the validity of the design policy and the accuracy of the implementation were evaluated within the scope of the assurance package. The TOE assumes threats and assumptions as described in the following sections.

1.1.2.1 Threats and Security Objectives

The TOE assumes threats as described below and provides the security functions to counter those threats.

Assets of the TOE, namely user document data and the data that have an effect on security functions, are susceptible to unauthorized disclosure or alteration through manipulation of the TOE, or through access to the TOE's network communications data.

To prevent unauthorized disclosure or alteration of those assets, the TOE provides security functions such as identification and authentication, access control, and encryption.

1.1.2.2 Configuration and Assumptions

The evaluated product is assumed to be operated under the following configuration and assumptions.

It is assumed that the TOE will be located in an environment where the physical components of the TOE and its interfaces are protected from unauthorized access. The TOE shall be configured and maintained appropriately according to the guidance documents.

1.1.3 Disclaimers

- The conformance to the PP claimed by this TOE includes the fax function. Therefore, the evaluated configuration includes a fax board as an optional feature of the MFP or TOE. Hence, the following are inconsistent with the evaluated configuration.
  > Configurations without a fax board
- The Identification and Authentication Function contained in the target of this evaluation does not apply to incoming print jobs. Although the protocol used in the submission of the print job contains an identification and authentication mechanism, that mechanism is out of the scope of this evaluation.

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 on 2013-06, based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[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] and the Observation Reports 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. Those concerns pointed out by the Certification Body were fully resolved, and the Certification Body confirmed 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 submitted by the Evaluation Facility and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

TOE Name: Canon imageRUNNER ADVANCE C2200 Series 2600.1 model

TOE Version: 1.1

Developer: Canon Inc.

The TOE consists of the following software, hardware, and licenses.

Table 2-1 Components of the TOE

Component Name	Description
(Japanese Name) Canon imageRUNNER ADVANCE C2200 Series (English Name) Canon imageRUNNER ADVANCE C2200 Series	Any of the following MFP: iR-ADV C2230, iR-ADV C2225, or iR-ADV C2220.
(Japanese Name) iR-ADV Security Kit-D1 for IEEE 2600.1 Ver 1.01 (English Name) iR-ADV Security Kit-D1 for IEEE 2600.1 Common Criteria Ver 1.01	It contains the control software and security kit license for "Canon imageRUNNER ADVANCE C2200 Series."
(Japanese Name) HDD Data Encryption Kit-C (Canon MFP Security Chip 2.01) (English Name) HDD Data Encryption Kit-C (Canon MFP Security Chip 2.01)	Hardware which encrypts all data stored in the HDD.

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

According to the procedure written in the guidance documents, the user operates the control panel of the MFP and confirms the identification information of the TOE components displayed on the panel.

3. Security Policy

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

In addition to offering MFP capabilities such as Copy, Print, and Scan, the TOE is capable of storing user document data in its hard disk and has the functionality for interacting with user terminals and various servers over the network.

The PP, to which the TOE is conformant, assumes an environment where a relatively high level of security is ensured and where accountability for actions is required, and specifies the security functional requirements for such an environment.

To supplement the use of the MFP functions, the TOE offers security functions that satisfy the security functional requirements specified in the PP. These include user identification and authentication, access control, HDD data encryption and data erase functions, and cryptographic communication protocols, and protect user document data and setting data that have an effect on TOE security functions, which are TOE assets, from unauthorized disclosure and alteration.

In terms of the use of the TOE, the following roles are assumed.

- U.NORMAL
  A User who is authorized to perform User Document Data processing functions of the TOE, such as Copy, Print, and Scan.

- U.ADMINISTRATOR
  The TOE user in this role has special privileges that allow configuration of security functions.

- TOE Owner
  A person or organizational entity responsible for protecting TOE assets and establishing related security policies.

The TOE assets are defined as follows.

- User Document Data
  User Document Data consist of the information contained in a user's document.

- User Function Data
  User Function Data are the information about a user's document or job to be processed by the TOE. This includes information such as print priority and print settings.

- TSF Confidential Data
  TSF Confidential Data are data used by the security functions, and for which integrity and confidentiality must be preserved. This includes information such as user password, Box PIN, and audit logs. This does not, however, include cryptographic keys, since the user has no interface to its access.

- TSF Protected Data
  TSF Protected Data are data used by the security functions, and for which only integrity must be preserved. This includes information such as user identification and access privilege information.

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Chapter 3.1.1, and to satisfy the organizational security policies shown in Chapter 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE assumes the threats shown in Table 3-1 and provides the security functions to counter them.

Table 3-1 Assumed Threats

Identifier	Threat
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons
T.DOC.ALT	User Document Data may be altered by unauthorized persons
T.FUNC.ALT	User Function Data may be altered by unauthorized persons
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons

3.1.1.2 Security Function Policies against Threats

The TOE counters the threats shown in Table 3-1 by the following security function policies.

(1) Countermeasures against threat "T.DOC.DIS," "T.DOC.ALT," and "T.FUNC.ALT"

These are threats to user data. The TOE counters the threats by the following functions: "User Authentication," "Function Use Restriction," "Job Output Restriction," "HDD Data Erase," "HDD Data Encryption" and "LAN Data Protection."

"User Authentication" and "Function Use Restriction" function of the TOE allow only the authorized users to use the TOE functions. For details, refer to the description of P.USER_AUTHORIZATION in Section 3.1.2.2.

"Job Output Restriction" function of the TOE enforces access control when an identified and authenticated user performs the operation such as Print, Fax TX (send), Delete, and Change Print Priority on print jobs and fax/I-fax jobs stored in the TOE, thereby ensuring that only the owner of the documents or U.ADMINISTRATOR gains access to perform these operations. The TOE determines that the identified and authenticated

user is the authorized document owner as follows:

- For documents submitted as print jobs, the identified and authenticated user is determined to be the owner of the document if his/her username matches the user name information of the document specified upon submission of the print job.

- For document data stored by fax/I-fax, the user is required to enter the correct Inbox PIN when the user operates the document data. 7-digit box PIN is assigned by U.ADMINISTRATOR to the Memory RX Inbox where these document data are stored. When U.ADMINISTRATOR accesses the TOE from Remote UI, if the U.ADMINISTRATOR enters the correct PIN, then the U.ADMINISTRATOR is determined to be the owner of the document data stored in the Memory RX Inbox.

"HDD Data Erase" function of the TOE permanently erases the HDD area where the document data are stored, by overwriting with random data upon deleting the document data, to prevent the deleted document data from being read from the HDD.

"HDD Data Encryption" function of the TOE encrypts all data stored in the removable HDD of the TOE, and prevents that the underlying information are disclosed or altered by tampering the detached HDD from the MFP. It uses the 256-bit AES encryption algorithm. Its cryptographic key is generated using the FIPS PUB 186-2 deterministic random number generator algorithm at start-up, and destroyed upon power off.

"LAN Data Protection" function of the TOE uses the secure communication protocol, IPsec, when the TOE communicates with other IT devices over the LAN, and protects the communicated data from unauthorized disclosure and alteration.

With the above functions, the TOE prevents unauthorized use of the TOE, unauthorized access to data stored in the HDD and communication data; thus, the TOE protects the data to be protected from unauthorized disclosure and alteration.

(2) Countermeasures against threat "T.PROT.ALT," "T.CONF.DIS," and "T.CONF.ALT"

These are threats to TSF data that affect the security functions. The TOE counters the threats by the following functions: "User Authentication," "Management," "HDD Data Encryption," and "LAN Data Protection."

"Management" function of the TOE allows only the authorized U.ADMINISTRATOR to manage user information and various configuration data. Note, however, that the authorized U.NORMAL can change own password.

"User Authentication," "HDD Data Encryption," and "LAN Data Protection" work as described in (1).

With the above functions, the TOE prevents unauthorized use of the TOE, unauthorized access to data stored in the HDD and communication data; thus, the TOE protects the data to be protected from unauthorized disclosure and alteration.

3.1.2 Organizational Security Policies and Security Function Policies

3.1.2.1 Organizational Security Policies

Organizational security policies required in use of the TOE are shown in Table 3-2. These organizational security policies are the same as specified in the PP except for addition of

P.HDD.ACCESS.AUTHORIZATION. P.HDD.ACCESS.AUTHORIZATION is augmented for the PP under the assumption that it would generally be required to use a removable HDD on the TOE.

Table 3-2 Organizational Security Policies

Identifier	Organizational Security Policy
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.
P.HDD.ACCESS.AUTHORIZATION	To prevent access TOE assets in the HDD with connecting the other HCDs, the TOE will have authorized access the HDD data.

3.1.2.2 Security Function Policies to Organizational Security Policies

The TOE provides the security functions to satisfy the organizational security policies shown in Table 3-2.

(1) Means for organizational security policy "P.USER.AUTHORIZATION"

This policy is realized by "User Authentication" and "Function Use Restriction" functions of the TOE.

"User Authentication" function of the TOE only permits the users who are successfully identified and authenticated to use the TOE. To enhance the identification and authentication mechanism, the TOE enforces a password policy to use passwords of a certain minimum length containing a mixture of character types, and a lockout policy whereby a lockout of certain duration is imposed upon a certain number of failed authentication attempts.

Incoming print jobs or fax/I-fax jobs are accepted without requiring identification and authentication. The resulting document data are stored within the TOE, and not automatically printed out nor transmitted. To print out or transmit document data stored in the TOE, the users must operate the control panel of the TOE, which will require identification and authentication.

"Function Use Restriction" function of the TOE performs access control on the use of the TOE functions, so that only the identified and authorized users with appropriate permissions are permitted to use the functions. For access control, users are assigned "roles" which are bound to permission information. This information is used to determine whether the use of the function is permitted to each user or not.

With the above functions, the TOE ensures that only the authorized users are permitted to use the TOE.

(2) Means for organizational security policy "P.SOFTWARE.VERIFICATION"

This policy is realized by "Self-Test" function of the TOE.

"Self-Test" function of the TOE checks the integrity of the cryptographic algorithm and the cryptographic key generation algorithm that are used by LAN Data Protection function, after decrypting the executable code which is encrypted and stored in the HDD, at start-up. Thereby, the integrity of the executable code of the TOE security functions is examined.

Note that the self-test function does not check all executable codes of the TOE security functions; however, the evaluator evaluates that if the integrity of the part of the TOE security functions is verified, the integrity of all other executable codes decrypted by the same mechanisms is also ensured.

(3) Means for organizational security policy "P.AUDIT.LOGGING"

This policy is realized by "Audit Log" function of the TOE.

"Audit Log" function of the TOE generates and stores audit logs in the TOE's HDD at the occurrence of security-relevant events when security functions are used. The stored audit logs can be viewed only by an authorized U.ADMINISTRATOR via a Web browser.

(4) Means for organizational security policy "P.INTERFACE.MANAGEMENT"

This policy is realized by "User Authentication" and "Forward Received Jobs" functions of the TOE.

"User Authentication" function of the TOE ensures that only identified and authenticated users are allowed to use the TOE. Additionally, a session will be terminated if a user leaves the session inactive longer than the specified time.

"Forward Received Jobs" function of the TOE restricts data received from any interface to be forwarded directly to the LAN without prior processing by the TOE.

These functions prevent the unauthorized use of the interfaces of the TOE.

(5) Means for organizational security policy "P.HDD.ACCESS.AUTHORIZATION"

This policy is realized by the Device Identification and Authentication function, which is part of "HDD Data Encryption" function of the TOE.

The Device Identification and Authentication function in the "HDD Data Encryption" function is provided by the HDD Data Encryption & Mirroring Kit-C, one of the

components of the TOE. The HDD Data Encryption & Mirroring Kit-C acquires the MFP device authentication ID from the MFP device when it is initially mounted. At each start-up, it uses this information for a challenge and response method to confirm the identity of the MFP device, and grants access to the HDD only if it confirms successfully that it is mounted on the authorized MFP device.

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 the use of the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE. These assumptions are the same as specified in the PP.

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	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures. * The meaning of "correctly configure" includes the description specified in (1) and (2) of Section 8.2 "Recommendations."
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

4.2 Environmental Assumptions

The TOE is an MFP designed to operate in a typical office environment, where the MFP is connected by an internal LAN, and the internal LAN is protected by Firewall, etc., from the threats of the external network. The assumed operational environment of the TOE is shown in Figure 4-1.

TOE users can operate the TOE from its control panel, from a PC connected via USB, or from a PC connected to the LAN.

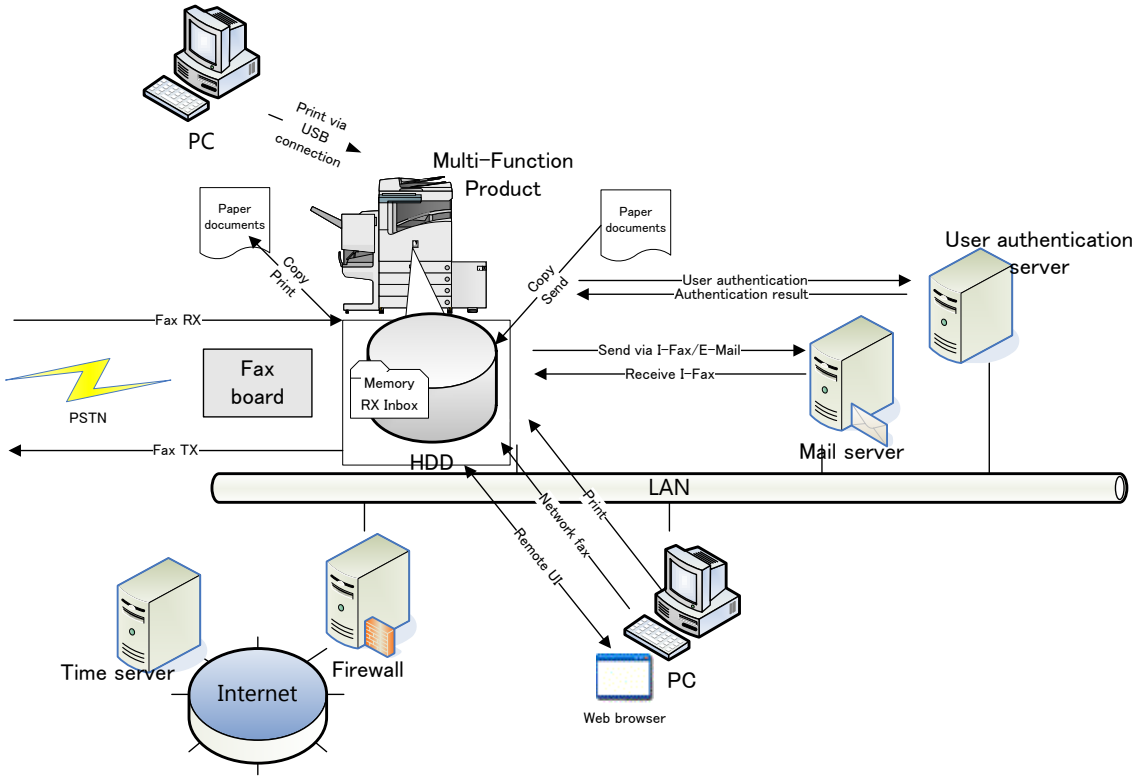

Figure 4-1 Operational Environment of the TOE

The operational environment of the TOE consists of the following components.

(1) Fax Board
It is attached to the TOE to provide fax transmission using the public telephone network (PSTN). The Fax Board is outside the scope of the TOE.

This evaluation was performed using the Canon Super G3 FAX Board-AH2.

(2) PC
It is a generic PC used by a user to connect to the TOE, via USB or internal LAN. It requires the following software.

- Printer driver: (Evaluation performed using) Canon LIPS LX Printer Driver Version 20.80
- Web browser: (Evaluation performed using) Microsoft Internet Explorer 8

(3) User Authentication Server
The TOE supports two methods of "User Authentication" of the TOE described in Chapter 3: "Internal Authentication" where authentication takes place using user information stored within the TOE, and "External Authentication" where authentication takes place using user information stored in an external server.

The User Authentication Server is the server that is necessary for the TOE when using External Authentication, and the authentication protocol to be used is either Kerberos or LDAP.

This evaluation was performed using eDirectory 8.8 SP2 as the authentication server software for LDAP authentication, and using Active Directory Domain Service as the authentication server software for Kerberos authentication.

(4) Mail Server
A Mail Server is installed as required to facilitate the I-fax capability of the MFP.

(5) Time Server
It is the NTP service commonly provided over the Internet. As long as the environment allows, it is recommended that a time server be configured in the TOE, to synchronize the time in the MFP that is used as the time stamp of audit logs. Otherwise, the time that is configured and maintained by the TOE's Management function is used instead.

Note that the reliability of software and hardware other than the TOE shown in this configuration is not subject to the evaluation.

4.3 Clarification of Scope

In this evaluation, it is considered that the security functional requirements for the identification and authentication specified in the PP regarding the MFP's Print function do not apply to the operations on submitting print jobs; rather, they apply only to the operations on document data accumulated in the MFP, created by the submitted print jobs. As such, the following security functions are considered out of the scope of this evaluation.

(1) The TOE supports various print protocols for the submission of print jobs. Some protocols have their own identification and authentication mechanisms, but those mechanisms are out of the scope of this evaluation. An example of this includes the identification and authentication mechanism in the IPP protocol.

(2) When submitting a print job to the TOE through a print driver, a user is asked to provide the user name and PIN. This input is not used by the identification and authentication function. A PIN is associated with each document data submitted as a print job, and the user must provide the correct PIN in order to print that data from the control panel (This is known as "Secured Print"). This behavior is outside the scope of this evaluation.
The user name is not authenticated for its validity, but is simply associated with the submitted print job. The user name is used by the access control function for the target of evaluation.

5. Architectural Information

This chapter explains the scope and the main components (subsystems) of the TOE.

5.1 TOE Boundary and Components

The configuration of the MFP or TOE as well as the IT environment other than MFP is shown in Figure 5-1. In Figure 5-1, the TOE is shown within the bold line box. User Authentication Server, Mail Server, PC, Time Server and User are outside of the TOE.

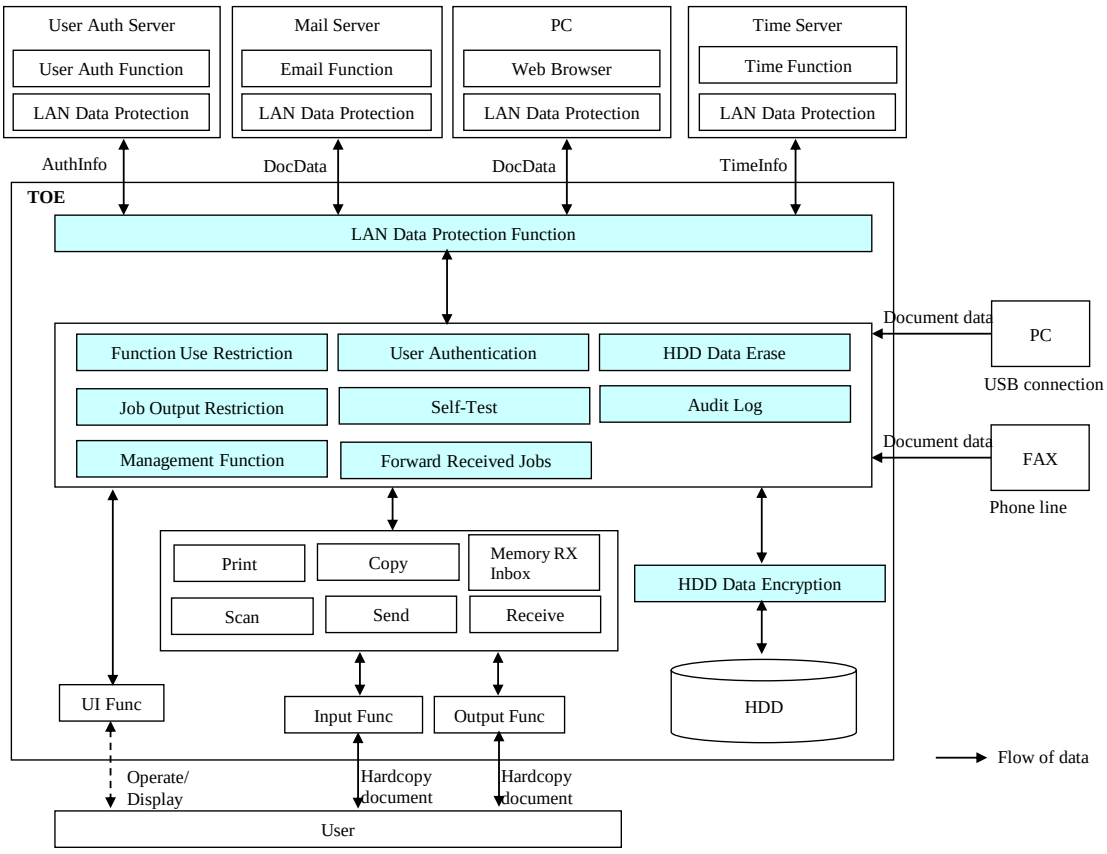

Figure 5.1 TOE boundary

In Figure 5-1, the components shown in blue box within the TOE are the security functions of the TOE described in Chapter 3, and the remaining components shown in white box within the TOE are the basic functions of the MFP. For details on the basic MFP functions, see Terminology in Chapter 11.

Users of the TOE operate the TOE from its control panel ("UI Func" in Figure 5-1), from a PC connected to the LAN using a Web browser ("Web Browser" contained in "PC" in Figure 5-1), or from a PC connected via LAN or USB using a print driver (indicated only as the "PC" and a print driver is not illustrated in Figure 5-1).

The security functions of the TOE are applied when the user uses basic MFP functions. The following describes the relation between the security functions and the basic MFP

functions.

(1) When a user submits a print job from a PC connected via LAN or USB, or when a fax/I-fax job is received, the jobs are accepted without requiring identification and authentication, and the resulting document data are stored within the TOE. The user may perform operations on the document data later, using the control panel or from a Web browser.

When the user attempts to access the basic MFP functions from the control panel or from a Web browser, "User Authentication" and "Function Use Restriction" function are applied, so that only authorized users are allowed to use the TOE. Subsequently, when the user attempts to execute an operation on a document data stored in the TOE, "Job Output Restriction" function is applied, so that only the owner of the document data or the Administrator is allowed to operate the document data.

When the user attempts to use "Management" function or browse audit logs provided by "Audit Log" function from the control panel or a Web browser, "User Authentication" function is applied, so that only the identified and authenticated user with Administrator privileges can gain access to the TOE.

Note that audit logs are generated by "Audit Log" function when these security functions are used.

(2) In the use described in (1) above, "HDD Data Encryption" function is applied to all data stored in the internal HDD, and "HDD Data Erase" function is applied when document data are deleted.

(3) In the use described in (1) above, "LAN Data Protection" function is applied when the TOE communicates with other IT devices over the LAN. In addition, "Forward Received Jobs" restricts data received from various interface to be forwarded without any TOE security functions applied.

5.2 IT Environment

When the external authentication method is used for "User Authentication" function of the TOE, Kerberos or LDAP protocol is used to query the information contained in the User Authentication Server to perform user identification and authentication. User account information is registered in the User Authentication Server through the management function of the User Authentication Server.

The time information recorded on the TOE's audit logs is provided by the TOE. The time information of the TOE is set and maintained by the Management function of the TOE, or can be synchronized with an external time server using the NTP protocol.

The TOE uses IPsec protocol to communicate with other external IT devices over the network. As such, those external IT devices need to have IPsec protocol configured as well.

6. Documentation

The identification of documents attached to the TOE is listed below. TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

(Japanese Name)

- imageRUNNER ADVANCE C2230F/C2220/C2220F e-Manual [FT5-4605(000)]
- iR-ADV Security Kit-D1 for IEEE 2600.1 Administrator Guide [FT5-4603(000)]
- ACCESS MANAGEMENT SYSTEM Kit-B1 Access Management System Individual Management Configuration Administrator Guide [FT5-4605(000)]
- HDD Data Encryption Kit User's Guide [FT5-2437(020)]
- To Read Before Using iR-ADV Security Kit-D1 for IEEE 2600.1 [FT5-4604(000)]

(English Name)

- imageRUNNER ADVANCE C2230/C2225 e-Manual [FT5-4608(000)]
- iR-ADV Security Kit-D1 for IEEE 2600.1 Common Criteria Certification Administrator Guide [FT5-4606 (000)]
- ACCESS MANAGEMENT SYSTEM KIT-B1 Access Management System Individual Management Configuration Administrator Guide [FT5-4608(000)]
- HDD Data Encryption Kit-C Series User Documentation [FT5-3328(010)]
- Before Using iR-ADV Security Kit-D1 for IEEE 2600.1 Common Criteria Certification [FT5-4607 (000)]

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance components 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.

7.2 Overview of Evaluation Activity

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

The evaluation has started on 2012-01 and concluded upon completion of the Evaluation Technical Report dated 2013-06. 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. Additionally, the evaluator directly visited the development and manufacturing sites on 2012-05, 2012-06 and 2012-07 and examined procedural status conducted in relation to each work unit for configuration management, delivery and development security by investigating records and interviewing staff. Furthermore, the evaluator conducted the sampling check of the developer testing and the evaluator testing by using the developer testing environment at the developer site on 2013-05.

Concerns found in evaluation activities for each work unit were all issued as the Observation Reports, and those were reported to the developer. Those concerns were reviewed by the developer, and all the concerns were solved eventually.

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

7.3 IT Product Testing

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

7.3.1 Developer Testing

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

1) Developer Testing Environment

The TOE used in the developer testing is iR-ADV C2230 model with the same TOE identification described in Chapter 2. The evaluator evaluated that it is sufficient to test a representative model only, since the differences between the MFP models are hardware performances such as printing speeds, and these differences do not affect the behavior of the security functions.

Details of the components of the developer testing environment are given in Table 7-1. The configuration for this testing is the operational environment of the TOE as described in Figure 4-1, except for the following differences. Besides these differences, this configuration is identical to the configuration specified in the ST, and the evaluator evaluates that these differences do not affect the purpose, which is to test the TOE's functions.

- Although included in the description in the ST, no firewall is used in the testing environment since it was not connected to the internet.

- Some tests use the phone line pseudo-exchanger which can emulate fax communication protocol that is the same as a public telephone line instead of the public telephone network (PSTN).

Table 7-1 Devices for Developer Testing

Device Name	Description
TOE	iR-ADV C2230 (MFP) HDD Data Encryption Kit-C
Fax Board	Super G3 FAX Board-AH2 Super G3 2nd Line FAX Board-AH1
User Authentication (Kerberos) Server 1 / Time Server	Windows Server 2008 Enterprise SP1 - Active Directory Domain Services - Windows Time
User Authentication (LDAP) Server 2 / Mail Server	Windows Sever 2003 Standard Edition SP2 - eDirectory 8.8 SP2 - Microsoft POP3 Service
PCs for tests (3 PCs)	Microsoft Windows 7 Professional - Microsoft Internet Explorer 8 (Web Browser)

The developer testing was performed in the same TOE testing environment as 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>

(1) By operating the user interfaces such as control panel, hard keys (such as power switch), and Remote UI, the developer confirmed the result of the operation (such as normal end, abnormal end, or error messages) and audit logs.

(2) To confirm the HDD Data Erase function, the developer used the SATA analyzer and captured to confirm the input/output data to/from HDD.

(3) To confirm the HDD Data Encryption function, the developer confirmed that the data encrypted by the TOE was consistent with the result of the data encrypted by the software in which the specified cryptographic algorithm was implemented.
In addition, for the cryptographic key generation, it was confirmed that the specified cryptographic key generation algorithm is implemented at the module level.

(4) To confirm the IPsec communication function, the developer captured communication data on the network by packet capture software and confirmed the behavior of IPsec function.
The developer also verified that the cryptographic key used for IPsec communication was generated by the specified algorithm, by confirming that the assumed pseudorandom number corresponding to the specified input was outputted.

<Developer Testing Tools>

Table 7-2 shows tools used in the developer testing.

Table 7-2 Developer Testing Tools

Tool Name	Description
Wireshark (Ver.1.2.11 Rev.34007)	Packet capture software.
SATA Protocol Suite (Ver.4.00)	Analyzer software.
SATA Tester	A tool to perform sending or receiving commands and data compliant with SATA, which is a common interface for HDD.
SATA Analyzer	A tool to confirm electric signals via SATA interface by connecting between SATA cables.

Tool Name	Description
ICE	The abbreviation of In-Circuit Emulator. It supports debugging by emulating the behavior of CPU.
AES library for FR	Encryption Library (for testing of HDD Encryption Board)
Pseudorandom number testing tool	A tool developed by the developer to confirm that a pseudorandom number generator for IPsec performs with FIPS 186-2 algorithm.
Phone line pseudo-exchanger	A unit that performs pseudo-exchanges of the phone line.
Printer Driver	Canon LIPS LX Printer Driver Version 20.80

<Content of the Performed Developer Testing>

Basic MFP functions and security management functions were operated from every interface, and the security functions to be applied to various input parameters were confirmed to operate according to the specification.

b. Scope of the Performed Developer Testing

The developer testing was performed on 432 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. By the depth analysis, it was verified that all the subsystems and subsystem interfaces described in the TOE design had been sufficiently tested.

c. Result

The evaluator confirmed the approach of the performed developer testing and the legitimacy 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 testing results expected by the developer and the actual testing results performed by the developer.

7.3.2 Evaluator Independent Testing

The evaluator performed the sample testing to reconfirm the execution of security functions by 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 ensure that security functions are certainly implemented from 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 independent testing was performed by evaluator using the same testing environment for the developer testing.

2) Summary of the Independent Testing

A summary of the independent testing is as follows.

a. Viewpoints of the Independent Testing

The evaluator devised the independent testing in terms of the following viewpoints, based on the developer testing and the provided evaluation documentation, in order for the evaluator him/herself to verify that the TOE security functions work as specified.

<Viewpoints of the Independent Testing>

(1) Since a case where multiple security functionalities operate simultaneously is not treated in the developer testing, the evaluator confirms it in the independent testing.

(2) The evaluator adds the test on the relationship between security functions and non-security functions.

(3) There are many variations for exceptional handling and cancel operations, but these cases are not tested enough in the developer testing. Therefore, the evaluator confirms these cases in the independent testing.

(4) In order to confirm that the functions to restrict the digit number to be input and to check the number of characters in Remote UI and control panel run correctly, the tests in which increased variations of input values are added.

(5) The tests to confirm that the permutational or probabilistic mechanism about passwords is as described in the functional specification are added.

b. Independent Testing Outline

The evaluator performed the sample testing of 60 items from the developer testing and the provided evaluation documentation. The evaluator devised the additional independent testing of 8 items from the developer testing and the provided evaluation documentation from the following viewpoints. An outline of the independent testing that the evaluator performed is as follows.

<Independent Testing Approach>

For the functions which are operated by operator's manipulating a Web browser and control panel, it is possible to observe the results through the error messages and the state of the screen, etc., so the test method which confirms those responses was used.

Regarding the external interfaces, the state of the TOE and audit logs change by stimulating the TOE via the devices connected to the TOE, so the test method which observes the results was used.

Regarding the functions related to IPsec communication and the communication by SNMP, etc., those are the functionalities which people cannot observe from the outside, so the test method which confirms the behavior with packet capturing software (Wireshark) or an SNMP-related tool (Net-snmp) was used as an alternative means.

As for the management of session ID, the Proxy type vulnerability analysis tool (Burp Suite) was used, and the test method which confirms its behavior was used.

<Independent Testing Tools>

In the independent test, the testing tools shown in Table 7-3 were added to the developer testing, and it was executed.

Table 7-3 Independent Testing Tools

Tool Name (Version)	Description
Net-snmp (Ver.5.6.1.1)	Application software which implements each version of SNMP. Only command functions, such as MIB browser function, are used in this test (snmpwalk, snmpset, etc.).
Burp Suite Pro (Ver.1.5.8)	Proxy type vulnerability analysis tool.
Printer Driver [AMS Printer Driver Add-in, PS Printer Driver, PCL Printer Driver, Fax Driver]	It is used to execute tests by increasing parameters about external interfaces.
USB Memory	It is used to execute tests by increasing parameters about external interfaces.

<Content of the Performed Independent Testing>

Table 7-4 shows viewpoints of the independent testing and the content of the testing corresponding to them.

Table 7-4 Content of the Performed Independent Testing

Outline of the Independent Testing	Viewpoint of Independent Testing
The functional test on user management function and Function Use Restriction (e.g., to confirm that the users who belong to the general user role are unable to access the management function specified in the ST)	(3)
The functional test on user authentication screen (e.g., to confirm the behavior of checking character length of user names and passwords)	(4)
The functional test on the password changes in local authentication (e.g., to confirm the variation of the characters which can be used for general users' passwords)	(3) (4) (5)
The functional test on the session management function of Remote UI (e.g., to confirm that the method of giving session ID is as described in the functional specification)	(2) (5)
The functional test on Job Output Restriction (e.g., to confirm that the behaviors of output jobs are not changed by the variation (protocols, drivers) of submitting jobs from PC)	(1) (3)

Outline of the Independent Testing	Viewpoint of Independent Testing
The functional test on simultaneous use of the user privileges (e.g., to confirm that administrators cannot login simultaneously, but other users can login simultaneously)	(1) (3) (4)
The functional test on external interfaces (e.g., to confirm that the information obtainable with SNMP is only the information described in the functional specification)	(1) (5)
The test that the TOE does not exhibit unauthorized behaviors after HDD or jobs reach the limits (and that error handling should be executed appropriately)	(3) (5)

c. Result

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

7.3.3 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) When network services other than the functions which are described in the design documents that the TOE provides at operation status, are started, security functions may be bypassed, and it may compromise the assets of the TOE.

(2) For the reason of the publicly-known vulnerabilities in the network service in operation, the operations other than the operations originally meant to be performed are executable, so the security functions of the TOE may be bypassed, and the assets of the TOE may be accessed.

(3) In Remote UI, there are pages (functions) where the session information is not checked, or there are problems in checks of the input used for the page specification, so identification and authentication as well as access control may be bypassed.

(4) The checks provided by Remote UI may be bypassed, and the unexpected behavior of the TOE occurs by specifying unauthorized values as input values; as a result, the security functions of the TOE may be bypassed, and the secure use of the TOE may be

affected.

b. Penetration Testing Outline

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

<Penetration Testing Environment>

The penetration testing was conducted, and the testing tools shown in Table 7-5 were added to the developer testing.

Table 7-5 Tools for Penetration Testing

Tool Name (Version)	Description
Nmap (Ver.6.25)	Port Scan Tool
Nessus (Ver.5.0.3)	Vulnerability Scanner
Netcat (Ver.1.11)	General TCP/UDP Communication tool

<Content of the Performed Penetration Testing>

Table 7-6 shows an outline of the penetration testing for the vulnerability of concern.

Table 7-6 Outline of Penetration Testing

Vulnerability of concern	Outline of penetration testing
(1)	Port scan was performed to the TOE using the port scan tool (Nmap), and the results were analyzed, including the result of (2). Although it was confirmed that a service which is not described in the design document had started, it was confirmed that it did not affect the security functions after specifying the kind of the service. In the interfaces (FTP, SMB, etc.) which may have a function to exhibit files and execute commands among the network services which the TOE provides, it was confirmed that the commands (OS or protocol) which are not permitted could not be executed.
(2)	By performing the scan with a vulnerability scanner (Nessus), it is confirmed that there are no publicly-known vulnerabilities in the network services which the TOE provides.

Vulnerability of concern	Outline of penetration testing
(3)	By directly accessing to the URL which can be externally accessed, and by directly specifying the URL of the screen called from other screens with a browser, it was confirmed that an applicable screen could not be accessed unless the login screen was displayed and authenticated. (The behavior of the check function of the session information was confirmed.)
(4)	By using Burp Suite (Proxy type vulnerability analysis tool), the following points were confirmed. - The behavior was confirmed by performing inputs that may trigger directory traversal after searching parts, in which files and pages inside the TOE are directly specified, in the input part of the screen which can be operated by general users. - To the input items of the screen (a login screen, a password change screen, an address book, etc.) which "those which the use of the TOE is not permitted" or "general users" can operate, the tools were used to confirm that a problem will not occur when inputting the unpermitted characters and long character strings. - To the input items of the screen (a user management function, various setting functions) which administrators can operate, the tools were used to confirm that a problem will not occur when inputting the unpermitted characters and long character strings.

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.

7.4 Evaluated Configuration

The conditions for the evaluated configuration of the TOE are as described in the guidance documents. The user must follow the guidance documents to set up the TOE. Some of the settings are fixed in this evaluation, because certain settings like disabling security functions weaken security. If any settings that affect security are changed to the value that is advised not to set in the guidance documents, then the MFP with those settings is no longer the evaluated configuration.

7.5 Evaluation Results

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

In the evaluation, the following were confirmed.

- PP Conformance:
  2600.1, Protection Profile for Hardcopy Devices, Operational Environment A
  (IEEE Std 2600.1™-2009)

  SFR packages conformance defined in the above PP:
  - 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A: Conformant
  - 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A: Conformant
  - 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A: Conformant
  - 2600.1-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment A: Conformant
  - 2600.1-NVS, SFR Package for Hardcopy Device Nonvolatile Storage Functions, Operational Environment A: Augmented
  - 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A: Augmented

- 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 EAL3 package
- Augmented 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.

7.6 Evaluator Comments/Recommendations

The evaluator recommendations for procurement personnel are not mentioned.

8. Certification

The Certification Body conducted the following certification based on the materials submitted by the Evaluation Facility during the evaluation process.

1. Contents pointed out in the Observation Reports shall be adequate.

2. Contents pointed out in the Observation Reports shall properly be solved.

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

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

5. 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 those 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 submitted Evaluation Technical Report, Observation Reports and related evaluation documentation, the Certification Body determined that the TOE satisfies all assurance requirements for EAL3 augmented with ALC_FLR.2 in the CC Part 3.

8.2 Recommendations

(1) The conformance to the PP claimed by this TOE includes the fax function. Therefore, the assured configuration specified, applies to the MFP or TOE, when it includes the use of the optional fax board.
As such, the following configurations were not assured by the evaluation:
- Configurations without a fax board.

(2) This evaluation was performed with use of the fax inbox feature disabled. If the use of fax inbox is enabled, then that is no longer the evaluated configuration.

(3) In terms of the security functional requirements specified in the PP, this evaluation acknowledges that the requirements for identification and authentication do not apply to incoming print jobs from PC. Consumers expecting identification and authentication to be enforced for incoming print jobs are therefore advised to take note that the TOE specifications may not be consistent with their needs.

(4) When external authentication is used, Kerberos and LDAP can be used to communicate with the user authentication server. Where this is the case, the assurance provided by this evaluation specifically applies only when Active Directory Domain Services for Kerberos and eDirectory 8.8 SP2 for LDAP are used as the authentication server software.

(5) When the audit log is read, there are cases where a message showing an abnormal condition that detected damages of the audit log is displayed. In those cases, the administrator contacts a service technician in the power-off state of the main unit by following the description contents of the guidance, before clearing the damaged audit log. Then, it can be restored to a normal state by asking the service technician for a backup operation of the audit log.

9. Annexes

There is no annex.

10. Security Target

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

Canon imageRUNNER ADVANCE C2200 Series 2600.1 model Security Target
Version 1.10 (June 28, 2013) Canon Inc.

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.

MFP	Multifunction Product
HCD	Hardcopy Device

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

Copy function	It produces duplicates of the hardcopy documents by scanning and printing.
External interface	An interface to receive data from time server as well as to receive and transmit jobs, such as prints and faxes (I-fax).
Fax Inbox	If a file received through fax/I-fax matches the specified forwarding conditions, it is stored in the Fax Inbox. You can print the stored file whenever necessary using the desired settings.
Hardcopy Device (HCD)	A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, MFPs (multifunction peripherals), MFDs (multifunction devices), "all-in-ones," and other similar products.
I-fax	Short for Internet Fax, which uses the Internet to receive and send faxes.
Inbox PIN	PIN used for access control to each mail box and inbox where document data received by fax/I-fax are stored are stored.
Memory RX Inbox	It refers to the area where document data received by fax/I-fax are stored.
Memory RX Inbox functionality	A function that allows document data received by fax/I-fax to be stored in the Memory RX Inbox. It provides operations such as print, send and delete of document data stored in the Memory RX Inbox.

Print function	It produces a hardcopy document from its electronic form stored in the TOE.
Print Settings	It contains various print setting options for selecting color/monochrome, paper type, and duplex printing, etc.
Remote UI	An interface that provides access to the MFP from a Web browser via the LAN, to allow the acquisition of operating status, perform job operations or BOX operations, and making various settings.
Scan function	It allows the conversion of data from its hardcopy form to its electronic form, to create document data.
Secured Print	PIN-based printing function of the TOE.
Send (Universal Send) function	It allows scanned document data or document data stored in a mail box/inbox to be received for transmission to an email address, shared folder on a PC, or I-fax transmission.
TOE Owner	A person or organizational entity responsible for protecting TOE assets and establishing related security policies.
TSF Confidential Data	Assets for which either disclosure or alteration by a User who is not an Administrator or the owner of the data would have an effect on the operational security of the TOE.
TSF Protected Data	Assets for which alteration by a User who is not an Administrator or the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.
U. ADMINISTRATOR	A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TOE security policy (TSP). Administrators may possess special privileges that provide capabilities to override portions of the TSP.
UI function	Allows users to operate the TOE from the control panel, and the TOE to display information on the control panel.
U.NORMAL	A User who is authorized to perform User Document Data processing functions of the TOE.
User Document Data	The asset that consists of the information contained in a user's document.
User Function Data	The asset that consists of the information about a user's document or job to be processed by the TOE.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme, March 2012, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, April 2013, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, April 2013, 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 3, July 2009, CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001 (Japanese Version 1.0, December 2009)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002 (Japanese Version 1.0, December 2009)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003 (Japanese Version 1.0, December 2009)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004 (Japanese Version 1.0, December 2009)

[12] Canon imageRUNNER ADVANCE C2200 Series 2600.1 model Security Target Version 1.10 (June 28, 2013) Canon Inc.

[13] Canon imageRUNNER ADVANCE C2200 Series 2600.1 model Evaluation Technical Report, Version 2.2, June 28, 2013, ECSEC Laboratory Inc., Evaluation Center

[14] IEEE Std 2600.1™-2009, IEEE Standard for a Protection Profile in Operational Environment A, Version 1.0, June 2009