Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2010-02-25 (ITC-0294)
Certification No.	C0287
Sponsor	Canon Inc.
Name of TOE	Canon imageRUNNER ADVANCE C5000 Series 2600.1 model
Version of TOE	1.0
PP Conformance	IEEE Std 2600.1-2009
Assurance Package	EAL3 Augmented with ALC_FLR.2
Developer	Canon Inc.
Evaluation Facility	Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security

This is to report that the evaluation result for the above TOE is certified as follows.
2011-03-29

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

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following criteria 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 C5000 Series 2600.1 model" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" 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 certification result in relation to IT Security Evaluation of "Canon imageRUNNER ADVANCE C5000 Series 2600.1 model version 1.0" (hereinafter referred to as "the TOE") developed by Canon Inc., and evaluation of the TOE was finished on 2011-03-17 by Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security (hereinafter referred to as "Evaluation Facility"). It reports to the sponsor, Canon Inc. and provides information to consumers and system operators who are interested in this TOE.

The reader of the Certification Report is 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 ST.

This certification report assumes general consumers to be a reader. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee individual IT product itself.

1.1 Product Overview

Overview of the TOE functions and operational conditions are as follows. Refer to and after Chapter 2 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, I-Fax Receive, and Mail Box capabilities. Although the MFP also supports a FAX board as an option, Fax is not included in the scope of this TOE.

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"), with the exclusion of fax-related functional requirements.

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 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

It is assumed that the evaluated products are managed under the following configurations 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 guidance documents.

1.1.3 Disclaimers

The Identification and Authentication Function contained in the target of this evaluation does not apply to incoming print jobs. Though the protocol used in the submission of the print job contains an identification and authentication mechanism, that mechanism is out of scope of this evaluation.

In terms of this evaluation, only Microsoft Internet Explorer 6 SP1 specifically, is evaluated for use as the Web browser for operating the TOE. Any and all other Web browsers and versions are out of scope of this evaluation.

1.2 Conduct of Evaluation

Evaluation Facility conducted IT security evaluation, and completed on 2011-03 based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[1], "IT Security Certification Procedure"[2], "Evaluation Facility Approval Procedure"[3] provided by Certification Body.

1.3 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Reports prepared by Evaluation Facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification oversight reviews are also prepared for those concerns found in the certification process. Those concerns pointed out by the Certification Body are fully resolved, and the Certification Body confirmed that the TOE evaluation is appropriately conducted in accordance with CC ([4][5][6] or [7][8][9]) and CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by Evaluation Facility and concluded fully certification activities.

2. Identification

The TOE is identified as follows;

Name of TOE:	Canon imageRUNNER ADVANCE C5000 Series 2600.1 model
Version of TOE:	1.0
Developer:	Canon Inc.

The TOE consists of the following software, hardware, and licenses.
Note that the Japanese names are originally written in Japanese and translated into English.

Table 2-1 Components of the TOE

Component name	Description
(Japanese Name) Canon imageRUNNER ADVANCE C5000 Series (English Name) Canon imageRUNNER ADVANCE C5000 Series	Any of the following MFP: iR-ADV C5051, iR-ADV C5045, iR-ADV C5035, iR-ADV C5030.
(Japanese Name) iR-ADV Security Kit-A1 for IEEE 2600.1 Ver 1.00 (English Name) iR-ADV Security Kit-A1 for IEEE 2600.1 Common Criteria Ver 1.00	Contains the control software and security kit license for "Canon imageRUNNER ADVANCE C5000 Series".
(Japanese Name) HDD Data Encryption / Mirroring Kit-C (English Name) HDD Data Encryption & Mirroring Kit-C	Hardware which encrypts all data stored in the HDD.
(Japanese Name) IPSec Security Board-B (English Name) IPSec Board-B	Hardware used to encrypt LAN data IP packets.
(Japanese Name) Data Erase Kit-C (English Name) Data Erase Kit-C	Contains the license for enabling the HDD Data Erase function of the control software.
(Japanese Name) Access Management System Kit-B (English Name) Access Management System Kit-B	Contains the license for enabling the access control function of the control software.

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 document, 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 the security services provided by the TOE, and under what policies and rules those functions are realized.

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 restriction, HDD data encryption and data erase functions, and secure communication protocols, which protect user document data and data that have an effect on TOE security functions, 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 provides the security functions to counter the threats shown in Section 3.1.1 and to meet 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 assumes the threats shown in Table 3-1 and provides functions to counter them. These threats are the same as those specified in the PP.

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", "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 allows only the authorized user 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, Preview, Send to Network, Delete, Change Print Priority, and Change Print Settings on print jobs and I-fax jobs stored in the TOE or document data stored in a box, thereby ensures 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 rightful document owner as follows:

- For documents submitted as print jobs, the identified and authenticated user is determined to be the owner of the documents if their user name matches the user name information of the documents which is specified in submitting the print job.

- For document data stored as a result of scanning or received by I-fax, the user is required to enter the correct box PIN when the user operates the document data. The boxes where these document data are stored are assigned per user, and pre-configured with a 7-digits box PIN. If the user enters the correct PIN, then the user is determined to be the owner of the document data stored in the box.

"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 ensure that the document data is never recovered.

"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-bits AES encryption algorithm. Its cryptographic key is generated using the FIPS PUB 186-2 deterministic random number generator algorithm, and destroyed upon the power off.

"LAN Data Protection" function of the TOE uses the encryption communication protocol, IPSec, when the TOE communicates with other IT devices over the LAN, and prevents the communication 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 assets from unauthorized disclosure and alteration.

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

These are threats to TSF data that affects the security functions. 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. The authorized U.NORMAL can change own password and the PIN for the mail box they use.

"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 assets from unauthorized disclosure and alteration.

3.1.2 Organisational Security Policies and Security Function Policies

3.1.2.1 Organisational Security Policies

The organisational security policies imposed on use of the TOE are shown in Table 3-2. These organisational security policies are the same as specified in the PP except for addition of P.HDD.ACCESS.AUTHORIZATION. P.HDD.ACCESS.AUTHORIZATION is augmented under the premise that it would generally be required to use a removable HDD on the TOE.

Table 3-2 Organisational Security Policies

Identifier	Organisational 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, TOE will have authorized access the HDD data.

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 3-2.

1) Means for organisational 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 to use the TOE who are successfully identified and authenticated. 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.

A print job or I-fax job is submitted without the identification and authentication. The resulting document data is stored within the TOE, and not automatically printed out or transmitted. To print out or transmit document data stored in the TOE, the user must operate the control panel of the TOE with the identification and authentication.

"Function Use Restriction" function of the TOE performs access restriction on the use of the TOE functions by the identified and authorized users, so that only users with appropriate permissions are permitted to use the functions. For access restriction, 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 that user or not.

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

2) Means for organisational 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 ensured.

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

3) Means for organisational 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 by an authorized U.ADMINISTRATOR only, via a Web browser.

4) Means for organisational 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 inactivity longer than the specified time.

"Forward Received Jobs" function of the TOE restricts data received from any external 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 organisational 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 "HDD Data Encryption" function is provided by the HDD Data Encryption & Mirroring Board, one of the components of the TOE. The HDD Data Encryption & Mirroring Board acquires the device authentication ID from the MFP device and stores it in FlashROM 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 correct MFP device.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate the TOE, as the useful information for an assumed reader to judge the use of the TOE.

4.1 Usage Assumptions

Assumptions required in the use of the TOE are shown in Table 4-1. These assumptions are the same as specified in the PP.
The effective performance of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions

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.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

4.2 Environment Assumptions

The TOE is a 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 from threats from the Internet. The assumed operational environment of the MFP is shown in Figure 4-1.

Users of the TOE can operate the TOE from its control panel, from a USB-connected PC, or from a PC connected to the LAN.

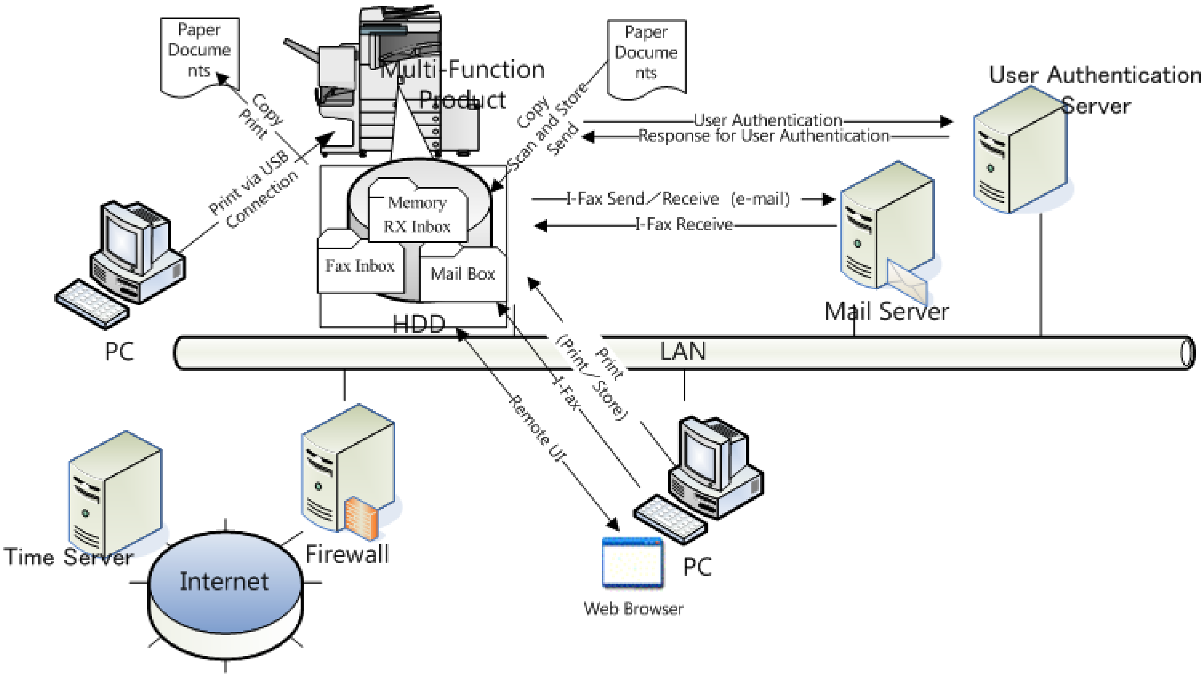

Figure 4-1 Operational Environment of TOE

The operational environment of TOE consists of the following components.

1) PC

Generic PC used by the user to connect to the TOE, via USB or internal LAN. The following software are required.

- Printer driver: (Evaluation performed using) Canon LIPSLX Printer Driver Version 20.30
- Web browser: (Evaluation performed using) Microsoft Internet Explorer 6 SP1

2) User Authentication Server

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

The User Authentication Server is the server that is used by the TOE for External Authentication and the authentication protocol it uses is Kerberos.

3) Mail Server

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

4) Time Server

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 timestamp on 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, the evaluator evaluates that the security functional requirements for the identification and authentication regarding the MFP's Print function specified in the PP, do not apply to incoming print jobs. Rather, they apply only when executing operations on document data accumulated in the MFP, created by the submitted print jobs. As such, the following security functions are considered out of 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, and those mechanisms are out of scope of this evaluation. Examples of this include the identification and authentication mechanism in the IPP protocol or in the FTP protocol for FTP print.

2) When submitting a print job to the TOE through a print driver, the 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 (This is known as "Secured Print"). This behavior is outside the scope of this evaluation.

   The user name is not checked for validity, but is simply associated with the submitted print job. The user name is used by the access restriction function.

5. Architectural Information

This chapter describes the objective and relevance regarding the scope of the TOE and the main components of the TOE.

5.1 TOE Boundary and Component

The configuration of the MFP or TOE and the IT environment other than MFP are 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.

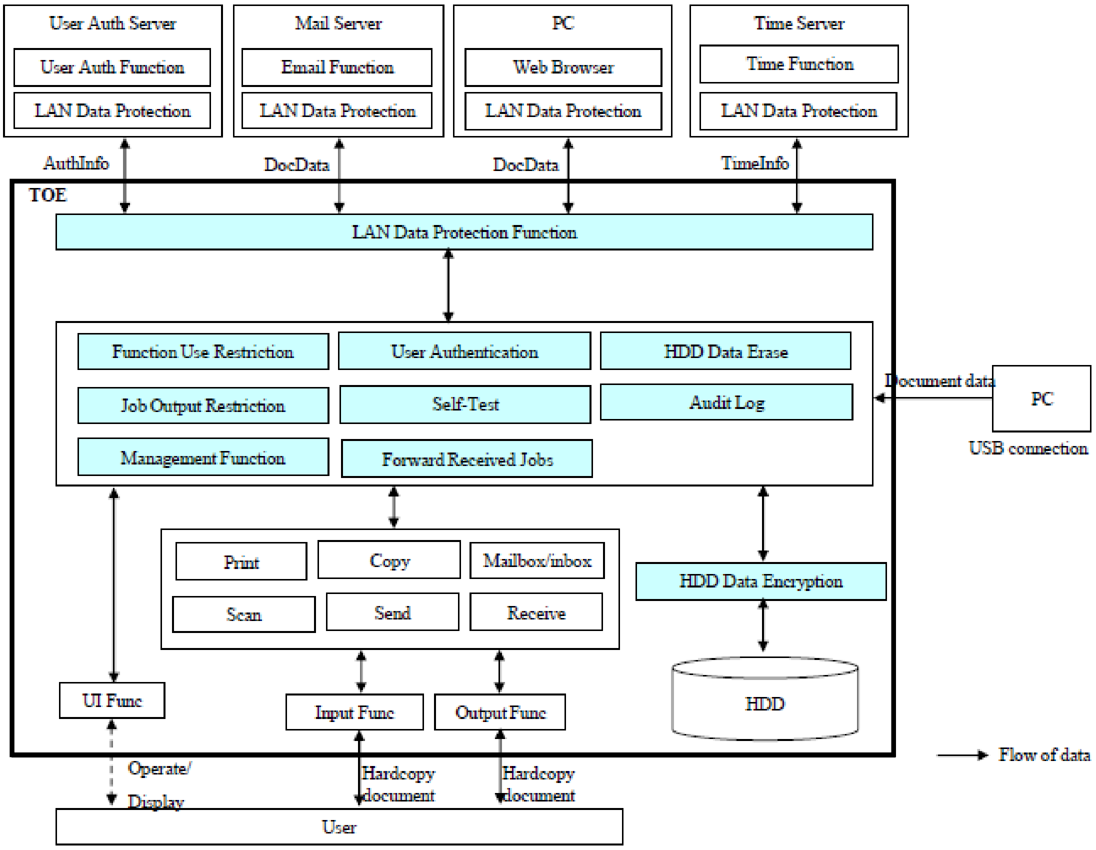

Figure 5-1 TOE Boundary

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

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

   When the user attempts to access the MFP basic 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. Also, "Forward Received Jobs" restricts data received from any external 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 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 IT devices over the network. As such, those IT devices need to have IPSec configured as well.

6. Documentation

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

(Japanese Name)

- imageRUNNER ADVANCE C5051/C5051F/C5045/C5045F/C5035/C5035F/C5030/C5030F e-Manual
  [FT5-3806-000]

- iR-ADV Security Kit-A1 for IEEE 2600.1 Administrator Guide
  [FT5-3805-000]

- ACCESS MANAGEMENT SYSTEM KIT-B1 Access Management System V3.0 Individual Management Configuration Administrator Guide
  [FT5-3806-000]

- HDD Data Encryption Kit User's Guide
  [FT5-2437]

- To Read Before Using iR-ADV Security Kit-A1 for IEEE 2600.1
  [FT5-3807-000]

Note that the Japanese names are originally written in Japanese, and translated into English.

(English Name)

- imageRUNNER ADVANCE C5051/C5045/ C5035/ C5030 e-Manual
  [FT5-3809-000 (US), FT5-3945-000 (AP)]

- iR-ADV Security Kit-A1 for IEEE 2600.1 Common Criteria Certification Administrator Guide
  [FT5-3808-000]

- ACCESS MANAGEMENT SYSTEM KIT-B1 Access Management System V3.0 Individual Management Configuration Administrator Guide
  [FT5-3809-000 (US), FT5-3945-000 (AP)]

- HDD Data Encryption & Mirroring Kit-C Series User Documentation
  [FT5-2440-010]

- Before Using iR-ADV Security Kit-A1 for IEEE 2600.1 Common Criteria Certification
  [FT5-3810-000]

Note that "US" shows the document for United States, "AP" shows the document for Asia Pacific.

7. Evaluation conducted by Evaluation Facility and results

7.1 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance components in CC Part 3. Details for evaluation activities are reported in the Evaluation Technical Report. In the Evaluation Technical Report, it explains the summary of the TOE, the content of evaluation and verdict of each work unit.

7.2 Overview of Evaluation Activity

The history of evaluation conducted was present in the Evaluation Technical Report as follows;

Evaluation has started on 2010-03 and concluded by completion the Evaluation Technical Report dated 2011-03. The evaluator received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluator directly visited the development and manufacturing sites on 2010-09, 2010-10 and 2011-03, and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff interview. Further, the evaluator executed the sampling check of the developer testing and the evaluator testing by using developer testing environment at developer site on 2010-12.

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

Concerns that the Certification Body found about the evaluation process was described as a certification oversight review, and it was sent to Evaluation Facility. After Evaluation Facility and the developer examine it, these concerns were reflected in the evaluation report.

7.3 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had executed. The evaluator executed the reappearance testing, additional testing and penetration testing based on vulnerability assessments, that are judged to be necessary based on the evidence shown in the process of the evaluation and results from the verification of the developer testing.

7.3.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer executed and the testing documentation of actual testing results. The overview of the evaluated developer testing is described as follows;

1) Developer Testing Environment

The testing configuration performed by the developer is the same as the operational environment for the TOE shown in Figure 4-1. The TOE used in developer testing is iR-ADV C5030 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 scanning and printing speeds, and there is no difference in the behavior of the security functions.

Note that the evaluator tests another MFP models that are not tested by the developer to verify machine independence. For details, see Section 7.3.2, Evaluator Independent Testing.

Configuration elements other than the TOE are listed in Table 7-1.

Table 7-1 Devices for Developer Testing

Device Name	Description
PC	The user's PC. - PC with Windows 2000 SP4 installed - Web browser: Internet Explorer 6.0 sp1 - Print driver: Canon LIPSLX Printer Driver Version 20.30
User Authentication Server/ Time Server	Serves as the authentication server used in external authentication and/or the Internet time server. - PC with Windows Server 2008 Enterprise SP1 installed. - Authentication server software: Active Directory Domain Services (Comes with the OS) - Time server software: Windows TIME (Comes with the OS)
Mail Server	Used as the server for I-fax transmissions. - PC with Windows Server 2003 Standard Edition SP1 installed. - Mail Server software: Microsoft POP3 Service (Comes with the OS) Simple Mail Transfer Protocol (Comes with the OS)

The developer testing is performed in the same TOE testing environment as the TOE configuration identified in the ST.

It should be noted however, that there are some dissimilarities with the configuration specified in the ST. Such as: the test environment used by the developer had no Internet connection, and therefore no Firewall; the Internet Time Server is substituted with the software on the User Authentication Server/Time Server. The evaluator evaluates that these dissimilarities do not affect the purpose, which is to test the TOE's functions.

2) Summary of Developer Testing

Summary of the developer testing is as follows;

a. Outline of Developer Testing

The testing performed by the developer is outlined as follows;

<Developer Testing Approach>

(1) Operate the user interfaces such as control panel, Web browser, printer driver, and confirm the output messages of the user interfaces, the TOE's behavior, and the contents of audit logs.

(2) To confirm the HDD Data Erase function, the HDD protocol analyzer is used to read the deleted contents of the HDD to ensure that the contents are overwritten with random data.

(3) To confirm the HDD Data Encryption function, encrypted data stored in the HDD is compared with data encrypted by known other tool, to ensure that TOE implements the cryptographic algorithm according to the specification. Also, for cryptographic key generation, random numbers are generated using various seed values, and the results compared with known data to ensure that TOE implements the cryptographic key generation algorithm according to the specification.

(4) To confirm the IPSec function, IPSec communication is established with the PC to ensure that IPSec communication is functioning properly. Also, a network analyzer is used to ensure that the secure communication protocol is according to specification.

(5) To confirm the Device Identification and Authentication function of the HDD Data Encryption & Mirroring Board, checks the behavior when mounted on the MFP with the correct ID and the behavior when mounted on a MFP with an incorrect ID.

<Developer Testing Tools>

The tools used for the developer testing are shown in Table 7-2 below.

Table 7-2 Tools for Developer Testing

Tool Name	Description
HDD Protocol Analyzer Catalyst Enterprises Inc ST4-31-0186	Tool that monitors the bus connected to the HDD and analyzes input/output data.
Network Analyzer Wireshark Version 1.2.1	Tool that monitors and analyzes data communicated over the LAN.
Encryption Library Fujitsu AES library for FR ver. 1.0	Used to compare encrypted data, to check the accurate implementation of the encryption algorithm.

<Developer Testing Effort>
MFP basic 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. Also, all acceptable setting values for the evaluated configuration such as internal or external authentication setting were confirmed to operate according to the specification.

b. Scope of Developer Testing Performed

The developer testing is performed about 275 items by the developer. By the coverage analysis, it was verified that all security functions and external interfaces described in the TOE functional specification had been tested. By the depth analysis, it was verified that all subsystems and subsystem interfaces described in the TOE design had been tested enough.

c. Result

The evaluator confirmed consistencies between the expected testing results and the actual testing results executed by the developer. The evaluator confirmed the testing approach performed by the developer and legitimacy of tested items, and confirmed that the testing approach and results are consistent with those described in the testing plan.

7.3.2 Evaluator Independent Testing

The evaluator executed the independent testing to reconfirm that security functions are certainly implemented based on the evidence shown in the process of the evaluation. The overview of the independent testing executed by the evaluator is described as follows;

1) Evaluator Independent Testing Environment

The configuration of the testing conducted by the evaluator was the same as the configuration of the developer testing.

Testing of the TOE performed by the evaluator was carried out using the iR-ADV C5035 and iR-ADV C5051 models with the same TOE identification described in Chapter 2.

The evaluator independent testing is executed in the same environment as TOE configuration identified in ST.

2) Summary of Evaluator Independent Testing
Summary of the evaluator independent testing is as follows;

a. Viewpoint of Independent Testing

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

<Viewpoint of Independent Testing>
(1) By testing other models not tested by the developer, confirm that the differences between the models are those of hardware performance (i.e., processing speed) only, and the differences does not affect the behavior of the security functions.

(2) In terms of sampling developer tests, extract test items from the testing performed by the developer so that all TSFI and security functions are included, and perform the same tests as the developer.

(3) In developer testing, since some interfaces were not rigorously tested to examine the behavior of the security functions, confirm the behavior using parameters not yet tested.

b. Outline of Independent Testing

The independent testing conducted by the evaluator is outlined as follows;

<Independent Testing Approach>

Using the same method as of the developer testing, the same testing and the testing with changed parameters are conducted.

<Independent Testing Tools>

The same testing tool as of the developer testing was used.

<Contents of Independent Testing Performed>

Table 7-3 shows outline of the independent testing conducted by the evaluator with corresponding viewpoints of independent testing.

Note that while developer testing covers all setting values, evaluator testing is performed using the default setting values that are set immediately after completing all installation procedures.

Table 7-3 Conducted Independent Testing

Viewpoint of independent testing	Outline of independent testing
(1)(2)	Based on the viewpoint, test items are extracted from developer tests, and the same tests are repeated to determine that the same results can be obtained. Out of a total of 275 test items, 107 test items were tested.
(3)	Confirm that the behavior is according to specification, when the length of the user password or box PIN is around the threshold value.
(3)	The TOE has multiple roles available for U.NORMAL. Confirm that whatever the role a use is assigned for U.NORMAL, a user will not be able to use the management functions only for U.ADMINISTRATOR according to the specification.
(3)	Confirm that the behavior is as expected, when a secured print job is submitted using a user name that is not registered in the TOE. (i.e., The Administrator can browse or delete all secured print jobs. For a non-Administrator, access is denied since the user name will not match).
(3)	Confirm that a log of the transmission error is generated according to the specification, if a document stored in a box is being transmitted to the network, and the LAN cable is unplugged.

c. Result

All the independent testing conducted by the evaluator was completed correctly, and the evaluator confirmed the behavior of TOE. The evaluator confirmed that all the test results are consistent with the expected behavior.

7.3.3 Evaluator Penetration Testing

The evaluator devised and conducted the necessary evaluator penetration testing about the possibility of exploitable concern at assumed environment of use and attack level. The overview of the penetration testing conducted by the evaluator is described as follows;

1) Summary of Penetration Testing
Summary of the penetration testing conducted by the evaluator is as follows;

a. Vulnerabilities of concern

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

Note that for cryptographic keys, the evaluator determines that attackers with the assumed attack potential cannot obtain or guess the cryptographic key, based on analysis of the mechanism used at TOE start-up to generate the cryptographic key and the developer tests for that mechanism.

(1) There is a concern corresponding to this TOE regarding the publicly available vulnerability information, such as the possibility of unauthorized use of network service, various vulnerability of Web.

(2) There is a concern in Web interfaces that the TOE operates unexpectedly for the input exceeding the limit value.

(3) There is a concern in Web interfaces that identification and authentication or access control mechanisms may be bypassed if the URL is specified directly or session management information is guessed.

(4) There is a concern that the TOE operates unexpectedly when powered OFF/ON during start-up or shut-down.

(5) There is a concern that the TOE operates unexpectedly when the same document data is accessed simultaneously from the control panel and from a Web browser.

(6) There is a concern that the TOE operates unexpectedly when the TOE's resources such as disk space are exhausted.

b. Outline of Penetration Testing
The evaluators conducted the following penetration testing to identify possibly exploitable vulnerabilities.

< Penetration Testing Environment>
Penetration Testing was conducted in the same environment as of the evaluator independent testing shown in Figure 7-2, but used by adding the PC with a tool for penetration testing. Details of the used tool are shown in Table 7-4 below.

Table 7-4 Tools for Penetration Testing

Tool Name		Description
PC for Penetration Testing		PC with Windows XP, which operates the following penetration testing tools.
	(a) Nessus 4.4.0	A tool that detects network service vulnerabilities. Vulnerability data is current as of December 3, 2010.
	(b) Nikto 2.03	A tool that detects Web server vulnerabilities. Vulnerability data is current as of December 3, 2010.
	(c) TamperIE	A tool that mediates communication between the Web browser (PC) and the Web server (TOE) to browse or alter communications. Tamper IE enables transmitted data to be tampered with and tramsmitted to a Web server, without being subject to web browser constraints.

<Contents of Penetration Testing Performed>
Table 7-5 shows outline of the penetration testing for the vulnerability of concern.

Table 7-5 Outline of Penetration Testing

Vulnerability of concern	Outline of penetration testing
(1)	- Using Nessus on the TOE, searched for any open ports and vulnerabilities. Confirmed that no ports are opened that should not be, and that no known vulnerabilities exist on the open ports. - Using Nikto, searched for vulnerabilities in the TOE's Web server function, and confirmed there are no known vulnerabilities.
(2)	- In the Change Password screen, using TamperIE to tamper with the communication between the Web browser and the TOE, so that a wrong-length password is transmitted. This correctly resulted in error, showing no abnormal behavior.
(3)	- In the Web browser's login screen, attempted to bypass login by specifying the desired URL directly, and confirmed that login cannot be bypassed. - During login from the Web browser to the TOE, using TamperIE to obtain session information, and confirmed they are random numbers that cannot be guessed by an attacker possessing the assumed attack potential.
(4)	- When the TOE is powered OFF during start-up, the TOE shuts down properly showing no abnormal behavior. - When the TOE is powered ON during shutdown, the TOE starts up after shutting down, showing no abnormal behavior.
(5)	- When the same document is accessed simultaneously from the control panel and a Web browser, one with the intent to delete the document, the other to merge and save under the same file name, the former delete operation and the latter save operation succeed,

	showing no abnormal behavior.
(6)	- When the HDD is full, attempted to save additional data, and confirmed that it results in error, showing no abnormal behavior. - Similar tests were performed to observe the behavior when the maximum number of registered users or the maximum number of secured print jobs is exceeded, which showed no abnormal behavior.

c. Result

In the penetration testing conducted by the evaluator, the exploitable vulnerability could not be found that attackers with the assumed attack potential could exploit.

7.4 Evaluated Configuration

The conditions for the evaluated configuration of the TOE are 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 the settings such as disabling the security functions weaken the security. If the settings affecting the 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 the conclusion that the TOE satisfies all work units prescribed in 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-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) 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 applied to the composed by corresponding TOE to the identification described in the chapter 2.

7.6 Evaluator Comments/Recommendations

The evaluator recommendations for users are not mentioned.

8. Certification

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

1. Contents pointed out in the Observation Report shall be adequate.
2. Contents pointed out in the Observation Report shall properly be reflected.
3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of 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 certification process were prepared as certification oversight reviews and were sent to Evaluation Facility.

The Certification Body confirmed such concerns pointed out in Observation Report and 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 submitted Evaluation Technical Report, Observation Reports and related evaluation deliverables, Certification Body determined that the TOE satisfies all components of the EAL3 augmented with ALC_FLR.2 in the CC part 3.

8.2 Recommendations

In terms of the security functional requirements specified in the PP, this evaluation interprets that the requirements for the identification and the authentication do not apply for incoming print jobs. Consumers expecting the identification and the 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.

9. Annexes

There is no annex.

10. Security Target

Security Target [12] of the TOE is provided within a separate document of this certification report.

Canon imageRUNNER ADVANCE C5000 Series 2600.1 model Security Target Version 1.17 (March 17, 2011) Canon Inc.

11. Glossary

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

MFP	Multifunction Product
HCD	Hardcopy Device

The definition of terms used in this report is listed below.

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. Uses the Internet to receive and send faxes.

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

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.

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.

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.

UI function
Allows the user to operate the TOE from the control panel, and the TOE to display information on the control panel.

Copy function
Produces duplicates of the hardcopy document by scanning and printing.

Receive function
Allows I-fax documents received in electronic form to be printed in hardcopy form, or transmitted in electronic form.

Output function
Allows the TOE to output hardcopy documents.

Scan function
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 function
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.

Print function
Produces a hardcopy document from its electronic form stored in the TOE.

Print Settings
Contains various print setting options for selecting color/monochrome, paper type, duplex etc.

Box
Refers to the mail box/inbox where document data created by scan, print, and I-fax jobs, are stored in the TOE.

Box PIN
PIN used for access control to mail boxes and inboxes where document data is stored.

Box functionality
(Mail box/inbox)
Allows scanned document data or document data specified from a PC to be stored in a mail box, or documents received by I-fax to be stored in an inbox. Also provide the operation such as print, send and delete to document data stored in a mail box or inbox.

Input function
A function to input hardcopy documents into the TOE.

Role
A role is a named group of user privileges used by access restriction functions. Privilege information contained in a role represents that a user is granted to execute each MFP function or not. Each user is assigned a role upon user registration.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01

[2] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02

[3] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 3 July 2009 CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 3 July 2009 CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: 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 C5000 Series 2600.1 model Security Target Version 1.17, March 17 2011, Canon Inc.

[13] Canon imageRUNNER ADVANCE C5000 Series 2600.1 model Evaluation Technical Report Version 3, March 17 2011, Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security

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