Research Report on the Security of MFPs

V2.0

March 2013

Information-technology
Promotion
Agency, Japan

English translation V1.0
September 2013
JISEC, IT Security Center,
Technology Headquarters, IPA

Notice:
This document is an English translation of the original report in Japanese, published by the Japan Information Technology Security Evaluation and Certification Scheme under IPA. Please note that URLs contained in this report were effective when the Japanese version was published, but some links may no longer work.

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 What is MFP?

MFP stands for Multi-Function Peripheral, Multi-Function Printer, or Multi-Function Product.

MFPs in this report refer to peripherals with the integrated functions, such as copy, print, scan, and fax.

The research targets of this report are the MFPs that require a high degree of information security functionality in such office environments as businesses and government agencies. Such MFPs are categorized in the Japanese product catalogs as “digital multifunction device,” “color multifunction device” or “monochrome multifunction device,” by their functions, but some are simply called “multifunction device.” In this report, it is referred to as “MFP,” which is an English abbreviation.

1.2 Background of this report

MFPs are IT products with security functions that represent Japan, and Japan has multiple vendors who are suppliers of MFPs to the world.

The MFP as a simple general office machine has been developed to have a role as a hub of information distribution in the office by providing connections to the LAN and information storage, etc., in recent years. Correspondingly, in response to the increasing demand for information security for the MFP, MFP vendors focus on the quality improvement of the information security functions, and have a number of certifications under the “Japan Information Technology Security Evaluation and Certification Scheme” operated by IPA.[1]

On the other hand, the MFP is becoming a more frequent target of attacks. The vulnerability that causes unauthorized operation of the MFP by exploiting the MFP’s remote control function was published in November 2011.[2] Due to the multiple functionality and sophistication associated with such improved conveniences as usage in the Internet environment, including the cloud computing environment, and support for smart devices, etc., more opportunities for attacking MFPs have been increasing in recent years. In this situation, even for the information security aspects, MFP vendors shall consider comprehensive countermeasures from the design stage against a wide variety of threats, including the risks of using a platform with the impact of known vulnerabilities as well as threats due to the network connection.

In general, the MFP is not recognized as an IT device whose security is important. There are cases where potential problems, such as an oversight at the design stage and problems with usage that the developers had not expected, are recognized later as vulnerabilities, or where configurations appropriate to the installation conditions and management of confidential information are not implemented (e.g., access methods to maintenance interfaces that no user could know, and administrator interface with access control have been published on the Internet).

[1] http://www.ipa.go.jp/security/jisec/index.html

[2] http://redtape.nbcnews.com/_news/2011/11/29/9076395-exclusive-millions-of-printers-open-to-devastating-hack-attack-researchers-say

1.3 Purpose of this report

The last research report (V1.0) comprehensively identified the vulnerabilities of the MFP regarding its security requirements, and described in detail the kinds of threats, the extent of attack potentials, the kinds of possible damages, and effective countermeasures for those, with respect to some notable items.

In this report, the viewpoints regarding the vulnerabilities that shall be noted in order to operate or develop the MFP are explained comprehensively and in detail. Specifically, the focus is on the vulnerabilities that create many opportunities for attacks, and the vulnerabilities that have existed for a long time but have been neglected, as they were not recognized by the parties involved. This report also researches from various perspectives and explains the vulnerabilities, which shall be considered initially for the MFP.

For the attack methods against these vulnerabilities explained in Chapter 7 and subsequent chapters, actual verification was conducted in the course of this research, and it includes successful attacks against some MFPs. Therefore, this report explains inspection methods, which are needed by parties involved to confirm the presence of vulnerabilities to the specific MFP, as well.

By recognizing the vulnerabilities described in this report, guidelines shall be provided for efforts to ensure security during the development process for vendors, countermeasures against problems in the operating environment as well as misuse by users, and measures to take for the suspected vulnerabilities in general functions of the MFP. Therefore, the purpose of this report is to improve the inspection standards of security inspection by utilizing this report.

1.4 Target readers

Target readers for this report are mainly developers who plan, design, and develop MFPs, as well as MFP users and evaluators who examine the MFP security functions.

1.5 Assumptions of this report

In this report, we assume an environment where information assets that can lead to a disadvantage to users (organizations) are stored when they are leaked, so that malicious users (attackers) can gain access to the information assets through contacts with the MFP on a scope that is not suspicious, or through the operation panel of the network or the MFP, assuming such MFP is connected to the intranet. In such an environment, MFPs that combine functions such as web server or file server are consequently required to ensure the security equivalent to the web server or file server.

The assumption of this report is to use high-end models among MFPs with a variety of authentication functions and the SDK. Some MFPs are not originally equipped with the functions that lead to the vulnerabilities described in this report. In addition, in case of securely using the certified products under the “Japan Information Technology Security Evaluation and Certification Scheme,” for example, some MFPs can be used by turning off some functions that lead to vulnerabilities before operation begins.

Because vulnerabilities are comprehensively identified in this report, readers should be aware that some items may not be relevant, depending on the MFP to be installed, the usage environment, or the security policy of the office.

1.6 Definitions of main terms

Definitions of main terms in this report are as follows. The meanings of terms other than those described here are supplemented in the footnotes, etc., when they appear:

Term	Definition
MFP	Abbreviation for Multi-Function Peripheral, Multi-Function Printer, or Multi-Function Product. It may also be called SPC (Scan Print Copy), AIO (All In One), or MFD (Multi-Function Device). MFPs in this report refer to peripherals with the integrated functions, such as copy, print, scan, and fax.
Japan Information Technology Security Evaluation and Certification Scheme	A Scheme in Japan: in the procurement of IT products by the government, etc., a third party (Evaluation Facility) evaluates appropriateness and reliability of the security functions of the IT products, based on ISO/IEC 15408, which is the international standard for security evaluation criteria, and the Certification Body certifies the evaluation results. Abbr.: JISEC (Japan Information Technology Security Evaluation and Certification Scheme)
Japan Cryptographic Module Validation Program	A Scheme in Japan: a third party conducts tests and certifies a cryptographic module, which is composed of hardware or software, etc., that is implemented with security functions, such as encryption functions, hash functions, and authorized signature functions, etc., listed as e-Government recommended ciphers, for appropriate protection of important information, such as security functions, cryptographic keys, and passwords, etc., that are stored inside. Abbr.: JCMVP (Japan Cryptographic Module Validation Program)
CVSS	Abbreviation for Common Vulnerability Scoring System. It is an open, comprehensive, and versatile evaluation method for the vulnerabilities of information systems, and provides common evaluation methods without relying on MFP vendors.
CEM	The standard that discloses the methodology used in the evaluation based on ISO/IEC 15408. Abbreviation for Common Evaluation Methodology. The formal name is Common Methodology for Information Technology Security Evaluation, and it is issued as ISO standard (ISO/IEC 18045).
SSD	A storage device using a flash memory as a storage medium. It is equipped with the same connection interface as that of a hard disk drive (HDD), and can be used as an alternative to a hard disk. Abbreviation for Solid State Drive.
SLC chip	One of the data recording systems in NAND-type flash memory. It stores 1 bit of data consisting of binary value of storage elements (memory cells). SLC is an abbreviation for Single Level Cell.
MLC chip	One of the data recording systems in NAND-type flash memory. It stores multi-bits of data consisting of three or more storage elements (memory cells). MLC is an abbreviation for Multiple Level Cell.
Maintenance interface	An interface used for maintenance of the MFP, such as setting and initialization of the MFP, and setting the administrator password, etc. It is broadly classified into two; a local maintenance interface with which maintenance personnel directly operate the MFP, and a remote maintenance interface with which maintenance personnel remotely operate the MFP.

LPR	A printing protocol via a TCP/IP network. LPR protocol is used to carry out printing using the printer or the MFP that is connected to a print server on the network, and it is specified in RFC 1179.
Page description language	A language which instructs the printer or the MFP by describing the output image when printing images or documents from a user terminal such as a personal computer.
Reverse-Engineering	To disclose the mechanism, specification, purpose, components, and elements of the technology, etc., of hardware or software, etc., by decomposing or analyzing.
Cross compiler	A compiler to generate an executable program on a different platform from a development platform.
Backdoor	Intrusion pathway from the back, which is created on a server or personal computer, etc. Some are created at the time of development, and some are created by malware or unauthorized access by an attacker, etc.
Buffer overflow	A vulnerability in which the data, whose size is greater than what is ensured, is written into the buffer when writing to the memory area allocated statically or dynamically. There is a possibility that privilege escalation or unauthorized access is performed due to this vulnerability.
Directory traversal	The attack method which accesses files in the directory that the administrator does not assume (authorize) by specifying relative path, etc.
Remote shell	CUI (Character User Interface) program that executes shell commands on another computer via network.
Port scan	To examine service availability externally via network, etc.
Black-box testing	To examine the functionality, etc., externally without peering into its internal structures. The antonym is white-box testing.

2. Research and Analysis Methods

In order to comprehensively extract vulnerabilities related to the MFP, this material introduces a research and analysis method as in the following Figure 2-1. From the left, "1. Functions and usage" is identified, and "2. Division of functions," and "3. Protected items" are identified. From "4. Threat and vulnerability analysis," "5. Assumed vulnerability list" and "6. Details of vulnerabilities unique to the MFP" on the right-hand side of the figure are produced as achievements. Details of vulnerabilities unique to the MFP explain the details of some vulnerabilities extracted from the assumed vulnerability list in regard to the configuration diagram, background, and causes.

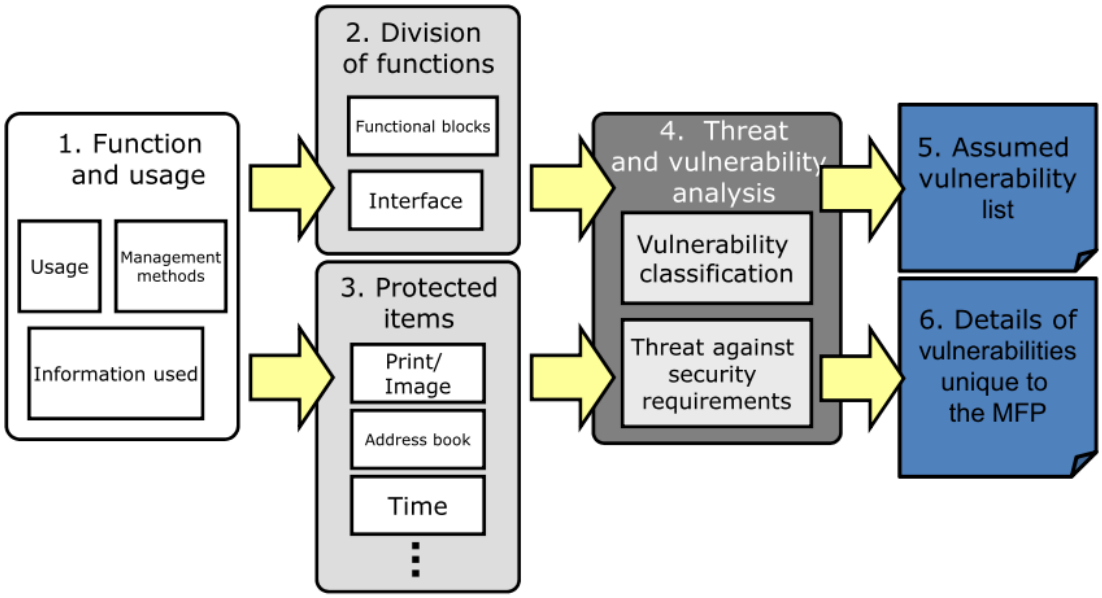


Figure 2-1 Overview of the research and analysis method

The procedure for this research specifies a list of threats to the information system in the usage environment of the MFP. A list of threats shall be sorted out according to the procedure of "threat modeling,"[3] which has been introduced as a "threat exposure procedure" in the IPA "Secure Programming Course." Threat modeling specifies the data flow from the system configuration diagram, and identifies the threats while tracing the boundaries of interfaces.

In this research, in order to specify the system configuration diagram, usage and functions of the MFP are shown in "1. Functions and usage" on the left in the figure. Next, shared functions on the systems of internal and external MFPs are identified in "2. Division of functions." The data flow is organized according to the usage of the MFP for specifying the information assets in order, which are primary assets to secondary assets, in the "3. Protected items." In "4. Threat and vulnerability analysis," as requirements for information

[3] Threat modeling – IPA "Secure Programming Course" threat modeling
http://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/c101.html
"Threat Modeling - Application security architecture" Frank Swiderski and others, translation by Yoko Watabe, Nikkei Business Publications, Inc. 2005

security in general, confidentiality, integrity and availability of ISO/IEC 27001, which are the standards of information security management, and four requirements (authenticity, accountability, non-repudiation, reliability) defined as optional, are applied. Anything identified as breaking these requirements is considered a threat.[4]

The purpose of this research is to comprehensively extract the vulnerabilities, in particular, while assuming examples of attack methods from a list of the threats in "4. Threat and vulnerability analysis." In such case, the CWE common vulnerability type list[5] is used to check the completeness.[6]

With respect to the 21 items including vulnerabilities which should be re-recognized by developers and users of the MFP, as well as vulnerabilities that became topics of the MFP in recent years among other vulnerabilities, detailed descriptions of attack methods against such vulnerabilities are presented. There are also some interviews of the parties related to MFP vendors, and verification experiments were conducted to ensure the concreteness of some items described in this report.

2.1 Arrangement of the usage and functions of the MFP

Among the publicly available MFPs provided by five major MFP vendors in Japan, the usages and functions of the models that are certified under the Japan Information Technology Security Evaluation and Certification Scheme are specified by using news sites and published materials.[7] The results from the interviews of some MFP vendors and from verification experiments, which were conducted for confirmation, are sorted out in Chapter 3.

2.2 Arrangement of the functional blocks

Functional blocks, which are considered to have been used for the MFP, were identified using publicly available information under the Japan Information Technology Security Evaluation and Certification Scheme. Functional blocks are organized in the range from "3.5 MFP system configuration examples" to "3.7 Software inside the MFP."

2.3 Specifying the data exchanged between functional blocks as assets to be protected

In order to specify the assets to be protected in the usage environment of the MFP, the data exchanged between functional blocks of hardware as well as main blocks of software are specified. Among them, the primary assets of the assets handled by the MFP users directly, and the secondary assets such as security control information, processing data related secondarily to use of the information system called the MFP, and the state in which a primary asset is recorded in a specific medium, shall be separated.

Arrangement of the primary assets and secondary assets is carried out in "5. Assets to be protected by the MFP."

---

[4] 27001 ISO / IEC - the equivalent Japanese industrial standard is JIS Q 27001:2006 http://www.isms.jipdec.or.jp/doc/JIP-ISMS111-21_2.pdf

[5] CWE common vulnerability type list (http://www.ipa.go.jp/security/vuln/CWE.html)

[6] The listed vulnerabilities in Chapter 6 and Web interface in Section 7.15 are confirmed to cover the CWE common vulnerability type list.

[7] Public product documentation, such as security target descriptions, catalogs, and white papers published by MFP vendors.

2.4 Listing threats and vulnerabilities by each asset

For all of the secondary assets in the state of specific information and medium of the primary assets, the threats are listed with completeness by applying the common seven security requirements to them. Vulnerabilities, which are possible causes, are listed as assumed vulnerability examples while citing instances of how the threats listed take shape in incidents or attacks.

A list of these threats, attack examples and assumed vulnerabilities are shown in the table in "6. Vulnerabilities assumed from threats."

2.5 Detailed explanations of notable vulnerabilities

From the perspective of the vulnerabilities listed, explanations given for vulnerabilities of the MFP that have been published in the vulnerability database,[8] news sites,[9] and international conferences such as Black Hat are studied, with respect to results of some actual verifications, attack methods and countermeasures to be taken by developers and users. The scoring for attack potentials on each item is described as a standard for the feasibility of the illustrated attack methods. For the items with more detailed explanations, it is confirmed that this report covers the perspectives of publicly known vulnerabilities that are actually reported, and verifies the vulnerability database as well as CVE as of July 2012.

[8] CVE (http://cve.mitre.org/cve/index.html)

[9] These are not general news sites, but news sites that are output as results of search using "MFP" and "vulnerabilities" as keywords in Google.

3. Usage and Functions of the MFP

3.1 Development history of the MFP

The MFP has been developing over time, while a variety of usages have been found. Figure 3-1 below shows the development history of the MFP as well as potential usages in the future from left to right in order.

Originally, MFP was a device that performed an "imaging" process mainly for copying, but fax is integrated into this, and the transferring function of digitized image data, as well as the network function, was added later so that its functions have been greatly increased. Then, more functions, such as "remote sharing," by which multiple users can share the MFP via network, and "application extension" to work in cooperation with existing business systems, were added. This has increased reliability as well as demand for the security of the MFP.

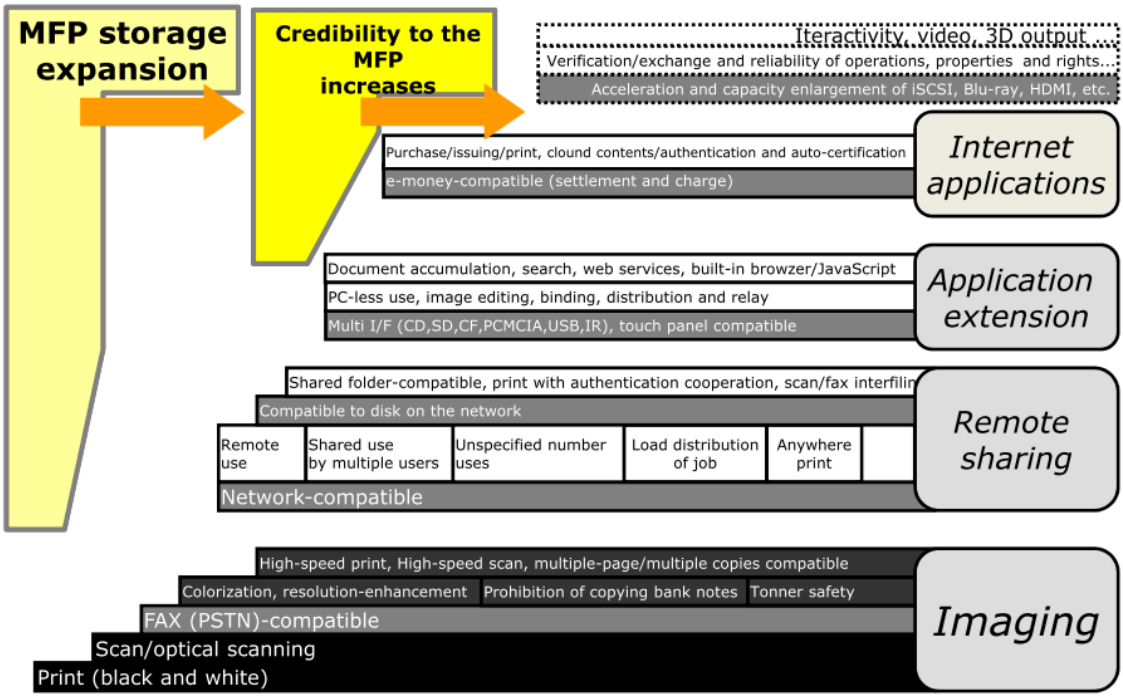


Figure 3-1 Development history of the MFP

The frame with the dotted black line in the upper-right corner of Figure 3-1 shows assumed examples of the possibility of function enhancement of the MFP in the future. This includes a role as a part of the social infrastructure and as an aspect of life kit functions. "Internet applications" has a way to utilize for more variety of usages by connecting the MFP with cloud services and services on the Internet. In the office environment of companies that is the assumption of this report, further development is expected in the future such as printing in a seamless environment across the offices in each location of the company.

The research targets of this report are MFPs used in the office environment with common functions, so functions that are only implemented on the MFP by a few vendors, as well as future functionality, are not discussed.

3.2 Security required for the MFP

Figure 3-2 below shows examples of types of security required for the MFP that are considered to be developing. However, vulnerabilities need to be comprehensively specified, because the MFP is implemented with a number of functions. Threats and vulnerabilities in the usage environment of the MFP are identified in the order of the usages and functions that are initially required for the MFP in this report.

Function category	*Function examples*	*Assumed threats and countermeasures*
Internet applications	- Search/indexing additional services - Characters/meaning recognition and classification services - Settlement/certification services	▼Threat: Ranked index information, access log leakage ▼Measures: Use of encryption HDD contains index
Application extension	- Extended application by a third party - Evaluation/recognition of specific document - Open certification/upgrading security	▼Threat: Lack of required authentication, and threat due to different implementations of extended application ▼Measures: Frameworking and proliferation of MFP substrate and security
Remote sharing	- Acceleration, file and function sharing - Sharing by multiple users by region - Measures for IPv4 addresses exhaustion	▼Threat: *Printing job is wiretapped at unexpected location* when bridging USB remotely ▼Measures: Apply encryption of printer driver communication or of communication channel When bridging the USB
Imaging	- High resolution and acceleration - High-speed encryption and signature	▼Threat: Uneasy operations with encryption due to high resolution and acceleration, operations with off-encryption ▼Measures: Use HW function (IP) such as encryption modules compatible with network disconnection, isolation/external encryption

Figure 3-2 Functions and security required for the MFP

“Internet applications” in Figure 3-2 shows applications not only of the functions built into the MFP, but also of a variety of functions on the Internet and network. One instance is collaboration with the services that provide indexes for fast searching of sharable documents stored inside the MFP. There are also other functions, such as extracting characters from the scanned images for an easy search, and detecting a face from the photographic images to classify them automatically. Besides, some MFPs have a content sales function in coordination with settlement functions of digital money and cash, as well as print functions for certifications such as resident cards in coordination with Basic Resident Register cards. Not only are they available for the sales and services, but for insurance application services, for example.

For Internet applications, the leakage of documents that are temporarily stored on the external storage media in conjunction with cloud services, and the leakage of index information that is necessary to search documents, are considered indirect threats in the usage environment of the MFP. Internet applications are not necessarily protected by the functions or operations of the MFP itself, because it is difficult to generalize, so they are not listed in the vulnerabilities in Chapter 6, but discussed in Chapter 9.

For “Application extension,” using extended application software developed by third parties other than MFP vendors, it has a feature to use a variety of functions. For example, there are linkage functions with external authentication functions and specialized file

processing. For authentication, some authentication procedures target a single existing function, but there are also open authentication procedures available in multiple functions. Such open authentication procedures require measures against threats, such as the maintenance of session information and the reuse of session information by impersonation, but the management tends to be too complicated due to its openness. Therefore, measures such as the adoption of the development framework that provides the integrated management of the session information are needed.

In "Remote sharing," a faster network makes high-speed file sharing and function sharing with remote areas easy to use. Some functions also have the ability to share a printing function on USB devices in remote areas in addition to file sharing. The network that supports remote sharing has been used on a regional basis and a national basis using TCP/IP. Currently, a protocol called IPv4 is mainly used for TCP/IP, but most MFPs implement a protocol called IPv6, with a wider address range than that of IPv4 and a strong possibility for more use in the future.

"Imaging" provides basic functions of the MFP, such as image processing for copying, printing, scanning and faxing, as well as resolution-enhancement and higher speed for printing and reading. Increases in the number of pixels and color depth, faster print speed, and faster paper feed are progressing as a unit. In response to this higher-speed development, security measures such as encryption processing have been becoming considerably faster.

3.3 Life-cycle in an environment of MFP use

Figure 3-3 below shows the life-cycle from the MFP utilization plan to disposal from the user's point of view. Within the general life-cycle of products, this research covers only the "Introduction," "Use," and "After use" phases. The left side of the figure shows work mainly done by users, and the right side of the figure shows work mostly outsourced to MFP vendors and professional suppliers.

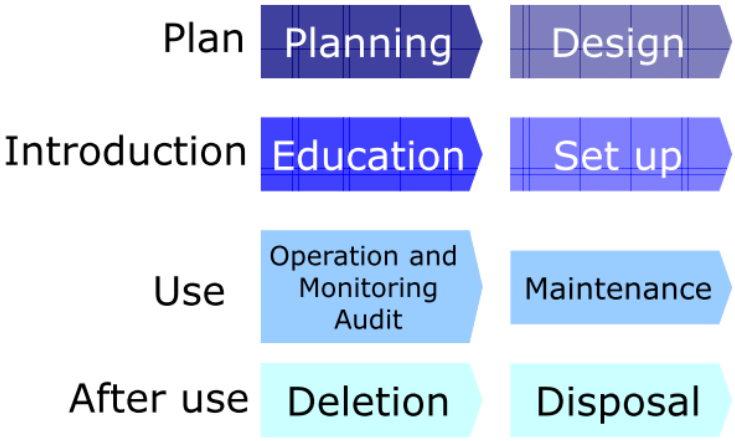


Figure 3-3 Life-cycle in the usage environment of the MFP

3.3.1 Plan

"Planning" refers to a stage to consider the purposes and desired effectiveness of using the MFP by users. The purposes for using the MFP include "the use of the MFP provides an easy step for document retrieving," "the safety of document exchanges increases while reducing the operating procedures," and "ensuring efficiency and reliability by automating the recording of necessary work and operations," etc. Specifying usage and the mechanism to achieve desired effectiveness according to the goal is to perform "Design."

In addition, assets to be protected, safety standards to be ensured, and other specific objectives are also examined in the planning and design stages. Safety standards and objectives can be specified as security policies, and in general, as the entire information system of the users including the MFP. Some parts of the security policies may be added or revised for the usage environment of the MFP.

3.3.2 Introduction

"Introduction" refers to education for MFP users and the installation of MFP device. Education for MFP users, informs general users about how to handle documents on the MFP and authentication methods, and provides contact information when users do not know how to operate, etc. For maintenance personnel and operators, trainings on the configuration and setup methods for some specific MFP models, monitoring and verification methods of MFP operations, and how to deal with breakdowns, are provided as well.

When installing MFP device, such device is properly positioned at specific places, and installation and initialization of the specific software are performed. Additionally, the relevant performance should be conducted by installing wiring with the related systems.

3.3.3 Use

In the "Use" phase, work performed mainly on the site where the MFP is used is categorized as "Operation and monitoring" and "Audit," while work performed by maintenance professionals is categorized as "Maintenance."

In addition to the work of changing the MFP configuration by administrators, “Operation” includes the use of MFP by general users. It is assumed that the MFP is operated on the closed network within the user’s site in general, so the monitoring of the MFP is considered to be the responsibility of users.

In “Audit,” it is considered whether an appropriate operation has been conducted from the records of incidents that have occurred during operations and from operating capacity information, as well as what measures should be taken from the results.

“Maintenance” includes work, such as repairing the main unit of the MFP as well as adding and replacing parts or software.

3.3.4 After use

“After use” involves the work of “Deletion” and “Disposal.” Users perform “Deletion” of the data and the configuration information before disposal. “Disposal” includes what should be done when waste disposers or secondhand goods dealers collect the MFP that is not used any more.

3.4 MFP from the viewpoint of information systems

Figure 3-4 below shows the usage environment of the MFP from the viewpoint of an information system. The MFP in the upper right of the figure operates in cooperation with other services, such as user terminals in the upper left or the accumulation and external processing in the upper middle of the figure, via the communication system in the middle. The remote management system on the bottom of Figure 3-4 enables the setup of the MFP from the other servers or terminals, instead of the console panel of the MFP. The remote management system also has the functions of authentication and authorization of users, of the main unit of the MFP, and of the accumulation and external processing services, respectively.

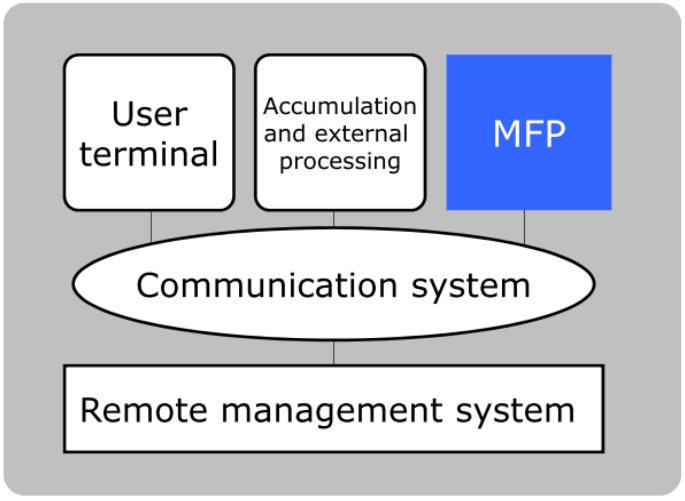


Figure 3-4 MFP from the viewpoint of an information system

3.4.1 User terminal

"User terminal" refers to a terminal that provides an input/output interface that uses the MFP via the network or communication system. MFP users include general users who print and fax as well as administrators who are responsible for the user management and configuration of the main unit of the MFP. The meaning of "terminal" is focused on the point that people conduct operations and displaying.

3.4.2 Accumulation and external processing

"Accumulation and external processing" mainly refers to the machine automation processing without manual operations by people among the external MFP systems. In the usage environment of the MFP in particular, providing long-term storage of documents, temporary storage of job data, and spool processing, is called "accumulation," whereas a variety of processing, such as the cooperation of image processing or character extraction with business systems, and the search processing of documents, are called "external processing."

3.4.3 Communication system

"Communication system" refers to the communication systems external to the MFP used to communicate with external systems. Some of the communication systems are equipped with Ethernet switches, IP routers and their wiring, as well as wireless LAN access points. When connecting to the MFP via a USB hub, the USB cable and the USB hub are also included.

"Communication system" in the usage of the MFP for general office is limited to the closed networks within a company, such as VPN or LAN in the company using the MFP. The MFP, user terminals, and accumulation and external processing, are all connected in a closed network within the company. Sometimes, a closed network within the company is commonly referred to as "internal network."

Exceptionally, there are cases for going through networks outside of the company or Internet, such as remote maintenance interfaces used by maintenance personnel outside of the company.

3.4.4 Remote management system

"Remote management system" refers to external MFP systems for performing authentication of users, etc., authority management, monitoring of operations and functions, and configuration management, etc., when MFP functions are used. Dedicated software provided by MFP vendors to perform configuration tasks, configuration changes, and maintenance, as well as browsers used for configuration changes in the MFP are considered as a part of the remote management system as well. The remote management system includes remote management, monitoring, and maintenance functions through the communication system.

3.5 MFP system configuration examples

Figure 3-5 below shows MFP system configuration examples. Blue "MFP" in the middle of the figure indicates the MFP. The MFP may be connected to portable media such as USB memory (hereinafter, removable media) and IC card reader for authentication. Some models may have them built into the main unit of the MFP.

The lower right corner of the MFP is the "Maintenance terminal" for maintenance personnel to conduct failure diagnosis of the MFP as well as backup. In the upper-left corner in the figure, there are a "User terminal" and an "Administrator terminal." MFP service is used by installing the MFP driver (printer scanner driver) inside the user terminal and communicating with the MFP. The administrator terminal is used to remotely configure the MFP.

The bottom right is a fax function. PSTN fax[10] performs an image transmission by an analog fax modem using the existing telephone network. IP faxing can be performed as a mail fax through the email servers, and IP fax makes an SMTP connection to the MFP of the other party directly with IP addresses as well as SIP[11] fax to perform the image transmission of fax using SIP.

Some existing PSTN fax may be used with IP using a device called TA (Terminal Adapter) that can be converted to SIP or H.323 procedure. There is a benefit of using the TA, such as reduction of the fax communication fee generated when using the existing PSTN, because the communication between the PSTN faxes in remote locations can be relayed via IP network or Internet. TA at the bottom right of Figure 3-5 shows an example of an IP-PSTN port of the MFP.

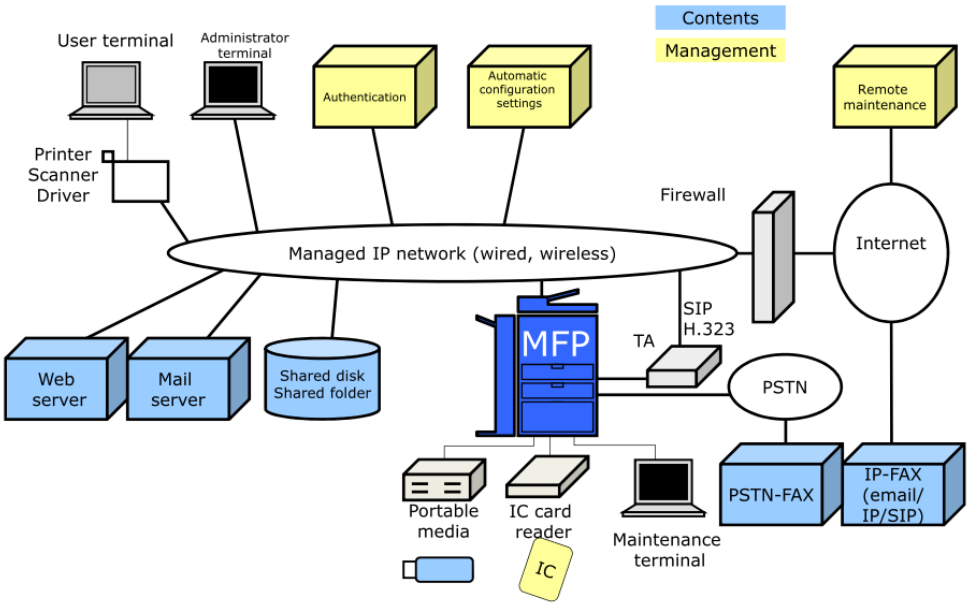


Figure 3-5 MFP system configuration examples

"Shared disk and Shared folder" to the left of the MFP are often used to store images received by fax and images scanned by the MFP. On the left of those, there is "Mail server," which is also the destination of the images sent from the MFP when such scanned images and the received fax images are received by mail. Administrators and users may receive notifications of processing errors or failures inside the MFP via mail server in some cases. "Web server" to the left of "Mail server" is used to make use of external images of the MFP by using a web browser built into the MFP, or is used to collaborate with the business systems outside of the MFP.

[10] Abbreviation for Public Switched Telephone Networks
[11] Abbreviation for Session Initiation Protocol (http://www.ietf.org/rfc/rfc3261.txt)

"Authentication," of the leftmost yellow square, is the authentication server outside of the MFP connected to the network, and is a staff authentication server of an in-house system installed in offices, for example. It may provide a single sign-on function. "Automatic configuration settings" to the right of "Authentication" has functions, such as automatically allocating IP addresses, synchronizing to the accurate time, and monitoring the operation of the MFP in the network including the MFP. "Remote maintenance" in the upper right corner of the figure is a maintenance service of the MFP by MFP vendors or maintenance businesses from a remote location. In the remote maintenance, the monitoring of the lives of the drums and toners as well as the number of papers used is conducted.

In this example, a server used for spooling the MFP, a monitoring server of the user's site and a proxy server used by the MFP are not mentioned, but they may be used depending on the environment of the users.

3.6 Hardware inside the MFP

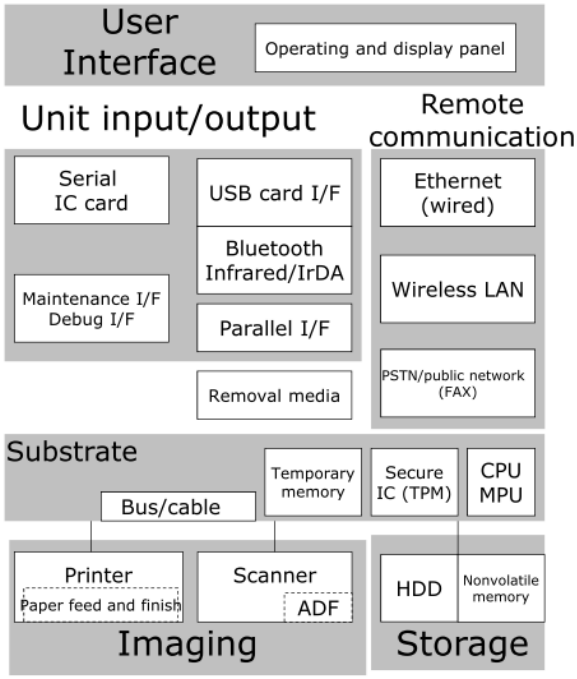


Figure 3-6 Hardware inside the MFP

The MFP is equipped with multiple functions, such as printing, scanning and networking, which work together. It is configured by combining several hardware devices, such as printers, scanners and a substrate, etc.

3.6.1 Hardware inside the MFP - Imaging

The printer is equipped with a paper feed mechanism to retrieve the papers from the paper tray, a paper sending mechanism from the inside to the outside, and a fixing mechanism for transferring the images. There is also a finishing mechanism as an additional function of the print function. The finishing mechanism is called "Finisher," etc. The finishing mechanism includes functions of sorting the prints per unit, stapling, and folding them.

The scanner is a device that highlights the document and reads the reflected light as digital data. It is equipped with a scanning table such as a glass plate to read one side of a document at a time. ADF (Auto Document Feeder) is mounted to continuously read multiple-page stacked documents. The scanning table has a moving scanner module to read a document placed on the scanning table. Some ADFs are equipped with a different scanner module other than a scanning table to load information at once when papers are fed into the scanner. Many MFP models have a scanner module built into the ADF of the MFP for realizing the fast scanning process.

3.6.2 Hardware inside the MFP – Storage

"Storage" is used for storing documents, temporary job data, and the settings values, etc., inside the MFP. Data in storage is rewritable with any manipulation by the users.

3.6.3 Hardware inside the MFP - Unit input/output

"Unit input/output" is a collective name that is uniquely given in this report for the selected interfaces which communicate face-to-face to the main unit of the MFP. Typically, there is a USB card interface, which can be mounted on multiple removable media, such as an SD memory card, a USB memory, or a CF card. Bluetooth and infrared (IrDA) interfaces are also considered to be connected to the MFP. The parallel interface is an interface that has been mostly used for older printers, and it used to be equipped with a terminal that connected to a printer.

"Unit input/output" also includes authentication interfaces, and maintenance/debug interfaces.

There is an IC card recognition device that authorizes users who operate the MFP console for authentication, and a biometrics interface.

The maintenance interface has a function to perform failure diagnosis of the MFP at the time of maintenance of the MFP. The debug interfaces are considered to be no longer available, but they are interfaces to check, change, or rewrite the state of the software running on a substrate when developing the MFPs. The debug interfaces control the CPU at the privileged level, so that it operates without any limitation or authority set inside the MFP.

3.6.4 Hardware inside the MFP - Remote communication

"Remote communication" is a collective name that is uniquely given in this report for the selected interfaces which communicate via multiple-stages of communication devices from the MFP. They are Ethernet, wireless LAN, and PSTN public networks (including PHS). These communication interfaces enable communications globally through routers, switches, and exchange devices. While remote communication is considered as a global interface, unit input/output is considered as a local interface of the MFPs.

3.6.5 Hardware inside the MFP - User interface

The "User interface" of the MFP has a liquid crystal display for displaying the MFP and a console panel (console, for short) that includes the keyboard. In addition to the MFP with a console built into the main unit, some models have an external console, and some of them are large.

3.6.6 Hardware inside the MFP – Substrate

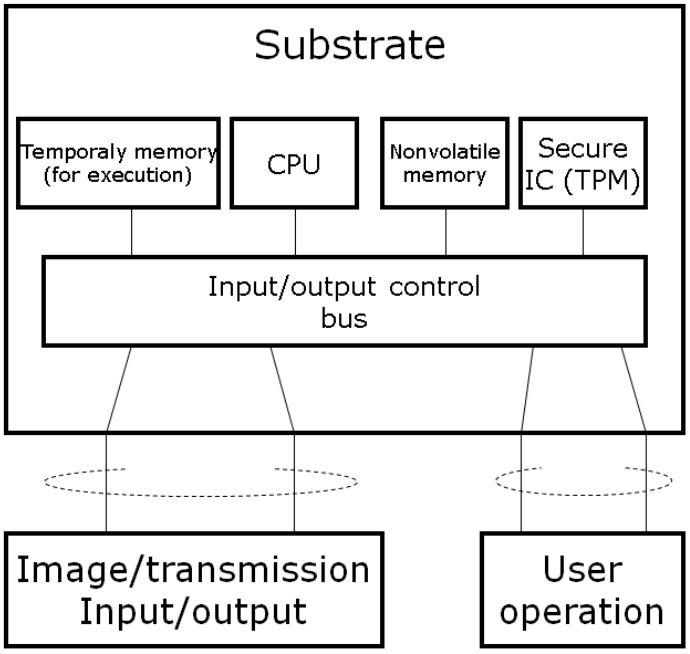


Figure 3-7 Hardware inside the MFP - Substrate and main interface

Figure 3-7 shows a substrate which is the hardware inside the MFP, and main interface. Temporary memory (for execution) refers to the volatile memory provided by DRAM (Dynamic Random Access Memory) etc., when executing the software. The "CPU" performs the arithmetic processing for executing the software. "Nonvolatile memory" is used to store software for execution and the set values for execution. "Secure IC (TPM)" is an IC capable of encryption processing which has a private key to the encryption processing inside. Secure IC (TPM: Trusted Platform Module) can store the private key securely without taking the key outside of the secure IC when performing cryptographic processing.

3.6.7 Hardware inside the MFP – Connection between modules

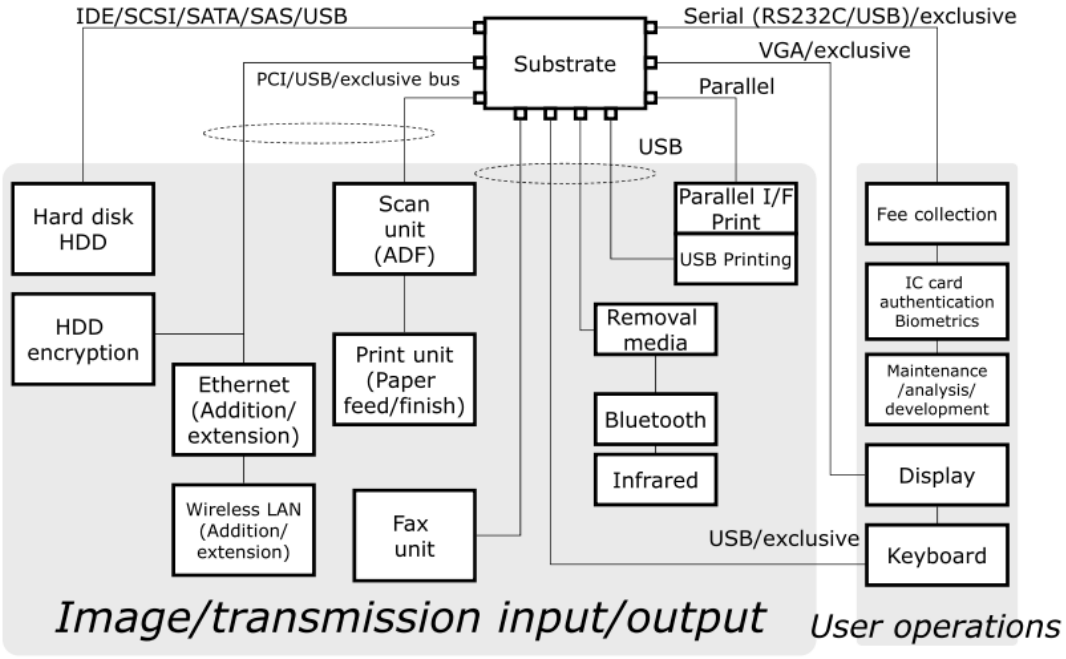


Figure 3-8 Hardware inside the MFP - Connection between units or modules

Figure 3-8 above shows the configuration of a connection between a substrate and other hardware inside the MFP. The figure also indicates how each hardware component is connected using interfaces from a substrate, but it does not indicate the connection between hardware components. For example, the Ethernet module is not necessarily connected to the substrate through the HDD encryption.

IDE/SCSI/SATA/SAS/USB to the left in the figure are among those that are the standard interfaces for hard disks. IDE (Integrated Drive Electronics) is an inexpensive interface for personal computers with a long history, but there is a disadvantage in that the connector tends to be larger due to the number of wires of cable. SCSI (Small Computer System Interface) has an advantage in that it can be connected to multiple devices such as scanners and is not limited to hard disks, but it needs as many wires of cable as IDE. While significantly reducing the number of wires of cable, SATA (Serial Advanced Technology Attachment) has been provided with higher speeds of transmission than IDE at low cost. Among hard disk interfaces, SAS (Serial Attached SCSI) is also standardized, but is generally expensive. A USB is also used as an interface to a hard disk, but it sometimes is difficult to secure a transfer speed.

HDD encryption in the second row on the left in Figure 3-8 shows the encryption/decryption functions for the data to be read from/written to the hard disk. Some “Ethernet” and “Wireless LANs” may be provided on the substrates, but some may be provided by adding other modules than the substrates. These HDD encryption modules and Ethernet modules are provided through a PCI (Peripheral Components Interconnect) bus, a USB bus, or an MFP vendor-specific dedicated interface, because a high-speed data transfer is needed, and the module itself can be smaller.

The print unit and scan unit play the core roles of the image processing of the MFP, and the MFP vendor-specific dedicated interfaces are used as well as high-speed interfaces, such as the PCI bus, for the usage between the substrates. Image processing functions, such as deployment of printed images and the processing of the scanned images, may be included on the side of the print unit and the scan unit.

Modules in the column to the right of the fax unit are slower interfaces. The primary usage of the fax unit is for monochrome faxing, but the real-time transmission of fax images is not considered so important for color image transmission. As the fax function is often treated as an optional function, it may be connected with general-purpose interfaces such as USB.

"Removable media," located to the right of the fax unit in the figure, refers to the modules for removable media, such as USB memory and SD card. Images from a digital camera can be input to the MFP by inserting or removing the media. "Bluetooth" and "Infrared" are the wireless interfaces that can input the print images to the MFP, and communicate with mobile phones or digital cameras at a close range. The difference with the wireless LAN is that infrared and Bluetooth do not connect with other networks in a wide area, but can limit the connection only to the surroundings of the MFP. The maximum radius of Bluetooth is about 10m, and that of infrared is about 10 cm in the absence of things that block the light.

"Display" and "Keyboard" at the bottom right of the figure refer to a console panel for display that is equipped with the main unit of the MFP, and a keyboard for operation. Some models have an independent display device and a keyboard external to the MFP.

"Fee collection" at the top right of the figure is a device that is used by inserting money as a fee to publicly available MFPs, etc. "IC card authentication, Biometrics" is a module for authenticating MFP users by using biometric information, such as fingerprints or a non-contact IC card. IC card authentication and biometrics are connected with the MFP substrate by USB or RS232C. "Maintenance/analysis/development" is used in order to examine the cause of the failure of the MFP in detail, and to update some settings as well as software. Because there is no usage of the development interface for the users in general, it is either deleted or disabled in the products.

"Fee collection" device is not discussed in this report, because using the MFP in an office environment is assumed in this report.

3.7 Software inside the MFP

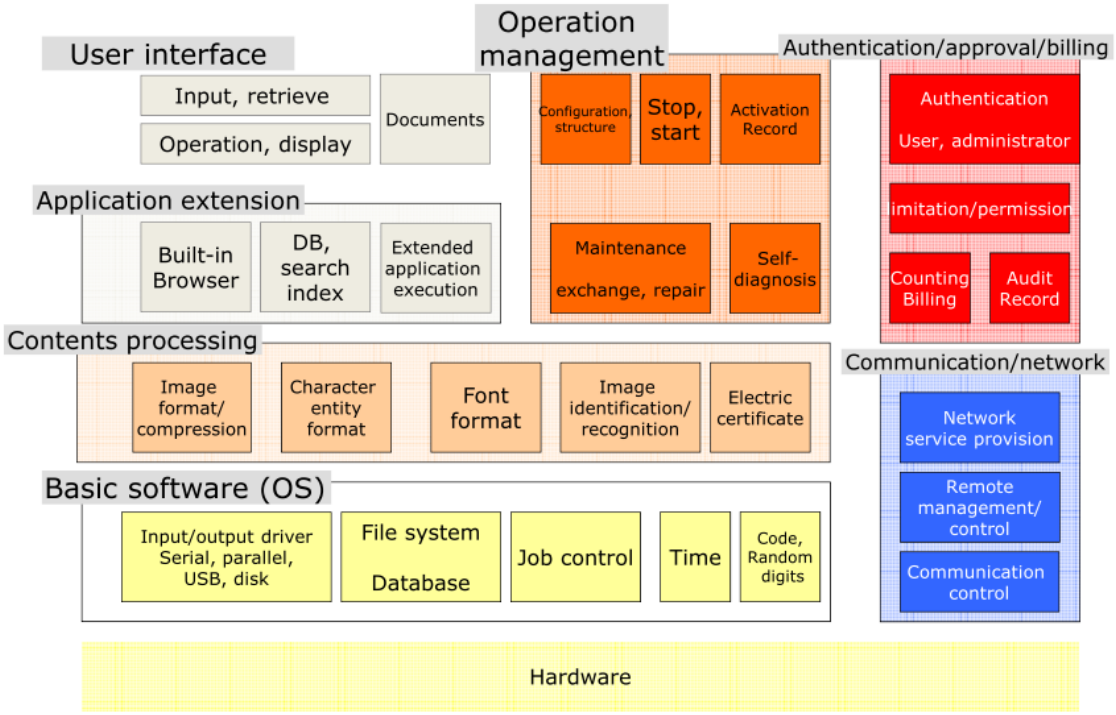


Figure 3-9 Software inside the MFP

The function blocks of the software, which are executed on the hardware of the MFP, are organized. Details of the function blocks are as follows:

3.7.1 User interface – Input, retrieve

"Input, retrieve" of the user interface refers to inputting and retrieving of original papers and prints.

"Network service provision" under the "Communication/network" indicates inputting and retrieving of job data via networks.

3.7.2 User interface – Operation, display

"Operation, display" of "User interface" refers to the operations and display using the console panel of the main unit of MFP and the keyboard. Operation guide and marks indicated by stickers, etc., on the main unit can be included if necessary.

3.7.3 User interface – Documents

"Documents" under the "User interface" refers to the operational materials which explain how to use the MFP, including user guides and manuals. All the uses of functions operated on the MFP are described in the materials.

3.7.4 Application extension – Built-in browser

"Built-in browser" under the "Application extension" refers to the web browsers built into the MFP. The built-in browser makes a request to the web services or web servers outside of the MFP in accordance with a prescribed process, and conducts interpretation of the HTML files received from the web servers as responses, and the execution of JavaScript to get necessary information. Some may have functions similar to the general web browsers, and a PDF reader, etc., may be added on.

Examples of the usage of built-in browsers include the operation of other MFPs and a data request for printing to a web server running on external business systems.

3.7.5 Application extension - DB, search index

"DB" refers to a database used in the MFP. It can be used to manage a large number of addresses, files stored as shared documents in the boxes in the MFP, and long-range job data. In some cases, a database with a general-use SQL language interface is used. The use of the SQL language interface in the MFP requires consideration, because a number of attacks against the DB and websites using SQL injection in the system have been reported.

"Search index" is an index of information used to search full-texts of the documents stored in the MFP.

The full-text search is performed based on one or more words throughout a large number of files at high speed, and the search index is prepared as organized data that indicates the document files shall be prepared word by word beforehand. Therefore, the search index contains words that are extracted from a large number of documents and its frequency, as well as document file names.

As the data of the search index tends to be larger than or equivalent to the size of the original papers, sharing between multiple users is common. Some documents require access control, for example, to permit writing and reading only for specific users, so that it is necessary to pay attention to handling the search index.

3.7.6 Application extension – Extended application execution

"Extended application execution" refers to the function that makes it possible to execute software, developed by third-party users or developers other than MFP vendors, on the MFP. In the "Extended application execution," applications developed in Java[12] can be executed, or specific instructions developed for the MFP can be executed in the browser inside the MFP.[13]

MFP vendors distribute a development environment called "SDK (Software Development Kit)" as an environment for developing extended applications for each MFP. In SDK, in general, API (Application Programming Interface) is provided with libraries and

---

[12] RICOH Developers Challenge
http://www.ricoh.co.jp/javachallenge/outline/
Canon MEAP - "The OS-independent by Java technology"
http://www.canon.us/technology/canon_tech/explanation/meap.html

[13] FujiXerox Apeos IntegrationPlus
http://www.fujixerox.co.jp/solution/dsp/product/integrationplus/index.html
KonicaMinolta OpenAPI
http://en.wikipedia.org/wiki/Konica_Minolta_OpenAPI

specifications to call services on the MFP and functions of drivers for the MFP, provided by the specific MFP vendors and specific models, from other software.

By using the SDK, third parties who are not MFP vendors can develop new software, enhance MFP functions, and operate in cooperation with other systems. Some SDKs operate with assumptions that software runs outside of the MFP or that software is installed into the MFP.

3.7.7 Content processing - Image format/compression

To print on paper, the MFP receives the images in a format determined in advance for each MFP, processes them, and then transcribes them onto paper. Therefore, the MFP has a function to process data of specific image formats at high speed. It can also directly import specific image formats, such as JPEG, TIFF, and PDF, or files using image compression format to decompress them.

3.7.8 Content processing - Character entity format

The MFP in general performs print processing based on the image data bitmapped. There are cases, however, as in PDF or PostScript, to independently decompress fonts built-in to the MFP and create print images when character code is received. On this occasion, support for the corresponding character entity format (character code) is required. In Japanese, there are multiple character codes, such as JIS, SJIS, EUC, and Unicode. They are called multi-byte character codes with a length of two or more bytes per character.

3.7.9 Content processing - Font format

Data called “Font” that defines the shape of the character is required to decompress an image of characters from the character code in the MFP as in PDF or PostScript. The MFP requires a process corresponding to the specific font format in order to decompress fonts. PostScript font is provided by MFP vendors for PDF or PostScript.

3.7.10 Content processing - Image identification/recognition

Some MFP models have a function to identify and recognize characters in the images received via fax or scanned inside the MFP. This function, however, is outside the scope of this report since it is not built-into the MFP generally.

3.7.11 Content processing - Digital certificate

Some MFP models produce a digital signature using a digital certificate for the digital files registered in the MFP or images scanned inside the MFP, and provide evidence that may be needed in business.

There is a method of encryption and digital signature of the content of email called S/MIME for mail faxing, and a digital certificate can be used.

This is not for processing the documents, but an encryption communication function of the SSL/TLS provides an authentication of a server/client using a digital certificate, as well as an exchange of the key.

3.7.12 Basic software (OS) - Input/output driver, serial, parallel, USB, disk

Generally, basic software (OS) includes control of all hardware and resource management functions, but the common functions of the MFPs on the market are identified in this report.

There are general-purpose OS's that are available for multiple embedded products for general use, and limited purpose-built OS's that are dedicated to the specific models or MFP vendors. A purpose-built OS has less visibility to attackers due to the exclusiveness of its source code, and the API of the OS is even undisclosed. On the other hand, general-purpose OS's are more recognized by attackers, because they are widely distributed as such systems as Windows, Linux, and VxWorks. However, they provide an advantage of acquisition of source code if necessary and verify them using a standard API. It is common for both types of OS to have a possibility of getting involved with a variety of vulnerabilities in connection with its high functionality and high performance.

Basic software (OS) of the MFP includes an input/output driver. As an external interface of the MFP, it controls the input and output of serial, parallel, USB, and hard disk.

3.7.13 Basic software (OS) - File system, database

Temporary job data and shared documents to be saved in the long term are stored inside the MFP. Some configuration information, usage history, and the audit records are stored either in the file systems or in the database inside the MFP.

3.7.14 Basic software (OS) - Job control

The multiple requests of printing, scanning, faxing, and copying, are directed to the MFP, and the MFP should process them in order as instructed. Some processing may take more than a few minutes, and other requests are held in the memory or on the hard disk inside the MFP in the form of a "Job."

Job control executes jobs by controlling the receiving jobs, running jobs, holding jobs, and completing jobs to produce some results.

3.7.15 Basic software (OS) - Time

In cases of the office MFP, the time shall be always synchronized in the system for the log that records operation history, encryption, authentication servers, and digital certificates. In the MFP, a component called the real-time clock keeps beating the time even when the power is off, and it operates at approximately the right time when the power is turned back on. Sometimes, the time server on the network is used to synchronize the time.

3.7.16 Basic software (OS) - Code, random digits

A process of calculating a hash value as well as processing for encryption is included in the "Encryption." When using an encryption in general, "Random digits" play an important role in order to generate a value hardly expected as an encryption key.

3.7.17 Management - Setting, configuration

There are many items in the “Setting, configuration” under the operation management of the MFP, and there can be several hundred or more items. Because each configuration item depends on the models of the MFP, the configuration per functional block is discussed without consideration for the details of individual configuration items.

3.7.18 Operation management - Stop, start

There is a power-saving function in the MFP to turn on the power-saving mode automatically. The power of the fax-installed machine is always turned on, but some models without fax may be turned off during non-business hours.

3.7.19 Operation management - Activation records

It records the number of copies or prints of the MFP per user, and records the history of operation management, such as adding or removing software and configuration changes.

3.7.20 Operation management - Maintenance, exchange, repair

Operation management includes functions that correspond to the failure of the MFP, and which perform replacement of software and hardware components. It contains license management functions as well.

3.7.21 Operation management - Self-diagnosis

Internal software checks the status of the hardware and software inside the MFP at the time of MFP failure, and reports defects or failure locations.

3.7.22 Authentication/approval/billing - Authentication, user, administrator

MFP authenticates users and administrators. Maintenance personnel are authenticated as well.

3.7.23 Authentication/approval/billing - Limitation/permission

Usage limitation and permission imposed by the MFP to all users and user groups.

3.7.24 Authentication/approval/billing - Counting/billing

Summary value of the number of times services are used, and the number of papers used for printing, copying, or scanning in a specific MFP. It is counted per MFP, in which maintenance businesses can use it as rationale to charge based upon its uses.

3.7.25 Authentication/approval/billing - Audit records

When using the security functions of the MFP, in particular, processing using a security function, or its success or failure from the results of the security processing, etc., is recorded. It can be referred to or summarized at the time of the regular audit of the operations regarding the security functions of the MFP.

3.7.26 Communication/network - Network service provision

The MFP stands by for requests from the network to provide services to the user terminals and other systems. When a request arrives from the external user terminal or another system, the MFP responds by performing some processing for this request. Such responses, processing, and responding to the other systems, are referred to as network services.

Because network services are provided by the server running on the MFP, they are also referred to as server functions. The server functions of the MFP include the SMB server and HTTP server that provide shared service functions of the MFP, the FTP server that provides file sharing services, and the SMTP server that provides transfer and delivery of the scanned or faxed image data.

In addition, there are some network service functions available for maintenance and management inside the MFP. For administration usage, the SNMP server responds and changes the running status inside the MFP.

3.7.27 Communication/network - Remote management/control

It is a function that allows administrators to configure the settings and perform configuration management of the MFP remotely. Maintenance pages or management pages provided on the web server in the MFP are used by opening from the administrator terminal.

3.7.28 Communication/network - Communications control

It is a function that allows control of communications over an IP network and procedural control of receiving and sending of faxes. IP network rather controls Ethernet and IPv4/IPv6 in comparison to “Network service.”

4. Data Flow when Using the MFP

The data flow when using the MFP is specified as the following configuration diagram. Data is categorized as content data such as documents and images, and control data such as instructions and controls. Content data is indicated by solid lines, and control data by dotted lines in the diagrams.

Since it is a common process to record all the operations regarding activation records, only data flow for reading is identified for the writing processing of activation records:

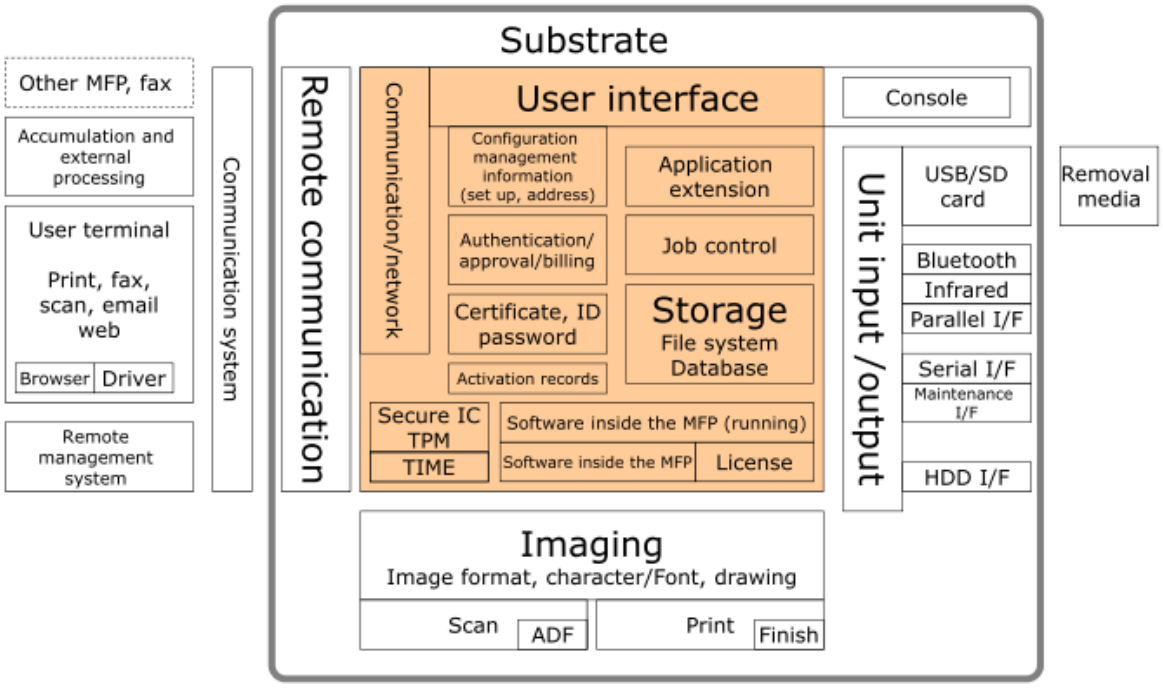


Figure 4-1 Configuration diagram of data flow when using the MFP

4.1 Printing

Figure 4-2 Data flow for printing instructions such as how to print and the images for printing are sent to the MFP from the user terminal. The print reception function within the communication and network module accepts the connection on the MFP. Upon receipt of the connection, a protected communications path is established, and it saves the job accepted in the file system after the authentication of users. For authentication, either the authentication data inside the MFP or the external authentication server of the remote management system is used.

After informing the job control of the stored job data, the job control sends a print instruction to the imaging unit while making adjustments with the other jobs, and prints them out.

When the MFP creates the session information of the user terminal after the authentication of the user terminal, the session information of the user terminal shall be deleted upon receiving the job:

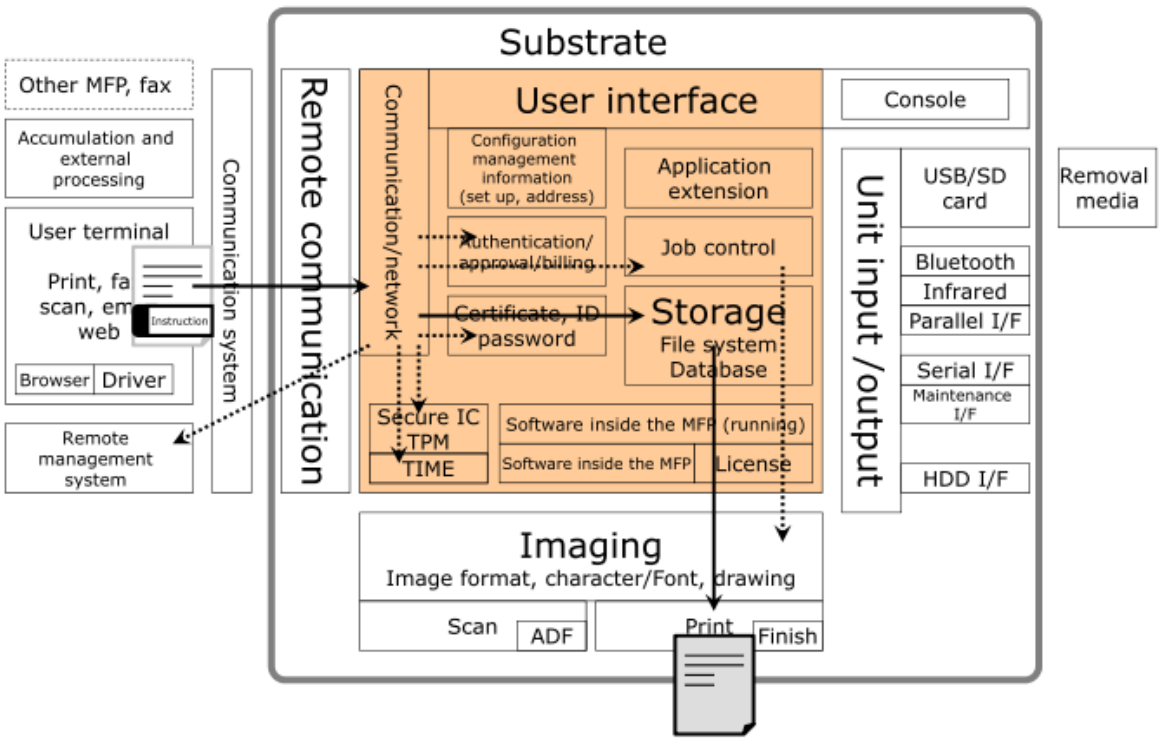


Figure 4-2 Data flow for printing

4.2 Load distribution printing

Figure 4-3 below shows the data flow for load distribution printing. The figure shows the data flow from immediately after receiving the job data.

The job control reviews the configuration management information from the instructions included in the job data, and specifies the MFP to give instruction for printing among external MFPs. The job control gives printing instructions to the print client function of the browser in the application extension with new instruction data, such as the number of copies and address of the client that have been specified.

The print client function establishes a protected communications path with another MFP using a communication and network function. At this time, it uses certificate, password, secure IC, and time inside the MFP. After the protected communications path has been established, the print client forwards the stored job data with the specified number of copies to the other MFP.

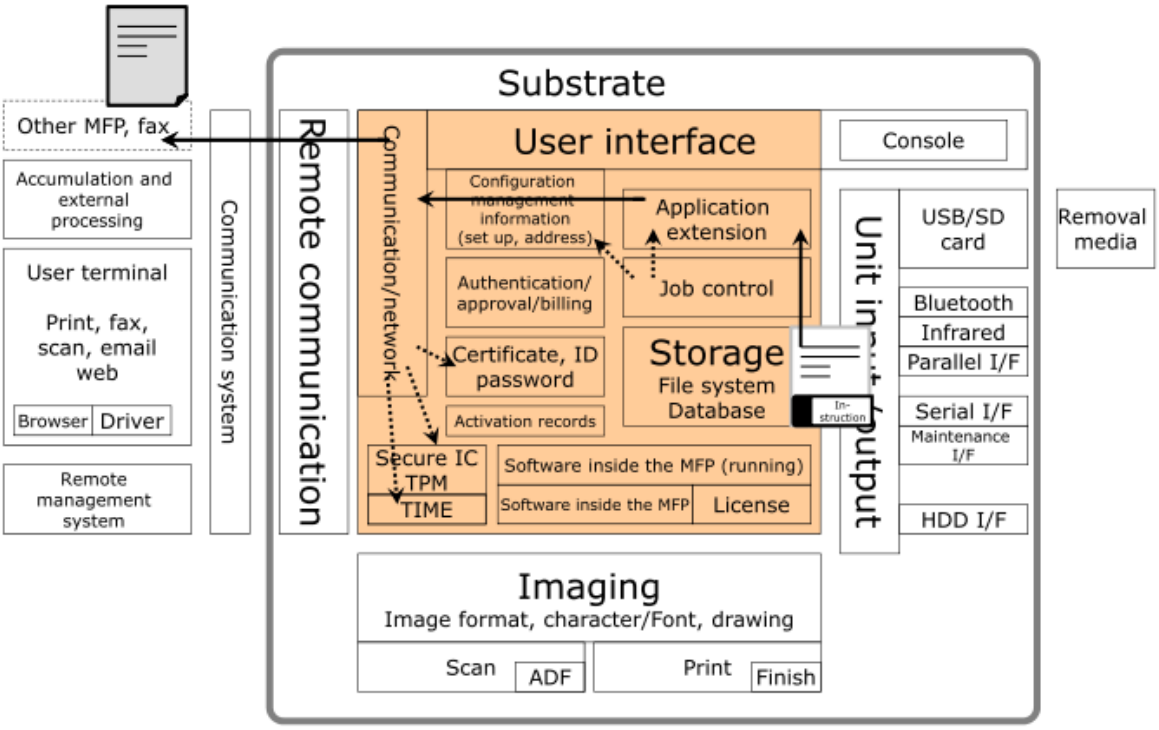


Figure 4-3 Data flow for load distribution printing

4.3 Scanning to X, faxing

Figure 4-4 below is a diagram showing the data flow for "scanning to X" to deliver scan results to something. "X" here refers to files (storage on the MFP), FTP, and email, etc., which are destinations and delivery methods of the scan results. Faxing is also included.

In front of the MFP, a user gives a job instruction to the MFP using the console. Then, the user scans from the console and gives an instruction as to where to deliver the scan results. If authentication is required to use the scanner, the user interface uses either the console or the IC card authentication device and the biometrics device, which is connected to the serial interface of the MFP, to authenticate as a user.

The user specifies the destination and the scanning method. The destination can be selected from the address book of the MFP. In some cases, shared address book on the remote management server may be used via remote communication. The user puts the original paper on the scanner table by this time.

As specified above, the identification information of the user, the destination, and the scan method, are all delivered to the job control as an instruction. The job control provides a control instruction to the imaging, and scan processing is performed in the scanning unit. As the result of the scan processing, the created file is passed from the imaging to the storage.

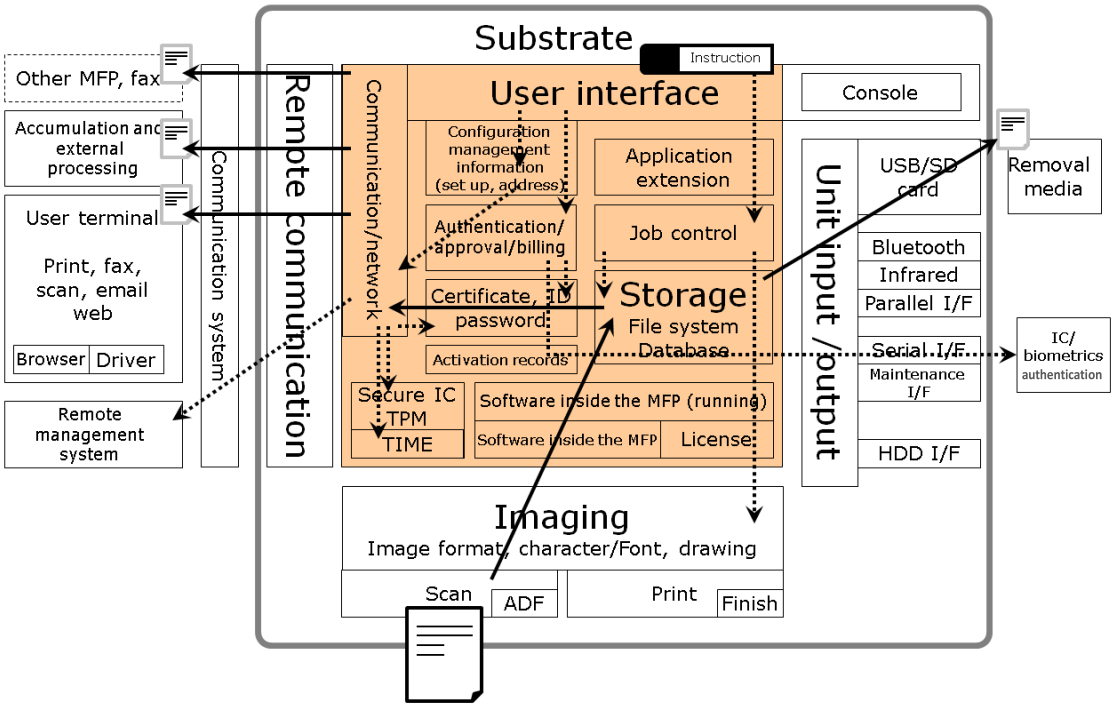


Figure 4-4 Scanning to X, faxing data flow

The file is delivered to the specified destination from the storage in accordance with an instruction given by the job control. The following is a list of the destinations:

1) Delivery to the other MFP and the fax: upper left in the figure
2) Server-delivery to the accumulation and external processing: the second from the upper left in the figure
3) Server-delivery to the user terminal: the third from the upper left in the figure
4) Delivery to the removable media: upper right in the figure

Among the above-mentioned destinations except for the removable media, mutual authentication, use of certificates, ID, and password, is conducted in order to establish a communications path protected by using secure IC and time.

Among the above-mentioned destinations, the accumulation and external processing may mostly require some sort of authentication processing. In such cases, either the authentication data inside the MFP or the external authentication server of the remote management system can be used.

The processing is completed when the delivery is completed for all the specified destinations.

The MFP automatically deletes the session information that was created for the “certificate, ID, password” when logout is executed by the user after the specified job is completed, or when a certain time has passed without any operations on the MFP.

4.4 Receiving fax

Figure 4-5 below shows the data flow for receiving fax. This flow refers to a procedure from the point of receiving a fax to the point where the information is stored in the storage. The authentication printing with a user authentication is specified in the printing procedure.

Either the original papers are read or fax images are sent to another MFP or fax from a computer at the "other MFP, fax" on the top left of the figure, and then from the "other MFP, fax," the fax images are received using the fax reception function of the "communication and network." The fax reception function includes PSTN fax, mail fax, and the SIP fax. In case of mail fax, certificates, secure IC/TPM, and time, being used to establish a protected communications path. In case of SIP fax, it does not dynamically establish a protected communications path in general, but ensures security by isolating or closing the "communication system."

Received fax images are then stored in the storage, and the reception result is passed on to the job control. The job control verifies the box distribution conditions by the fax numbers or the destination numbers, and specifies new destinations either to deliver to the confidential boxes or servers, or to print on the paper.

The print processing after this is the same as the data flow in "Printing," and the processing other than printing after this is the same as the data flow in "Scanning to X," after storing the images in the storage.

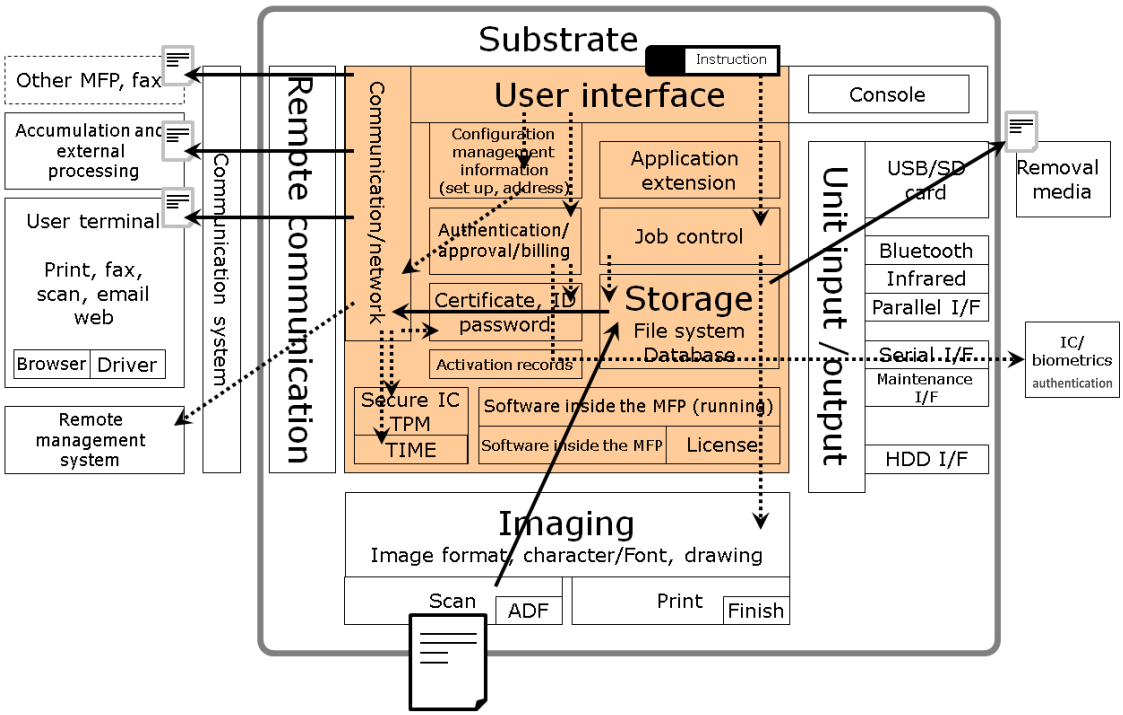


Figure 4-5 Data flow for receiving fax

4.5 Copying

Figure 4-6 below is the data flow for copying. A user gives a copying instruction from the console. A user authentication is performed as necessary. Either the authentication data inside the MFP or the external authentication server of the remote management system is used for authentication using password, IC card, or biometrics. When performing a user authentication with the authentication server external to the MFP, the authentication request for the user who wants to copy shall be made via "communication and network" to the authentication server on the "remote management system."

The user specifies the processing condition for copying using the console. When specifying settings values established beforehand or load distribution of the printing, the information that users or administrators have set up among the settings configuration information shall be used as a reference.

By this time, the user has placed the original papers on the scanner table or ADF.

When an instruction for copying by the user is given, the instruction is forwarded to the job control, and the copying will begin. The job control sends the instruction for copying to the imaging. The original papers are scanned and stored in the storage. Stored images then are forwarded to the printer to print. Images can be stored by creating files on the hard disk or in memory (temporary memory, DRAM).

User logs out from the console upon completion of the specified job, or the MFP automatically logs out after a certain time has passed without any operation, and the session information in the "certificate, ID, password" of the MFP is deleted.

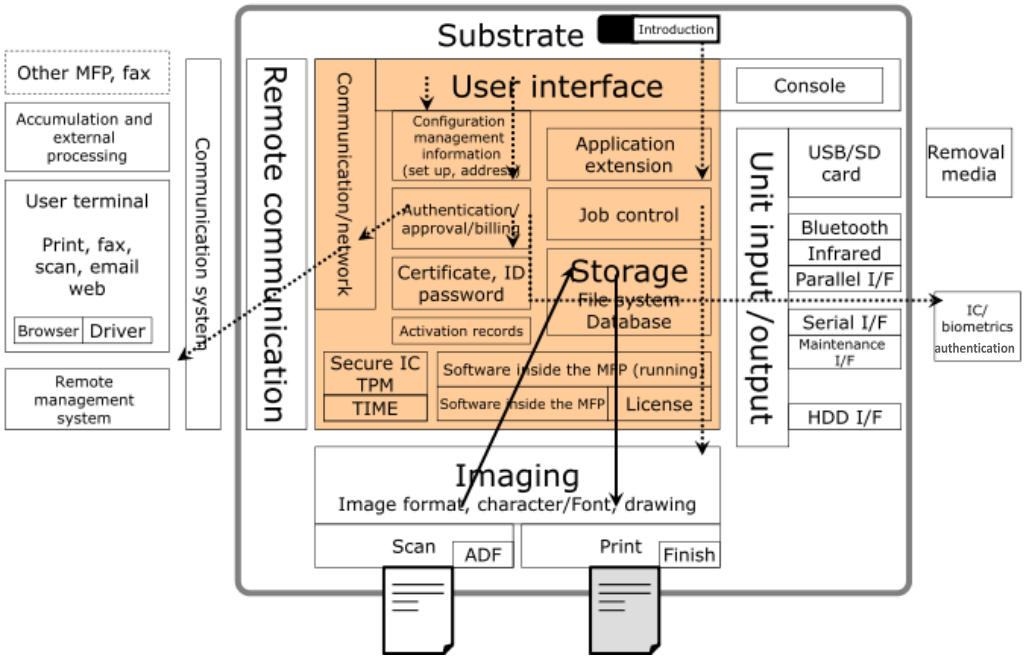


Figure 4-6 Data flow for copying

4.6 Setting the configuration management information and acquisition (console)

Figure 4-7 below shows the data flow when setting the configuration management information and acquisition of the MFP. The configuration management information of the main unit of the MFP includes "certificate, ID, password," and the operations of "secure IC/TPM" as well as changes to "time." The procedure for giving instructions from the MFP console is shown in this figure.

MFP administrators give instructions for changing the configuration management information from the console. Therefore, an authentication procedure for administrators shall be performed. The user interface gives an instruction to the "authentication/ approval/billing" for authentication processing for administrators. IC card and biometrics shall be performed as necessary. In some cases, IC card and biometrics may require authentication by the authentication server in the "remote management system."

When an administrator authentication is acquired, the setup menu of the configuration management information is displayed on the user interface, and the change, overwriting, addition, and deletion of the contents of "configuration management information," "certificate, ID, password," "secure IC/TPM," and "time," are displayed and retrieved. For secure IC/TPM, important and confidential information, such as private key, cannot be retrieved, but the names and identification names of the private key are displayed.

Administrators perform the logout procedure upon completion of the job, and the session information created in the "certificate, ID, password" of the MFP is deleted.

Administrators do not operate software or licensing, since maintenance personnel change them.

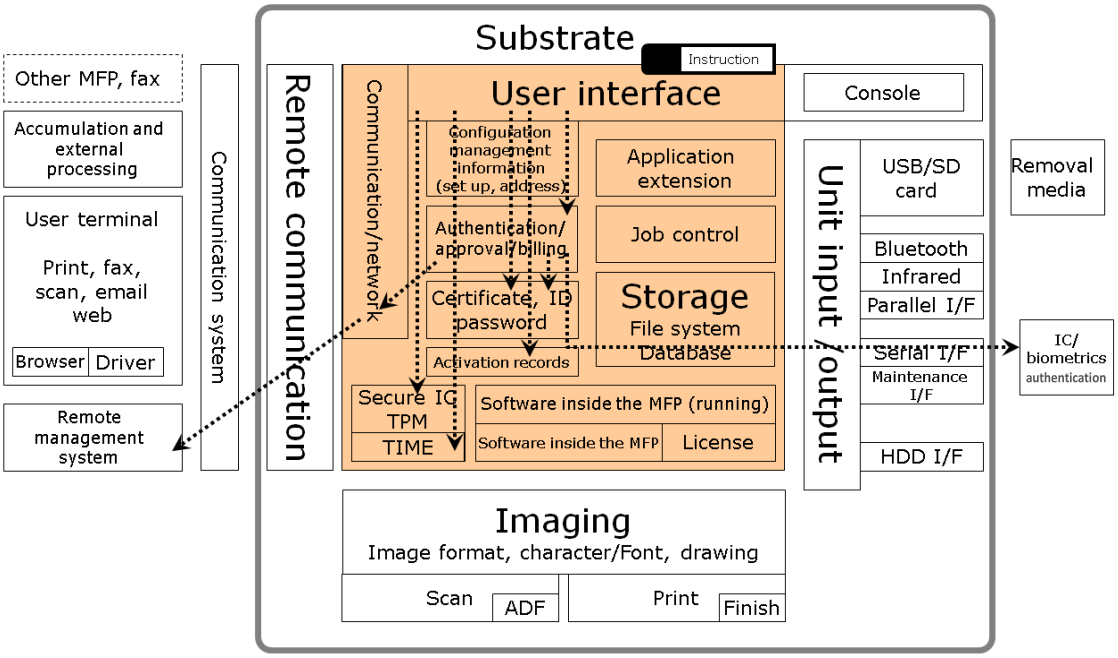


Figure 4-7 Data flow for setting the configuration management information and acquisition

4.7 Setting the configuration management information and acquisition via remote communication

Figure 4-8 below shows the data flow when setting the configuration management information and acquisition of the MFP via remote communication.

Administrators establish a communications path protected by SSL or SSH in the management servers of "communication and network" of the MFP from administrator terminals in the remote management system, and then log in. "Certificate, ID, password" is used for establishing a protected communications path, and for some cases, "secure IC/TPM" and "time" are additionally used. Then, an authentication of administrators who have a connection request from a distance shall be performed from the MFP to the authentication server of the remote management system.

After a protected communications path is established between the MFP and the administrator terminal, administrators can change multiple data inside the MFP by manipulating the setup page or a command line provided by the user interface upon completion of the authentication of administrators. For the "configuration management information," settings values are added, changed, or deleted. The "certificate, ID, password" are also added, changed or deleted. For the "Secure IC/TPM," private key and its attribute information are added or deleted. For the "time," it is only changed. Common operations include reading of the data or values, although the private key of the "secure IC/TPM" cannot be read.

Administrators perform the logout procedure upon completion of the job, and the session information created in the "certificate, ID, password" of the MFP is deleted.

Administrators do not operate software or licensing, since maintenance personnel change them.

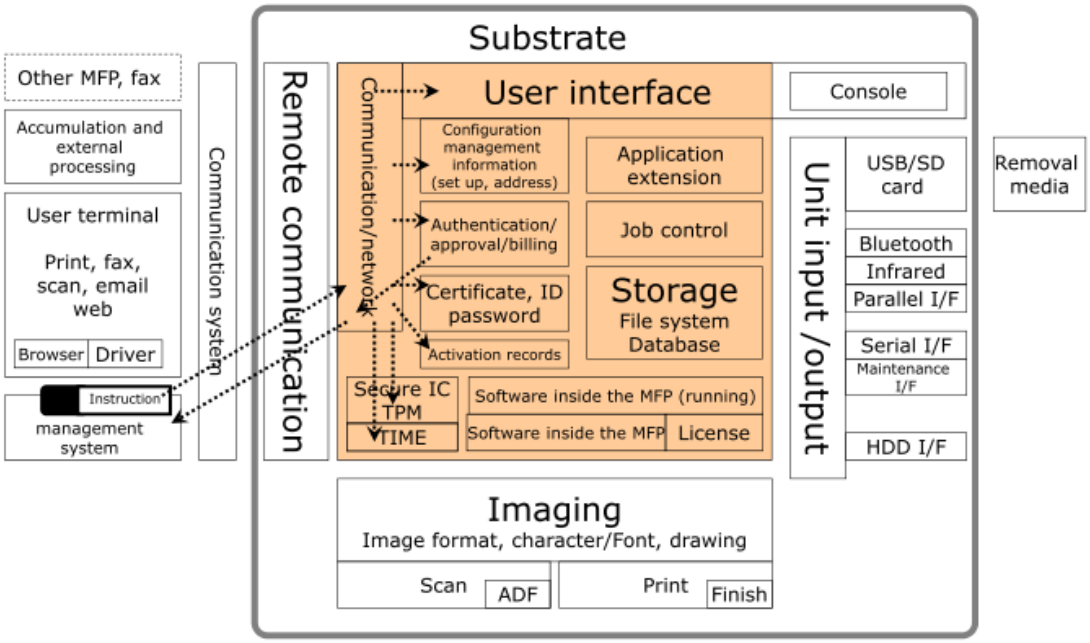


Figure 4-8 Data flow for setting the configuration management information and acquisition via remote communication

4.8 Maintenance, parts replacement, billing, and diagnosis

Figure 4-9 below shows the data flow for maintenance, parts replacement, billing, and diagnosis.

Maintenance personnel of the MFP perform an authentication for maintenance personnel using the console. An authentication procedure outside of the MFP is omitted because it is the same as other data flows. It shows only the data flow of the authentication for maintenance personnel carried out inside the MFP. Maintenance personnel perform the authentication by entering ID and password from the keyboard, using the console of the MFP. For some cases, the maintenance terminal is connected to the maintenance interface to operate from the command line or simple menu on the maintenance terminal. For the maintenance interface, its existence is sometimes unknown, or even if it exists, it may not require authentication.

After the authentication for maintenance personnel is completed, the menu for the maintenance personnel is displayed to select necessary processing from the console.

A diagnostic process is performed usually at times of maintenance work, such as inspection, and parts replacement. During the diagnostic process, individual diagnostic functions of hardware in the figure are performed, and results are retrieved, and there is also a consistency inspection for data and files. The diagnostic functions inside the MFP are described in the operation manual for maintenance. Although it is not confirmed because it is not open to the public, it is believed that diagnosable items and targets vary depending on the models and MFP vendors.

Maintenance personnel perform the logout from the console upon completion of the job, and the session information created in the "certificate, ID, password" of the MFP is deleted.

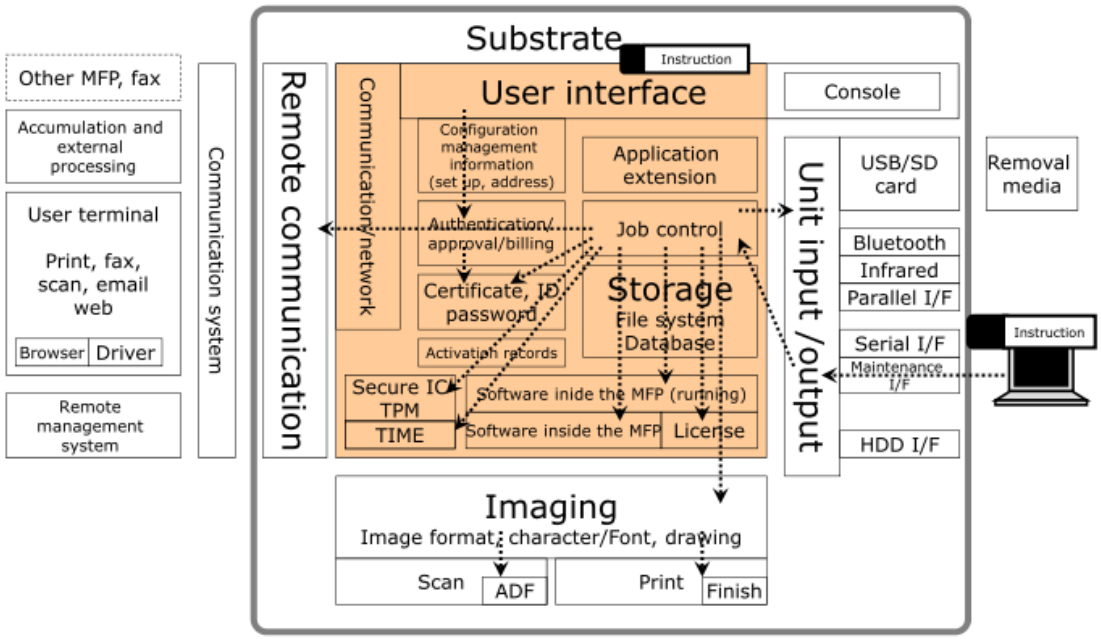


Figure 4-9 Data flow for maintenance, parts replacement, billing, and diagnosis

5. Assets to be protected by the MFP

5.1 Primary assets in an environment of MFP use

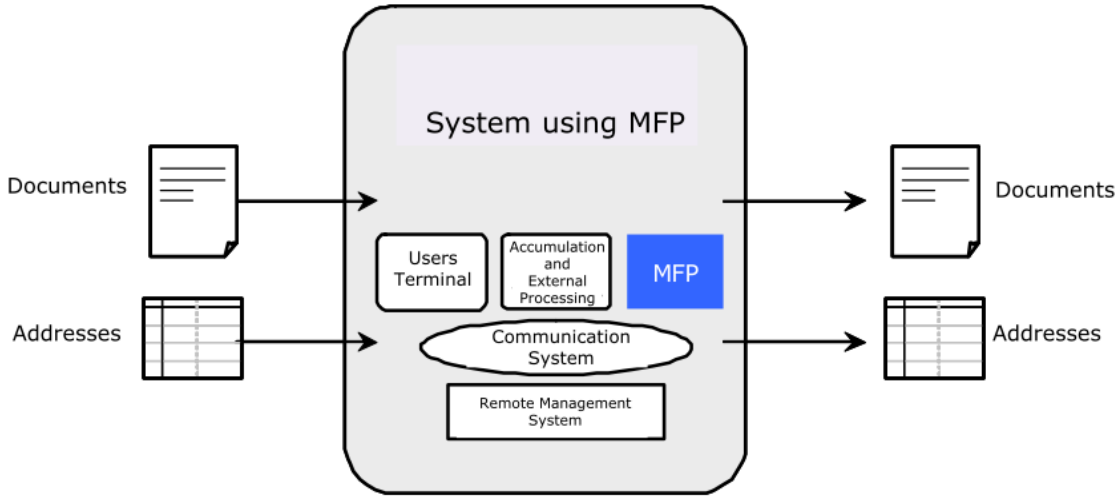


Figure 5-1 Data flow when using MFP

As seen from users, the direct purpose of using the MFP is the storage and distribution of documents. When users perform the storage and distribution of documents, information assets to be protected directly are positioned as "primary assets." Figure 5-1 above shows the concept of the MFP processing addresses and documents, which are the primary assets. Documents are the information to be distributed and saved. Addresses are the information that represents the destinations to distribute to.

Primary assets are insubstantial because they are information assets. Substantial information assets vary case by case in concrete terms. In this manner, when the MFP is used as one of the information systems, concrete information assets that are necessary to protect the primary assets are positioned as "secondary assets." For example, documents in a paper medium mean original papers or prints. Data describing the digitized images and image contents on the pages is handled as bit strings in memory and files called job data on the MFP. Addresses and the destination addresses are stored as part of the control instructions. Information for authentication and security is also considered a secondary asset that is necessary to protect the primary assets.

Primary assets and secondary assets are defined as "protected assets" in Chapter 7 and subsequent chapters.

5.2 Secondary assets as targets to be protected to use the MFP

Table 5-1 below shows secondary assets associated with the usage environment of the MFP. They are divided into four categories.

"Main unit of the MFP" refers to devices and software inside the MFP. Removable media such as USB memory and SD card are not in the main unit of the MFP, but are categorized as the "Main unit of the MFP" because it is used closely with the MFP. The MFP can be operated with these devices and software together.

"Run-time data" refers to information assets to be exchanged during the copying and printing processes.

"Other systems" refers to external hosts and devices that provide services such as management and authentication from the outside of the MFP for the MFP to be operated. Because the vulnerability of the main unit of the MFP is the major subject in this research, details of the other systems are not studied, but only the external interfaces of other systems are focused on and analyzed.

"Activation results information" refers to original papers, prints, files, and records obtained after processing.

Table 5-1 Secondary assets as targets to be protected to use the MFP

Category	Secondary assets
Main unit of the MFP	Main unit (Hardware)
	Software inside the MFP
	Usage license, maintenance license
	Removal media
Run-time data	Job data (spool, image, destination, control)
	Management/configuration information
	Digital certificate, ID, password, Session information
	Accurate time

Category	Secondary assets
Other systems	Communication system (Switch, DHCP, DNS, NTP)
	Remote management system (Authentication, configuration management, monitoring, maintenance)
	General user terminal
	Accumulation and external processing (spooler, shared folder, email, Other business systems)
Activation results information	Original papers, prints
	Shared files in the MFP
	Usage history, audit record
	Billing information for MFP use

The next chapter describes detailed analysis of threats to these secondary assets. An overview of each secondary asset and main points that are required from security perspectives, are summarized as a reference as follows:

5.3 Main unit of the MFP

5.3.1 Main unit (Hardware)

It refers to the main device of the MFP. It is divided into several units as described in "3.6 Hardware inside the MFP." It is necessary that the correct main device is mounted and is wired correctly.

5.3.2 Software inside the MFP

The software to operate the MFP. It is mounted by dividing it into several applications and modules as described in "3.7 Software inside the MFP."

Software can be added or updated relatively easily, but the correct software is required inside the MFP. Unauthorized software shall be eliminated.

5.3.3 Usage license, maintenance license

While users are using the MFP, the user rights of the installed software and the user rights of maintenance services are issued by MFP vendors, distributors, or maintenance businesses, as usage license and maintenance license, and are registered on the MFP, respectively.

There is a variety of terms and conditions of license, but the analysis is performed on the assumption that the agreement period of license is usually limited, and the license becomes invalid when the agreement period expires, and the appropriate functions with the license will be terminated. On the other hand, unscheduled functions or services may operate if a non-contracted license is registered.

5.3.4 Removable media

It refers to media that can be easily inserted and removed, such as SD memory cards and USB flash memory. They are not the main unit of the MFP, but are considered as main unit of the MFP, because they are hardware that can be mounted on the main unit of the MFP.

Some removable media are used to exchange documents by users, and some are used to perform configuration of the management information and software of the MFP by maintenance personnel. Although the slots of removable media for users and the slots of removable media for maintenance personnel are distinguished with different usages, it is pointed out in the list of threats and vulnerabilities in each case when they have to be handled differently.

5.4 Run-time data

5.4.1 Job data (spool, image, destination, control)

The job data is a record of image data, such as printing, faxing, copying, and delivery, as well as control information.

Image data includes digitized images and drawing instructions to reproduce the images of the display area of prints and original papers.

The control information includes forwarding addresses or destinations, its forwarding procedure, output destinations of prints, and finish conditions. Finish conditions include image processing methods such as positioning of the images in prints, number of copies, and output tray. The processing in accordance with the finish conditions is performed with a device called a finisher.

The control information may include authentication information. For example, in the case of a simple authentication printing using only the user ID set on the MFP without using an authentication server when printing with a user authentication, user IDs that are input from general user terminals are written in the job data, and the job data may be stored in the spool of each user on the MFP.

5.4.2 Management/configuration information

Information for setting and registering on the MFP to operate the MFP under the prescribed conditions, or configuration information stored on the MFP.

For example, there are strings of necessary addresses, path names, numbers, and call names to cooperate with other systems, while the MFP operates the security functions,

such as authentication, to provide the prescribed services and to ensure the necessary security.

The management/configuration information includes information for the MFP to terminate a certain function, as well as information for usage restrictions of specific functions by specific users, etc.

5.4.3 Digital certificate, ID, password, session information

It is digital information used to respond to a request for authentication. A digital certificate has a public key that can validate a private key. The private key is stored in the storage device, such as secure IC and TPM, to match it with the secure IC to perform the calculation process during authentication. There is no need for the public key to be kept confidential. ID and password shall be stored in the non-volatile memory that can be referred to at the MFP startup, or in the storage inside the MFP, for the matching process during the authentication process.

The session information is like a token for giving permission per usage session of other systems or for users who use services. It includes the cookie information of the web browser, session ID in the URLs, and session ID in the request data in the HTTP POST requests.

5.4.4 Accurate time

Accurate time is needed to record the history of sending and receiving fax. When recording the history of operations, the time at that time is also recorded as a record. The time in the history information of operations shall be accurate to check the records of other MFPs or other systems.

The time also is the basic information used to perform cryptographic communication, signature, and verification. It is important for the time of self-signed certificates as well.

For the functions of authentication, approval, and billing, in order to manage the authenticated time and the duration that can continue the authorization, synchronized accurate time is needed between the MFP and the authentication server as well as the server that provides the single sign-on function.

For the software licensing, accurate time is also needed to compare when the license terms are specified.

5.5 Other systems

5.5.1 Communication system (Switch, DHCP, DNS, NTP)

A server that provides basic information for the network and communication devices to connect to the other systems that perform remote communication with the main unit of the MFP.

Communication devices include Ethernet switches, IP routers, and wireless LAN access points, as well as the wiring for such devices.

Servers that provide basic information about the network include DHCP server, DNS server, and NTP server. DHCP server performs automatic assignment of IP addresses, as well as the distribution of IP addresses of router and DNS. The DNS server responds to search requests for IP addresses among host names, and the search reverse to that. In order

to synchronize the time between the hosts in the systems and multiple MFPs, the NTP server responds with the accurate current time.

5.5.2 Remote management system (Authentication, configuration management, monitoring, maintenance)

Remote management system includes authentication server, configuration management server, monitoring server, and maintenance terminal, etc. Management applications on the terminal for administrators used to change settings of the MFP and the web server on the MFP are part of the remote management system.

The authentication server holds user IDs, passwords, or certificate information to respond to requests for authentication of users from other hosts including the MFP. The configuration management server has functions by which administrators can configure multiple MFPs collectively, etc. The monitoring server has a function to report abnormalities to administrators or to other systems by reviewing the operating status of one or more MFPs on a regular basis.

The maintenance terminal performs diagnosis of the MFP and installation of additional software or licensing when the maintenance of the MFP is required. For such maintenance work, the maintenance server may perform processing regularly instead of terminals.

5.5.3 General user terminal

A terminal that is used for services for MFP users, such as printing, faxing, scanning, and retrieving files stored temporarily or for a long time on the MFP. The user terminal receives faxes by retrieving files from the MFP. Copying is not performed from the user terminal.

These services for MFP users are never used by maintenance personnel. It is intended to run as a user terminal when used for testing. The remote management system includes MFP configuration as well as change of the configuration management information, such as address book, from the user terminal.

On user terminals, in general, driver software compatible with a specific model of the MFP is additionally installed. For some driver software, ID and password that are required to instruct the MFP to print and retrieve scanned images may be set up. When using mail fax, email address and client certificate of the user may be specified.

5.5.4 Accumulation and external processing (Spooler, shared folder, email, other business systems)

Being located outside the MFP, it stores and delivers documents. It usually operates as a server without direct manipulation by people. It is a part of the information system needed to use the MFP, and includes spool server for jobs, shared folder, mail server, and web server for business systems. The spool server is a server to temporarily keep a print job on the MFP, and has an authentication function for users, a distribution function of job data for the MFP, and the load distribution processing function. Shared folder is a service used by multiple users to share information on the network disks in which digital files are stored. The mail server is used to deliver mail fax and email, and consists of a server sending and receiving emails (SMTP), an email forwarding server (SMTP), and a mailbox server that provides email messages to the mail box (POP3, IMAP4).

Sometimes, email forwarding servers and mailbox servers may be located outside of the organizations that use the MFP. MFPs that are the destinations of fax may be located in other organizations. It is assumed that non-disclosure agreements shall be concluded

between those organizations to protect the confidentiality exchanged with each other. As for vulnerabilities of the MFP, it is regarded that vulnerabilities can be found in either organization, regardless of differences in MFP vendors or MFP models to be used.

5.6 Activation results information

5.6.1 Original papers, prints

Original papers refer to papers to be read when copying or scanning. Prints refer to papers output by the MFP when copying, printing, or faxing. Contents in the documents are included.

5.6.2 Shared files in the MFP

Shared files inside the MFP are digital files that are shared in the MFP, including the images of documents. Some may contain additional control information, such as destinations, PDF, and job data. Shared files can be viewed and updated by users of the external terminals of the MFP.

5.6.3 Usage history, audit records

Information on an MFP; for example, which user has done what and when, what request is made by whom, and what is the result. It may include addresses of the hosts or servers, as well as authentication ID when processing was performed.

The usage history and audit records are sometimes recorded inside the MFP, and other times recorded outside the MFP. In general, the access control is set so that the audit records can be accessed only by administrators. Administrators periodically review audit records to make sure that there are no security breaches or unauthorized access, and perform early detection of incidents.

5.6.4 Billing information for MFP use

It includes information about the number of prints and copies made using the MFP. This information is given to the MFP vendors, etc., automatically or manually by the users, and it is used for billing.

6. Vulnerabilities assumed from threats

In this chapter, vulnerabilities that are considered to be the causes of the threats in the usage environment for the MFP are listed, respectively.

6.1 Extractions of the threats

In this chapter, the requirements for information security are categorized into the following seven types in Figure 6-1 to identify the threats comprehensively.

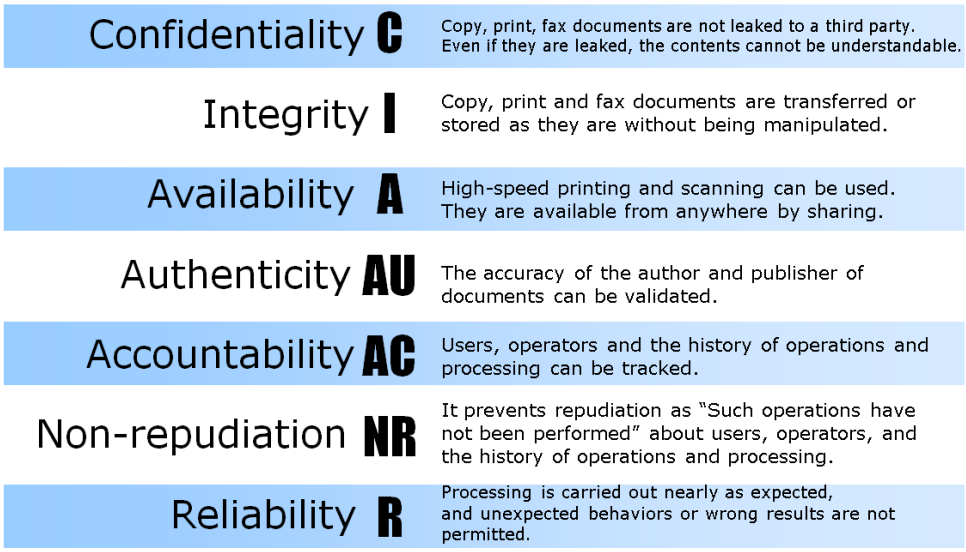


Figure 6-1 Requirements for information security - Seven types

In this chapter, threats are identified by considering the hypothetical breach of security against 16 types of secondary assets specified in Chapter 5. These identified threats are listed in the column, "T. Threat to these secondary assets," of the table in "6.3 Main unit (Hardware)." These threats are further illustrated in "M. Examples of attack methods or incidents that realize these threats" that the feasibility of the attack methods or operation errors can be expected on a certain level at this point. The vulnerabilities to be considered as causes of the incidents are listed in "V. vulnerabilities that may cause the examples of attack methods or incidents."

The vulnerabilities listed in this chapter do not distinguish between the necessary attack potentials for attacks and opportunities for attacks. Users should examine the items to consider in accordance with the security policy of the office where the MFP is used, or with protected assets handled by the MFP, and make a decision if measures must be taken or not.

6.2 Those who should take measures against threats

The vulnerabilities listed in this chapter point out those who should take measures against such threats. They fall into two categories: users and developers. "Users" refers to companies that purchase and actually use the MFP, which include persons responsible for the companies, administrators of the information assets and personal information, regular staff, and temporary staff. On the other hand, "developers" are in a position to incorporate

functional security measures, and “developers” is a collective term for those who have responsibilities in design, development, functional testing related to security, and delivery, including management, in MFP vendors, and for those who are maintenance personnel, etc., of the maintenance side after products are delivered.

Those who should take measures against such threats are checked per vulnerability listed. If the security function that the developer should implement is not implemented, users will take measures for vulnerabilities they encounter during operations. On the other hand, the prevention of defect and termination of the MFP due to its operation by users in a poor environment may be supported by developers with such functions as a power-off protection function. However, those who should take measures are selected in a general sense in this chapter. Items with diagonal lines in the column of those who should take measures mean items as reactions by the normal functions of the MFP or related applications, which neither users nor developers can deal with in general.

6.3 Main unit (Hardware)

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- Assets are wiretapped by direct connection to the terminals on the main unit of the MFP or during wiring. Or, they are wiretapped by giving the electrical impact on the main unit of the MFP.	- Bus on the substrates, debug terminals, module bus terminals, and connection terminals on the main unit of the MFP, are electrically connected to wiretap the communication data on the terminals or on the bus.	- Vulnerability that the MFP is in a state of being physically operable by attackers - Vulnerability that connection methods or communication methods can be easily predicted because the interfaces between the main unit of the MFP are standard interfaces - Vulnerability that the communication data on the interfaces between the units of the main unit of the MFP is not protected	✓	 ✓ ✓
		- Immediately after turning on or off the power switch, an attacker operates the MFP in a privileged state without authentication, and turns off the protection function of the MFP by manipulating a specific keyboard or sending a break signal from a serial port.	- Vulnerability that the function module stops or defects from the electrical effects - Vulnerability that the MFP can be operated in a privileged state if a hardware interrupt is invoked or specified keys are manipulated during startup after turning on the power or shutting down the processing after the shutdown command is given		✓ ✓
		- An attacker impersonates maintenance personnel to retrieve the board, including the DRAM, on the substrate of the MFP, quickly cool it down, and read the data inside the DRAM, so that a cryptographic key that remains on the DRAM is leaked.	- Vulnerability that the MFP is in a state of being physically operable by attackers - Vulnerability that the cryptographic key on the DRAM is not protected	✓	 ✓
		- An attacker easily obtains a copy of the software on the MFP by retrieving the non-volatile memory (FlashROM, etc.) of the substrate or a HDD.	- Vulnerability that the MFP is in a state of being physically operable by attackers - Vulnerability that the stored software on the substrate is not protected	✓	 ✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
2. Integrity	- Part or all of the main unit of the MFP, or wiring, is changed.	- An attacker changes the HDD of the main unit of the MFP to obtain unprotected confidential documents, unprotected address books, unprotected certificates, IDs, and passwords, in the HDD. [Changing the main unit]	- Vulnerability that the MFP is in a state of being physically operable by attackers (Vulnerability that a third party can directly access the devices and the terminals in the main unit of the MFP to add or change devices and parts of the main MFP) - Vulnerability that the stored data in the storage is not protected	✓	
		- An attacker installs an additional scanner in the paper discharge port of the printer or inside the ADF, to obtain confidential documents and print results by changing with an additional scanner or flash memory. [Changing the main unit]			✓
		- An attacker rewrites the setup and configuration management information for the MFP by changing non-volatile memory on the substrate (EEPROM and NVRAM, etc.). [Changing devices]	- Vulnerability that the MFP is in a state of being physically operable by attackers - Vulnerability that the non-volatile memory can be easily identified and changed	✓	✓
3. Availability	- Part or all of the main unit is stolen or destroyed, and the MFP is disabled. - Either power cable or communication wire is pulled off or removed, and the MFP is disabled. - The MFP does not start because of the great fluctuation of the power voltage, or the MFP stops in the middle of the operations.	- The MFP is disabled due to theft or destruction of the hardware module for encryption or temporary memory for execution inside the main unit of the MFP.	- Vulnerability that the MFP is in a state of being physically operable by attackers (Vulnerability that a third party can directly access the devices and the terminals in the main unit of the MFP to take out some devices or parts in the MFP)	✓	
		- Either power cable for the main unit of the MFP or the scanner is stolen, and the MFP is disabled.			
		- The operation of the MFP is stopped because of the electrical load by directly connecting or using electromagnetic waves, to the power system or signal switching system of some devices in the main unit of the MFP.	- Vulnerability that the MFP is in a state of being physically operable, or in a condition that the unauthorized devices can be installed nearby, by attackers - Vulnerability that the function module stops or defects from the electrical effects - Vulnerability in which there is a defect of the hardware module due to electromagnetic waves from the outside	✓	✓ ✓
4. Authenticity	- Addition or removal of the devices is unknown because it is unable to verify whether the devices mounted on the main unit of the MFP is correct.	- An attacker obtains confidential documents and some addresses by installing a fake HDD unit on the main unit of the MFP, allowing it to record the job data or the files of confidential documents.	- Vulnerability in which it cannot be verified whether the device is correct, such as the HDD being directly connected to the main MFP or mounted on the main MFP		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
5. Accountability	- Even if part or all of the main unit is added or removed, the details and causes cannot be verified.	- HDD in the main unit of the MFP is changed by an attacker, but no measures can be taken because when it was done or who did it is unknown.	- Vulnerability in which the addition or removal of an HDD, which is directly connected to the main MFP or mounted on the main unit of the MFP, are not recorded		✓
6. Non-repudiation	- Part or all of the main unit is added or removed by some maintenance personnel, but who specifically did it cannot be proved.	- HDD in the main unit of the MFP is changed by an attacker, but no measures can be taken because a fake ID of the impersonated maintenance personnel is entered into audit records of the maintenance recorded by the MFP.	- Vulnerability that the names, IDs, passwords, and session information of other users are reused in the history, allowing impersonation (unverifiable vulnerability) - Vulnerability in which arbitrary time or arbitrary user IDs can be recorded when recording in the history		✓ ✓
7. Reliability	- Appropriate processing cannot be done due to the mistakes of some devices of the main unit of the MFP or its wiring, lack of parts, or insufficient parts.	- Because the wiring of the main MFP is wrong, encryption module is bypassed, and the data is recorded without cryptographic processing for the HDD, resulting in the leakage of confidential documents that remain in the MFP at the time of its disposal. - Temporary memory shortage can cause incomplete delivery and output for part of the processing, and a problem of the defect would never be recognized. - When digital certificates are created on the MFP, a private key of a digital certificate is saved to an unprotected file on the hard disk in case the secure IC/TPM is not inside the MFP. The private key can be leaked to an attacker who has accessed inside the MFP.	- Mistakes of installation location or wiring in the main unit - Vulnerability in which it cannot be verified or it is not verified whether the configuration of wiring and devices of the main unit of the MFP (resource capacity, processing capacity, and presence of the functions, etc.) is correct or not, when realizing the specific usages, such as “basic operation" or “security mode.”		✓ ✓

6.4 Software inside the MFP

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- Software inside the MFP is leaked. - Information in the running software inside the MFP is leaked.	- Software that is stored on the MFP is wiretapped in the communication system while it is added or upgraded through the remote administrative system, resulted in the leakage of the software.	- Vulnerability due to unprotected communication between the remote administrative systems and the MFP, or that the protection is imperfect		✓
		- An attacker connects to the debug interface inside the MFP, controls the debug interface without authentication, and downloads the software by giving instructions to the file system inside the MFP.	- Vulnerability that debug interfaces with standard command systems, such as GDB and JTAG, are easily guessed - Vulnerability that interfaces, which are used to retrieve MFP, operate to make the MFP available without authentication		✓ ✓
		- Arbitrary code is entered by taking advantage of any vulnerabilities of the software running on the MFP (by obtaining the privileged mode) to retrieve the software by giving instructions to the file systems inside the MFP.	- Vulnerability that arbitrary code is allowed to run on the MFP - Vulnerability that the control by the privileged mode inside the MFP (the administrator mode or an authorization-free state inside the MFP) is taken over.		✓ ✓
		- An attacker obtains the symbol names, the run-time addresses, and the machine language instructions of the software running on the MFP, to develop and sell the attack code for the MFP, by connecting to the debugger interface of the MFP that should not originally remain.	- Vulnerability that the debug interface inside the MFP remains while operating (Vulnerability that the execution state of the software at the machine language level of the MFP is easily controlled or taken over)		✓
		- An attacker easily obtains a copy of the software on the MFP by accessing the non-volatile memory (FlashROM, etc.) of the substrate, and develops and sells the attack code by easily analyzing the contents and behavior of the software to identify vulnerabilities.	- Vulnerability that allows the software on the MFP to be retrieved, and easily analyzed or reverse-engineered		✓
		- By the extension application developed by a third party using the SDK for the MFP, a function to respond to anything without authentications about the contents of the address books inside the MFP is exploited and the contents of the address books are leaked.	- Vulnerability that allows the specific confidential data to be published without authentication, when the extension application developed by a third party using the SDK is performed with the privileged mode inside the MFP		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
2. Integrity	- Some or all of the MFP are changed or added with unauthorized software, and appropriate processing cannot be performed due to the removal or deletion of some software (before and during execution).	- The extension application execution service that should not be used on the MFP operates, and an attacker executes arbitrary commands to obtain confidential documents.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators (in cases of the services that have not been operated are performed by mistake) - Vulnerability that the services inside the MFP that should not be performed are performed, or that the ports that should not be opened are open	✓	✓
		- An attacker adds arbitrary code to obtain confidential documents during the processing of the MFP, because some software inside the MFP are located where even a third party or users can rewrite it.	- Vulnerability of the software inside the MFP that is located where non-maintenance personnel can rewrite it		✓
		- Unauthorized software is injected by tampering with communication data in the communication systems, when the software inside the MFP is added or upgraded through the remote administrative systems.	- Vulnerability due to unprotected communication between the remote administrative systems and the MFP, or that the protection is imperfect		✓
		- An attacker connects to the internal or external debug interfaces inside the MFP or to the software exchange interfaces, controls interfaces without authentication, and gives instructions to the internal file systems or software upgrade functions inside the MFP to add or upgrade the unauthorized software.	- Vulnerability that the interfaces for adding or rewriting software inside the MFP operate to make the MFP available without authentication		✓
		- An attacker stopped the audit record function of the MFP by injecting the unauthorized code to take advantage of the input vulnerability of the LPR. As a result, the operations continued to run without history records, being damaged from the attack without knowing the contents of operation by the attacker since then.	- Vulnerability of the arbitrary code that is allowed to be performed on the MFP using the data entered - Vulnerability that the control of the privileged mode inside the MFP is taken over - Vulnerability of the specific software functions that are executed on the MFP while they are bypassed or stopped		✓ ✓ ✓
		- An attacker inserts a hook into the running software so that only the authentication function in the specific service ports is accepted by the MFP by taking advantage of the input vulnerability of the MFP. Then, the attacker can access the MFP to attack by impersonating another system without authentication, so the business data of the other systems is leaked.			
		- An attacker uses the input vulnerability of the MFP and tampers with the random number generation function of the MFP to return the same random number all the time. The attacker decrypts the encrypted SSL/TLS communication that is processed by the cryptographic processing using the random number generation function, so passwords and confidential documents of the other systems are leaked.			

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
3. Availability	- Some or all of the software inside the MFP is deleted or destroyed, or its operation is stopped by exploiting the vulnerabilities of the software, so the MFP is disabled (before and during execution).	- Broken software is injected by tampering with the communication data in the communication system, when the software inside the MFP is upgraded through the remote administrative system.	- Vulnerability due to unprotected communication between the remote administrative systems and the MFP, or that the protection is imperfect		✓
		- An attacker connects to the internal or external debug interfaces of the MFP, or to the software upgrade interfaces, controls interfaces without authentication, and gives instructions to the internal file systems or the software upgrade function of the MFP to delete the software or rewrite it with the destroyed software.	- Vulnerability that the interfaces for deleting or rewriting software inside the MFP operate to make the MFP available without authentication		✓
		- Arbitrary code is entered by taking advantage of any vulnerabilities of the software running on the MFP (by obtaining the privileged mode) to delete or rewrite the software by giving instructions to the file systems inside the MFP.	- Vulnerability that arbitrary code is allowed to run on the MFP - Vulnerability that the control of the privileged mode inside the MFP is taken over		✓ ✓
		- Some extension applications using the SDK consume a large amount of memory, and the server function of the main unit of the MFP stops.	- Vulnerability that some extension applications using the SDK consume a large amount of resources, such as CPU and memory, and the functions of the main unit of the MFP or extension application stop working		✓
4. Authenticity	- Changing of the software cannot be detected because the software on the MFP or software to be introduced by downloading or by memory, cannot be verified its appropriateness.	- Maintenance personnel mistakenly introduce an older version of the software that disables some functions.	- Vulnerability that the software to be added or upgraded to the MFP cannot be verified as authorized software		✓
		- A third-party developer, who has no authority to distribute software as an extension application for the MFP, creates extension applications that can be installed on the MFP, and installs into a specific MFP.			
5. Accountability	- Even if there is an alteration to the software on the MFP, its cause cannot be specified.	- Maintenance personnel mistakenly introduce an older version of the software and disabled some functions, but which maintenance personnel has performed via which interface is not specified.	- Vulnerability that several maintenance personnel share maintenance authority, and an attacker cannot be identified - Vulnerability of user authentication that is not performed during maintenance - Vulnerability that the maintenance history is not recorded - Vulnerability that the required information, such as the time, user IDs, and operation names of the maintenance, is missing from the maintenance history		✓ ✓ ✓ ✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
6.Non-repudiation	- Some or all of the software on the MFP are changed by some maintenance personnel, but who specifically did it cannot be proved.	- There is a record that the specific maintenance personnel mistakenly introduced an older version of the software, but he/she denies it, and there is no proof.	- Vulnerability that the names, IDs, passwords, and session information of other users are reused, allowing impersonation (unverifiable vulnerability) - Vulnerability that arbitrary time or arbitrary user ID can be recorded when recording in the history and audit information		✓ ✓
7. Reliability	- The MFP is disabled when software to be upgraded or added to the MFP is not located in the right place, wrong code or unauthorized code is mixed, or part of software is missing. - Vulnerability of the software inside the MFP is discovered, and it is actually exploited.	- During the remote upgrading procedure of the software by maintenance personnel, an incomplete form of software is installed by either injecting a packet that indicates the communication ends, or injecting software upgrade completion message to skip the procedure.	- Vulnerability that whether the software to be added or upgraded is installed correctly cannot be verified - Vulnerability that the processing of verifying whether the software is installed correctly can be bypassed or interrupted		✓ ✓
		- An attacker performs an intrusion test or a fuzzing test against the specific MFP to discover vulnerabilities, and attacks the vulnerabilities of the MFP to execute arbitrary code on the MFP.	- Vulnerability that the planning and implementation of the software testing on the MFP are not sufficient (including OS, library and middleware, introduced from outside, or in-house development)		✓
		- If multiple extension applications using the SDK are introduced on the MFP, in which multiple large job data are input, job data is lost due to the race conditions in the acquisition of the memory.	- Vulnerability created by race conditions in the multiple extension applications using the SDK		✓
		- A third party of goodwill discovered vulnerabilities and reported to the MFP vendor, but they neither responded nor were any actions taken, so the person who reported disclosed the vulnerabilities. Then, a malicious attacker developed and sold software for attacks, which causes damages on a large scale, and the compensation for damage has been claimed.	- Artificial vulnerability that there are no plans or measures available after vulnerabilities of the MFP are found		✓
		- An attacker tampers with messages that have the S/MIME signatures on the fax mail by using the vulnerability that the MD5 hash function is prone to collision, and the messages look like having a properly signed digital signature when they are received.	- Vulnerability that the encryption strength of the encryption and hash function is less than required		✓
		- MFP cannot connect to the server with a 1024 bit RSA key of the SSL server certificate with the SSL/TLS protection, because the key processing of 512 bit length RSA cryptography is not supported.			
		- MFP does not support either SSL 3.0 or TLS 1.0.			

6.5 Usage license, maintenance license

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- Usage license permission information of the MFP in the user environment is leaked or exposed. The usage license fee and the maintenance license fee used by a third party are imposed.	- On the console on the MFP, an attacker displays the license information registered with the MFP, takes a note of such license code string, and uses it by entering as license information to other MFP.	- Vulnerability that the license information of the MFP for administrators is viewed by attackers	✓	
		- An attacker accesses the public folders on the MFP via USB or networks, retrieves digital files to be licensed, and uses another MFP by entering and registering.	- Vulnerability that the digital files to be licensed for the MFP are published by mistake on the MFP		✓
		- An attacker retrieves the license information that is registered in the hard disk of the MFP by scanning the HDD directly. In case of being encrypted, the cryptographic key is retrieved by scanning.	- Vulnerability caused by lack of encryption or hashed protection of the license information in the storage of the MFP - Vulnerability that the cryptographic key is not sufficiently protected when license information is encrypted		✓ ✓
2. Integrity	- Part or all of the usage licenses are changed, which causes either the software of the MFP of the licensed users do not operate, or the MFP of the non-licensed users operates.	- A used MFP is sold with another user's license input, and non-licensed users can use the MFP.	- Vulnerability that users do not delete the license information at the time of disposal - Vulnerability of no validity period of the license information - Vulnerability that the specific unique information of the license information, such as model names, serial numbers, and the names of the software, are not verified	✓	 ✓ ✓
3. Availability	- Usage license becomes invalid by changing the time, etc., which disables the MFP	- While the MFP that already obtains the correct license information entered is operating, it stops operating because the incorrect license information is re-entered. (operational mistake or attack)	- Vulnerability that invalid license data is input to the MFP, which disables the MFP - Vulnerability that the wrong time is set up for the MFP, which disables the MFP	✓ ✓	
		- While the MFP that already obtains the correct license information entered is operating, it stops operating one year before the contract period is over, because the time of the MFP is set a year earlier. (operational mistake or attack)			

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
4. Authenticity	- Because it is unknown whether the usage license is correct, non- licensed users can use the MFP using the forged usage licenses.	- An attacker, such as a secondhand goods dealer or reseller, inputs the license information of another company, or inputs forged license information, in order to use the MFP.	- Vulnerability that the license information issued can be used not only for specific models, but other models - Vulnerability that the license information issued is not sufficiently validated inside the MFP, so that the MFP can be operated with the license information created by a third party		✓ ✓
		- Because the license information consists of several digits, it is identified by trial and error by adding the numbers one at a time to find out the license information that can be registered to exploit it.	- Vulnerability that the character string that should be input to the MFP as a license for the MFP, is easily guessed, or created by characters in order		✓
5. Accountability	- Even if the usage license is invalid or forged, its cause cannot be specified.	- A used MFP with the license information of another company is sold, because the changing of such license information is not recorded.	- Vulnerability that the history of changing license is not recorded - Vulnerability that the history logs of the operation for changing license do not include enough information (date, user IDs, access tracks, contents of operations, and results).		✓ ✓
6. Non-repudiation	- Deletion or changing of usage license/maintenance license is conducted by maintenance personnel, but who specifically did it cannot be proved.	- Since the license information changing is recorded when it is done within the organization, either the user ID is rewritten, or the service is terminated by inputting a license that causes the MFP not to operate, by adding the record which indicates operations by other users.	- Vulnerability that the record of the operation for changing license, in which the user IDs are recorded, can be tampered by a third party [vulnerability that logs can be tampered]		✓
7. Reliability	- Depending on the specific license data or specific environment conditions, it is not determined either invalid license data to be valid, or valid license data to be valid.	- An attacker creates license information that causes defect of the validation function for the license information, and inputs it into the MFP, and then non-licensed users can use the MFP, or the attacker can implement arbitrary code.	- Vulnerability that the license validation function is bypassed because of the termination of the license validation function, if there is an unexpected value in the license information - Vulnerability of the license parameters that causes a buffer overflow		✓ ✓

6.6 Removable media (for users, for administrators)

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- Information that has been recorded without protection to the removable media is leaked by the theft of the removable media. - The information that is transferred at the connection point of the slots and the media in the slots of removable media is wiretapped.	- An attacker removes to obtain the media that is left in the slot of removable media. Or, a different user collects it by mistake, which causes the leakage of confidential documents.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	
		- SD card with backed up management/configuration information, including passwords on the MFP, is removed by a person other than administrators because they forgot to remove it, and confidential documents are copied and leaked.	- Vulnerability that the removal of the removable media cannot be easily detected visually or aurally - Vulnerability that the secondary assets, such as management/configuration information or confidential documents that were recorded on the removable media, are not protected by encryption, etc.		✓ ✓
		- Digital files in the removable media have been encrypted, but confidential documents are leaked to attackers because the cryptographic key is one of the common character strings of the medium.	- Vulnerability that digital files in the removable media have been encrypted, but the cryptographic key is easily guessed or is one of the common character strings of the medium	✓	
		- An attacker obtains the removable media that is left in the MFP, and obtains confidential documents remained on the removable media by using a default common password that is used in the encryption function of the removable media.			
		- A probe is mounted on the device of the slot side or contact point between the media and the slot, and is sent from the wiretapping device attached to it, and confidential documents or management/configuration information, including passwords, are leaked to an attacker.	- Vulnerability that the MFP is physically operable by attackers - Vulnerability that transfer data between the media slot and the removable media is not encrypted or is insufficiently protected	✓	 ✓
2. Integrity	- Unprotected information in the removable media is tampered.	- After the media is inserted into the slot of the removable media, an attacker rewrites the original confidential documents in the media, which have no other copies, by removing the removable media that is left in the slot.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators - Vulnerability that there are no functions to protect the document data in a removable media	✓	 ✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
2. Integrity	- Unprotected information in the removable media is tampered.	- After the media is inserted into the slot of the removable media, an attacker rewrites the configuration information in the media in order to input it into the other MFP by removing the removable media that is left in the slot, and then the attacker inputs it into twenty other MFPs.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators - Vulnerability of the configuration information read without authorization - Vulnerability that there are no functions to protect the document data in a removable media	✓	✓ ✓
		- Digital files in the removable media were encrypted, but an attacker rewrote the configuration information because the cryptographic key was one of the common character strings on the medium.	- Vulnerability that digital files in the removable media have been encrypted, but the cryptographic key is easily guessed or is one of the common character strings of the medium	✓	
		- An interventional device is inserted into the device of the slot side or contact point between the media and the slot, and confidential documents and management/configuration information are rewritten.	- Vulnerability that the MFP is physically operable by attackers - Vulnerability that transfer data between the media slot and the removable media is not encrypted or is insufficiently protected.	✓	✓
3. Availability	- The removable media is either stolen or destroyed to block the use of reading and writing, which disables the removable media.	- After the removable media is left with the original data saved on it, it was collected by an attacker or somebody else, which disables the use of the original data.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators - Vulnerability that the removal of the removable media cannot be easily detected visually or aurally	✓	✓
		- The slot of the removable media is destroyed to disable the removable media.	- Vulnerability that the MFP is physically operable by attackers	✓	
4. Authenticity	- Whether the specific removable media is approved by administrators of the organization cannot be confirmed.	- An attacker prepares an SD card to create defects inside the MFP, and intrudes the MFP, causing the leakage of confidential documents.	- Vulnerability that the removable media has neither identification functions nor authentication functions		✓
5. Accountability	- Users cannot be identified from the read/write history of the specific removable media.	- Large quantities of confidential documents are transferred from inside the MFP to the removable media, which may be leaked to an attacker, but which user performed cannot be identified.	- Vulnerability that the usage history of the operation of the removable media is not recorded		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
6. Non-repudiation	- There are no grounds to prove the record of user ID or the time for users in the read/write history of the specific removable media.	- A large number of photo printings had been performed from the SD card, but which user performed could not be identified by the user ID in the record.	- Vulnerability that the user ID is recorded for the operations, but such user ID can be entered with arbitrary character strings by users [vulnerability that logs accept arbitrary user ID]		✓
		- Unauthorized configuration information was entered from a SD card, but which card was entered could not be identified.	- Vulnerability that the user ID is recorded for the operation, but its record can be tampered by a third party [vulnerability that logs may be tampered]		✓
7. Reliability	- For a removable media that is attached to the MFP, part of the directory or the contents of digital files in the media are not readable, or the file names are no longer displayed as the job names.	- Huge files are stored on the SD card, but when reading them onto the MFP, other files cannot be read.	- Vulnerability of abnormal end in the middle of the processing if there is a file larger than a specific size in the removable media		✓
		- If Unicode characters are used for a specific language for the file names of the SD card, they are not displayed as file names, but the operation menu goes back to the initial state.	- Vulnerability that arbitrary code is executed if unexpected characters for file names are written on the removal media		✓

6.7 Job data (Image, destination, control)

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- Job data that is exchanged inside the main unit of the MFP, or between the MFP and other systems, is leaked, and documents and addresses are also leaked.	- An attacker interferes in the USB memory port for general users with another USB hub, and wiretaps the job data to be entered into the MFP.	- Vulnerability that the job data or communications paths sent/received to/on the interfaces between the units inside the MFP are either not protected, or the protection is imperfect		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- Job data that is exchanged inside the main unit of the MFP, or between the MFP and the other systems, is leaked, and documents and addresses are also leaked.	- Job data that is exchanged by the MFP on one of the following routes is wiretapped: bus and terminal inside the MFP, between the MFP and the external USB devices, between the MFP and the external Bluetooth or infrared communication device, between the MFP and devices that communicate over IP/AppleTalk/IPX; or by job transmission routes as follows: IP, TCP, raw9100, LPR, HTTP, FTP, SMB, IPP, SOAP, WebDAV, SMTP, POP3, IMAP4, SSL/TLS, IPsec, Ethernet, wireless LAN, USB, Bluetooth, infrared/IrDA, AppleTalk, IPX, and Parallel Interface.	- Vulnerability that the job data or channels sent/received between the MFP and user terminals, other systems, or remote management systems, are either not protected, or the protection is imperfect		✓
		- Since the mail header of the email fax is not encrypted with S/MIME, an attacker can collect the senders' addresses and destination addresses by wiretapping on the unprotected communications paths with SMTP, POP3, or IMAP4.			
		- Job data is obtained by unauthorized persons on the following devices: HDD inside the MFP, user terminals, accumulation and external processing servers that spool job data, proxy servers, and removable media.	- Vulnerability that the job data processed on the other systems is either not protected, or the protection is imperfect - Vulnerability that the secondary assets, such as management/configuration information or confidential documents that are recorded on the HDD inside the MFP, are not protected by encryption, etc.	✓	✓
		- An attacker intrudes general user terminals to obtain unprotected job data that remained inside, causing the leakage of confidential documents.			
		- An attacker steals the hard disk that was used for the MFP with partial defects due to a replacement for maintenance, and obtains confidential documents from the unprotected job data that remains in the hard disk.	- Vulnerability that the job data processed on the other systems is either not protected, or the protection is imperfect		✓
		- By sending a large number of requests to the MFP, an attacker makes the MFP overloaded to prevent it from overwriting or deleting job data. Then, the attacker takes out a spool file inside the MFP by using another vulnerability, which resulted in the leakage of confidential documents.	- Vulnerability of the job data that is neither deleted nor overwritten at the end of the processing of the job data		✓
2. Integrity	- Job data that is exchanged inside the main unit of the MFP, or between other systems, is tampered to cause the leakage of the document destinations, the names of the boxes to save, and the addresses are tampered.	- Job data that is exchanged by the MFP on one of the following unprotected routes is wiretapped: bus and terminal inside the MFP, between the MFP and the external USB devices, between the MFP and the external Bluetooth or infrared communication device, between the MFP and devices that communicate over IP/AppleTalk/IPX.	- Vulnerability that the job data sent/received to/on the interfaces between the units inside the MFP is either not protected, or the protection is imperfect. - Vulnerability that the job data sent/received between an input/output device and the MFP is either not protected, or the protection is imperfect.		✓ ✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
2. Integrity	- Job data that is exchanged inside the main unit of the MFP, or between other systems, is tampered to cause the leakage of the document destinations, the names of the boxes to save, and the addresses are tampered.	- An attacker interferes in the communications paths between the MFP and other systems to insert box names and destination addresses by tampering with job data, and confidential documents are leaked to the attacker by sending the copy of the job data. The target of interference is one of the following routes of the job transmission procedure: IP, TCP, raw9100, LPR, HTTP, FTP, SMB, IPP, SOAP, WebDAV, SMTP, SMTP, POP3, IMAP4, SSL/TLS, IPsec, Ethernet, wireless LAN, USB, Bluetooth, infrared/IrDA, AppleTalk, IPX, and Parallel interface.	- Vulnerability that the job data sent/received between remote communication devices and the MFP is either not protected, or the protection is imperfect - Vulnerability that the communication system used for the MFP is in a state of being physically operable by attackers	✓	✓
		- Using one of the following devices, job data is tampered by persons with no authorization for the job data: HDD inside the MFP, user terminals, accumulation and external process servers that spool the job data, and proxy servers.	- Vulnerability that the job data processed on the other systems is either not protected, or the protection is imperfect		✓
3. Availability	-The transmission and processing of job data are disabled, and copying/printing/faxing/delivery functions of the MFP are no longer available.	- It continuously creates job data to the MFP, including unexpected values in the processing of the MFP, and repeatedly stops the jobs to find the job data that causes defects and termination (fuzzing). It causes the processing functions for the following job transmission process to defect or overloaded that stop the processing: IP, TCP, raw9100, LPR, HTTP, FTP, SMB, IPP, SOAP, WebDAV, SMTP, SMTP, POP3, IMAP4, SSL/TLS, IPsec, Ethernet, wireless LAN, USB, Bluetooth, infrared/IrDA, AppleTalk, IPX, Parallel interface, and ITU-TT.30.	- Vulnerability resulting in receiving unexpected job data, or defect in the processing		✓
		- An attacker injects a termination or interruption message in each transmission process (TCP FIN, etc.), or key exchange failure message to lose the session, against the specific session between specific MFP and other systems (user terminals, accumulation and external processing, and remote management), and abnormally terminates the session.	- Vulnerability that the communication system used for the MFP is in a state of being physically operable by attackers	✓	
		- It causes VLAN authentication functions, communication functions, remote management functions, and the external authentication functions other than the following job transmission of the MFP, to defect or overloaded that stop the job transmission: 802.1x, EAP, DHCP, DNS, NTP, SNMP, SSH, TELNET, LDAP, Kerberos, X.509, and OCSP.	- Vulnerability that cannot restrict the processing demand to its acceptable capacity		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
3. Availability	- The transmission and processing of job data are disabled, and copying/printing/faxing/delivery functions of the MFP are no longer available.	- The transmission of job data is interrupted by destroying, disconnecting, or electromagnetically interfering with the communications paths between the MFP and other systems.	- Vulnerability that the communication system used for the MFP has the potential for being interfered physically by attackers	✓	
		- The transmission of job data is interrupted by disconnecting, or electromagnetically or optically interfering with the wires in the communications paths between the MFP and input/output devices.	- Vulnerability that the communication system used for the MFP has the potential for being interfered physically, electromagnetically, and optically by attackers	✓	
		- The transmission of job data is interrupted by disconnecting, or electromagnetically interfered with the wires between the bus inside the MFP or between units.	- Vulnerability that the MFP is in a state of being physically operable, or in a condition that the unauthorized devices can be installed nearby, by attackers	✓	
4. Authenticity	- Users to input job data or names of the other systems for some processing requests cannot be confirmed or verified.	- A non-user prints with the MFP by inputting the job data to the MFP, using a job data transmission procedure without authentication (LPR or raw9100, etc.).	- Vulnerability that there is no authentication function for the job data transmission procedure		✓
		- An attacker can attack repeatedly without authentication to find vulnerabilities and to make the next attack successful, because there is no authentication procedure when establishing a connection for accepting job data in the LPR and raw9100 servers running on the MFP.			
		- An attacker who impersonates the other MFP inputs job data to a specific MFP and performs printing by using a fake machine that has the IP address of the other MFP.	- Vulnerability of connection authentication being not performed during transmission of job data		✓
		- Because the communication of the authentication procedure that is exchanged with other systems is not protected when the MFP establishes connections to accept job data, user IDs and passwords are leaked to an attacker, which allows impersonation.	- Vulnerability of connection authentication communication that is unprotected during transmission of job data		✓
		- If a job data contains the information to identify users, user identification information in the job data is tampered to make it look as if another user is outputting the job.	- Vulnerability of connection authentication communication that is unprotected during transmission of job data		✓
		An attacker emails to arbitrary email addresses on the specific MFP to exploit the MFP as a spam server, by inputting an arbitrary job control command for the job data to be sent to the MFP.	- Vulnerability that execution permissions, for the job control command of each job data received by the MFP, are not examined (per MFP, host, or system, etc.)		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
5. Accountability	- In the course of transfer, transmission, or disposal of the job data, the modules, the systems, and which user gave instructions to each process, are not identified to determine the cause of the specific processing.	- In the fax transmission process of the mail transfer type, an attacker changes the job data transmission and injects other fax images using arbitrary SMTP server in the middle of the transmission, but which server is used for rewriting is unknown.	- Vulnerability that servers operated by other organizations with different operational policies interfere with the route of the job data transmission	✓	
		- Some processes are interrupted and fail when the job data with the specified multiple destinations are input into the MFP, but which processes failed and were disposed are unknown.	- Vulnerability that multiple processing results for the job data, or the exceptional processing results, such as failure and disposal, are not recorded - Vulnerability of recording with insufficient information, such as time, users, and processing details, when exceptional processing results are recorded		✓ ✓
6. Non-repudiation	- For a specific process in the course of job data processing, modules, systems, and which user gave the instruction are recorded, but cannot be proved.	- Because anyone can input jobs data in the LPR, when an attacker stops the MFP services by inputting a large volume of job data with identification information of arbitrary users to the specific MFP, there is no information in the job data to identify the attacker.	- Vulnerability that the user IDs, passwords, and the session information of other users can be reused, allowing impersonation (unverifiable vulnerability) - Vulnerability of having no information to identify an attacker, or information can be tampered when the history and audit information are recorded		✓ ✓
7. Reliability	- Job data is confused with another job, and the image data and the destinations are changed. - Image data is destroyed, and the appropriate image is not output. - Job transfer process is exploited and is used to attack the other systems.	- When an attacker continues to send the job for the specific address to the MFP at the same time during/before/after the job data transmission to outside the MFP, another job data destination is replaced, and the attacker receives a copy of the job data, causing the leakage of confidential documents.	- Vulnerability of insufficient implementation on exclusive control of the job data destinations, or multiplexing control of the job		✓
		- While the attacker or other system is processing the acceptance, against the MFP performing acceptance processing of a user job data, an attacker implements exclusive job data or controls, such as data from outside the job control, or data that ignores the transfer data length of the TCP RESET and HTTP, and makes the MFP either save the wrong job data or execute arbitrary codes.	- Vulnerability of insufficient implementation of parameter check of the job data		✓
		- In the processing while the MFP is making inquiries to other systems, an attacker gives a heavy load to the other systems from the specific MFP by giving a large volume of unauthorized job data, and stops or defects the other systems by making the specific MFP make unauthorized inquiries.	- Vulnerability of insufficient implementation of parameter check of the job data - Vulnerability that cannot limit the processing demand to its acceptable capacity		✓ ✓

6.8 Management/configuration information

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- Important information, such as hosts on which asset information is concentrated, is identified by the leakage of configuration information of the main unit of the MFP, or the configuration information to communicate with other systems.	- A maintenance personnel exploits his/her authority to take out the management/configuration information inside the MFP by copying.	- Vulnerability of insufficient education and inadequate contracts with maintenance personnel		✓
		- An administrator copied the configuration information into the SD memory, and lost it, so the management/configuration information is leaked to a third party.	- Vulnerability that the configuration information of the MFP is saved outside the MFP without any protection - Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	✓
		- An attacker exploits the MFP console or administrator terminal, which are left logged in after an administrator is authenticated with the administrator mode on the MFP, and retrieves the management/configuration information by impersonating the administrator to cause the leakage.	- Vulnerability that the MFP console website or the administrators' management website on the MFP are not automatically closed after a few minutes of inactivity - Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	✓
		- An attacker creates a key logger to attack the USB cable between the substrate and the console keyboard, to wiretap the management/configuration information.	- Vulnerability that the job data communicated on the interface between the units inside the MFP is either not protected, or the protection is imperfect - Vulnerability that the MFP is in a state of being physically operable by attackers	✓	✓
		- An attacker attacks vulnerabilities of services running on the MFP, to execute arbitrary code inside the MFP, and copies the management/configuration information by using a privileged operation, causing the leakage of the management/configuration information.	- Vulnerability that the privileged operations are performed by intruding into the MFP from the external interfaces		✓
2. Integrity	- In the management/configuration information, the security functions are disabled to make it impossible to configure the prescribed security policy. - There are so many displayed items that they easily cause mistakes. Because the settings values consistency is not verified between the items of the management/configuration information, it is not possible to achieve the target service conditions.	- An attacker exploits the MFP console or administrator terminal, which are left logged in after an administrator is authenticated with the administrator mode on the MFP, and changes the configuration information by impersonating the administrator.	- Vulnerability that the MFP console website or the administrators' management website on the MFP are not automatically closed after a few minutes of inactivity - Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
2. Integrity	- In the management/configuration information, the security functions are disabled to make it impossible to configure the prescribed security policy. - There are so many displayed items that they easily cause mistakes. Because the settings values consistency is not verified between the items of the management/configuration information, it is not possible to achieve the target service conditions.	- Administrators introduced the MFP settings to achieve the prescribed security policy, but the communication data was not protected because some items among several hundred others were wrong. They continued to be used, because there was no warning message.	- Vulnerability of difficulty to determine if the MFP configuration is designed to conform to the specific security policy or go against		✓
		- An administrator stopped the unnecessary services of the MFP as instructed in the operation manual, and operated only the services that are used. However, an attacker discovered the service ports that are not listed in the operation manual by examining the service ports of the MFP, and attacks the service ports by performing a vulnerability research to intrude the MFP.	- Vulnerability of the services, for which the privileged operations are performed by intruding into the MFP - Vulnerability that the services inside the MFP that should not be performed are performed, or that the ports that should not be opened are open		✓ ✓
3. Availability	- The configuration information of the main unit of the MFP and other configuration information used to communicate with other systems are either destroyed or deleted, so the setting configuration information registered in advance is disabled. - The configuration information cannot be input or upgraded.	- An attacker impersonates an administrator to login to the MFP management console to delete the configuration information.	- Vulnerability due to insufficient authentication strength (e.g., administrator passwords are too simple or have not been changed for a long time, etc.) - Vulnerability due to a lack of implementation that can maintain sufficient authentication strength	✓	 ✓
		- The overload, due to a large volume of requests by an attacker, caused the management console not to be able to open, and all remote controls were no longer functioning while dozens of MFPs continue to print.	- Vulnerability of the communications control functions not being properly implemented		✓
4. Authenticity	- Whether the configuration information of the main unit of the MFP and other configuration information used to communicate with other systems have correct values are not verified.	- The MFP setups that were supposed to be the same as the other MFPs were in violation of the company security policy (e.g. HDD encryption functions were not turned on, or S/MIME use was off.).	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	
		- Because port numbers or addresses of other systems connected to the MFP are wrong, the services are not provided, or wrong information is distributed.	- Vulnerability that there is no way to verify port numbers and addresses set in the MFP, for other systems that the MFP communicates with	✓	
5. Accountability	- Which user changed or deleted the configuration information of the main unit of the MFP and other configuration information used to communicate with other systems, cannot be verified in the history.	- In a few months after the operation, dozens of MFPs were set a little differently from one after another, but there is no way of knowing which of the administrators made those setups and when such setups were performed. No safety measures of configuration management can be taken.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators (A record for the operation of management/configuration information)	✓	

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
6. Non-repudiation	- Information associated with a user, who changed or deleted the configuration information of the main unit of the MFP and the other configuration information used to communicate with other systems, is recorded, but there are no definite grounds to prove it.	- When an attacker changes the management/configuration information by impersonating an administrator, he/she adds the name of another administrator to leave another user ID in the operation record in order to disrupt the recorded contents.	- Vulnerability of accepting the rewriting of logs by administrators, etc.		✓
		- Multiple users can login with the same user ID, so which user had performed an attack is unknown.	- Vulnerability that the same user ID can have multiple, simultaneous setups		✓
7. Reliability	- Information that was entered as the management/configuration information is neither displayed nor saved properly. - Some of the management/configuration information entered are neither saved nor displayed.	- The administrator password is left blank, but it is left as it was because there was no warning. Multiple users without authorization can change the configuration information of the MFP by impersonating administrators, resulting in the leakage of confidential documents.	- Vulnerability of the accepted management/configuration information, which has no way to confirm mistakes, such as contradicted setups or out of its scope, or which is not confirmed		✓
		- The MFP stops when the configuration information is about to be changed while multiple MFP processes are converged. Then, it does not start up, or there is something wrong with behaviors of some functions after start-ups.	- Vulnerability that the configuration information in the MFP are replaced with unexpected data after processing or at the time of interruption of processing, when accepting the updated processing of management/configuration information, including software upgrades, and even if the processing resources are not sufficient, the processing continues		✓
		- The MFP never starts up when it tries to start again, when the software on the MFP is to be added or upgraded while multiple MFP processes are converged.	- Vulnerability that the running processing inside the MFP is interrupted or moved to an abnormal state without considering the load on the processing running on the MFP, when the accepted management/configuration information is processed		✓
		- An administrator attempted to change the settings by using the administrative page on the web server of the MFP, but part of the security functions could not be activated, because a part of the settings values hide in the web browser that was being used. Therefore, confidential documents were wiretapped by an attacker.	- Vulnerability of the MFP management pages, depending on the difference in versions or in browsers; some of the setups, descriptions, the menu, and input values, are not displayed, displayed incorrectly, or are hard to identify		✓

6.9 Digital certificate, ID, password, session information

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- Private keys of the digital certificates for the main unit of the MFP, as well as IDs and passwords of users or other systems are leaked, and they are exploited for impersonation of servers and documents.	- Administrators' IDs and passwords are wiretapped and leaked via any of the following routes: on the bus between units, network/remote communication, input/output units, such as USB, SD memory, and Bluetooth.	- Vulnerability that the communication data on the interfaces between the main units of the MFP is not protected		✓
		- An attacker impersonates an administrator to use the MFP administrator mode, causing the leakage of shared documents in the MFP to the attacker.	- Vulnerability of the default administrator passwords being used because the MFP is not set up accurately when being installed - Vulnerability of the absence of administrator passwords	✓ ✓	
		- An attacker impersonates an administrator to login, and continuously leaks confidential documents by adding the attacker's address to the delivery route of documents.	- Vulnerability that IDs, passwords, and session information are easily predicted (e.g., using a character string in the dictionary, enumeration of the same character, IP address, time, etc., or a bias in the random number generated)	✓	
		- An attacker wiretaps the unprotected communications between the MFP and the business systems, and connects to the business systems by impersonating an MFP to exploit the passwords, IDs, and session information, which are obtained by wiretapping. The information handled by the business systems is retrieved or rewritten by the attacker.	- Vulnerability that the configuration information, including IDs, passwords, and session information, is transferred or saved outside of the MFP without any protection (the leakage in the communications paths between other systems, histories of the URLs or paths are handed over, or there are no authentication procedures to protect passwords)		✓
		- Digital certificates, IDs, and passwords that are left inside the MFP after the disposal of the MFP are leaked to a third party.	- Vulnerability that the configuration information, including IDs, passwords, and session information, is transferred or saved outside of the MFP without any protection (the leakage from the storage, non-volatile memory, history, or records) - Vulnerability that digital certificates, IDs, and passwords are not totally deleted from inside the MFP		✓ ✓
		- The administrator terminal is hijacked by malware injected by an attacker, and all of the certificates, IDs, passwords, and session information inside the MFP are leaked to the attacker.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1.Confidentiality	- Private keys of the digital certificates for the main unit of the MFP, as well as IDs and passwords of users or other systems are leaked, and they are exploited for impersonation of servers and documents.	- Private keys of the digital certificates inside the MFP are retrieved from the MFP, and an attacker sends faxes to other companies by impersonating an MFP to make it look like the other organization has placed an order.	- Vulnerability that private keys of digital certificates are retrieved from inside the MFP without permission - Vulnerability that private keys of the digital certificates are not stored securely		✓ ✓
2. Integrity	- User IDs and passwords are tampered, and the users cannot use the services provided by the MFP. - Private keys of the digital certificates for the main unit of the MFP are changed and tampered, and security functions using the digital certificates either stop working or are disabled. - Digital certificates of their own or of another company have been tampered, and documents provided by an impersonated sender are accepted.	[Digital certificates] - An attacker impersonates an administrator to login, and replaces the private key for digital certificates of the main unit of the MFP with the other private key that is made by the attacker, and continuously wiretaps the ongoing SSL/TLS communication on the server of the MFP.	- Vulnerability that private keys of the digital certificates are not stored securely		✓
		- An attacker exploits the SQL injection to tamper with the management/configuration information inside the MFP, so the other side cannot read the mail fax sent to them, or cannot verify the contents of the mail fax received from other companies. In some cases, it may lead to misunderstandings that the mail faxes sent by attackers are recognized as documents from the other specific company.	- Vulnerability of the authentications that are bypassed at the time of accessing the management/configuration information - Vulnerability that there are no functions to verify the credibility of certificates		✓ ✓
		[IDs, passwords] - An attacker impersonates an administrator using the ID and password of the administrator that is often used, to login to the MFP and change or delete the ID or password of the user to disable the MFP.	- Vulnerability that IDs, passwords, and session information are easily predicted (e.g., using a character string in the dictionary, enumeration of the same character, IP address, time, etc., or a bias in the random number generated)	✓	
		- An attacker wiretaps unprotected communications between the administrator terminal and the MFP, to retrieve the administrator's ID and password, and impersonates an administrator to create another administrator ID. Then, the attacker continuously collects documents and addresses that are exchanged on the MFP.	- Vulnerability that configuration information, including IDs, passwords, and session information, is transferred or saved outside of the MFP without any protection (tampering in the communications paths between other systems, there are no authentication procedures to protect passwords or selected) - Vulnerability that all the digital certificates, IDs, and passwords can be added and changed with all the authority needed, if there is an administrator' ID and password available		✓ ✓
		- An attacker retrieves the HDD from the MFP, creates a copy of the HDD, and retrieves administrator's ID and password by extracting.	- Vulnerability that the configuration information, including IDs, passwords, and session information, is transferred or saved outside of the MFP without any protection (tampering on the storage, or tampering in the non-volatile memory)		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
2. Integrity	- User IDs and passwords are tampered, and the users cannot use the services provided by the MFP. - Private keys of the digital certificates for the main unit of the MFP are changed and tampered, and security functions using the digital certificates either stop working or are disabled. - Digital certificates of their own or of another company have been tampered, and documents provided by an impersonated sender are accepted.	[Session information] - If "POP before SMTP Authentication" is established on the MFP, and if the IP address of the MFP within some minutes after the authentication on POP3 or IMAP4 impersonates a source IP address, SMTP mail transmission service can be used without authentication, so an attacker impersonates an MFP to send mail faxes or spam mails.	- Vulnerability of easily being impersonated, because IP address is used for session information		✓
		- An attacker impersonates as if another user terminal is making a request to a confidential box being used, and retrieves the contents of the confidential box by specifying arbitrary session information or without session information.	- Vulnerability that the authorized session information with valid authentication has not been checked, or the checks are insufficient, at the time of a request being made		✓
		- An attacker makes a request to the MFP scanner box by using the session information of the user who logged out, and confidential documents in the scanner box are leaked.	- Vulnerability of the session information that can be used even after a user is logged out without being deleted		✓
3. Availability	- Private keys or digital certificates created or registered in the MFP are deleted, and the verification of digital signatures, file encryption, or server certificates, is no longer available. - CA certificates are deleted or tampered, and the server certificates, signing on the documents, and the code signing, are not verified hierarchically. - Because there are no corresponding CA certificates in the MFP, the MFP cannot verify the digital certificates obtained by users. - IDs and passwords of users and other systems are either deleted or tampered, and the MFP is disabled or other systems are no longer available from the MFP.	[Digital certificates] - An attacker impersonates an administrator, changes the MFP time setting one year ahead, and disables the main unit of the MFP, email addresses, and digital certificates for other systems stored in the MFP. The MFP continues to operate while communications paths and the contents are left unprotected, and the attacker easily wiretaps on the network, causing the leakage of documents.	- Vulnerability that the enabled/disabled state of the certificates inside the MFP is difficult to understand		✓
		- Although the host name of the main unit of the MFP was changed, the server certificates inside the MFP stopped working, because the certificates inside the MFP were not replaced.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators - Vulnerability that the enabled/disabled state of the certificates inside the MFP is difficult to understand - Vulnerability that whether the MFP operates according to the site security policy is difficult to understand	✓	 ✓ ✓
		- An attacker destroys secure IC/TPM parts inside the MFP or the data in the parts by an electromagnetic attack, etc., and stops the security functions using the MFP server certificates and the MFP client certificates.	- Vulnerability that the MFP is in a state of being physically operable, or in a condition that the unauthorized devices can be installed nearby, by attackers	✓	

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
3. Availability	- Private keys or digital certificates created or registered in the MFP are deleted, and the verification of digital signatures, file encryption or server certificates is no longer available. - CA certificates are deleted or tampered, and the server certificates, signing on the documents, and the code signing, are not verified hierarchically. - Because there are no corresponding CA certificates in the MFP, the MFP cannot verify the digital certificates obtained by users. - IDs and passwords of users and other systems are either deleted or tampered, and the MFP is disabled or other systems are no longer available from the MFP.	- The digital certificates for the main unit of the MFP inside an MFP are intruded due to mistakes of operation or the vulnerability of communication and network modules, and the digital certificates for the main unit of the MFP are either tampered or recreated. Thus, users cannot use the SSL/TLS server function and the S/MIME protection function.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators (operation mistakes) - Vulnerability of the services, for which the privileged operations are performed by intruding into the MFP	✓	✓
		[IDs, passwords] - When the authentication continues to fail repeatedly, it disables the IDs or passwords for a few minutes to a few hours or longer, so an attacker continues to cause authentication failures using the victim's ID repeatedly to make it disabled.	- Vulnerability of the access permission that an attacker can attempt authentication repeatedly		✓
		- An attacker sets the MFP time one year ahead to disable the passwords inside the MFP that have an expiration period, and stops the communication with other systems that do not have automatic updating functions.	- Vulnerability that the services are no longer available due to the expiration of passwords		✓
		[Session information] - An attacker sends logout requests of the other authorized users to the MFP, and makes it log out without the consents of the users. Then, the attacker makes the MFP conduct the authentication procedure again to attack for interference or wiretapping IDs and passwords.	- Vulnerability that the authorized session information can be deleted by any third party		✓
		- An attacker impersonates a user without specifying the secret value provided by the MFP in the previous operation for the session of the other authorized user, and the session of the user is disabled.			

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
4. Authenticity	- IDs and passwords of the specific users or other systems cannot be verified as to whether they are provided by authorized administrators. - The specific digital certificates cannot be verified as to whether they are issued by a specific, authentic certificate authority.	- Because some MFPs mistook some user IDs as other users' IDs due to mistakes by administrators, some users' print jobs were input into spool boxes of other users' to cause the leakage of confidential documents to unauthorized personnel.	- Artificial vulnerability that ID and password string could be assigned to different users by mistake when they are set up in multiple MFPs	✓	
		- An MFP is set up to make requests to the external authentication servers by accepting the ID and password strings from the MFP users, using the external authentication servers. By exploiting this, an attacker made requests to the MFP on the password for a specific ID with brute-force attack, made the MFP confirm with the authentication server by inquiries, and exploited the MFP with password cracking.	- Vulnerability that the MFP responds to the user terminals that do not need to be responded for the authentication (Incorrect setup for the range of the connection permission to the MFP, opening up unnecessary service ports) - Vulnerability that the MFP itself or the authentication servers respond to the authentication requests without delay or lock regardless of the consecutive authentication failures of a specific ID		✓ ✓
		- An attacker passes fake certificates of Company A to Company B, and Company B sends a fax addressed to Company A, which is received by the attacker.	- Vulnerability that the digital certificates have not been correctly implemented on the MFP (Mistakes of certificate issuance procedure, expiration, differences in the owner identifier [DN] strings, improper CAs, insufficient protection of private keys, no confirmation of the names [CN], vulnerable cryptographic methods or use of vulnerable cryptographic keys) - Vulnerability that the improper CA certificates are mixed with the certificates issued by the Certification Authority (CA) inside the MFP (root CA certificates and intermediate CA certificates)	 ✓	✓
5. Accountability	- Who created and registered the digital certificates in the MFP cannot be specified. - IDs and passwords of users and other systems cannot be verified in the changed operational history as to whether they are configured as new.	- An attacker impersonates an administrator to login to the MFP, registers other certificates by rewriting the digital certificates inside the MFP, and stops the security functions that use certificates inside the MFP. When and who did this is unknown, because there is no record.	- Vulnerability of no record of digital certificate requests created inside the MFP		✓
		- An attacker impersonates an administrator to login to the MFP, and adds an ID for the attacker to use. When and who did this is unknown, because there is no record.	- Vulnerability that the operational history, for such items as IDs and passwords that are deleted, added, or changed inside the MFP, is not recorded		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
6. Non-repudiation	- For a record of the name of a specific administrator who registered digital certificates in the MFP, it cannot be proved that the administrator actually performed the specific operation. - Even if there is a record of a user who newly registered, changed or deleted the IDs and passwords of users or other systems, it cannot be proved because there are no grounds for it.	- An attacker impersonated an administrator and temporarily deleted the digital certificates of the MFP. The attacker pretended as if another administrator had operated it by adding fake information to the working record, or pretended as if another administrator had operated it by deleting the operation record.	- Vulnerability of accepting the rewriting of logs by administrators, etc.		✓
7. Reliability	- For IDs and passwords of users or other systems, the length or type of characters is neither properly entered, displayed, nor saved. Sometimes, character strings are shortened, or are inserted or added when they are not displayed. - Some digital certificates cannot be verified, because the corresponding private keys for the specific digital certificates are not correctly assigned.	- Because IDs and passwords sent by MFP users or other systems to the MFP were unexpected values, the operations to list the information inside the MFP were performed; for example, arbitrary code was executed inside the MFP, or an instruction was injected into another module inside the MFP.	- Vulnerability of the accepted digital certificates, IDs, passwords, or session information, which have no way to confirm mistakes, such as contradicted setups or out of its scope, or which is not confirmed - Vulnerability that the software inside the MFP defects if digital certificates, IDs, passwords, or session information are sent/received from/by the MFP without memory protection		✓ ✓
		- During the specific processing or when there is a large amount of load, the verification of the public key certificates attached to the S/MIME emails or server certificates received are interrupted and bypassed specific.	- Vulnerability that the configuration information in the MFP are replaced with unexpected data after processing or at the time of interruption of processing, when accepting the updated processing of digital certificates, IDs, passwords, or session information, and even if the processing resources are not sufficient, the processing continues		✓
		- If there is a large amount of processing or a specific processing, SSL/TLS communication cannot be performed correctly, or the correct S/MIME processing cannot be performed by mail fax.	- Vulnerability that the running processing inside the MFP is interrupted or moved to an abnormal state without considering the load on the processing running on the MFP, when digital certificates, IDs, passwords or session information are processed		✓
		- Fake CA certificates (root, middle) or validation authority (OCSP, etc.) are registered, and server certificates of the fake servers of other systems are wrongly validated, so information assets are leaked to attackers by using the fake servers.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
7. Reliability	- For IDs and passwords of users or other systems, the length or type of characters that is neither properly entered, displayed, nor saved. Sometimes, character strings are shortened, or are inserted or added when they are not displayed. - Some digital certificates cannot be verified, because the corresponding private keys for the specific digital certificates are not correctly assigned.	- Because there is no function to update a digital certificate that another user used before, or update a password that is leaked and needs to be disabled, the former user who used the old certificate, ID, or password, or an attacker who obtained such information, intrudes the MFP.	- Vulnerability that there are no functions to update digital certificates, IDs, and passwords - Vulnerability that there is no periodical password updating	✓	✓
		- If the same user IDs as privileged users on the external file sharing servers, are registered with blank passwords using the MFP console, external file sharing servers can be accessed without passwords of the privileged users, by just logging in with blank passwords using the MFP console. Thus, confidential documents are leaked to unauthorized third parties or users.	- Vulnerability that the different user names that are used in the different authentication procedures are associated incorrectly at the time of user authentication or authorizations for services	✓	

6.10 Accurate time

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	(There is no confidentiality for the standard time due to its global consistency.) (Even if the offset value that indicates the discrepancy of seconds in the main unit of the MFP compared to the world standard time is leaked, the risk is low, and there is no direct threat: time zone, daylight savings time)	- When an attacker makes an inquiry to the built-in web server of the MFP, the time inside the MFP is obtained without authentication. When it is found that the time inside the MFP is significantly deviated, the attacker can wiretap by specifying the communications path where security functions that depend on the time are stopped.	- Vulnerability that the maintenance of the internal time inside the MFP is not performed when using security functions that depend on the time	✓	

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
2. Integrity	- It becomes difficult to audit and monitor when the time of history data deviates significantly. - The accurate time is disabled because of the significant deviation. - The time inside the MFP is significantly staggered, and most of the digital certificates inside the MFP are not available, to perform signature verifications, decryptions, and non-repudiation by signature.	- An attacker impersonates an administrator to change the MFP time setting to a month ahead to stop the communications path protection function using the SSL/TLS and the content protection function for email forwarding documents using S/MIME. The attacker wiretaps and tampers with the documents on the communications paths.	- Vulnerability due to insufficient authentication strength (e.g., administrator passwords are too simple or have not been changed for a long time, etc.) - Vulnerability due to a lack of implementation that can maintain sufficient authentication strength	✓	✓
		- While the license information was being used during the effective period, an attacker interfered with the NTP communication and responded to the MFP with the tampered messages so as not to synchronize the clocks inside the MFP. As a result, part or all the functions that require license, including the security functions of the MFP, stopped.	- Vulnerability that the communication destinations of the NTP (multicast, etc.) are not specified	✓	
		- The ARP of the NTP server was forged by attackers, and the MFP performed time synchronization with the time which was significantly delayed using fake NTP servers.	- Vulnerability that the mutual authentication is not conducted with the communication destinations of the NTP	✓	
		- An attacker had made the MFP time significantly deviated at the time of the attack, so the time of the attack was not properly recorded. Although it was recorded, it was deleted during the periodic processing on the next day, as the record was out of the storage period, and the records were not left.	- Vulnerability that the time synchronization of the NTP is not confirmed, or warnings of time synchronization failure are difficult to understand		✓
3. Availability	- The accurate time is no longer available or displayed.	- The time response function of the MFP stops when it receives an unauthorized accurate time zone value by mail fax. Then, the security functions, operational history records, and the recording function of audit log stop, or a function of the software module whose license period is examined stops.	- Vulnerability that the MFP time response function stops working when an unauthorized accurate time zone value is received		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
3. Availability	- The accurate time is no longer available or displayed.	- Since the time inside the MFP was not correct, web pages on the MFP that use cookies stopped performing because the session information was determined to be always invalid.	- Vulnerability that a stop or failure of the real-time clock hardware is not detected		✓
		- Kerberos authentication always failed, because the time inside the MFP was not correct. Because the single sign-on function of the centralized authentication servers was not used, the authentication by password input was performed on the unprotected communications paths, resulting in the leakage of passwords to attackers.			
		- The MFP have been used without security functions being operated, because the time inside the MFP remains as an initial value (1970) after starting up the MFP while the battery of the real-time clock inside the MFP runs out. Documents and passwords are wiretapped on the communications paths.			
4. Authenticity	- Which time source is synchronized with the time inside the MFP cannot be confirmed. - Whether the NTP time source is the specified time source cannot be identified, and a fake source can be referred.	- An administrator specified the right host name of the NTP server for the MFP, but an attacker responded back to the MFP with fake DNS data to connect to the fake NTP. The MFP displays the name of the NTP server host that is connected, but the MFP time remains deviated because the IP address of the NTP server that is connected is unknown, and it is unknown as to whether it is performing as it was setup.	- Vulnerability that the time synchronization source for the NTP is neither managed nor displayed - Vulnerability due to unprotected communication between the NTP servers and the MFP for the time synchronization, or that the protection is imperfect		✓ ✓
5. Accountability	- The host name of the time source and the time device names, described in the record when the time inside the MFP is synchronized, are not confirmed.	- A part of NTP servers in use on the specific MFP fails to cause synchronization with the abnormal time, but no measures can be taken, because which NTP server shall be stopped is unknown due to no history recorded.	- Vulnerability of insufficient history records, such as the time synchronization processing of the NTP, or synchronization sources used are not recorded even if there are records		✓
6. Non-repudiation	- It cannot be proved that the other systems provided the wrong time to synchronize the time inside the MFP.	- An attacker impersonated one of the NTP servers that an MFP is using, and the MFP synchronized the wrong time when the attacker responded to time synchronization. This record was left on the MFP, but this MFP did not protect the NTP communication, so there is no proof that the specific NTP server responded with an incorrect time.	- Vulnerability due to unprotected communication between the NTP servers and the MFP for the time synchronization, or that the protection is imperfect		✓
		- A history of the time synchronization has been recorded, but it is disabled for verification, because there is a possibility that the record is tampered.	- Vulnerability of accepting the rewriting of logs by administrators, etc.		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
7. Reliability	- The start-up time is significantly deviated. - The time is synchronized with the standard time, but the time offset of the region is not output. - The time fluctuates without synchronizing the standard time when the time passes. - It is impossible to arrange output documents in order of time.	- The dates of job data, emails, and files, sent to other systems, are significantly deviated because the clock battery in the used MFP has run out. As a result, since job execution records are sorted and displayed by dates from the latest, job records copied and forwarded illegally by an attacker are unnoticed, because such job records are sorted out as old records.	- Vulnerability that a stop or failure (loss of battery, etc.) of real-time clock hardware is not detected		✓
		- A used MFP has been used without the time settings since its purchase, but the time is disabled for the history record when referring to the operation records of other systems, because the time information of operational history for auditing or management, and error records, deviate significantly.	- Vulnerability that can be migrated to the operating state without setting the time at the initial MFP setting - Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	✓
		- An administrator set up the time inside the MFP using the MFP console, but it caused a one year deviation because the administrator mistook the digit in the year. Therefore, digital certificates with a correct expiration period were determined as expired and were not used in the MFP.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	
		- The time inside the MFP is deviated because the time cannot be synchronized with the time of the specified NTP server.	- Vulnerability of the NTP procedure that cannot be properly processed		✓
		- The MFP time becomes an abnormal value after one year of operations without turning off the power. The usage right of the MFP is determined to be invalid in comparison with the license period of the MFP, resulting in part or all of the MFP functions no longer being available.	- Vulnerability that the clock inside the MFP generates several numeric overflows (16 bit signed/unsigned, 32 bit signed/unsigned, second/ms/us)		✓
		- Digital certificates with 30 years validation are created as of 2010, and were installed on the MFP, but the validity of the digital certificates cannot be verified because the comparison of the date and time inside the MFP is not properly processed.	- Vulnerability of having a year 2038 problem in the time processing of the MFP (32 bit overflow)		✓
		- When setting the time zone that is advanced by 5 hours and 30 minutes from the Greenwich Mean Time and the daylight saving time that is advanced by 1 hour, only an offset of 5 hours and 0 minutes is reflected for the time of fax documents.	- Vulnerability that does not support minutes for the time zone and daylight saving time - Vulnerability that the MFP does not maintain the Greenwich Mean Time (GMT) - Vulnerability of incomplete processing for the time zone and daylight saving time		✓ ✓ ✓

6.11 Original papers, prints

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- Original papers or prints containing confidential information are leaked to a third party.	- A third party reads original papers or prints that are left on the copying table or output tray, or takes out a copy by copying or scanning.	- Vulnerability that the MFP is in a state of being physically operable by attackers	✓	
			- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	
			- Vulnerability of unconditional paper outputs by remote printing or receiving of faxes		✓
2. Integrity	- Original papers or prints are either replaced or changed.	- A third party replaces original papers or prints that are left on the copying table or output tray, with fake documents.	- Vulnerability that the MFP is in a state of being physically operable by attackers	✓	
			- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	
			- Vulnerability of unconditional paper outputs by remote printing or receiving of faxes		✓
		- About 10 pages were copied simultaneously while Mr. A was copying a large volume, but part of Mr. A's prints were mixed with the others because of the processing errors, due to a large volume of processing accepted by the network concurrently.	- Vulnerability of a resource shortage due to interruption by the multi-stage processing or race conditions that cause errors on execution control of the finisher		✓
3. Availability	- Original papers cannot be read automatically. - Prints cannot be output to the appropriate print tray.	- Original papers cannot be automatically read because a foreign matter that is inserted into the ADF by an attacker.	- Vulnerability that the MFP is in a state of being physically operable by attackers	✓	
		- An attacker removes a cable to the ADF of the MFP and a cable to the finisher in order to disable the ADF and the finisher.			
		- The ADF and the finisher do not work properly due to the generation source of a strong electromagnetic wave near the MFP, so they are disabled.	- Vulnerability that unauthorized devices are installed nearby, by attackers	✓	
		- Papers and toner cartridges that were loaded in the MFP are stolen, which disables copying/printing/fax reception.	- Vulnerability that the MFP is in a state of being physically operable by attackers	✓	

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
3. Availability	- Original papers cannot be read automatically. - Prints cannot be output to the appropriate print tray.	- Papers and toner cartridges that were loaded in the MFP are run out, which disables copying/printing/fax reception.	- Vulnerability of unconditional paper outputs by remote printing or receiving of faxes		✓
4. Authenticity	- Whether original papers are collected by the authorized users is unknown. - Whether prints are collected by the authorized users is unknown.	- A third party collects original papers output by the ADF, causing the leakage of confidential documents.	- Vulnerability that the MFP is in a state of being physically operable by attackers - Vulnerability of unconditional paper outputs by remote printing or receiving of faxes	✓	
		- A third party collects the prints in the output tray, causing the leakage of confidential documents.			✓
5. Accountability	- For some scan data and fax data, the user who input the original papers cannot be identified. - For some prints, the user who copied cannot be identified.	- A fake order instruction arrives at a company via fax with the name of the company as a sender, but the individual sender cannot be identified.	- The user authentication function is not provided when using the MFP - Vulnerability that the authentication results of MFP users are not recorded along with the operational history		✓ ✓
		- A large number of prints are output from an MFP, but the individual who performed the output cannot be identified.	- The user authentication function is not provided when using the MFP - Vulnerability that the authentication results of MFP users are not recorded along with the operational history		✓ ✓
6. Non-repudiation	- For some scan data and fax data, the user ID of an individual who input the original papers is recorded, but there are no grounds to prove it. - For some prints, user ID of an individual who output is recorded, but there are no grounds to prove it.	- An attacker scans the fictitious receipts/invoices, stores and circulates them. However, when it is pointed out after the audit, the attacker claims that the data is scanned by someone else, and it cannot be proved.	- Vulnerability of accepting the rewriting of logs by administrators, etc.		✓
		- For a large amount of color prints, the individual whose user ID was in the output record denies the performance and it cannot be proved.	- Vulnerability of accepting the rewriting of logs by administrators, etc.		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
7. Reliability	- A large volume of original papers and prints cannot be output in the correct order. - Incorrect output and storage are conducted if the interrupt processing is performed in multiple stages. - Prints can neither be printed as images nor finished as specified: i.e., positioning and images of the output are different; it cannot be discharged into the appropriate tray; prints are not output by specified number as instructed; collating does not work; stapler does not work; punching does not work; it staples/punches on the wrong spots; and folding does not work or is wrong.	- Thousands of pages have begun printing, but image positioning, page order, or binding of some prints become failure by accepting a large number of requests from an attacker. They became a waste disposal, and caused damages due to delay in the specified delivery date.	- Vulnerability that the resources inside the MFP are not sufficient when the MFP receives a large amount of processing, and the processing as instructed cannot be performed because part or all of the job data are destroyed or mixed		✓
		- Thousands of pages have begun printing, but the binding of all prints became failure because of the electromagnetic interference from an attacker, causing a waste disposal. A large amount of toners and hundreds of thousands of papers are wasted.	- Vulnerability that unauthorized devices are installed nearby by attackers	✓	
		- Piling up of punching wastes, failure of a large volume of printing by wrong staples for replacement	- Vulnerability that piling up of punching wastes and wrong staples for replacement are not noticeable (the security policy leakage or insufficient awareness on security policy among administrators)	✓	
		- Paper jams or several papers were drawn in at the same time in the middle of a large volume of printing, because several sheets of different thickness papers were mixed in the paper tray, causing printing failure.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	

6.12 Shared files inside the MFP

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- Files containing confidential information are leaked to a third party from the shared folders in the main unit of the MFP.	- An attacker changes the request argument to find out the path names of the configuration management files that contain passwords inside the MFP.	- Vulnerability that the names of the undisclosed shared folders and files can be read due to insufficient examinations of the requests to the shared folders inside the MFP		✓
		- An attacker tricks the SQL injection to the request argument, and retrieves confidential files, regardless of any restrictions.			
		- Confidential files were leaked to a third party, because such confidential files were in the public folder in the shared folder in the MFP.	- Vulnerability that confidential documents are placed in the public folder by mistake (Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators)	✓	
		- Confidential files were in the confidential folder, but such information could be leaked to the wrong authority, because attackers could get the files with the privileges of general users or guests.	- Vulnerability that proper usage authorization has not been implemented - Vulnerability that proper users cannot be authorized, and the allocation processing of proper usage authorization cannot be performed	✓	✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- Files containing confidential information are leaked to a third party from the shared folders in the main unit of the MFP.	- By using a search function for shared folders inside the MFP, confidential document names can be disclosed to anyone. In some cases, such documents can be leaked to a third party by downloading them as they are.	- Vulnerability that undisclosed file names are leaked when a search is performed - Vulnerability that allows bypassing of security functions by opening files through searching		✓ ✓
		- Confidential information is leaked to unauthorized users by taking advantage of the absence of authorization when displaying files in shared folders in the MFP using the console, outputting them to SD memory, printing them on paper, faxing them, delivering them to inboxes, delivering them to folders in other systems such as PCs, delivering them via emails, or sending them to URLs in other systems.	- Vulnerability that allows bypassing of security functions depending on the types of the output destinations		✓
		- An attacker impersonates an administrator to create and obtain backups including shared folders inside the MFP, which results in the leakage of confidential documents in shared folders.	- Vulnerability due to insufficient authentication strength (e.g., administrator passwords are too simple or have not been changed for a long time, etc.) - Vulnerability due to a lack of implementation that can maintain sufficient authentication strength	✓	 ✓
		- Maintenance personnel collect and bring back defective HDDs when they replace storage devices. They can retrieve files in the shared folders which contain confidential documents.	- Vulnerability caused by a lack of encryption protection of data in the storage, etc., or the protection is imperfect		✓
2. Integrity	- Files in the shared folders in the main unit of the MFP are either replaced or changed.	- An attacker uses SQL injection or command injection against a DB engine inside the MFP to rewrite files.	- Insufficient examinations of the contents of the requests, such as folder names, path names, ID numbers, and attributes, etc., in shared folders in the MFP		✓
		- Some data are changed when certain documents are input while generating requests that create a resource overflow or a race condition inside the MFP.	- Vulnerability that causes data change due to a resource shortage or race conditions during the massive processing on the MFP		✓
		- Due to overload, some or all of the search indexes or databases for document management are destroyed.			
		- An attacker successfully bypasses the authentication procedure, either by sending an "Authentication completed" message during the procedure, or by sending a request during the authentication process, against the authentication procedure of the shared file server in the MFP.	- Vulnerability that allows bypassing of authentication for shared files inside the MFP		✓
		- An attacker wiretaps unprotected communication between administrator terminals and the shared file servers in the MFP, impersonates an administrator against the shared file servers by exploiting the retrieved session information, and changed the shared files inside the MFP with other files using the administrator privilege.	- Vulnerability due to unprotected communication between the shared files inside the MFP and other systems		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
2. Integrity	- Files in shared folders in the main unit of the MFP are either replaced or changed.	- An attacker impersonates an administrator to retrieve backups, tampers with them, and rewrites them (restore) to tamper with the shared files inside the MFP.	- Vulnerability due to insufficient authentication strength (e.g., administrator passwords are too simple or have not been changed for a long time, etc.) - Vulnerability due to a lack of implementation that can maintain sufficient authentication strength	✓	 ✓
		- An attacker removes storage parts, rewrites the sector in the storage parts, and puts them back in the MFP to tamper with the shared files in the MFP.	- Vulnerability caused by a lack of encryption protection of data in the storage, etc., or the protection is imperfect		✓
3. Availability	- Services of shared folders in the main unit of the MFP are disabled, or it takes a very long time to respond (for retrieving, writing, updating, and listing files).	- An attacker uses SQL injection or command injection against a DB engine inside the MFP to delete files inside the MFP or document information in the DB.	- Vulnerability that a resource shortage, or stop or delay of processing, due to insufficient examinations of the requests to shared folders inside the MFP		✓
		- An attacker sends a large number of requests that fail authentication for the MFP, and the MFP locks out authentication for most users for a while.	- Vulnerability that a function to reject authorized users is exploited when authentication failure continued by the requests of attackers		
		- A request that generates an infinite loop of processing in the shared folders in the MFP is injected, and it makes the MFP responses slow, or causes it to stop.	- Vulnerability that services on the shared folders become unavailable due to the accumulation of a large volume of requests and processing (pressure from the processing memory, CPU processing volume, and bus bandwidth; pressure of disks from temporary files, document files, and the log files)		✓
		- The MFP receives a large volume of requests, and the shared file services in the MFP stop.			
		- The storage device inside the MFP is either removed or defects, and it disables all the shared files inside the MFP.	- Vulnerability that the MFP is in a state of being physically operable by attackers	✓	
4. Authenticity	- Which user created part or all of the files in shared folders in the main unit of the MFP is unknown.	- User attributes are not recorded when the files are created in the shared files in the MFP, and an attacker can create files of unknown users any time.	- Vulnerability that the digital signature of the author of the shared folders inside the MFP is not used - Vulnerability that user attributes of the shared folders inside the MFP do not indicate the author of the documents		✓ ✓
		- An attacker sends the specified job files with an unusually long user ID to the MFP, and the shared file management software inside the MFP saves the files without recording the user attribute information.	- Vulnerability that the recording process of the user identification function and identification information is bypassed when shared files are created on the MFP - Vulnerability of the shared folders inside the MFP that the input value is not examined sufficiently at the time of storage		✓ ✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
5. Accountability	- Who created or viewed the specific files in shared folders of the main unit of the MFP cannot be traced back in the history.	- An attacker conducts a directory traversal to view all of the MFP shared folders, identifies the names and divisions of the authors who create important documents to conduct more attacks. Activities of the attacker cannot be detected through monitoring and auditing by the MFP operators, so attacks cannot be prevented.	- Vulnerability that the operational history of the shared files inside the MFP is not recorded		✓
6. Non-repudiation	- The IDs of the users who created, updated, and viewed the specific files in shared folders of the main unit of the MFP were recorded, but it cannot be proved even if the users deny such performances.	- An operator confirmed the record of a user viewing a large number of files, but the viewing record of the user was not his/hers, because it could be easily tampered or injected.	- Vulnerability of accepting the rewriting of logs by administrators, etc.		✓
7. Reliability	- Document files that are input, or part of the contents of the document files retrieved, are changed with the other jobs or other files. - Document files that are input disappear when they are retrieved. - Arbitrary code is executed.	- While an attacker is generating requests to create a resource overflow or a race condition inside the MFP, some data are changed when specific documents are input.	- Vulnerability of a resource shortage due to a large volume of processing or processing errors due to a race condition		✓
		- While an attacker is generating requests to create a resource overflow or a race condition inside the MFP, the processing of saving some documents becomes imperfect. It appears that the documents are saved from general users, but they cannot be retrieved because they are not saved.	- Vulnerability of a resource shortage due to interruption by the multi-stage processing or processing errors due to a race conditions		✓
		- An attacker injects a command to specify unauthorized file attribute values, and generates an overflow in the shared file management software inside the MFP, to execute arbitrary commands.	- Vulnerability that arbitrary code is executed due to a lack of examination of input shared file attribute valuesinside the MFP (path names, IDs, attribute values, and file data)		✓

6.13 Usage history, audit records

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- One or more destination addresses, senders' numbers, server addresses in the usage history or audit records are leaked.	- An attacker tricked the SQL injection to the request argument, and took out the usage history regardless of any restrictions.	- Vulnerability that the names of the undisclosed shared folders and files can be read due to insufficient examinations of the requests to the MFP, and vulnerability that the examination of the authentication and authorization is bypassed by injecting the command (command injection)		✓
		- The usage history was in the confidential folder, but it was leaked to the wrong authority, because attackers could get the files using the privileges of general users or guests.	- Vulnerability that the authentication and authorization of the users of the usage history and audit records are not properly set up, or the allocation processing cannot be performed properly		✓
		- The usage history is leaked to a third party because the information is in the public folder in the MFP.	- Vulnerability of the usage history published in the folder that does not require authorization		✓
		- If the usage history is accessed via a search function, it is leaked to a third party due to unauthorized downloading.	- Vulnerability that allows bypassing of security functions by opening files through searching		✓
		- The usage history is leaked to unauthorized users by taking advantage of the absence of authorization, when displaying the usage history using the MFP console, outputting it to SD memory, printing it on paper, faxing it, delivering it to inboxes, delivering it to folders in other systems such as PCs, delivering it via emails, or sending it to URLs in other systems.	- Vulnerability that allows bypassing of security functions depending on the types of the output destinations		✓
		- An attacker impersonates an administrator to create and obtain backups including the usage history, which results in the leakage of the usage history.	- Vulnerability due to insufficient authentication strength (e.g., administrator passwords are too simple or have not been changed for a long time, etc.) - Vulnerability due to a lack of implementation that can maintain sufficient authentication strength	✓	✓
		- Maintenance personnel collect and bring back defective HDDs when they replace storage devices. They can retrieve the usage history, resulted in the leakage.	- Vulnerability caused by a lack of encryption protection of data in the storage, etc., or the protection is imperfect		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
2. Integrity	- A part of the usage history or audit records that are recorded are tampered.	- An attacker tampers with the time, user ID, or processing of the specific records of the usage history and audit records by SQL injection or command injection.	- Vulnerability that the usage history and audit records are tampered due to a lack of examinations of the requests		✓
		- In order to disrupt the usage history, an attacker injected the records into the usage history record modules inside the MFP as if the other user had done it.	- Vulnerability that the authentication and authorization of the users for addition or deletion of the usage history and audit records are not properly set up, or the allocation processing cannot be performed properly		✓
		- An attacker updated the usage history without authentication.			
		- An attacker updated the usage history by being authenticated as a general user.			
		- An attacker tampered with the usage history that was placed in a writable folder.	- Vulnerability of the usage history published in the folder that does not require authorization		✓
		- An attacker either sent unauthorized forms of usage history requests to the MFP, or requested to complete the authentication before the authentication was completed. The MFP updated the usage history without any authentication.	- Vulnerability that the internal data can be deleted, added, or updated, due to insufficient examinations of the requests to the MFP - Vulnerability that allows bypassing of security functions by the interfaces which accept requests		✓ ✓
		- An attacker impersonates an administrator to update the usage history inside the MFP.	- Vulnerability due to insufficient authentication strength (e.g., administrator passwords are too simple or have not been changed for a long time, etc.) - Vulnerability due to a lack of implementation that can maintain sufficient authentication strength	✓	 ✓
		- An attacker retrieves backups, tampers with the usage history, and returns after writing.	- Vulnerability caused by a lack of encryption protection of data in the storage, etc., or the protection is imperfect		✓
		- An attacker removes the storage, tampers with the usage history, and returns the storage to the original location.			
3. Availability	- Display, confirmation, and examination of the usage history or audit records are no longer available.	- An attacker deletes all the usage history and audit records by SQL injection.	- Vulnerability that the files and the processing can be accessed, due to insufficient examinations of the requests to the MFP		✓
		- An attacker can force quit the history recording process inside the MFP by a command injection.			
		- An attacker sends a large volume of requests to the MFP, and disables the usage history recording on the MFP to conduct attacks.	- Vulnerability that the usage history become unavailable due to the accumulation of a large volume of requests and processing (pressure from the processing memory, CPU processing volume, and bus bandwidth; pressure from temporary files, document files, and log files)		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
3. Availability	- Display, confirmation, and examination of the usage history or audit records are no longer available.	- An attacker impersonates an administrator to stop the usage history from being recorded, or takes advantage of the input vulnerability of the MFP to stop the operation of the usage history, or rewrites the executable code to conduct the normal terminations without the recording process.	- Vulnerability that the software functions which record the usage history can be disabled or are being bypassed		✓
		- An attacker deleted the usage history without authentication.	- Vulnerability that the usage history can be deleted without sufficient authorization		✓
		- An attacker deleted the usage history by being authenticated as a general user.			
		- An attacker deleted the usage history that was placed in a writable folder.	- Vulnerability that the usage history is recorded at deletable or rewritable locations		✓
		- An attacker removed the storage, accesses the storage from another computer to delete the usage history, and returned the storage to the original location.	- Vulnerability that the usage history data on the storage is not protected		✓
4. Authenticity	- Regarding the deletion of the usage history or audit records, there is no proof of who did it, and the recorded time is not even reliable.	- Because the user attributes are not recorded even if the usage history inside the MFP is deleted, an attacker can delete the usage history any time after attacks	- Vulnerability that users are not identified during the usage history operations		✓
		- An attacker adds records to the usage history operation records inside the MFP by specifying an arbitrary user ID, to make it impossible to identify the administrator who deleted it.	- Vulnerability that user IDs added during the usage history operations can be changed to arbitrary value		✓
5. Accountability	- Regarding the deletion of the usage history or audit records, the records of who performed the processing cannot be specified.	- Although the usage history that was there the day before was deleted, the individual administrator who did it is unknown.	- Vulnerability that deleting operation of the usage history is not recorded		✓
6. Non-repudiation	- Even if there is a record that a specific user deleted the usage history or audit records, it cannot be proved, because there are no grounds for it.	- The user ID of an administrator was recorded as a user who deleted the usage history, but the individual who deleted it is unknown, because an attacker could tamper to an arbitrary character string.	- Vulnerability that the existing usage history records of the MFP can be modified		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
7. Reliability	- The usage history or audit records are not recorded with accurate time, authentic user IDs, and correct processing names. - Some or all of the history of actual activities are not recorded.	- The time inside an MFP becomes 1970 when it starts until an administrator adjusts the time manually. An attacker sends an unauthorized packet to restart the MFP before the attack, and attacks the MFP leaving the record of attack as an old record. When the administrator adjusts the time, the old record of attack is automatically deleted, and the administrator will not be able to confirm attacks.	- Vulnerability that the MFP cannot maintain the accurate time		✓
		- Because there is a function on the MFP that allows the usage history and the audit information to be modified later, an attacker deleted the records immediately after the attack against the MFP.	- Vulnerability that the existing usage history records of the MFP can be modified		✓
		- User IDs in the audit records of an MFP are always the same, so the records of confidential documents retrieved by an attacker after attacking the MFP cannot be specified.	- Vulnerability that the MFP does not record user information of identified users and authorized users when recording the usage history		✓
		- Incorrectly processed names or only part of the messages are recorded due to abnormality of the numerical data range and the message length for some usage history inside the MFP, so the attack methods by an attacker cannot be analyzed.	- Vulnerability that the incorrectly-processed names and value are recorded for some usage history of the MFP		✓
		- An attacker sends an unusually long user ID to the MFP so that a function to record the history will not record the user attribute information.	- Vulnerability that user IDs which are recorded in the usage history or audit records do not reflect the results of user authentication (always a fixed or undefined value)		✓

6.14 Billing information for MFP use

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- Billing information and usage information are leaked to unauthorized persons.	- An attacker tricks the SQL injection to the request argument, and retrieves the billing information without proper authorization.	- Vulnerability that the authentications can be bypassed due to insufficient examinations of the requests to the MFP		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- Billing information and usage information are leaked to unauthorized persons.	- Billing information is leaked to a third party, because such information is in the MFP public folder.	- Vulnerability of billing information that is published in the folder that does not require authorization		✓
		- Billing information is leaked to the wrong authority, because attackers can get the files with the privileges of general users or guests.			
		- If billing information is accessed via a search function, it is leaked to a third party due to unauthorized downloading.	- Vulnerability that allows bypassing of security functions by opening files through searching		✓
		- Billing information is leaked to unauthorized users by taking advantage of the absence of authorization when displaying the billing information using the console, outputting it to SD memory, printing it on paper, faxing it, delivering it to inboxes, delivering it to folders in other systems such as PCs, delivering it via emails, or sending it to URLs in other systems.	- Vulnerability that allows bypassing of security functions depending on the types of the output destinations		✓
		- An attacker exploits the administrator terminals that are left logged in, and creates and obtains backups including the billing information inside the MFP, which results in the leakage of confidential documents, IDs, passwords, and the session information of the spooled job data.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	
2. Integrity	- Some or all of the billing information for MFP use is tampered, and appropriate billing information of users is not collected or appropriate billing is not made to users.	- An attacker rewrote the usage billing information with the value of 30% less by exploiting an SQL injection, and reduced monthly payment to the maintenance businesses by 30%.	- Vulnerability that the usage billing information can be rewritten by a command injection due to insufficient examinations of the requests to the MFP.		✓
		- An attacker impersonated an administrator to rewrite the usage billing information of the MFP to zero.	- Vulnerability due to insufficient authentication strength (e.g., administrator passwords are too simple or have not been changed for a long time, etc.) - Vulnerability due to a lack of implementation that can maintain sufficient authentication strength	✓	 ✓
		- An attacker impersonated maintenance personnel to rewrite the usage billing information of the MFP as doubled values.			
		- An attacker specified the usage billing summary API for the remote maintenance of the MFP to rewrite the usage billing information of the MFP to zero.	- Vulnerability of the interfaces that are not open to users (e.g. remote maintenance interfaces) - Vulnerability of the external interfaces that are not authenticated		✓ ✓
		- An attacker inserts an additional process on the http proxy for the remote maintenance of the MFP, in a manner that the billing number of the accounting report message is rewritten to zero, and the monthly pay-per-use to the maintenance businesses becomes zero.	- Vulnerability that the communication data of the remote maintenance interfaces are either not protected, or the protection is imperfect		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
2. Integrity	- Some or all of the billing information for MFP use is tampered, and appropriate billing information of users is not collected or appropriate billing is not made to users.	- An attacker changed the EEPROM parts inside the MFP, and wrote the usage billing information to charge excessive fees.	- Vulnerability that the MFP is in a state of being physically operable by attackers	✓	
		- An attacker removed or destroyed the storage parts that were to write the usage billing information inside the MFP, and the MFP continued to be used without recording any billing information.			
3. Availability	- Usage accounting information is not added even if the MFP is used. - Billing information cannot be retrieved because the maintenance function or the remote maintenance function becomes disabled or inaccessible.	- An attacker injected a code inside the MFP to reduce 60% of the billing to the maintenance personnel by bypassing the process to add the usage billing only during the time period of frequent usage of the MFP.	- Vulnerability that the processing which adds usage billing is disabled or is bypassed		✓
		- An attacker continuously conducted the wrong maintenance personnel authentication, so that the maintenance businesses were not able to login.	- Vulnerability that a function to lock the maintenance personnel mode for a certain period of time is exploited if incorrect passwords in the maintenance personnel authentication are entered a few times in a row (along with console authentication and remote authentication)		
		- An attacker impersonated an administrator to delete the usage billing information.	- Vulnerability that allows administrators to delete the billing information		✓
4. Authenticity	- Whether the billing information for MFP use is correct or not is unknown, so it is unknown even if the billing information for the MFP is tampered.	- An attacker specified the usage billing summary API of the MFP, and injected the negative value to change the usage billing information to reduce the charge.	- Vulnerability that interfaces, which are not open to users, operate - Vulnerability that external interfaces which exchange the usage billing information are not authenticated		✓
		- An attacker exploited the usage billing summary API of the MFP, and injected excessive usage value to increase the bill by 60% more than the actual usage billing information to increase the charge.	- Vulnerability that the source information which adds the usage billing information is not identified or specified		✓
5. Accountability	- It is not possible to determine the cause even if the billing information for MFP use is initialized or tampered to an unexpected number.	- The software inside the MFP did not install a function to record the operational history of the usage billing information that was an option.	- Vulnerability that there are no functions to record the operational history of the usage billing information		✓
		- The software inside the MFP that records the operational history of the usage billing information did not have functions to record user IDs.	- Vulnerability that the operational history of the usage billing information does not record any of the times, user IDs or operation types		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
6.Non-repudiation	- Some or all of the usage billing information for MFP use is deleted or tampered by some maintenance personnel, but who specifically did it cannot be proved.	- After an attacker deleted the usage billing information, the attacker injected an operational history via API as if a remote maintenance business deleted it, to make it difficult to determine the user who deleted it.	- Vulnerability that user IDs are recorded in the record of operations, but such user IDs can be tampered by users		✓
7. Reliability	- The billing information for MFP use is no longer an appropriate value under certain conditions, such as many and big job data is concentrated, which causes incorrect billing.	- An attacker continued to input the jobs that took a long time to be executed to avoid the usage billing information being added, by creating a certain race condition inside the MFP, and kept executing a large volume of other jobs.	- Vulnerability related to race conditions and resource management		✓
		- An attacker had made the MFP time significantly deviated at the time of the attack, so the time of the attack was not properly recorded. Although it was recorded, it was deleted during the periodic processing on the next day, as the record was out of the storage period, and the records were not left. (It is also described in “Accurate time.”)	- Vulnerability that the MFP cannot maintain the accurate time		✓
		- As a result of distributed processing of 1,000 copies into four MFPs, excessive usage was charged for 4,000 copies of work.	- Vulnerability of charging double for the print job data that is shared with another MFP (bug)		✓

6.15 Communication system (including Switch, DHCP, DNS, NTP)

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- Wiring or connectors for the MFP to communicate are exposed, and they are easily wiretapped by inserting another device. Radio waves are easily wiretapped. - A switching hub or VLAN can be easily connected without physical restrictions or authentication, so wiretapping and third-party mail relay are easily conducted. (Communication devices include DNS, DHCP, and NTP.)	- An attacker inserts a device between the communication system cables to wiretap unprotected communications as follows, and collects and records IDs and passwords the mail server. Unprotected communications: IPv4, IPv6, DHCP, ARP, ICMP, ICMPv6, LLMNR, Rendezvous, TCP, UDP, UPnP, DNS, TELNET, SNMP, SMTP, POP3, IMAP4, SIP, FTP, HTTP, SMB, LPR, raw9100, IPP, etc.	- Vulnerability due to unprotected communications between other systems and the MFP, or that the protection is imperfect		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- Wiring or connectors for the MFP to communicate are exposed, and they are easily wiretapped by inserting another device. Radio waves are easily wiretapped. - A switching hub or VLAN can be easily connected without physical restrictions or authentication, so wiretapping and third-party mail relay are easily conducted. (Communication devices include DNS, DHCP, and NTP.)	- USB printer ports of the MFP, USB memory ports, and USB authentication unit ports, are transmitted via TCP/IP, and extended to remote locations. However, because the communications are not protected, confidential documents and card numbers for authentication are wiretapped and leaked to attackers.	- Vulnerability due to unprotected communications between other systems and the MFP, or that the protection is imperfect		✓
		- An attacker decrypts the WEP key of the wireless LAN used by the MFP to retrieve IDs and passwords from the FTP protocol for the external shared file servers that MFP communicates. The attacker impersonates an MFP to retrieve documents in the shared file server.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators (policy related to encryption strength)	✓	
		- An attacker uses the VLAN distribution protocol on a remote switching hub to create an Ethernet port that belongs to a VLAN dedicated to the MFP, and connects to the same VLAN as the MFP. Then, the attacker impersonates a default gateway of the MFP to perform a third-party relay attack.	- Vulnerability due to unprotected communications between other systems and the MFP, or that the protection is imperfect		✓
		- The MFP was not isolated on the network because either the MFP was connected to the wrong VLAN, or IPsec configuration was wrong. It was connected to the same network as that of general users, resulting in the wiretapping of unprotected communications.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators (network cable connection or incorrect settings)	✓	
2. Integrity	- Unprotected communications of the MFP is tampered. - A third-party mail relay is conducted using a general-purpose interface, such as USB/SCSI, to tamper with image data and addresses of the print, scan, and fax. (Communication devices include DNS, DHCP, and NTP.)	- An attacker tampers with the host name resolution responses from the DNS server, because they are not protected, so the requests from the MFP since then are directed to the host prepared by the attacker.	- Vulnerability due to unprotected communications between other systems and the MFP, or that the protection is imperfect		✓
		- An attacker inserts a device between the communication system cables to interfere with unprotected communications, and tampers with IDs and passwords for the mail servers. Other unprotected communications: IPv4/IPv6, DHCP, ARP, ICMP, ICMPv6, LLMNR, Rendezvous, TCP, UDP, UPnP, DNS, TELNET, SNMP, SMTP, POP3, IMAP4, SIP, FTP, HTTP, SMB, LPR, raw9100, IPP, etc.			

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
2. Integrity	- Unprotected communications of the MFP is tampered. - A third-party mail relay is conducted using a general-purpose interface, such as USB/SCSI, to tamper with image data and addresses of the print, scan, and fax. (Communication devices include DNS, DHCP, and NTP.)	- Because the response messages from the DHCP/DHCPv6 server were not protected, the MFP that has received the tampered DHCP response messages begins to always use the attacker-supplied default gateway since then.	- Vulnerability that the mutual authentication is not conducted for the communications between other systems and the MFP		✓
		- USB printer ports of the MFP, USB memory ports, and USB authentication unit ports are transmitted via TCP/IP, and extended to the remote locations. However, because the communications are not protected, an attacker interferes to tamper with the job data and the number of prints that always print one extra copy, so confidential documents are leaked.	- Vulnerability due to unprotected communications between other systems and the MFP, or that the protection is imperfect		✓
		- An attacker decrypts the WEP key of the wireless LAN used by the MFP, and interferes with the MFP communications of the external shared address servers that are not protected. Then, the attacker adds him/herself to the group addresses to receive the copies of the files that are sent to the specific group by the MFP, so confidential documents are leaked.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators (insufficient awareness on the encryption strength)	✓	
		- The MFP was not isolated on the network because either the MFP was connected to the wrong VLAN, or IPsec configuration was wrong. It was connected to the same network as that of general users, resulting in the tampering with unprotected communications.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators (network cable connection or incorrect settings)	✓	
3. Availability	- The MFP becomes disabled due to the theft of communication device, wire cuts or theft, or terminal disconnection. - The MFP is no longer available, because the communication devices stop working. - Communication with the MFP or communication between the MFP and other systems is not available due to the incorrect configuration of the communication systems. (Communication devices include DNS, DHCP, and NTP.)	- As a result of disconnecting the Ethernet cable that was connected to the MFP, an attacker stopped the MFP services which do not require communication.	- Vulnerability that the MFP is disabled without the communication system		✓
		- The MFP services, which do not require communication, stopped, due to the defect of the switching hub or wireless LAN access point.			
		- The MFP cannot provide services due to wrong configuration of the VLAN, IPsec, or VPN, or the MFP is not connected to the specific VLAN ports or specific Ethernet ports.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators (network cable connection or incorrect settings)	✓	

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
4. Authenticity	- The device of the communication partner cannot be verified as to whether it is specified by the prescribed security requirements or not. (Communication devices include DNS, DHCP, and NTP.)	- Communication with the NTP servers used by the dozens of MFPs is not authenticated, which allows accesses by fake NTP servers.	- Vulnerability that the mutual authentication is not conducted for the communications between other systems and the MFP		✓
		- Fake host name information is mixed in the responses from the DNS servers, which leads to fake hosts when files are written in the external shared folders of the MFP.			
		- IP addresses of fake DNS servers are injected from the fake DHCP.			
5. Accountability	- The devices used for communication with the fake source addresses cannot be specified. (Communication devices include DNS, DHCP, and NTP.)	- There is a phenomenon that the time of the MFP varies greatly, but whether it is a defect of the NTP server is unknown because there is no record.	- Vulnerability that the MFP does not record IP address configuration, which is set up on the communication system, as a history on the MFP		✓
		- Fake IP addresses are injected into the MFP, but from which DHCP server cannot be identified to take a countermeasure.			
		- It contains data to attack vulnerabilities in the DNS responses, but which host injected or responded cannot be identified, because there is no record.			
6. Non-repudiation	- Even if there is a record of an address that specifies the communication partner, it cannot be proved when an administrator of the other side of the system denies it. (Communication devices include DNS, DHCP, and NTP.)	- Although the communication record contains user IDs, it is disabled as a proof, because arbitrary user IDs can be input.	- Vulnerability that user IDs are recorded in the communication record, but such user IDs can be tampered		✓
		- Because the communication record is injectable from any hosts, records by attackers are mixed, and the cause of the defect cannot be specified.			
		- Because it is possible to impersonate other hosts using the group key that is used between the communication partners connected by IPsec, the user terminal assumed to be attacked from the connection record cannot be identified.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	
7. Reliability	- Proper operation cannot be implemented, because data sent through the communication system is confused with other data, or a portion of the data received is missing. (Communication devices include DNS, DHCP, and NTP.)	- If the loading of the communication systems exceeds the capacity, IP packet loss generates. Consequently, the MFP performs the retransmission processing, but a race condition or a resource shortage occurs because the processing load increases in the MFP. The process can be interrupted or remain incomplete while still processing.	- Vulnerability due to race conditions or a resource shortage		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
7. Reliability	- Proper operation cannot be implemented, because data sent through the communication system is confused with other data, or a portion of the data received is missing. (Communication devices include DNS, DHCP, and NTP.)	- An attacker sends complex multi-type requests to the DNS, DHCP, and NTP servers. However, the MFP cannot receive appropriate responses because some packets or response messages are either missing or changed due to race conditions in the servers.	- Vulnerability on other systems	✓	
		- An attacker intrudes any of the DNS, DHCP or NTP servers by taking advantages of known vulnerabilities to execute arbitrary codes. The MFP either cannot receive appropriate responses, or the above-mentioned servers attack the other related systems, such as the MFP.			

6.16 Remote management system

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	[During the use of remote management functions] - The use of the unauthorized remote management functions. - Shared files with confidential information and multiple addresses stored inside the MFP are leaked via remote management functions. [Remote management system itself] - External address book and the backup data are leaked to attackers by attacking the management systems.	- An attacker wiretaps the unprotected communication among communications that send and receive address books of the MFP, and the contents of the address books are leaked to the attacker: registration and update of the address books; backups of the address books; address book synchronization for defining single fax delivery, mail delivery, and server delivery; address book synchronization for defining multiple delivery processing; and references of address books for control from other systems.	- Vulnerability due to unprotected communications between other systems and the MFP, or that the protection is imperfect		✓
		- An attacker intrudes using vulnerabilities on the configuration management servers or imposes on requests, and obtains the same data as the address book used on the MFP or the backup data of the MFP that are stored on other systems	- Vulnerability of the other systems	✓	
		- An attacker intrudes any of the management servers, authentication servers, or audit servers by taking advantages of known vulnerabilities to execute arbitrary codes. The MFP either cannot receive appropriate responses or the above-mentioned servers attack the other related systems, such as the MFP.			

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
2. Integrity	[During the use of remote management functions] - Addresses that are input or retrieved to/from the MFP, and the configuration information, are tampered. [Remote management system itself] - Configuration information of the external management systems is tampered, and the MFP behaves unexpectedly. - Parts of the authentication servers are changed, or parts of the authentication data are tampered to disable services.	- An attacker interferes with the communications between the MFP and the maintenance terminals or administrator terminals by using the ARP impersonation on the communications paths. The attacker then tampers with the addresses that are input into the MFP to add attacker's own address, and continues to wiretap confidential documents.	- Vulnerability due to unprotected communications between other systems and the MFP, or that the protection is imperfect		✓
		- Interface ports to perform remote maintenance of the MFP should be closed by default, but are open. An attacker connects to the ports to exploit the remote maintenance function.	- Vulnerability that the API or parts of the remote service interfaces of the MFP still have the API running, which can be executed by the commands with administrator privilege.		✓
		- By exploiting the CSRF vulnerability of the remote backup functions of the MFP, an attacker causes the web browser of administrators or maintenance personnel to open the specific URL, and performs arbitrary administrative functions.	- Vulnerability that the CSRF attacks against the terminal browsers of administrators and maintenance personnel are successful		✓
3. Availability	[During the use of remote management functions] - Destroyed settings are input into the MFP by an attacker, and either the MFP becomes unavailable or defects. [Remote management system itself] - Responses of the authentication servers stop, and the MFP becomes unavailable. - Responses of the audit servers stop, and the operational information becomes unavailable. - Responses of the configuration management servers stop, and the new addresses are no longer added. Address book research becomes unavailable.	- An attacker tampers with the messages of the configuration change instructions to the MFP from the unprotected configuration systems, and the destroyed configuration data is registered with the MFP, which causes either the MFP to stop or certain function to become unavailable.	- Vulnerability due to unprotected communications between other systems and the MFP, or that the protection is imperfect		✓
		- An attacker impersonates a user terminal to access the remote management interfaces of the MFP, and attempts authentication many times using IDs and passwords. Then, the authentication server for the MFP detects the consecutive login failures, and prohibits the administrator login for a while (a few minutes). By performing this task continuously, other management functions of the MFP are disabled.	- Vulnerability that a function to reject login by administrators is exploited when the authentications continue to fail		
		- An attacker prevents the collection of the operational information of the MFP by taking advantage of the vulnerability of the monitoring server to stop the monitoring server.	- Vulnerability of the remote management systems (in cases of the remote management system prepared by developers)		✓
		- An attacker prevents the address selection on the MFP by taking advantage of the vulnerability of the configuration management server, and by deleting the shared address books to synchronize the MFP with empty address books.			

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
4. Authenticity	[During the use of remote management functions] - The authentication request responses, address book responses, configuration setting change requests, and maintenance requests from remote management systems are not from the authorized remote management systems. [Remote management system itself] - Whether some management servers and authentication servers handle the requests to the specific MFP correctly cannot be confirmed.	- Either using the authentication servers that are correct or the systems that are not verified by the MFP, an attacker prepares a fake authentication server to communicate with the MFP to exploit the MFP by making another malicious terminal impersonate a user.	- Vulnerability that the mutual authentication is not conducted between remote management systems and the MFP		✓
		- An attacker impersonates a monitoring server of the MFP, and sends a large number of monitoring request messages to the MFP to overload the MFP.	- Vulnerability due to unprotected communication between the remote administrative systems and the MFP - Vulnerability that the mutual authentication is not conducted between remote management systems and the MFP		✓ ✓
		- An attacker makes an administrator open the specific URL, conducts CSRF attacks against usage terminals of the administrator to make the administrator obtain backup data of the MFP and forward to the attacker-supplied folders that can be obtained by fraud, and the attacker obtains the backup data of the MFP.	- Vulnerability that the CSRF attacks against the terminal browsers of administrators and maintenance personnel are successful (It is not examined that requests for important operations and functions have associations with the information specific to the previous operation in the stateless communication (HTTP, etc.) after the authentication between the MFP and other systems.)		✓
		- An attacker tampers with response messages to the MFP from the address book server on the communications paths, and changes the address with the attacker's address to obtain confidential documents.	- Vulnerability due to unprotected communication between remote administrative system and the MFP, or that the protection is imperfect		✓
		- An attacker hijacks the control of the authentication server to execute arbitrary codes by taking advantage of the known vulnerabilities, and makes it response that the authentication of the remote management system required by the MFP is all correct. As a result, the MFP accepts the connections from the fake management servers.	- Vulnerability of the authentication servers (in cases of the remote management system prepared by developers)		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
5.Accountability	[During the use of remote management functions] - Requested processes by the MFP from remote management systems or responses from remote management systems, are supposed to be recorded inside the MFP, but are not. [Remote management system itself] - Investigation cannot be conducted when there is a defect, because the history that remote management systems requested, as to which MFP, and the results as well as failure reasons, are not recorded with the remote management systems.	- Because the history of communications to the address book was neither recorded in the MFP nor in the address book server, it was unknown that an attacker searched for and requested the address book data externally to retrieve it, and sold it to outside contractors. .	- Vulnerability that the communication history is not recorded between remote administrative systems and the MFP		✓
		- There is a missing piece in the monitoring server records, but there was no time described in the communication history with the remote management system. Because the type of processing that was conducted by the MFP during the period without monitoring records cannot be specified, no measures are taken.	- Vulnerability that the communication history with remote management systems does not record any of the times, user IDs, or operation types		✓
		- A request is made to the MFP from the configuration server, which performs configuration changes with the administrator privilege, but the request is not found in the MFP. When and what requests are sent by the configuration server cannot be confirmed, because there is no history in the configuration server, so no measures can be taken.	- Vulnerability that the communication history is not recorded in remote administrative systems		✓
6. Non-repudiation	[During the use of remote management functions] - When requests are made from remote management systems, it cannot be proved that the names of the authentication servers, monitoring servers, and management servers are not tampered or impersonated. [Remote management system itself] - When requests made by some MFPs to other MFPs from the remote management system are recorded, it cannot be proved that the names of the hosts and the user IDs are not tampered or impersonated.	- There was a record of using the management functions of the MFP via remote management system that an administrator illegally takes out the backup data inside the MFP. However, an attacker cannot be identified, because arbitrary value can be injected into the operational history inside the MFP, or there is a vulnerability of possible tampering.	- Vulnerability that the IP addresses of the remote management systems are recorded in the record of operations, but such IP addresses can be tampered		✓
		- There was a record in the remote monitoring system for the MFP that a specific MFP was performing normally. Because the state notification sent by an attacker is fake, the anomaly detection cannot send an alarm when it is attacked by the attacker (SNMP).	- Vulnerability that the remote administrative systems do not verify the validity of the MFP to be monitored		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
7. Reliability	[During the use of remote management functions] - The MFP cannot perform processing with remote management systems. - MFP cannot process the multiple requests from remote management systems in the order in which they are received, or by priorities, causing irregularity. - Not all the requests accepted are processed, and a part of them is not processed. Parts of the requests are replaced with other requests, or parts of the processing are redundantly processed. - Some requests that are accepted are processed repeatedly, and never stop. [Remote management system itself] - The MFP cannot perform processing due to defects in the remote management system itself. - Either the authentication servers accept user IDs mistakenly, or the MFP stops working, because parts of the passwords being processed are missing. - The results are unexpected, because monitoring servers monitor the wrong MFPs. - Appropriate addresses cannot be retrieved because of the missing address data in the shared server of address book, due to mishandling.	- When a URL that is in the email text sent by an attacker is opened on the browser of the administrator terminal, an unauthorized JavaScript code is executed. Then, the attacker copies all the address contents of the shared address book server that the administrator is logged in.	- Vulnerability that the CSRF attacks against the terminal browsers of administrators and maintenance personnel are successful		✓
		- When requests to the MFP become more than a certain number, the authentication responses from the authentication server to the MFP no longer can be properly handled, which give an unintentional privilege to a third party. An attacker takes advantage of this to obtain administrator privileges.	- Vulnerability that the configuration information is destroyed by changing settings of the same MFP by multiple users at the same time		✓
		- When a certain type of pending job data increases, the address to be deleted remains, because the instructions to be processed in the order of deletion and addition is reversed for making changes to the address book inside the MFP from the management server. Then, an attacker takes advantage of this to send fake messages to the other MFP users, because remaining addresses become outside of its control.	- Vulnerability related to race conditions and resource management		✓
		- During the processing of a large volume of job data, updating of the address book is interrupted due to a resource shortage in the MFP.			
		- Because the times inside the several MFPs are all different, it takes a few extra hours to confirm the completion of the distributed processing on multiple MFPs by the monitoring server.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	
		- Because an attacker intrudes the remote management systems by taking advantage of the vulnerability of the remote management system, the remote management system can no longer handle certain responses in the correct order, and the MFP does not work properly.	- Vulnerability of the remote management systems	✓	
		- An ID and password of a general user is leaked, while this general user has administrator privilege and uses the same ID and password as an administrator. An attacker connects remotely to the MFP as an administrator to retrieve all the configuration information, IDs, and passwords, and sells confidential documents and addresses while using them to attack other hosts.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	
		- Although the SNMP has monitored a certain MFP, the monitoring is no longer available because it became undefined value after the byte counter of job data is flooded with 32 bits, or because the comparison is not possible due to packet data volume that is also counted with the job data volume.	- Vulnerability that the state value of the MFP that responds with SNMP is wrong (wrong measurement methods, measuring object and the response target value are changed, improper numeric conversions and type conversion)		✓

6.17 User terminal

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- IDs and passwords for the authentication that are stored in the driver software executed on the user terminals are leaked. - Because spool files stored in the user terminals are not protected, the documents and addresses in the spool files are leaked. - The MFP model and addresses are identified through the regular state confirmation query to the MFP from the user terminals.	- By the cross-site request forgery attack against user terminals, it makes users print, fax, or deliver the documents with the transmission history of the users to arbitrary addresses, and those documents are leaked to attackers.	- Vulnerability that it is not examined that requests for important operations and functions have associations with the information specific to the previous operation in the stateless communication (HTTP, etc.) after the authentication between the MFP and other systems)		✓
		- An attacker takes advantage of the vulnerabilities of the driver API for the MFP or SDK API for the MFP on the user terminal to execute arbitrary codes, and send copies of confidential documents to arbitrary addresses.	- Vulnerability of the driver software for the MFP provided by MFP vendors or the MFP SDK library (numerical processing, information leakage, input confirmation, security functions, race conditions, resource management) (print driver, fax driver, scan driver)		✓
		- An attacker manipulates the malware that is already running on the user terminals to obtain the addresses and passwords that are set up for the drivers for the MFP, or spool files that contain confidential documents.	- Vulnerability that digital certificates, IDs, and passwords are stored without any protection on the driver for the MFP of the user terminals		✓
		- An attacker wiretaps unprotected communications between the user terminals and the MFP, and retrieves the IP addresses, model, user IDs, and passwords of the MFP to prepare for attacks.	- Vulnerability due to unprotected communication between the MFP and other systems (other MFPs, user terminals, accumulation and external processing, remote management systems)		✓
		- The malware exploiting the vulnerability of the applications other than the MFP was running in the user terminals, and the copies of the files that were exchanged with the MFP, including the input and output of the scan and print, were transferred to the attacker.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	
2. Integrity	- The driver software that runs on the user terminals or the condition of the running software is tampered by attackers to execute arbitrary code. - Configuration information setup for the driver software that is stored in the user terminals and the authentication information are tampered. - Messages between the MFP and user terminals are tampered.	- An attacker takes advantage of the vulnerabilities of the driver API for the MFP or SDK API for the MFP on the user terminal to execute a code that attacks a certain vulnerability, takes control of user terminals, and tampers with the job data.	- Vulnerability of the driver software for the MFP provided by MFP vendors or the MFP SDK library (numerical processing, information leakage, input confirmation, security functions, race conditions, resource management) (print driver, fax driver, scan driver)		✓
		- An attacker infects user terminals with malware, rewrites the configuration information, IDs, and passwords of the driver for the MFP on the user terminals, and makes users send confidential documents to the attacker as well, which were supposed to be sent only to the MFP.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
2. Integrity		- Due to interference by fake ARP on the communications paths of the user terminals and the MFP, interference by fake wireless LAN, and interference by fake proxy server, an attacker tampers with the job data between the user terminals and the MFP, and sends copies of confidential documents to him/herself.	- Vulnerability due to unprotected communications between other systems and the MFP, or that the protection is imperfect		✓
		- The malware exploiting the vulnerability of the applications other than the MFP was running in the user terminals, and the copies of the print images were delivered to the attacker as well because the spool files at the time of printing have been tampered.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	
3. Availability	- The MFP is disabled because the driver software that is executed in the user terminals is either deleted or destroyed. - The MFP is disabled because configuration information setup for the driver software that is stored in the user terminals or authentication information is either deleted or tampered.	- The MFP is disabled because the driver for the MFP installed on the user terminal is already destroyed.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	
		- An attacker takes advantage of the vulnerabilities of the driver API for the MFP or SDK API for the MFP on the user terminal to terminate or go out of control of the user terminal, and disables the MFP.	- Vulnerability of the driver software for the MFP provided by MFP vendors or the MFP SDK library (numerical processing, information leakage, input confirmation, security functions, race conditions, resource management) (print driver, fax driver, scan driver) - Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	✓
		- The MFP is disabled because the user terminal has been intruded, and the driver for the MFP is deleted.			
		- The MFP is disabled because the user terminal has been intruded, and the setup information of the driver for the MFP is either deleted or destroyed.			
		- An attacker inserts the session completion messages to the sessions communicating between the MFP and the general user terminals to force quit the session (wireless LAN, TCP, SSL/TLS).	- Vulnerability due to unprotected communications between other systems and the MFP, or that the protection is imperfect		✓
		- An attacker sends a large number of requests to the service ports on the user terminals or service ports on the MFP, to stop the services.	- Vulnerability of race conditions or a resource shortage on the service ports for user terminals		✓
		- The malware exploiting the vulnerability of the applications other than the MFP was running on the user terminals, and when a certain MFP was used to print, the copies were transferred to an attacker because the printing was performed only for the specified MFP.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
4. Authenticity	- The driver software to be installed on the user terminals cannot be verified as to whether it is the right software for the MFP. - The user terminal that the driver software for the MFP to be installed on cannot be verified as to whether it is the right terminal to use the MFP.	- The driver software for the MFP installed on a user terminal comes with malware. Because there was no warning, the user continued to use it, and it caused the leakage of confidential documents.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	
		- A user terminal uses an unmodified OS with known vulnerabilities, and it was already infected with malware. The driver for the MFP was installed to allow the attack to stop services to the MFP.			
5. Accountability	- Whether the software in the user terminals is used by authorized users with the right procedure cannot be confirmed retroactively.	- A fake order instruction arrives at a company via fax with the name of the company as a sender, but the individual sender cannot be identified.	- Vulnerability that the user authentication is not conducted to use the MFP for faxing		✓
		- A large number of prints are output from the MFP, but the individual who performed the output cannot be identified.	- Vulnerability that there is no functions to record the authentication results of MFP users along with the operational history - Vulnerability that a function to record the authentication results of MFP users along with the operational history is not used	✓	✓
6.Non-repudiation	- It cannot be proved by showing evidence, regarding impossible tampering with the operational records recorded by the driver software and the processing records.	- When the driver processes the operation record every time the driver software is used on the OS of the user terminals, the information in the usage history is disabled because the operation record can be tampered, such as inputting an arbitrary character string to the operation record.	- Vulnerability that the host names of the user terminals are recorded for its operations, but such host names can be tampered		✓
		- The usage history recorded on the user terminals was not available because it was tampered by the malware infecting the user terminals.			
7. Reliability	- Applications related to the driver software of the user terminals either mistakes the data or causes data to go missing. - The control of the driver software is hijacked, and jobs are replaced as jobs of the different data and the different users.	- When the printing is executed that contains the specific data, the prints do not come out as expected, or confidential documents are leaked because other job data or printing files' contents are mixed in the printing results.	- Vulnerability of the driver software provided by MFP vendors (numerical processing, information leakage, input confirmation, security functions, race conditions, resource management) (printer driver, fax driver, scan driver)		✓
		- By taking advantage of the vulnerability of the printer driver, an attacker hijacks the control of the printer driver to rewrite the printer driver settings, and sends duplicates of the print to the attacker as well when the printing is executed, so confidential documents are continuously leaked.			

6.18 Accumulation and external processing (Spooler, shared folders, emails, other business systems)

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- Documents are leaked by wiretapping on the communications paths, because the communication conducted by the accumulation and external processing servers is not protected. - Confidential documents that are retrieved from other systems by the MFP for the specific processing are leaked on the MFP. - Confidential documents are leaked on the accumulation and external processing servers (servers for accumulating documents, proxy servers, or content converting servers).	- An attacker wiretaps the unprotected communications between the MFP and accumulation and external processing servers to obtain the job data that contains confidential documents. The attacker sells the obtained data, and the confidential information is leaked.	- Vulnerability due to unprotected communication between other systems and the MFP, or that the protection is imperfect		✓
		- When documents are delivered to multiple destinations at the same time, part of the communication to deliver to some MFPs is not protected, because multiple MFP models and multiple MFP vendors are used. An attacker wiretaps only unprotected communications and confidential documents are leaked.			
		- Some general users are able to view unauthorized files in a shared folder outside of the MFP if they make delivery requests on the MFP, causing the leakage of confidential documents to outsiders.	- Vulnerability that there is a difference in attributes of authors or privileges of files between the MFP and other systems	✓	
		- On a website, image data scanned on the MFP is always stored in the specific public folders of the external shared folder, so someone may mistakenly replaces them with materials that have similar document names to cause the leakage of confidential documents to unauthorized persons.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators - Vulnerability of complex setting conditions which lead to erroneous operations, as well as confusing results	✓	✓
		- When documents are delivered to multiple destinations at the same time, functions are misused, such as delivery, confidential, box, send, print, mail, server transmission, and URL transmission, because the terminology varies depending on MFP vendors while MFPs of multiple MFP vendors are used. It causes unnecessary printing, or copying of documents to the improper servers, so confidential documents are leaked to outsiders.			
		- An attacker intrudes in the spool servers where the job data to the MFP is accumulated, and copies such job data for him/herself to obtain confidential information that is contained in the job data.	- Vulnerability of the other systems	✓	
2. Integrity	- Documents or addresses are leaked on the accumulation and external processing servers (servers for accumulating documents, proxy servers, or content converting servers).	- An attacker interferes with the unprotected communications between the MFP and the accumulation and external processing servers, tampers with the job data that contains confidential documents, and makes the support center send new passwords to users to obtain confidential documents.	- Vulnerability due to unprotected communications between other systems and the MFP, or that the protection is imperfect		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
2. Integrity	- Documents or addresses are leaked on the accumulation and external processing servers (servers for accumulating documents, proxy servers, or content converting servers).	- An attacker impersonates an accumulation and external processing server, which returns fake temporary responses to the MFP. The MFP redirects and connects to the fake accumulation and external processing server that is prepared by the attacker.	- Vulnerability due to unprotected communications between other systems and the MFP, or that the protection is imperfect		✓
		- On the spool servers or file servers that store scan results, the job data or scan result files are stored in the rewritable public folders without authentication, so the attacker can delete all of them.	- Vulnerability of the security policy leakage or insufficient awareness on security policy among administrators	✓	
		- An attacker intrudes in the spool servers by exploiting the vulnerability of the spool servers that the job data is intensively input to the MFP, and tampers with the job data that contains confidential information.	- Vulnerability of the other systems	✓	
3. Availability	- Accumulation and external processing servers either stop or defect by termination, defect, or hijacking of the MFP. - Accumulation and external processing servers stop, causing the MFP is disabled to the users.	- An attacker performs fuzzing test against the ports that the MFP communicates with accumulation and external processing servers, and creates messages that intrude against the specific vulnerability to send it to the specific MFP using malware infected with general PCs. The MFP that received such messages either stops or defects, so it is disabled.	- Vulnerability that the MFP specifies the hosts or servers that connect to the ports to communicate with accumulation and external processing servers, but no restrictions apply - Vulnerability of unprotected communication between the MFP and the accumulation and external processing servers - Vulnerability that the mutual authentication is not conducted between the MFP and the accumulation and external processing servers - Vulnerability of the MFP that stops or defects if it receives unexpected data through the communication ports of other systems		✓ ✓ ✓ ✓
		- An attacker inserts messages, such as “communication completed” or “message ends,” by impersonating against the specific sessions between the MFP and the accumulation and external processing server to abnormally terminate the sessions.			
		- An attacker inputs a large volume of job data that permits load distribution processing to the MFP that has a load distribution configuration. It disables multiple MFPs at the same time, including the MFP to be load distributed.	- Vulnerability that cannot restrict the processing demand to its acceptable capacity - Vulnerability that no restrictions set on the processing demand to its acceptable capacity	 ✓	✓
		- An attacker stops the shared file servers by taking advantage of the vulnerability of the shared file servers, and disables the MFP scanner function as well as the fax delivery function for the file forwarding via the shared file servers.	- Vulnerability of the accumulation and external processing servers	✓	

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
4. Authenticity	- Documents and addresses are sent/received between the MFP and fake accumulation and external processing servers.	- Confidential documents are leaked to attackers because digital files are stored in the fake shared file server that the attacker has operated.	- Vulnerability that the mutual authentication is not conducted between the MFP and the accumulation and external processing servers		✓
		- A fax mail was sent to the MFP via the fake mail server that an attacker has operated, and a user sent money to the wrong account after receiving a fake billing fax impersonating an sender.	- Vulnerability that there is no mutual authentication configuration between the MFP and the accumulation and external processing servers	✓	
5.Accountability	- A server that transfers the data processed by the specific accumulation and external processing servers cannot be confirmed. The cause of the defects cannot be identified. - Whether the correct route is used for communication cannot be confirmed.	- There is no record in the MFP when an attacker sends fake delivery requests to the MFP by taking advantage of a vulnerability of a certain mail server, so no measures are taken because the mail server used for the attack is not identified.	- Vulnerability that the communication history with the accumulation and external processing servers is not recorded.		✓
			- Vulnerability of the accumulation and external processing servers	✓	
		- For communication between the accumulation and external processing servers and the MFP, there was a large number of communication history of authentication failures recorded. Because the host name of the communication partner was forged on the DNS server, the server could not be identified from the host name.	- Vulnerability that the host names that are reversed can be forged in the DNS, among those obtained from the communication history recorded on the MFP with user terminals	✓	
6. Non-repudiation	- The certainty of the information that identifies the server cannot be proved by showing evidence, regarding the processing records of a specific accumulation and external processing server.	- IP addresses are recorded at the time of authentication in the transfer records with the accumulation and external processing servers. However, an attacker can use non-recorded IP addresses to make attacks using the session information, because services can be used from other IP addresses.	- Vulnerability that the IP addresses of accumulation and external processing servers are recorded for the operational history, but such IP addresses can be tampered		✓
		- The data in the transfer records between the accumulation and external processing servers and the MFP is found to be tampered by SQL injection, so it is disabled to investigate causes.			
		- During the multi-stage delivery using the fax relay function, it shall be ensured that the unauthorized fax is not relaying in the middle of the transmission , but some items in the communication record that show from where the incoming fax calls came are missing in the second stage of mail faxing, so its route cannot be confirmed.	- Vulnerability that the communication history with the accumulation and external processing servers is not recorded.		✓
			- Vulnerability that the communication history with the accumulation and external processing servers does not contain enough records		✓

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
7. Reliability	- Job data that the MFP received from accumulation and external processing servers is corrupted. - Job data that is sent from the MFP to accumulation and external processing servers is neither correctly saved nor processed.	- An attacker impersonates the specific operation server to the MFP, and returns fake response messages. An SQL injection is used to the fake HTTP response messages, and it destroys the database inside the MFP.	- Vulnerability that the SQL command can be entered due to insufficient examinations of the requests to the MFP - Vulnerability of unprotected communication between the MFP and the accumulation and external processing servers		✓ ✓
		- When the specific data acquisition requests to the specific business systems are sent from the MFP, either failure responses are returned, or session time-outs occur. However, the software inside the MFP repeats the processes until a success response is returned, which causes a resource shortage because multiple processes start up since then.	- Vulnerability of insufficient race conditions and resource management		✓
		- An attacker inputs processing requests to another MFP that are sent from the MFP for the load distribution, makes the spool server redirect again to input, and indefinitely makes the job data to be cyclically processed.	- Vulnerability that identification information is not confirmed, such as the destinations of job data - Vulnerability of unprotected communication between the MFP and the accumulation and external processing servers		✓ ✓
		- Fax images and scanned image files sent from the MFP are not saved properly and become unavailable, because external file servers are intruded by taking advantage of their vulnerabilities.	- Vulnerability of the accumulation and external processing servers	✓	

7. Detailed description of vulnerabilities

In this chapter, items that should be noted in particular are discussed in detail among the vulnerabilities related to the MFP listed in the previous chapter. Specifically, well-known attack methods that are open to the public and became topics in recent years, as well as the vulnerabilities that have been reported as actual cases, are described comprehensively.[14] Each description shows an overview, explanation, and measures for vulnerabilities. Specific attack methods related to the vulnerabilities are presented in the description. Measures are listed by users (mainly administrators), developers, and evaluators, and are intended to be the references for the vulnerabilities of the MFP from their own perspectives. "Evaluators," who are concerned parties seen in this chapter for the first time, are those who are in a position to confirm vulnerabilities of the MFPs, such as third parties to conduct vulnerability testing services of the MFPs and the persons in charge of the development vendors who conduct their own inspection of the security functions.

7.1 Assumptions about attacks

As mentioned in Section 1.5, the vulnerabilities related to the MFP described in this chapter are not necessarily applied to all the MFPs, but it is assumed that the MFP should have the functions concerned, and those functions should be available to operate.

The attacks in this report mean the acts for the purpose of tampering with or viewing by unauthorized users or unauthorized third parties to access protected assets defined in Chapter 5. For example, the following acts are considered to be attacks:

1) Third parties or users access to protected assets of other users.
2) Third parties or users access to unauthorized protected assets by using administrator functions or maintenance functions.
3) Third parties or users access to unauthorized protected assets by putting the MFP into an abnormal state.

On the other hand, accessing users' protected assets by maintenance personnel or administrators of the companies that introduced the MFP is possible by using privileges such as, for example, functions to initialize (change) passwords. However, the restrictions on these functions shall be addressed in the policies and provisions of the companies that have introduced the MFP or MFP vendors themselves. Therefore, for the operating conditions of the MFP, it is assumed in this report that the concerned parties who have privileges, such as administrators and maintenance personnel, perform appropriately. The security in the manufacturing and delivery of the MFP is also assumed to be assured. Manufacturing and delivery processes are discussed in Chapter 8.

7.2 Seriousness and attack potential evaluation

The values of the seriousness and attack potential evaluation that are described in the detailed description items refer to the results of the calculations using the CVSS calculation tool[15] for the accessibilities to the vulnerabilities described, and the attack potential required, respectively.

[14] Vulnerabilities related to the MFP listed on CVE (Common Vulnerabilities and Exposures Number) from January 2010 to July 2012 are all categorized in the items described in this report.
[15] http://jvndb.jvn.jp/cvss/ScoreCalc2.swf?lang=ja&g=1

In the CVSS 2.0 Base, chances of being attacked increase as the color becomes redder.

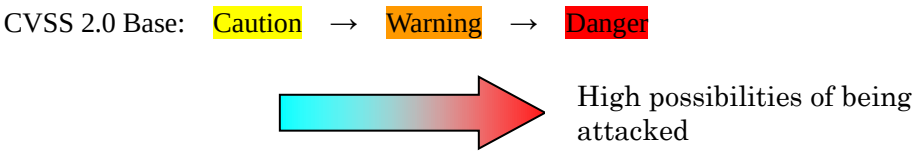


Figure 7-1 Attack potential diagram

Regarding the vulnerabilities in the following description, some vulnerabilities are not easily prevented in reality with measures only focusing on the MFP functions; such as the attacks described in "1. Confidentiality" in Section 6.3, which require advanced technique with limited chances; i.e., the operating MFP in a company is opened without anybody noticing it, and the RAM (volatile memory) is quickly cooled and is taken to a place with facilities that enable it to be used for attacks within a short time while the data is still available to analyze. Such vulnerabilities do not even appear on CVE, etc. This chapter, therefore, comprehensively describes the items that users, developers, and evaluators shall recognize and take measures for, and the items most likely to be attacked as real problems at the present time.

7.3 Problems with data protection of the storage media

The typical storage media that has been built into the MFP in recent years is the HDD. The MFP that is assumed to handle protected assets shall protect assets, such as temporarily stored confidential document data on the HDD, configuration information, and passwords of users and administrators that are permanently stored. On the other hand, an HDD that is built into an MFP is easy to view, and it usually can be removed or replaced. Therefore, even if an HDD falls into the hands of attackers, a mechanism that does not allow the leakage of data (protected assets) on the HDD is needed.

It is basic, but the full-spectrum encryption of the HDD is considered to be as secure as security measures for the protected assets stored on the HDD. The encryption of some data on the HDD and the lock using HDD passwords are known to be vulnerable. In recent years, however, there are no MFPs that are security-conscious, for example HDDs are protected only by locking passwords, among products of the Japanese MFP vendors.

7.3.1 [HDD encryption]

The first attack that shall be kept in mind is performed as an attacker removes the HDD from the MFP that has no full-spectrum encryption on the HDD to read the stored protected assets by connecting to PCs or other MFPs. This attack is easy for users who can access the MFP directly in the local environment. The risk of such attack is high, and the necessary attack potentials are low. In addition to the removal of the storage medium, such as an unencrypted HDD, etc., which is also scored in this section, the attacking procedures are discussed with the assumption that the HDD is implemented with encryption, since most MFPs are implemented with encrypted HDDs nowadays.

The measures for HDD encryption are also effective for the MFP that is implemented with the hibernation function (to hibernate). Because the protected assets in the volatile memory are temporarily deployed on the HDD, there is a possibility that such protected assets in the volatile memory (basically, attack on such assets is difficult) are leaked by removing the HDD in a hibernation state.

7.3.2 [Full-spectrum deletion at the time of disposal]

In cases when users return leased MFPs or dispose MFPs, it is desirable to bring back the conditions in which the data on the HDD cannot be recovered by performing the full-spectrum overwrite deletion of the contents of the HDD, which is built into the MFP. There are some overwrite deletion methods, such as Pentagon (DoD5220.22-M)[16] and The Gutmann overwrite method[17] that are said to make data recovery impossible. These methods have been actually introduced in the current MFPs. If an attacker obtains the MFP after its disposal, he/she would have to spend a very long time performing an attack. Even if it is encrypted by a computationally secure algorithm, it is desirable to perform a full-spectrum overwrite deletion of the storage medium in consideration of the leakage of keys and passwords to create keys.[18]

[16] http://www.usaid.gov/policy/ads/500/d522022m.pdf
[17] http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html
[18] In cases when the keys are created from the passwords entered by the users, such keys may be leaked by a dictionary attack, etc., performed over a long time.

7.3.3 [Attack methods and measures]

An attack in which a user (an attacker) removes a full-spectrum encrypted HDD from the MFP and replaces it with the HDD encrypted with his/her own key, is discussed in this section. Using this method, the protected assets recorded on the HDD of the MFP are stored in a format that the attacker can read which results in the loss of confidentiality of the protected assets.

To make this attack successful requires some conditions. A key to decrypt the existing HDD is not needed, but the attacker needs to set a key to decrypt the replaced HDD to the MFP. In cases when the decrypted data are exchanged between the MFP and the HDD, equipped with an encryption chip, an attacker can copy the MFP configuration information without anybody noticing that the HDD was replaced.[19] It is appropriate to establish the same settings as for an operating MFP, because it is impossible to read such configuration information on the encrypted HDD that is removed, when the configuration information is on the HDD. In such case, however, the attacker may need to have the same type of MFP. In cases of the MFPs that store the configuration information in the nonvolatile RAM instead of on the HDD, this preparation may not be necessary.

For measures against such attacks of replacing the HDD, functional measures, specifically, functions that uniquely identify and validate the HDD are effective. The information that can uniquely identify the HDD that has been used (the hash value of the unique identifier for the individual HDD) shall be kept on the HDD, and it is desirable to have an error but not to operate when the HDD is replaced. As long as the function for entering keys for the HDD decryption is not available to the users who will be the attackers (unless they are entered using the management or maintenance functions, etc.), the replaced HDD is no use.[20]

Supplement: Implementation of the right cryptographic algorithm

There are two matters that shall be considered for the encryption of an HDD. One is the encryption strength, specifically, the strength of the algorithms to be encrypted, key lengths, and keys. The other is the mechanism of the key management.

There are schemes to confirm the encryption strength, such as to confirm whether the cryptographic algorithm is correctly implemented or not. A cryptographic algorithm can be confirmed with CMVP based on FIPS140-2 by NIST (National Institute of Standards and Technology), and with “Japan Cryptographic Module Validation Program” by IPA. For example, users can check with the evaluation criteria to confirm whether the encryption mechanisms for the protected assets are validated under these schemes, or whether the implementation of the cryptographic algorithm is reliable or not. The strength of the keys when generating them can be verified using these schemes.

Supplement: Key management

For key management, keys would be stored eventually in plain text somewhere in the MFP, even in cases when the keys are managed by encryption using another key. Where the plain text key is stored, and how it is protected, become important. When the plain text key is stored in the RAM, etc., the possibility of the leakage of protected assets still remains. An effective means to store the key that should be kept confidential is believed to be the installation of a

[19] For example, DriveTrust, etc. of Seagate has an encryption chip on its HDD.
http://www.seagate.com/docs/pdf/whitepaper/TP564_DriveTrust_Oct06.pdf

[20] Later-mentioned vulnerabilities shall be considered related to the maintenance functions.

TPM.[21] The TPM has tamper-resistance, such as deleting the contents of the memory, when someone is trying to gain unauthorized access to the internal memory of the TPM.

Supplement: Storage of protected assets on removable media such as USB memory

In cases when the protected assets are stored on a removable medium, such as USB memory, it is desirable for users to ensure the security of the removable medium using the encryption function that is similar to that of the HDD. For example, in the case of USB memory, protected assets saved in USB memory when it is running are limited to the owner's USB memory. There is only a small chance of access by other users, but there is a strong possibility of losing the USB memory. It is required for users, who perform the operations to store the protected assets in the USB memory, to select the USB memory certified by CMVP or the "Japan Cryptographic Module Validation Program" and to have the operational policies as described above.

7.3.4 [Causes and discussion]

The use of generic products causes the removal of storage media, such as HDDs, because it is easy for attackers to visually recognize them. However, the removal of the products from the MFP is performed the same way as for appliances and server products, and is not limited to the MFP. Users shall take measures with such matters in their operations. Developers are required to implement the protection using encryption so that the existing protected assets are computationally secure and will not be read, and also to implement a proper management of the information for decryption of the encrypted data. On that basis, it is important to implement the necessary functions in response to the security level for the products by confirming measures against changing of HDD as described above, or reading the key information from the RAM.

[21] http://www.trustedcomputinggroup.org/developers/trusted_platform_module/

7.3.5 Measures

[Operation guide]

1) Enable the encryption function, or select the MFP that is implemented with the function.
2) Execute the full-spectrum deletion function on disposal/return. (Select the MFP that is implemented with the full-spectrum deletion function.)
3) Confirm the safety assurance of the keys and cryptographic algorithm used for encryption.
4) The PIN code[22] shall be appropriately managed in cases when the private keys are protected by the TPM, etc.
5) In cases when USB memory is used for protected assets storage, for example, select the certified products under CMVP or "Japan Cryptographic Module Validation Program."[23]

[Development guide]

6) Implement the full-spectrum encryption function on the HDD.
7) Implement with the full-spectrum overwrite deletion function for the storage area with protected assets in the MFP.
8) Implement (select) the mechanism of encryption that ensures safety.
9) Implement the validation function to detect unauthorized replacement for replaceable parts, such as HDDs, etc.

[Verification guide]

10) In cases when the HDD encrypted protection is evaluated, confirm the strength of the cryptographic algorithm and private keys, methods to generate keys, and the safety of the storage location.
11) If there is no verification on the HDD, confirm the input of code, etc. to decrypt the decryption keys of the HDD or their strength.

7.3.6 References

Date of publication	Source
March 2009	Unlocking of HDD passwords http://homepage3.nifty.com/3gatudo/hddlock.htm#hdd Article about HDD locking passwords can be reset with the DOS tool that is published
July 2008	Defeating Encrypted and Deniable File Systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications http://www.cs.washington.edu/research/security/truecrypt.pdf Examples of the existence of vulnerabilities in the encryption for only some limited area of the HDD
May 2012	CRYPTOGRAPHIC MODULE VALIDATION PROGRAM (CMVP) http://csrc.nist.gov/groups/STM/cmvp/index.html Description of CMVP based on FIPS140-2 in North America
August 2012	Japan Cryptographic Module Validation Program (JCMVP®) http://www.ipa.go.jp/security/jcmvp/index.html Description of "Japan Cryptographic Module Validation Program," by IPA
April 2009	Risk of hibernation http://www.st.rim.or.jp/~shio/winsec/hibernation/ Description of the risk related to handling data that is deployed on the HDD during hibernation

[22] A personal identification number that consists of several digits. PIN refers to Personal Identification Number.

[23] The certified products are listed in MODULE VALIDATION LISTS (http://csrc.nist.gov/groups/STM/cmvp/validation.html), and in Cryptographic Module Validation List (http://www.ipa.go.jp/security/jcmvp/val.html), respectively.

7.3.7 Seriousness and attack potential evaluation (reference value)

[Attack assumptions]

As a worst case scenario, MFPs that are stored on the HDD, where the protected assets containing configuration information are not encrypted, will be discussed. A removed HDD can be mounted easily on a PC equipped with a general-purpose OS in some cases, but the following is assumed for scoring:

- An attacker has the same type of MFP that he/she is attacking.
- Protected assets on the HDD are not deleted.
- The MFP is physically accessible.

[Scoring]

CVSS 2.0 Base value: 6.6 (Warning)

Attack source category	Exploitable locally only
Complexity of attack criteria	Low
Pre-attack authentication requirement	No authentication operation required
Confidentiality	Overall impact
Integrity	No impact
Availability	Overall impact

[Attack assumptions]

The attack discussed next is the leakage of protected assets that are stored on the HDD; as described above in the attack methods. It is caused by changing the encrypted HDD and collecting data from it after a certain period of time. In this case, again, an attacker possesses the same type of MFP that shall be used with the following assumptions:

- The MFP is physically accessible.
- Protected assets on the HDD are not deleted.
- The input of decryption keys of the HDD is open to users.
- The identification verification function of the HDD is not implemented on the MFP.

[Scoring]

CVSS 2.0 Base value: 4.4 (Warning)

Attack source category	Exploitable locally only
Complexity of attack criteria	Moderate
Pre-attack authentication requirement	No authentication operation required
Confidentiality	Partial impact
Integrity	Partial impact
Availability	Partial impact

7.4 Information leakage caused by equipped SSD

Traditionally, the MFP has a built-in HDD as a large capacity storage medium to store protected assets. Most MFPs take measures against the leakage of protected assets in such ways as by overwrite deletion of data and encryption, as described in Section 7.3, because of the risks of removal of HDDs by third parties or users, and the property that the deleted data is easily recovered.7.3

In recent years, the HDD has been replaced by the SSD for the higher-speed data access and the reduction of failure rate. Some MFPs have both a built-in HDD and SSD, and only the data that requires high-speed access is stored on the SSD. In either case, measures, such as SSD encryption or data deletion, are required as long as protected assets are stored on the SSD.

7.4.1 [Special features of SSD]

For the purpose of description, the SSD is defined in this report as shown in Figure 7-2, "Relationship between logical blocks and physical blocks."

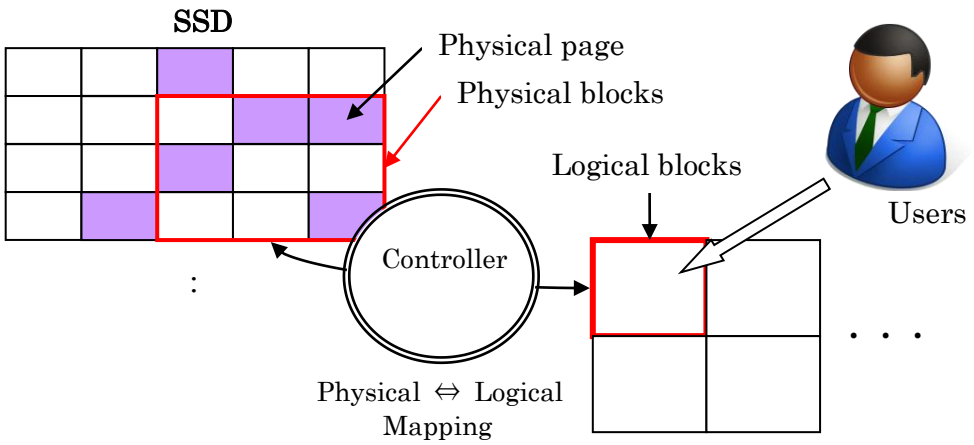


Figure 7-2 Relationship between logical blocks and physical blocks

The storage area of the SSD is divided into block/page unit. While the logic blocks are for users to access, the physical blocks are supported by the controller. Therefore, users cannot be aware of the physical area so that it is impossible to access any physical area. The supports vary depending on circumstances of the physical area. This is done in order to prevent only part of the blocks/pages from reaching the upper limit of the number of rewrites, which is a defect of the SSD, and is referred to as wear leveling function. In fact, the upper limit is a hundred thousand rewrites on the SLC chip, and ten thousand rewrites on the MLC chip of the SSD.

Taking into account the possibility that the SSD may be removed, the temporary saved data can be deleted in a manner similar to that used for HDDs by overwriting 3 times using the Pentagon method (DoD5220.22-M), or 35 times using the Gutmann method. In addition, it is extremely difficult to implement the overwrite deletion function of any physical area by block/page unit due to the wear leveling function as mentioned above.

7.4.2 [Attack methods and measures]

The removal of the SSD from the operating MFP, and the removal of the SSD from the disposed MFP or returned MFP are considered as attacks, as with the case of HDD.

As described above, it is difficult to implement the overwrite deletion function of any physical block/page unit due to the properties of the SSD. There is a strong possibility that the overwrite deletion function for temporary stored data is not implemented. On the other hand, the SSD built into the MFP is visually identifiable, and it can be confirmed that some MFPs are connected with standard connectors. In this case, it is possible to remove the SSD if the main unit of the MFP is accessible. Data encryption of the SSD is effective as a preventive measure against information leakage due to the SSD removal.

It is also effective to implement a full-spectrum overwrite deletion function in addition to the encryption against the leakage of protected assets at the time of disposal or return of the MFP. The physical area of an SSD cannot be accessed, but the SSD controller may be implemented with the full-spectrum deletion without being affected by the wear leveling function, because the SSD controller is implemented with the function to release (reset) the charge of all the physical areas and to reset it to the factory settings.

However, it has been reported that the function to release (reset) the charge to the controller is implemented by mistake in some SSDs.[24] If MFP vendors implement the full-spectrum deletion function, the selection of an appropriate SSD shall be considered as well.

As a feasible implementation of the MFP functions, encrypting of the SSD and resetting of the physical area at the time of MFP disposal or return are considered to be effective.

Supplement: Attackers' viewpoints

The property that any SSD physical blocks/pages are not accessible makes it difficult even for attackers to attack the data stored on the SSD. High technology is required to recover from the excess blocks some data that is logically deleted without using the overwrite deletion method, etc. (i.e., data on the excess blocks not visible via controller, even if it remains on the page physically), by accessing the physical pages/blocks bypassing the controller.

7.4.3 [Discussion]

One of the purposes for equipping the MFP with an SSD is to improve the access speed to the data, including protected assets. If this purpose is thought to be of great importance, the encryption that is an effective means of countermeasure may not be implemented in some cases. For the data on the excess blocks that remains due to the removal of logical data, it is said that high technology is needed to attack, so that no problems may occur. However, the data on the block that is supported logically and the data on the SSD that is not deleted can be accessed, as with the case of the data on the HDD. In cases when protected assets are stored on the SSD, the developers of the MFP vendors are required to use the encryption function when storing the data on the SSD.

[24] A team from the University of California, San Diego, reported at the 9th USENIX Conference on File and Storage Technologies in February 2011.

7.4.4 Measures

[Operation guide]

1) In cases when protected assets are stored on the SSD, enable the encryption function, or select the MFP that is implemented with the function.
2) In cases when protected assets are stored on the SSD, enable the full-spectrum deletion function on disposal/return, or select the MFP that is implemented with the function.
3) Confirm the safety assurance of the keys and cryptographic algorithm used for encryption.

[Development guide]

4) If the SSD and the HDD are used together, confidential information is assumed not to be stored on the SSD.
5) Implement the encryption function on the SSD.
6) Implement the full-spectrum deletion function on the SSD.
7) Select an SSD on which a full-spectrum encryption function is implemented correctly.
8) Implement (select) the mechanism of encryption that ensures safety.

* If the measure 4) is taken, other measures are not necessary.

[Verification guide]

9) By understanding the properties of the SSD, the verification shall be performed in accordance with the properties of the SSD. Attack potentials against excess blocks are always rated based on the latest information. In cases when attacks are possible, it is verified that the functions that the MFP is implemented with can be countered.

7.4.5 References

Date of publication	Source
February 2011	Reliably Erasing Data From Flash-Based Solid State Drives http://static.usenix.org/events/fast11/tech/full_papers/Wei.pdf Report of the SSD that is inappropriately implemented with the reset function
2011	NPO Institute of Digital Forensics Research Column http://www.digitalforensic.jp/expanel/diarypro/diary.cgi? no=399&continue=on Article on flash memory forensics
July 2011	Article on ITmedia Enterprise http://www.itmedia.co.jp/enterprise/articles/1107/16/news001.html Article on the means of data protection on the SSD
N/A	Intel SSD optimizer website http://www.intel.com/jp/consumer/Shop/diy/features/ssd/optimizer/p1.htm Article of special features of the SSD

7.4.6 Seriousness and attack potential evaluation (reference value)

[Attack assumptions]

Attacks by accessing the protected assets on the SSD built into the operating MFP are discussed here. It is assumed that the SSD is removed from the MFP in the same way as in the attack to the HDD. However, the scoring greatly differs between the protected assets that are in the excess block and are not logically supported, and other protected assets, due to the properties of the SSD (while the scoring for both types of protected assets is the same for the HDD). In this section, considering the properties of the SSD, the impact on confidentiality is assumed to be partial.

- An attacker has the same type of MFP that he/she is attacking.
- The MFP is physically accessible.
- The encryption function is not implemented on the SSD.

[Scoring]

CVSS 2.0 Base value: 5.4 (Warning)

Attack source category	Exploitable locally only
Complexity of attack criteria	Low
Pre-attack authentication requirement	No authentication operation required
Confidentiality	Partial impact
Integrity	No impact
Availability	Overall impact

7.5 Problems of access to local maintenance interfaces

There are maintenance interfaces in the MFP other than interfaces that can be accessed by users (general users and administrators, etc.). Maintenance interfaces are also categorized by local maintenance interfaces that are directly operated by the maintenance personnel at the main unit of the MFP, and the remote maintenance interfaces that are operated remotely by using http and other protocols. Vulnerabilities on the local maintenance interfaces are discussed in this section, in the light of information that has been published in recent years.[25]

7.5.1 [Functions of the local maintenance interfaces]

Main functions that are operable from the local maintenance interfaces are as follows:
- Checking toner and checking/resetting counter
- Settings (restrictions)/initialization of the MFP functions
- Settings/initialization of the administrator passwords
- Fine adjustments of the MFP functions and operations

If an attacker exploits the functions that can be manipulated from the maintenance interfaces, it is possible even for non-maintenance personnel to initialize the settings of the administrators, change users' authentication data as an administrator, and view and manipulate the protected assets. If the MFP is leased/rented and charges a fee, the billing information can be modified by changing the counter. In many MFPs, therefore, local maintenance interfaces are protected by means of special confidential operations and authentication with strong passwords, or by one of those.

7.5.2 [Attack methods and the impacts]

Some MFPs have special confidential operations as the means of protection for the local maintenance interfaces. Considering the costs of maintenance personnel, it is less likely that the operating procedures would vary by each MFP, and the same specific procedure may be applied by the product type or model number of vendors in some cases. In this case, the major assumption is that there will be no leakage of the operating procedures.

However, in fact, the special operating procedures used to access the maintenance interfaces of some MFPs (key operations by the operation panel of the MFP) have been published on some Q&A sites overseas, etc., and the actual MFP maintenance interfaces may be accessible by following the procedures published. That is to say, protections by the specific operation procedures will be lost at the point that those procedures were published. Besides, if an attacker uses such public information to contact the MFP, the attack would be extremely easy.

[25] Attacks by exploiting the firmware update function of the maintenance interfaces are described in Section 7.7, and web-based maintenance interfaces using the http protocol are described in Section 7.16.

1. The "TECH MODE" of the model name / model name

According to official sources from **vender name**, the brother of **model name**, the in the same way constructed **model name**, has a so-called "Tech Mode", where a service technician (or you!) can do some tests or adjust some additional settings.

1.1. Entering and leaving the "TECH MODE"

To enter the TECH MODE (or to leave it) ...

1. Press the [ ] key
2. on the keypad quickly enter [ ] [ ] [ ] [ ] [ ]

If the menu / display is configured to use a language different from English (e.g. German, French...) the display will change to the English language (*Ready* instead of *Bereit* etc.). There will also be a clock displayed instead of the zoom percentage values. In the end the display will look similar to this:

```
Ready
14: 32        TECH
```

To leave the TECH MODE just repeat the above mentioned procedure or just wait a moment, as the **model name** will leave TECH MODE automatically after some time. You will recognise this by the absence of TECH MODE in the display. If you normally use a different language for the display, the display will revert to the configured language after leaving TECH MODE.

Figure 7-3 Publicly available operations for entering maintenance mode

7.5.3 [Causes and discussion]

The direct cause of the attacks discussed in this section is that the procedures for access to the maintenance interfaces have been published. However, a fundamental problem lies in the implementation in that the means of protection of the maintenance interface relies on the "fixed key operation" that can be operated with administrator privileges as well. Maintenance interfaces require the same protection of passwords that are equivalent to the user interfaces as well as administrator interfaces.

It is unlikely, in a general sense, that multiple MFPs controlled by one maintenance person are managed with all different passwords. If a certain number of MFPs are managed by the same password, and the password is not updated, it is extremely vulnerable if such password is published as well as the above-mentioned specific operation procedures. It is confirmed from research that the input information considered to be passwords has actually been published in some cases.

To counter these vulnerabilities, the ideal operations are to use different passwords to access maintenance interfaces of each MFP. In addition, it is desirable to protect the MFP with stronger passwords than users' and administrators'. In cases when the same passwords or regular passwords are used for a certain number of MFPs, persons who know the special operating procedures and passwords (such as maintenance personnel) shall be specified. For perfect management, non-disclosure agreements, which would be effective on a permanent basis, and educational activities, etc., would be necessary. In addition, to limit the persons who have physical accessibility to the MFP to only personnel who can control could be a general measure against the leakage and tampering of the protected assets by external attackers. Even in

the case of having access restrictions, it is impossible to prevent attacks by authorized users who have physical access to the MFP.

Supplement: Examination of initial passwords

The vulnerabilities due to putting back factory settings that are similar to the attack technique against vulnerabilities described in this section are described in Section 7.6. The passwords of the maintenance interfaces may be reset to the fixed initial passwords by taking advantage of these vulnerabilities, even if the passwords are protected.

Supplement: Hidden interface

There may be other confidential "hidden interfaces" than the maintenance interfaces described in this section. For example, there would be interfaces that provide functions to confirm the contents of the memory and the specific access methods to the embedded OS which is installed for failure handling and debugging. It may require special handling that even maintenance personnel are not aware of, or connection to a special connector installed inside the MFP. In comparison to the maintenance interfaces that are described in this section, the risk that its existence and access procedures of the special interfaces only known to some developers are published, may be low. Developers shall still protect these interfaces assuming threats, including leakage, similar to those of the maintenance interfaces.[26]

7.5.4 Measures

[Operation guide]

1) The MFP that handles protected assets shall be checked with the protection mechanism of the maintenance interfaces at the time of selecting the MFP.

[Development guide]

2) The authentication strength of the maintenance interfaces shall be stronger than the one for users or administrators.
3) Hidden interfaces shall also be protected against the assumed threats.
4) For the maintenance interfaces and the hidden interfaces, a mechanism that does not use the same operations and passwords among multiple products shall be implemented.

[Verification guide]

5) The presence of interfaces and the fact that the operation procedures are confidential shall not be the security grounds.
6) Verify that the authentication strength of the maintenance interfaces is sufficient. In such case, the uniqueness and predictability of passwords shall be considered.

7.5.5 References

* Information is omitted in this section in consideration of the exploitation.

[26] An implementation, such that the debug screen is displayed on the user interfaces when an exception occurs, shall not be performed for security reasons.

7.5.6 Seriousness and attack potential evaluation (reference value)

[Attack assumptions]

The cases when a user attacks by using the access procedure to the local maintenance interfaces are assumed (obtaining protected assets of other users and administrators, or tampering with the counters related to billing, etc.).

- It shall be the model that does not take the above measures in the Development guide.
- The procedure for accessing the maintenance interfaces has been published.

[Scoring]

CVSS 2.0 Base value: 7.2 (Danger)

Attack source category	Exploitable locally only
Complexity of attack criteria	Low
Pre-attack authentication Requirement	No authentication operation required
Confidentiality	Overall impact
Integrity	Overall impact
Availability	Overall impact

7.6 Problems of resetting to the factory settings

Even for MFPs that handle protected assets, such as those based on the assumptions described in this report, there is a tendency in a factory default condition for convenience to be given priority, so the security of the protected assets is not considered in some cases. The convenience here refers to the conditions, namely, the use of the communications protocol described in Section 7.11 not being limited to the minimum, or strong passwords for users or administrators, etc., not being set up. Password settings of the factory settings may be also initialized to access the maintenance interfaces.

7.6.1 [Attack methods and the impacts]

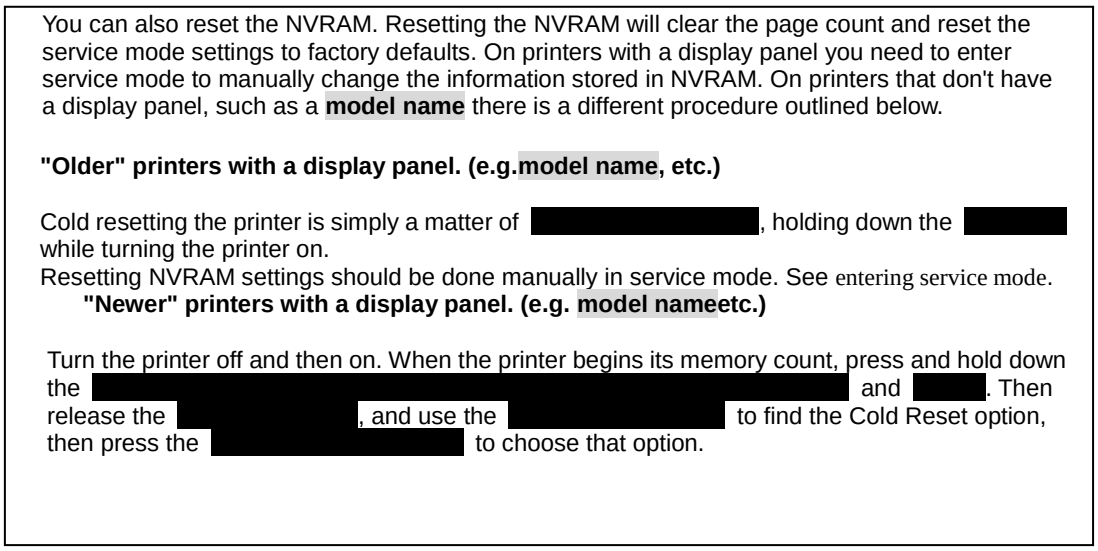
Attack by tampering with the settings of the MFP by resetting to the factory default settings is discussed. The following scenario can be considered as attacks against the integrity and confidentiality of the protected assets:

1) Figure out the basic configuration information of the MFP and the registered user IDs, etc.
2) Reset the MFP to the factory settings.
3) An attacker resets the basic configuration information to create a user account by impersonating an administrator.
4) Then, the attacker obtains the protected assets of each user stored in the MFP.

The basic configuration information of the above procedure 1) is the information that users usually know, such as IP addresses assigned to the MFP, etc. User IDs, etc., are the information that users, who can be attackers, can guess by checking the user IDs of others registered with the MFP. In addition to the integrity and the confidentiality of those assets, the availability of the protected assets will be lost at the time the configuration is reset to the factory settings.

Taking those into consideration, it is required that users cannot reset to the factory settings by themselves for the MFPs whose factory settings are not secure. In other words, a mechanism to protect the procedures to reset to the factory settings should be equivalent to, or stronger than, the authentication for users and administrators, or a mechanism to access the maintenance interfaces.

However, in reality, there are cases when users can reset to the factory settings using the special operation procedures in some MFPs. For example, information as shown in Figure 7-4 has been published.



You can also reset the NVRAM. Resetting the NVRAM will clear the page count and reset the service mode settings to factory defaults. On printers with a display panel you need to enter service mode to manually change the information stored in NVRAM. On printers that don't have a display panel, such as a **model name** there is a different procedure outlined below.

"Older" printers with a display panel. (e.g.model name, etc.)

Cold resetting the printer is simply a matter of [redacted], holding down the [redacted] while turning the printer on.
Resetting NVRAM settings should be done manually in service mode. See entering service mode.

"Newer" printers with a display panel. (e.g. model nameetc.)

Turn the printer off and then on. When the printer begins its memory count, press and hold down the [redacted] and [redacted]. Then release the [redacted], and use the [redacted] to find the Cold Reset option, then press the [redacted] to choose that option.

Figure 7-4 Published procedures for putting back the factory settings (overseas MFPs)

7.6.2 [Causes and discussion]

In such cases, even if the procedures that should be confidential have been published, they are not regarded as an attack method leading to information leakage, because the function to reset to the factory settings is considered to be one of the maintenance functions with the impact of clearing the settings and protected assets. However, in reality, once the attack is performed as described above, the risks are no longer overlooked, as the protected assets stored in the MFP afterwards would be exposed to attackers.

The general measure to this vulnerability is to disable the functions for users and for third parties to reset to the factory settings by making the authentication and usage restrictions more robust as with the case of the maintenance interfaces. For example, this measure could be easily realized only from the menu after connecting from the maintenance interfaces, by installing the function to reset to the factory settings. The assumption is that the maintenance interfaces are strongly protected.

As a countermeasure to reduce the impact when it is reset to the factory settings is to make the settings secure. This security by default performs only minimum services in the initial state, and such services shall be limited to the secure range of usage. The risk management of the operational side is given weight to expand the settings such that services are operated as necessary. This idea has an advantage in case things will turn out to be secure even if there is a configuration information leakage during the MFP installation.

Supplement: Status display

For the MFP that is assumed to be used in a secure environment, it is desirable to be secure by default. There may be some MFPs that are shipped with the general services activated for the convenience of users, in addition to usage in a secure environment. It is desirable that such MFPs be implemented with functions that enable users to identify the security status at a glance. It is also desirable that such MFPs are implemented with functions that can identify the settings status, such as the time of resetting to the factory settings, regardless of being secure by default.

7.6.3 Measures

[Operation guide]

1) An MFP that handles protected assets shall be checked with the function to reset to the factory settings at the time of selecting the MFP.
2) Make sure that the MFP is set to a secure state when using it.

[Development guide]

3) Place the function to reset to the factory settings in the menu of the maintenance function, to establish a strong proprietary authentication mechanism.
4) When implementing a proprietary authentication mechanism, the mechanism that does not use the same operations and passwords for multiple products shall be implemented.
5) If the MFP can be in a non-secure state by its settings, a mechanism by which users can identify the current security status shall be implemented.
6) Apply the concept of security by default for the MFPs that are assumed to be used in security-conscious environments.

[Verification guide]

7) Confirm that the authentication strength is sufficient until a function to reset to the factory settings is performed. In such case, the uniqueness and predictability of passwords shall also be considered.
8) Operate and examine all settings items that have an impact on security status by checking the indicator to determine if the security status and the actual MFP status do not differ from each other.

7.6.4 References

* Information is omitted in this section in consideration of the exploitation.

7.6.5 Seriousness and attack potential evaluation (reference value)

[Attack assumptions]

As described in the attack methods of this section, the attacks by unauthorized access against the protected assets that are stored after the attackers reset the MFP in accordance with the user environment, after resetting the factory settings from the operation panel of the MFP, are discussed here.

- It shall be the model that does not take the above measures in the development guide.

[Scoring]

CVSS 2.0 Base value: 5.9 (Warning)

Attack source category	Exploitable locally only
Complexity of attack criteria	Moderate
Pre-attack authentication requirement	No authentication operation required
Confidentiality	Partial impact
Integrity	Partial impact
Availability	Overall impact

7.7 Problems from exploiting the firmware update function

The MFP with the maintenance interfaces that provide maintenance functions via the intranet or external networks has a firmware update function in many cases as part of the maintenance functions. By using the firmware update function to update the unauthorized firmware and to operate the firmware, it is possible to induce unauthorized operations of the MFP and access to the protected assets.

In the article published in November 2011, the professors from Columbia University demonstrated that, it is possible to overheat the fixing roller of the MFP by exploiting the firmware update function and operating the unauthorized programs. Details of the attack methods presented in the article are described as follows:

7.7.1 [Attack methods and the impacts]

Step 1. Confirmation of the firmware updates

The procedures for firmware update vary depending on MFP models and vendors, but some MFP firmware updates have been published. Therefore, firmware updates are performed easily by following these procedures. For example, if keywords such as "remote firmware update LPR command" are used for search, the procedures for firmware update using the LPR can be found.

Remote firmware update by using the LPR command

NOTE: This remote firmware update method is for use in Windows 2000 Service Pack 3, Windows XP, Windows Server 2003, and Windows Server 2008.

Complete the following steps to update the firmware by using the LPR command.

1. From a command window, type the following:
   lpr -P -S -o l
   OR
   lpr -S -Pbinps
   where IPADDRESS can be either the TCP/IP address or the hostname of the product, and where FILENAME is the filename of the .RFU file.
   NOTE: The parameter (-o l) consists of a lowercase "O", not a zero, and a lowercase "L", not the numeral 1. This parameter sets the transport protocol to binary mode.
2. Press Enter on the keyboard. The messages described in the section Printer messages during the firmware update appear on the control panel.
3. The download process begins and the firmware is updated on the product. This can take several minutes.

Figure 7-5 Excerpt from the firmware update by using the LPR command

Step 2. Confirmation of the official firmware updates

First of all, official firmware should be prepared. Try to obtain the official firmware, suitable for the devices that can be attacked, from the links on the pages that are found above, or with the keywords such as "[vendor name] [model name] firmware download."

Once the firmware is obtained, binary data of the firmware can be modified to create unauthorized firmware.

For example, the later-mentioned "7.7.4 References: PRINT ME IF YOU DARE - Firmware update attack and the rise of printer malware -" introduces the binary information of the firmware, and they are the lists of the PJL commands in which their meaning can be read. Firmware is found out to be the 7M data according to the description of "@PJL UPGRADE SIZE=792990," and there is a description of the actual firmware data at the end of the "@PJL ENTER LANGUAGE=ACL <CR> <LF>." ACL stands for Advanced control language, and is a language used for the MFP firmware description. The important thing here is that the

firmware part has not been encrypted and is only being compressed. This indicates that firmware can be created as long as the syntax is figured out.

Step 3. Confirmation of the verification function of the MFP firmware

Most of the current MFPs have a function to verify the validity of files, using the encryption technology called electronic signature. The verification using an electronic signature creates private keys and signatures from the hash value of the firmware to confirm that the hash value uploaded to the MFP and the hash value created from the signatures are the same. Therefore, when an attacker who does not know the private keys tries to create unauthorized firmware, electronic signatures that can pass validation cannot be created due to the property that the hash values of the digital signature do not collide.

Some MFPs do not use the encryption technology, but perform only verification by the CRC check, etc. In fact, the following information was published as a guidance as of May 2012. In this model, firmware files can be uploaded once the CRC check is cleared because there is no other description of firmware errors found.

Control panel message	Description	Recommended action
CODE CRC ERROR	An error has occurred during a firmware upgrade.	1. Reinstall the firmware. 2. If the problem persists, contact **Vendor name** Support.

Figure 7-6 Public information of the firmware verification methods

Step 4. Confirmation of the unauthorized firmware

Up to Step 3, the method for uploading arbitrary firmware impersonating official firmware to the MFP is confirmed. After that step, if the firmware with arbitrary code embedded is created, it is possible to induce unauthorized behavior on the MFP and access to the protected assets by using some maintenance interfaces of the MFP. In the article, the reverse-engineering of the binary assembly was performed to understand the syntax by building different hardware, and the attack was successful. In addition to the costs for building hardware and debugging environments to analyze the MFP as a target of attack, several technologies, such as reverse-engineering or electrical circuits, may be required. If someone publishes the specific unauthorized MFP firmware, attacks can be conducted by using it.

The article claims that the fixing roller of the MFP can continue to be heated up using the unauthorized firmware.

Supplement: Developers' viewpoints

The MFP vendors who have pointed out the above problems have published on their websites about their thermal breakers designed to prevent overheating of the fixing roller, so they claim that there would be no problem. However, they do not deny possible unauthorized firmware rewriting, and commented that there would be no problem as long as the MFP is not connected to an external network without a firewall. This does not deny the possibility of findings that the vulnerabilities have an impact on the attacks from the internal networks where attackers are present.

All of the necessary ports for rewriting the firmware are not necessarily open, but many MFP web interfaces are published and can be found by searching in SHODAN or Google as of May 2012, which confirms that external access is possible.

7.7.2 [Causes and discussion]

The problem for the MFP is that the unauthorized firmware can be uploaded. The reasons are that the firmware upload function using the maintenance interface function only performs integrity checking of firmware data by CRC, and the binary of firmware to be updated is not encrypted. As described in the comments by the vendors in the supplement, the implementations that are described here may be sufficient if it is assumed that the maintenance interfaces that access from the internal networks cannot connect from the outside and all the users on the internal networks are reliable. For usage in real situations, however, it is desirable that the maintenance interfaces are robust enough against attacks from outside, because they are connected externally (via telephone line and WebDAV servers other than Ethernet). In cases when the encryption of the firmware to be updated is applied, it is necessary to consider the key management and cryptographic algorithms, as described in Section 7.3.3.

7.7.3 Measures

[Operation guide]

1) Terminate the maintenance interface via network, if it is not needed.
2) Use the MFP equipped with a strong verification function (electronic signature, etc.) for the firmware binary data that is updated.
3) Use the MFP equipped with an encryption function that uses secure algorithms for the firmware binary data that is updated.

* It is effective to terminate the maintenance interfaces via networks as a solution, but it would lose the convenience which is the original purpose of using the MFP. The selection of the devices that are implemented with the validation function by electronic signatures or encryption of firmware binary data, etc., could be the realistic measures. It is desirable to make it a condition to select MFPs that are implemented either with encryption or strong correctness verification.

[Development guide]

4) Provide a strong verification function (electronic signature, etc.) for the firmware binary data that is updated.
5) Provide an encryption function with secure algorithms for the firmware binary data to be updated. (Private keys used for encryption shall be securely managed).

* It is desirable to implement strong correctness verification in consideration of the availability of the MFP.

[Verification guide]

6) Confirm that the correctness verification function of the firmware binary data is not exploited by assumed attackers.
7) Confirm that the encryption function of the firmware binary data is appropriately implemented with a secure specification, and that the operation of the encryption function is a secure procedure, from the security perspectives in specifications, designs, development environments, and delivery/installation (including updating procedures). (It is also necessary to confirm that private keys are not leaked.)

7.7.4 References

Date of publication	Source
November 2011	Exclusive: Millions of printers open to devastating hack attack, researchers say http://redtape.msnbc.msn.com/_news/2011/11/29/9076395-exclusive-millions-of-printers-open-to-devastating-hack-attack-researchers-say Article about the vulnerabilities using the maintenance interfaces of the MFP, published by the professors from Columbia University
December 2011	CVE-2011-4161 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4161 The vulnerability information on the firmware update function of some MFPs of HP
December 2011	PRINT ME IF YOU DARE - Firmware update attack and the rise of printer malware - http://ids.cs.columbia.edu/sites/default/files/CuiPrintMeIfYouDare.pdf Materials describing the attack procedures published by the professors from Columbia University

7.7.5 Seriousness and attack potential evaluation (reference value)

[Attack assumptions]

This section limits attacks to those from neighboring networks as an attack category. In cases of security-conscious environments, update functions using the fax line are assumed to be dysfunctional, and the communications is controlled externally, such by a firewall. The following are assumptions:

- The firmware update function can be accessed without authentication.
- It shall be the model that does not take the above measures in the Development guide.

[Scoring]

CVSS 2.0 Base value: 7.9 (Danger)

* It will be 8.3 (Danger) when unauthorized firmware is published.

Attack source category	Possible attacks from neighboring networks
Complexity of attack criteria	Moderate
Pre-attack authentication requirement	No authentication operation required
Confidentiality	Overall impact
Integrity	Overall impact
Availability	Overall impact

7.8 Problems due to vulnerabilities of the embedded OS

Conveniently, quite a lot of MFP vendors have chosen the open-source embedded Linux (MontaVista, Wind River, Timesys, Denx etc.) in recent years because of the OS price and the convenience of development by open-source and the convenience of being able to add some functions. On the other hand, such introductions of multi-function built-in OS's can cause the security defects embedded in the MFP in some cases. Specifically the following: Risks of vulnerabilities of the development language functions such as buffer overflow that may be inherited from the results of development by the cross compiler on the PC, abuse of the services for remote operations by default (NFS, Tftpboot, Gdbserver, etc.), the possibility of leakage of, and tampering with, protected assets by taking advantage of the vulnerabilities of the embedded Linux or various installed applications and the possibility that the MFP will not work properly due to denial-of-service attack.

In this section, risks from the vulnerabilities of the embedded Linux or various applications that are installed, and the problems of usage under the default settings are pointed out.

7.8.1 [Attack methods and the impacts]

MontaVista has published widely the vulnerability information of their products on the website shown in the references. According to this vulnerability information, four vulnerabilities of MontaVista Linux (except for the Carrier Grade Edition) have been reported as of October 2012 as follows:

Table 7-1 Examples of vulnerabilities of the embedded Linux

CVE	Explanation[27]
CVE-2012-1165 (JVNDB-2012-001801)	The mime_param_cmpfunction in crypto/asn1/asn_mime.c of OpenSSL has vulnerabilities of becoming denial-of-service (NULL pointer dereference and application crash).
CVE-2012-0884 (JVNDB-2012-001735)	Vulnerability that the data to be decrypted readily exists, because the implementation of the PKCS #7 and Cryptographic Message Syntax (CMS) of OpenSSL does not properly restrict specific operations.
CVE-2012-0814 (JVNDB-2012-001739)	Vulnerability exists that the important information is obtained, because the auth_parse_options function of auth-options.c in the sshd of OpenSSH outputs debug messages, containing authorized_keys command options.
CVE-2012-0021 (JVNDB-2011-003659)	When the threaded MPM is used, vulnerability to be denial-of-service (daemon crash) exists because log_cookie function in mod_log_config.c located in the mod_log_config module of the Apache HTTP Server does not properly handle the character strings of %{}C format.

Above-mentioned CVE-2012-1165 and CVE-2012-0884 are the vulnerabilities related to the implementations of OpenSSL that are provided (supported) together with the embedded Linux (MontaVista Linux). In cases when the MFP introduced the embedded Linux has been used with the above-mentioned vulnerabilities left untouched, possible denial-of-service attacks as well as wiretapping of the communications data, etc., between the MFP and the client terminals, etc., may be performed.

In Wind River Linux, five vulnerabilities in version 3.1 and four vulnerabilities in version 3.0 are found in SecurityFocus due to the vulnerabilities of mainly Linux kernel. (Details are

[27] Excerpts of the vulnerability information from JVN iPedia (http://jvndb.jvn.jp)

described in the reference information.). By exploiting these vulnerabilities, there are possibilities that unauthorized access to the protected assets may be performed or that the MFP will not operate properly by the denial-of-service attacks.

In addition to the risks due to the vulnerabilities of the embedded Linux as described above, there may be possibilities that unnecessary network services are running on the MFP when the embedded Linux has been used by default settings without using the security settings, etc. In cases when there are vulnerabilities in the implementation of unnecessary network services, or appropriate security settings for the encryption and identity authentication, etc., are not performed, there are possibilities that the various risks on the information security, such as the leakage or tampering by unauthorized access to the protected assets, may occur.

Additionally, when the MFP starts up, it is confirmed that some models display the information about the OS, etc., on the panel. In cases such information (banner information) is exploited, there are possibilities that unauthorized access to the protected assets and information leaks, etc., may occur due to the attacks against vulnerabilities of the OS, etc.

7.8.2 [Causes and discussion]

In recent years, the embedded Linux has been introduced in a number of MFPs, because of low costs and its convenience of development that is the benefits of open source. While it has these benefits, there are possibilities that various risks to information security may occur, such as the leakage and tampering of the protected assets stored in the MFP by unauthorized access by attackers who exploit unnecessary services and the vulnerabilities of the applications that run on the MFP or on the embedded Linux.

To respond to the above-mentioned risks, developers need to take measures, such as applying security patches (or providing notifications and distributions to the users) as necessary according to the vulnerability information about the embedded OS (Linux) that has been introduced. In addition, because unnecessary services are possibly running, it is desirable to check the operation status and the vulnerabilities of the implementation using port scanners or vulnerability scanner, etc., before the product is released, as with the case of general Linux servers, etc.

7.8.3 Measures

[Operation guide]

1) The methods of applying security patches, etc., and the vulnerability information of the embedded OSs and applications that have been introduced to the MFP shall be confirmed with the MFP vendors.

[Development guide]

2) Thorough observations on the coding provisions that do not bring language vulnerabilities (buffer overflow, etc.) in the cross-compile environment shall be made.
3) Vulnerabilities of an embedded OS and the applications that run on it shall be confirmed, and if necessary, security patches shall be applied, or the function to counter vulnerability shall be implemented.
4) Check that unnecessary services, or the services whose vulnerabilities have been published, are not running, by using the system configuration information, the port scanners, or vulnerability scanners, etc., and terminate or delete such services as necessary.
5) Implement in such a manner that banner information of the OS or application (module) version that is running will only be presented when necessary.
6) Explain specifically the vulnerability information and applications of the security patches, etc., to users in the guidelines, etc.

[Verification guide]

7) Examine the presence or absence of vulnerabilities of the embedded OS and the applications that run on it, and whether they are executable or not.
8) Verify that unnecessary services, or the services whose vulnerabilities have been published, are not running, by using the system configuration information, the port scanners, or vulnerability scanners, etc.
9) Ensure that the means of notification of vulnerability information and applications of the security patches, etc., are clearly described in the users' guidelines, etc.

7.8.4 References

Date of publication	Source
Frequently updated	CVE Vulnerabilities List (MontaVista) http://www.mvista.com/cve_vulnerabilities.php Vulnerability information (CVE: Common Vulnerabilities and Exposures) of the products provided by MontaVista has been widely published
Frequently updated	SecurityFocus http://www.securityfocus.com/ Website of vulnerability information on products provided by various vendors
December 2009	Linux e1000 Driver 'Jumbo Frame' Handling Remote Security Bypass Vulnerability http://www.securityfocus.com/bid/37519 Examples of vulnerabilities related to Wind River Linux (circumvention of security functions)
March 2010	Linux Kernel Bluetooth Sysfs File Local Privilege Escalation Vulnerability http://www.securityfocus.com/bid/38898 Examples of vulnerabilities related to Wind River Linux (privilege escalation, denial-of-service attack)
January 2010	Linux Kernel 'ipv6_hop_jumbo()' Remote Denial-of-Service Vulnerability http://www.securityfocus.com/bid/37810 Examples of vulnerabilities related to Wind River Linux (denial-of-service attack)

7.8.5 Seriousness and attack potential evaluation (reference value)

[Attack assumptions]

A case is assumed that there are vulnerabilities that allow the embedded Linux to execute arbitrary code remotely (internal LAN), and the attack tools have been published, which invoke the shell that can take advantage of an OS administrator command of the MFP by using the vulnerability.

[Scoring]

CVSS 2.0 Base value: 8.3 (Danger)

Attack source category	Possible attacks from neighboring networks
Complexity of attack criteria	Low
Pre-attack authentication Requirement	No authentication operation required
Confidentiality	Overall impact
Integrity	Overall impact
Availability	Overall impact

7.9 Vulnerability related to SDK (Software Development Kit)

The SDK, described in this section, refers to the development environment of the applications that can be installed on the main unit of the MFP for enhancement of the MFP functions. For example, it is intended to customize user interfaces of the MFP operation panel that are attached to the MFP for the users' ease-of-use suitable for the usage environment. In addition to the user interfaces, the SDK has the following functions:

- Copying, printing and scanning
- Device configuration management and job management
- Network settings
- File and folder (box) operations, etc.

As mentioned above, functions equivalent to the built-in functions for users by default on the MFP can be used from the applications developed with the SDK. This indicates that the protected assets can be accessed by using the applications developed with the SDK. Therefore, among the applications developed by users using the SDK, only those applications, which are determined by the developers of the MFP vendors that they do not reduce the security functions of the main unit of MFP, can be added with the electronic signature by encrypting. Users install the files that are signed and encrypted by the developers of the MFP vendor onto the MFP. At that time, the main unit of the MFP verifies the signatures, and decrypts them.

7.9.1 [Attack methods and the impacts]

The "standard loader" requires signatures by MFP vendors on the files as described above, when the applications developed by users are uploaded to the MFP. Therefore, malicious application files are not uploaded.

However, the loaders published by a vendor in 2002 had a function that allows application upload without signature verification. It was considered not to be a problem if users do not introduce the "loader without signature verification," because the unauthorized applications would not be uploaded as long as there was no "loader without signature verification" introduced. However, attacks can succeed.

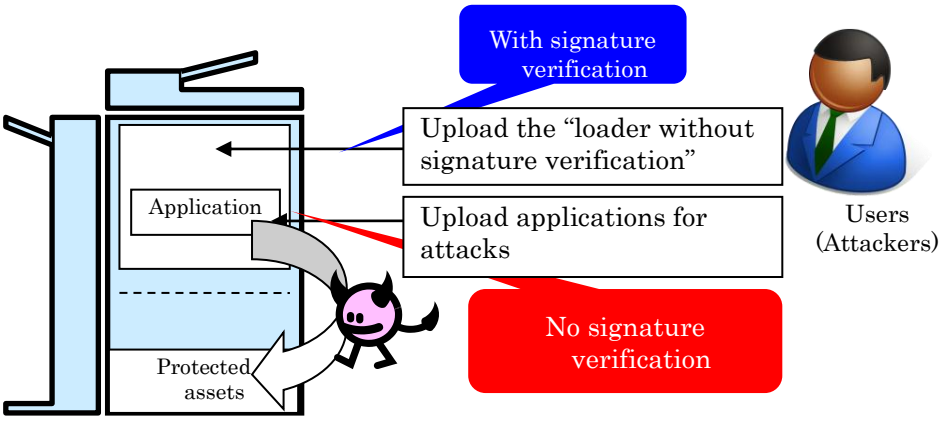


Figure 7-7 Unauthorized application installation using SDK

1) Upload the "loader without signature verification" using the "standard loader (loader with signature verification)."
2) Upload applications for attacks using the function of the "loader without signature verification."
3) Attack the protected assets using the function of applications for attacks.

7.9.2 [Causes and discussion]

The cause of the successful attacks is a fact that the "loader without signature verification" was officially published by the vendor. In other words, it was an application signed by the vendor. The "loader without signature verification" can be uploaded without any problem to the MFP that is not introduced with the "loader without signature verification," because the application is signed. Then, a maliciously created application was just uploaded according to the specifications of the SDK that provides file operation command, etc., using the function of the "loader without signature verification."

The "loader without signature verification" was considered to be an application published for the MFPs that do not handle protected assets. However, as a result of exploiting the application, the protection function that "applications that are not signed are not uploaded" was disabled. When the developers of the MFP vendors provide protection functions of the SDK, applications that are provided for those environments, where protected assets are not handled, should be managed in an integrated manner to prevent them from becoming a backdoor.

Supplement: Memory area protection breakthrough

In addition, the SDK protects the protected assets and the MFP with restriction to the memory area that can be accessed by the applications uploaded by using the SDK, such as Sandbox of Java. If one of the SDK libraries or functions has the parameters that cause buffer overflow, there is a possibility that the memory area is broken through, and the MFP operations and the protected assets can be attacked. In fact, the JRE has a report about the vulnerabilities caused by defects of the functions of the SDK.

Supplement: Protection of the applications developed by the users

It is necessary to consider the encryption that makes the applications created by users confidential. It is difficult to assume that different keys are used for each different MFP for encryption (decryption), considering the environment of the MFP. If the created applications are considered to be assets, users may want to check the encryption mechanism provided by the developers.

7.9.3 Measures

[Operation guide]

1) Confirm with the developers that protection functions, such as encryption and signatures provided by the SDK, meet the security policies of the users.
2) Operate the SDK by enabling the signature verification function. (The debug mode is used only in an environment where the SDK is developed).

[Development guide]

3) The assessment criteria for the applications to be signed shall be standardized, including applications for products whose security is not their concern.
4) Conduct a test of buffer overflow, etc., against all the libraries and functions provided for the SDK.

[Verification guide]

5) Verify that unauthorized application uploads cannot be made using the SDK.
6) Verify that vulnerabilities, such as buffer overflow, do not exist in the memory protection functions of the SDK.
7) Ensure that the functions that are provided by the SDK do not lower the security level of any of the original MFP functions.

7.9.4 References

Date of publication	Source
2003	MEAP technical description http://gijutsu.jbmia.or.jp/03kaisetu-canon.pdf MEAP functional overview and the description of the protection mechanism
July 2002	Vulnerability in ChaiVM EZloader http://en.securitylab.ru/notification/235126.php Article about EZloader that does not perform signature verification
January 2012	CVE-2012-0507 http://cve.mitre.org/cgi-bin/cvename.cgi? name=CVE-2012-0507 Vulnerability report on BOF of JVM that can exceed Sandbox limitations

7.9.5 Seriousness and attack potential evaluation (reference value)

[Attack assumptions]

When uploading the application, which can upload any other application described in this section, onto the MFP, it is assumed that the use of the upload function of the applications using the SDK generally is restricted to administrators. However, the cases when attackers break through the administrator authentication, are assumed here. The following statement is also an assumption:

- An attacker can use the development environment of the SDK.

[Scoring]

CVSS 2.0 Base value: 7.9 (Danger)

Attack source category	Possible attacks from neighboring networks
Complexity of attack criteria	Moderate
Pre-attack authentication requirement	No authentication operation required
Confidentiality	Overall impact
Integrity	Overall impact
Availability	Overall impact

7.10 Problems due to vulnerabilities of applications introduced to the user terminals

Applications[28] that are provided by MFP vendors and introduced to the user terminals have possible accessibility to the protected assets in the MFP. Even if the MFP is secure, it is considered that the protected assets are leaked from the vulnerabilities of the software provided for the user terminals. Developers shall provide to users the latest vulnerability information about the applications that are introduced into the user terminals, and users need to regularly check the vulnerability information such as CVN, etc., and conduct careful operations such as temporarily halting the application introduced to the user terminals when the vulnerability is published.

7.10.1 [Attack methods and the impacts]

For applications that are provided by MFP developers and introduced to the user terminals, there have been lots of vulnerabilities reported in recent years as shown in the references. Most of these vulnerabilities are not used to attack the main unit of the MFP directly, but allow the attacks on the user terminals where the applications are to be installed. In simple logic, protected assets on the user terminals (scan data or fax) before being sent to or after having been received from the MFP can be exposed to the threats of tampering and leakage, and protected assets in the MFP may be affected indirectly, if the administrator terminals are hijacked. Many of them may be caused by buffer overflow, but some applications with vulnerabilities to simpler attacks have been reported as well.

For example, by using a vulnerability of an application introduced into the user terminal, which was reported in August 2011 as described in the references below, an attacker can attack the user terminal with the application installed by taking the following steps:

Vulnerabilities used for the attacks are directory traversal with the SaveXML function of the application. Install the vbs and mof files in the system directory under Windows and use the mof file to execute the vbs file as follows: In order to install them, the following command should be executed to open the unauthorized web pages and files in the user terminals to be attacked.

```
- hoge.SaveXML("../../../../../WINDOWS/system32/hoge.vbs","UTF-8");
- hoge.SaveXML("../../../../../WINDOWS/system32/wbem/mof/hoge.mof","UTF-8");
```

Figure 7-8 Examples of files that are installed to attack user terminals

Execute any vbs file, which is set up by using the Windows Management Instrumentation service, using the mof file. Then, protected assets on the user terminals can be emailed, or a remote shell can be provided using the vbs file. Inspection codes have been published in the Exploit Database[29] of Metasploit that can be a reference for creating attack codes.

As a next step, attackers obtain information for accessing the main unit of the MFP by analyzing the applications on the hijacked user terminals, or by collecting the data.[30] Then, the attackers access the MFP as administrators or users to obtain protected assets on the MFP illegally, etc.

---

[28] Software products provided by MFP vendors that come with the MFPs, such as printer drivers, etc., or that can be downloaded from the Internet.

[29] http://dev.metasploit.com/redmine/projects/framework/repository/entry/modules/exploits/windows/browser/hp_easy_printer_care_xmlsimpleaccessor.rb

[30] For example, setting up packet analyzer or key loggers

7.10.2 [Causes and discussion]

For applications that are assumed to be used on the MFP which handle protected assets and that are intended to be introduced to the user terminals provided by the MFP vendors, it is required to ensure the security level of the applications so that the security level of the application will not be lowered by vulnerabilities. It is important to use the source code inspection tool[31] or review the source code manually, as is done for typical applications as measures, to prevent vulnerabilities from being mounted. Unlike the examination of the applications built into the MFP, the vulnerability testing of the printer driver is relatively easy for evaluators, because a debugger, such as gdb or Ollydbg, suitable for the execution environment can be used.

Supplement: Vulnerabilities of OS and applications for the user terminals developed by third parties

The above-mentioned attack methods can be used against the OS and applications developed by third parties. There is a possibility that the MFP and the applications provided by MFP vendors on the user terminals may be indirectly attacked by using the vulnerabilities of these applications. For example, even if there is no vulnerability caused by the application that was provided by a MFP vendor, and in cases when an attacker has acquired OS administrator privileges on the user terminal using the vulnerability of the OS, the user passwords to access the MFP may be leaked by performing debugging of the applications provided by the MFP vendor or embedding by keylogger, etc., as described earlier. What users should not confuse is that such vulnerabilities caused by the OS on the user terminals, other applications, and MFP management software created by third parties shall be dealt with by users during operations. In reality, more than 12 vulnerabilities[32] of iPrint Client[33] provided by Novell were published on CVE since 2011. Some of the vulnerabilities are high-risk, which causes arbitrary code executions.

---

[31] Source code review “Secure Programming Course C/C++” by IPA
http://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/c103.html

[32] CVE-2011-4186 CVE-2011-4185 CVE-2011-1708 CVE-2011-1707 CVE-2011-1706 CVE-2011-1705 CVE-2011-1704 CVE-2011-1703 CVE-2011-1702 CVE-2011-1701 CVE-2011-1700 CVE-2011-1699, etc.

[33] http://www.novell.com/ja-jp/documentation/nw6p/pdfdoc/iprntenu/iprntenu.pdf

7.10.3 Measures

[Operation guide]

1) When considering the applications that are introduced to terminals as interfaces to the protected assets, confirm that the applications provided by MFP vendors meet the policies of users.

* It should be noted that other software on the user terminals, in addition to the applications that are provided by MFP vendors, also need to be managed.

[Development guide]

2) When providing applications for user terminals, they have to be manageable with a security level equivalent to what is provided for the MFP.

[Verification guide]

3) Regarding applications that are provided by MFP vendors, it needs to be examined for their impact on the protected assets and examined as necessary.

7.10.4 References

Date of publication	Source
October 2011	Vulnerability of the MFP vendors' applications to be introduced to user terminals http://web.nvd.nist.gov/view/vuln/detail? vulnId=CVE-2011-3163 Vulnerabilities of the HP software from which the workflow-metadata information can be obtained
March 2011	Vulnerability of the MFP vendors' applications to be introduced to user terminals http://web.nvd.nist.gov/view/vuln/detail? vulnId=CVE-2011-0279 Vulnerability of the HP software that does not properly configure authentication settings of device templates
May 2010	Vulnerability of the MFP vendors' applications to be introduced to user terminals http://web.nvd.nist.gov/view/vuln/detail? vulnId=CVE-2010-1558 Vulnerability of the HP software that protected assets can be obtained by exploiting the e-mail function
August 2011	Vulnerability of the MFP vendors' applications to be introduced to user terminals http://web.nvd.nist.gov/view/vuln/detail? vulnId=CVE-2011-2404 Vulnerability of the HP software that protected assets can be obtained by exploiting the directory traversal
December 2010	Vulnerability of the MFP vendors' applications to be introduced to user terminals http://web.nvd.nist.gov/view/vuln/detail? vulnId=CVE-2010-3920 Vulnerability of Seiko Epson printer driver by the temporary unauthorized privilege

7.10.5 Seriousness and attack potential evaluation (reference value)

[Attack assumptions]

The case of the user terminal being hijacked using the vulnerability described in the attack methods is discussed in this section. The following are assumptions: In general, attacks on the MFP are conducted by exploiting the hijacked user terminals. In such a case, confidentiality, integrity and availability are all impacted overall. However, the procedure used until the user terminal is hijacked is discussed here.

- Protected assets shall be on the user terminal.

[Scoring]

CVSS 2.0 Base value: 4.3 (Warning)

Attack source category	Possible attacks from networks
Complexity of attack criteria	Moderate
Pre-attack authentication requirement	No authentication operation required
Confidentiality	Partial impact
Integrity	No impact
Availability	No impact

7.11 Problems due to vulnerabilities of many protocols

This section presents a comprehensive outline of a standardized protocol. MFP is one of the devices among the embedded devices to operate and implement many protocols at the same time. Because each protocol has its own respective vulnerability, the MFP that is implemented with a number of protocols needs constant monitoring of vulnerability of the protocols implemented by vendors. Maintenance systems are needed to perform such tasks as notification to the users and application of patches, etc., when the vulnerability is determined to have an impact on the implementation of the MFP.

7.11.1 Details

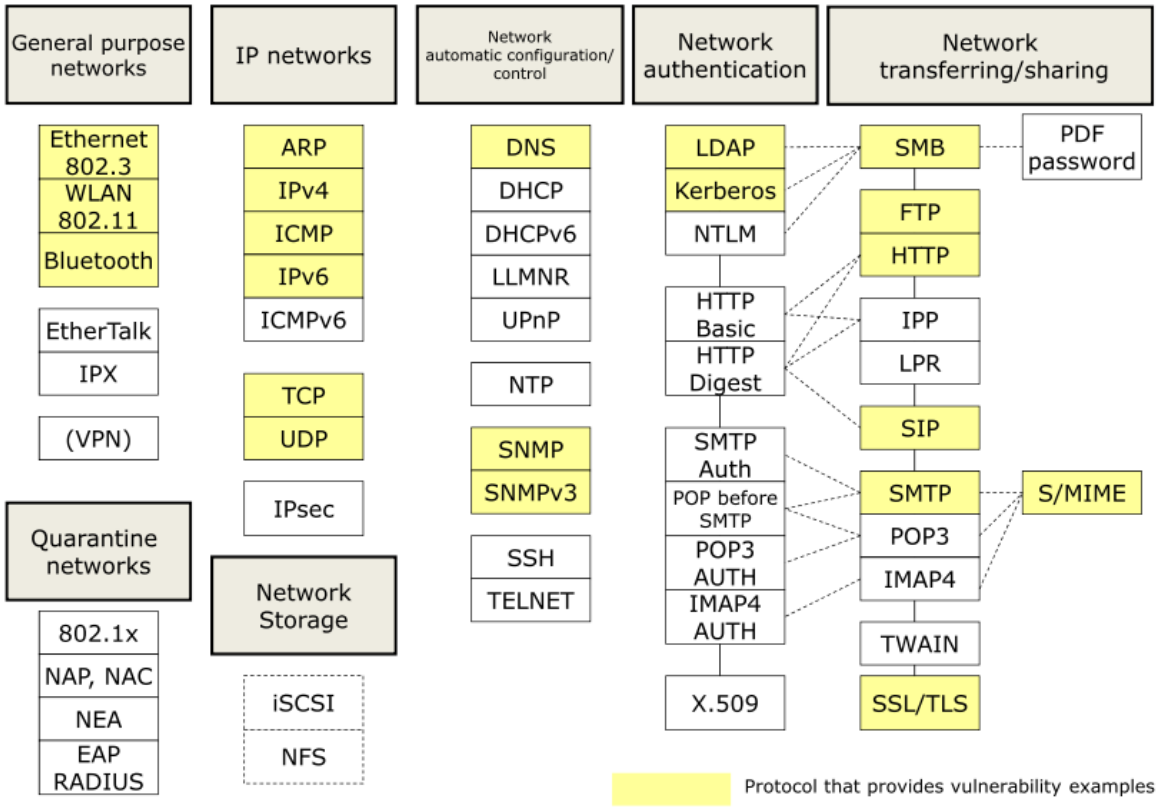


Figure 7-9 A list of communications protocols that are commonly used on the MFP

Figure 7-9 shows a list of communications protocols commonly used on the MFP. “General-purpose networks” on the upper left are physical communications protocols, such as Ethernet and wireless LAN. “Quarantine networks” are used for such purposes as to isolate important hosts, such as MFPs, on the independent networks to automatically isolate the terminals on the networks where important software has not been updated. “IP networks” are procedures for transmitting application protocols, such as HTTP, by interconnecting multiple networks to support the Internet. “Network storage” is a procedure that handles storage devices such as a hard disk on the network. There is no such device for the current major MFPs. “Network automatic configuration/control” is a procedure by which IP addresses can be automatically distributed, host names can be converted to IP addresses, and service names can be publicized to other machines. “Network authentication” is a procedure for the user terminals or administrator terminals that are connected over the network to the MFP to verify users using

user IDs between terminals and the MFP. “Network transferring/sharing” is a procedure for performing the storage and exchange of document data via the MFP.

Dotted lines in the right half of Figure 7-9 shows the relationship between the transfer protocols and the authentication protocols related to or corresponding to them. For example, a file sharing protocol, called SMB, uses LDAP, Kerberos, and NTLM as authentication protocols. HTTP uses HTTP Basic authentication and the HTTP Digest authentication. Because the IPP is HTTP-based, it uses similar authentication protocols. The SIP is a type of protocol similar to HTTP, and uses the same procedure as HTTP Digest authentication. There is a certification procedure called SMTP AUTH and POP before SMTP to transfer emails. POP3, a procedure to access the mail boxes, uses authentication protocol dedicated to POP3 (POP3 AUTH), and POP before SMTP uses this. More sophisticated IMAP4 uses an authentication protocol dedicated to the IMAP4 (IMAP4 AUTHENTICATION) to access the email boxes.

PDF password in the upper right corner of Figure 7-9 is a function to encrypt PDF files using passwords. This is not a communications protocol, but is one of the protection functions of the contents that are available for MFP users. S/MIME of the middle right in Figure 7-9 protects email contents as well, and it also encrypts image data in the emails, and detects the tampering of image data using electronic signatures.

Multiple protocols exist for each category above. Thereby, users can select the protocol suitable for their environment.

For example, “network transferring/sharing” performs writing to and reading from the SMB servers using SMB as a file transfer protocol. The FTP is a procedure for writing to and reading from the FTP servers. Web services using the SOAP that are more enhanced on the HTTP protocol are provided; in addition to writing and reading, publishing services are also available for the HTTP.

Not all protocols are needed for the environment of specific users. However, vendors who ship products globally have reasons to equip them with multiple protocols.

Products with these functions implemented had their respective vulnerabilities in the past. It is believed that current MFPs do not contain these vulnerabilities, but that is not necessarily always the case, because MFP functions are large even for software.

7.11.2 [Attack methods and the impacts]

There are multiple ways to attack multiple protocols implemented in the MFP, from simple methods to advanced methods that require multiple steps, depending on the respective protocol.

The details about individual methods are omitted in this report, but various vulnerabilities have been discovered in recent years for the main protocols of the MFP that are based on TCP/IP.

1) Vulnerabilities of the Ethernet (IEEE 802.3)

Ethernet (IEEE 802.3) is a protocol to replace the Ethernet frame on the wire, and does not have a function to protect the communications data. Ethernet is a simpler protocol than IP without the routing function, but the network configurations have to be carefully performed, because they are connected with the same Ethernet segment spreading to an unexpected scope with the world wide Ethernet connection services.

A recent example of a vulnerability related to Ethernet is that some Ethernet device drivers did not check the size of the Ethernet frame (CVE-2009-4537). Vulnerabilities are discovered as the “Broadcom NetXtreme management firmware vulnerability to a buffer overflow (JVNVU #512705)” in some cases, because remote management software has been added to the Ethernet card (or module).

Ethernet continues to change in such ways as achieving high-speed communications exceeding 10gbit/sec, and enhancing operation management functions to increase reliability while getting more popular as an inexpensive standard communications interface.

2) Vulnerabilities of wireless LAN

Wireless LAN has the ad hoc mode that connects terminals directly and the infrastructure mode by which terminals communicate via access points, and the authentication in ad-hoc mode is difficult. Originally, the access points that relay communications of other terminals should be operated in well-controlled conditions, but a third party can easily navigate the fake access points to connect wirelessly and invisibly, and easily connect to the fake access points to the wireless LAN terminals.

Currently, it has not been used in security-conscious environments, but there is a problem that the encrypting key can be decrypted in a matter of a few minutes in the WEP.

Regarding the security of wireless LAN, there are measures such as those used by the protection system called WPA/WPA2 communications. The usage of secure wireless LAN is introduced on the website, such as "Risks in the wireless LAN, Ministry of Internal Affairs and Communications,"[34]etc.

3) Vulnerabilities of Bluetooth

Bluetooth is a wireless communications standard that is used at a relatively short distance using a frequency band of 2.4GHz. It uses the encryption by the stream cipher "E0" corresponding to keys up to 128bit long, and the authentication challenge-response method by the pre-shared PIN. General usages are the wireless connection between devices that are connected at all times, such as PC keyboards and audio speakers, etc. They are also used for the data transmission and reception between the tablet terminals and on the smart phones. Some MFPs have printing functions, etc., that receive data from the terminals via Bluetooth. Bluetooth has a profile[35] with a possibility of a backdoor such as SPP and DUN due to its specifications. It is said that there is a high risk of vulnerability embedded, such as buffer overflow, etc., when the profile is implemented.[36]

4) Vulnerabilities of TCP/IP

The vulnerabilities of TCP/IP are summarized in the "Revised Research Report on Known Vulnerabilities of TCP/IP, 5th Edition" by IPA. It contains vulnerabilities of ARP, IPv4, ICMP, TCP, and UDP, and the software to verify these vulnerabilities, "TCP/IP Related Known Vulnerability Assessment Tool V5.0," is also distributed.

As TCP/IP operates in the OS kernel in general, the impact is great if vulnerabilities are attacked, causing such events as the OS stopping.

5) Vulnerabilities of IPv6

With the depletion of the 32-bit address of IPv4, IPv6 was standardized by the United States Department of Defense in 1982 and has become available for most MFPs. The "Security impact by IPv6 introduction and the measures"[37] presented at the 13th Information Security

[34] Risks in the wireless LAN
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/ippan12.htm
[35] The unique communication procedure implemented for each type of devices
[36] http://www.net-security.org/secworld.php?id=11663
[37] http://www.imes.boj.or.jp/citecs/13symp/ref2.pdf

Symposium, regarding possible vulnerabilities on the networks due to the protocol specifications. 36 vulnerabilities related to IPv6 on the implementation leakage of OS's and applications are reported from January 2011 to July 2012 on the CVE public information. Those service interruptions by DOS attacks due to OS implementation leakage and those bypassing the access control lists have been confirmed.

6) Vulnerabilities of DNS

DNS is a protocol used to convert host names, such as www.example.jp, into IP addresses. In cases when only IP addresses are used without using the host names, DNS is not required. However, DNS is often required in case of using the mail fax via the Internet.

The typical vulnerability of DNS is the "DNS cache poisoning" that injects fake IP addressed to the hosts that are attempting name resolution in DNS by exploiting the lack of protection of DNS messages. A method, DKA (Dan Kaminsky Attack), was discovered in 2008, and it was pointed out that it has a great impact. Since then, a protection method called DNSSEC has being introduced gradually to handle the vulnerabilities of DNS.

7) Vulnerabilities of SNMP and SNMPv3

SNMP is a protocol for monitoring the operations mainly of the communications devices and network devices. SNMP performs MIB (Management Information Base), a process that responds with type values from the hierarchical name labels to access the information indicating the operation state in the communications devices. On the SNMP protocol, message data of both requests and responses are encoded in a binary format called ASN.1 (Abstract Syntax Notation One), but a number of vulnerabilities are found in SNMP mainly of the implementations of its interpretation of ASN.1.[38]

There was a vulnerability that the administrator passwords can be obtained when entering OID such as ".iso.3.6.1.4.1.11.2.3.9.4.2.1.3.9.1.1.0" to the HP printers in 2002.[39] The users need to be limited in cases when the protected assets are in the information viewable on SNMP. Therefore, the identification and authentication function has been added to SNMPv3, but the vulnerabilities have also been discovered in the implementation of the authentication procedures.[40]

Since then, SNMP provides easy selection of the transmission method to protect communications by separating the specification that defines the SNMP message type from the specification that defines the transmission of SNMP messages (RFC5590).

SNMP has a feature of query processing that traces hierarchical MIB information in a tree. Therefore, some problems may occur in the operations of devices with many inquiries of MIB information recursively, if there are wrong settings or no limit to the processing volume.

In addition, there are implementations that can define specific actions, such as "action" based on the monitoring results via SNMP. Such implementations may allow executions of the arbitrary commands, if actions are performed without examinations of the fake SNMP responses.

[38] http://www.ipa.go.jp/security/ciadr/20020213snmp.html
[39] http://securitytracker.com/id/1004860
[40] http://jvn.jp/cert/JVNVU878044/

8) Vulnerabilities of FTP

The FTP (File Transfer Protocol) has been very popular, because it has been the standard protocol for file transfer over the Internet earlier than HTTP.

However, the FTP does not have procedures to protect communications over a long period of time. Protective settings using IPsec were also difficult due to the complex structure of the control TCP ports and the data transfer TCP ports that were separated. Improvements have been made such that the FTP is used on the SSL/TLS, and that the control TCP ports and the data transfer TCP ports are the same. However, there is no description in the products catalogs whether they are introduced to the MFPs, so it could not be confirmed.

There is already a case that some FTP commands were exploited. The FTP port command is an instruction that connects the TCP ports of any host's port number to the other the FTP servers. An example of exploiting the port command is the "FTP bounce attack." The FTP site command is a function to execute arbitrary commands on the connected FTP server, and it is very dangerous to operate the FTP servers having this function. The FTP cwd command is a command to move the current directory on the connected FTP servers. The cwd command is used in combination with the FTP put command that writes files or the FTP get command that reads files. However, it generally limits the accessible directories as some sub-directories on the FTP servers to prevent the operations to the directories and files that require privilege.

As a usage of the FTP server, there is an anonymous FTP server that does not require authentication. Anybody can use FTP servers by sending "ftp" or "anonymous" as user IDs when logging in with the FTP protocol, and sending any password string. The implementations of some FTP servers need attention to be paid to the FTP server operations, because normally they may operate as anonymous FTP servers.

From the above circumstances, it is considered that considerable care for FTP use is required in an environment that uses the MFP.

9) Vulnerabilities of HTTP and HTTPS

The HTTP-based deletion services are installed into most MFPs because of their efficient functions by utilizing the graphical user interfaces of the web browsers, and used quite extensively. In addition, services that have specialized applications are HTTP-based, as well, such as "IPP (Internet Printing Protocol)" that provides printing functions, "Web Services" that provides automated processing between web servers, and "WebDAV" that provides access to the shared files. HTTP communications are described in detail in Section 7.15 because there are many vulnerability viewpoints.

The vulnerabilities of HTTPS have great impact, as well, because HTTPS (HTTP over SSL/TLS) that protects HTTP communications path is also extremely popular. Vulnerabilities of the renegotiation (it re-establishes a connection during SSL/TLS communication) function of SSL/TLS have been reported in recent cases.

10) Vulnerabilities of LDAP and Kerberos

LDAP and Kerberos are typical protocols to perform authentication and authorization intensively on the networks. If LDAP and Kerberos are efficiently used, authentication can be done without user registrations for every single MFP, which enables centralized management of the password updates. However, the impact is great since authentication information and authorization information are converged.

LDAP shall be used in conjunction with SSL/TLS, because it does not have a function to protect communications. For Kerberos, version 4 and consecutive versions have the encryptions

embedded into protocols. The LDAP servers may contain requests to execute LDAP injection when searches are requested, such as for email addresses and IDs.

Recent vulnerabilities of LDAP include "Vulnerability of the denial of LDAP services (DoS) in JVNDB-2009-001779 - Active Directory."[41] For Kerberos, "Vulnerability of the denial of kadmind services (DoS) in JVNDB-2010-001344 - MIT Kerberos" should be referred.[42]

11) Vulnerabilities of SMB

SMB (Server Message Block) is a protocol that provides file sharing services. Some higher-level protocols called CIFS are also available, but they are referred to as SMB, including CIFS in general.

SMB file sharing services are used to transfer files that were scanned from the MFP, or to retrieve scanned images stored in the MFP from the user terminals, etc. Fax images that are received via fax may be transferred directly from the MFP to the user terminals. It also may be used for requesting the MFP to print.

The authentication procedure called NTLM has been used in SMB, but it has an improved NTLMv2 because there is a problem of the easy cracking of passwords when passwords are exchanged in NTLM. The NetBIOS protocol used in the SMB can be easily deceived by an arbitrary fake response of resolving the SMB server names to the IP addresses using the broadcast. SMB file sharing servers that ran on Windows earlier than Windows XP SP1 have vulnerabilities that the file sharing function operates without passwords.[43]

The "vulnerability that arbitrary code is executed in the RPC code generator of JVNDB-2011-005032-Samba" is about serious vulnerabilities and has been published in recent years.[44]

12) Vulnerabilities of SIP

SIP (Session Initiation Protocol) is a protocol to perform session control between two terminals. SIP and RTP (Real-time Transport Protocol) are used for fax transmission on the MFP.

SIP has several specifications to protect communications, but the communications protection function is not used in general, because SIP communications is supposed to be performed between the communications carriers. On the other hand, the implementation of such products using the SIP have vulnerabilities that can communicate with SIP servers and SIP terminals on the Internet if IP address is specified, without protective functions for the communication. For SIP, there is also a problem of unwanted incoming calls that are called "SPIM," which are like spam mails of e-mail.

The vulnerabilities of SIP are described in the "Revised Research Report on Known Vulnerabilities of SIP, 3rd Edition" by IPA.[45] "Evaluation tool on Known Vulnerabilities of SIP V2.0" by IPA is distributed as well.[46]

---

41 Vulnerability of the denial of LDAP services (DoS) in JVNDB-2009-001779 - Active Directory" -http://jvndb.jvn.jp/ja/contents/2009/JVNDB-2009-001779.html

42 Vulnerability of the denial of kadmind services (DoS) in JVNDB-2010-001344 - MIT Kerberos -http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-001344.html

43 http://itpro.nikkeibp.co.jp/members/NBY/techsquare/20021129/3/

44 http://jvndb.jvn.jp/ja/contents/2011/JVNDB-2011-005032.html

45 Revised Research Report on Known Vulnerabilities of SIP 3rd Edition http://www.ipa.go.jp/security/vuln/vuln_SIP.html

46 Evaluation tool on Known Vulnerabilities of SIP V2.0 http://www.ipa.go.jp/security/vuln/vuln_SIP_Check.html

13) Vulnerabilities of SMTP, POP3, and IMAP4

SMTP is a protocol that transfers emails, and POP3 and IMAP4 are protocols that provide access to email boxes. These have existed earlier than HTTP, and have been popular.

SMTP had various problems, because there were no authentication procedures or protection procedures for communications in the specifications. Currently, there are still problems such as receiving advertisements and a large volume of "spam mails" that computer viruses are attached to.

A variety of vulnerabilities have been discovered in the implementations of these email protocols. SMTP command has vulnerabilities on SMTP expn commands that deploy alias addresses and member names on the mailing lists, as well as on SMTP vrfy commands that verify the presence of email addresses without authentication. SMTP auth commands are procedures for user authentication by the SMTP protocol, but it has a high possibility of the password being cracked if the SMTP auth procedures are wiretapped to change hashed password strings. In addition, it is necessary to protect the SMTP communications path with SSL/TLS or IPsec to use SMTP securely, because there is no function to protect messages on the SMTP communications path.

The recent SMTP information leakage vulnerabilities are described in "Information leakage vulnerabilities in the SMTP component of Microsoft Windows."[47] Vulnerabilities of authentication password exchange procedure of POP3 are described in "Vulnerabilities of password leakage on APOP."[48] Vulnerabilities of response processing in both cases of IMAP4 and POP3 in recent years are reported in "Vulnerabilities of integer overflow in inetcomm.dll of multiple Microsoft products."[49]

S/MIME is a protection specification of messages and contents for the secure exchange of emails and messages. Digital certificates need to be operated properly to ensure S/MIME protection. It is also necessary to understand the cautions, such as the headers indicating sources and destinations of the emails in the S/MIME not being protected. For more detailed S/MIME usage, "Email security - encryption and electronic signature using S/MIME" should be referred.[50]

---

47 JVNDB-2010-001391 - Information leakage vulnerabilities in the SMTP component of Microsoft Windows - http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-001391.html

48 JVNDB-2007-000295 - Vulnerabilities of password leakage on APOP http://jvndb.jvn.jp/ja/contents/2007/JVNDB-2007-000295.html

49 JVNDB-2010-001471 - Vulnerabilities of integer overflow in inetcomm.dll of multiple Microsoft products - http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-001471.html

50 Refer to "Email security - encryption and electronic signature using S/MIME" by IPA http://www.ipa.go.jp/security/fy12/contents/smime/email_sec.html

7.11.3 [Causes and discussion]

1) Many protocols

The MFP has various levels of protocols. As BMLinkS[51] distributed by an industry association of the MFP JBMIA, there are activities to develop a common driver compatible with multiple models of MFPs of multi vendors. However, the existing protocols have dependencies on one after another, such as user terminals' conditions or constraints with other systems, and it is not easy to put them into one protocol to aggregate.

It is effective for the fundamental countermeasures by developers that unnecessary services are not implemented, and that the information, which can be accessed from the necessary services to operate, should be narrowed down to its minimum. As users, it is effective not to start up the non-used services for operation.

In real attacks, attackers conduct port scans for the MFP to verify that these services are running. The MFP may be excluded from the target of attacks during the early stages of attacks by suppressing the port scan and concealing the services. There are two major ways to control the port scan. One is to modify the kernel so as not to respond to scanning to some extent, and the other is to modify the kernel for all 65,535 ports to respond to scanning. Both methods are effective in terms of available ports (services) not being identified. However, port scans need to be handled on the assurance of no impact on the services and functions that are implemented on the MFP and on the linkage function with external devices.

2) Measures including ex-post facto measures against the vulnerabilities that are still being discovered

As mentioned above, many services are running on the MFP along with rich functions of the main unit of the MFP. Therefore, the vulnerabilities of the MFP cannot be totally eliminated. Vulnerabilities of the software, as listed in "7.11.2 [Attack methods and the impacts]," are reported on some implementation of any protocols. In fact, vulnerabilities of SMB implemented onto many MFPs were reported and published in April 2012.

Assuming that the vulnerabilities of the MFP cannot be totally eliminated, MFP users and developers of the MFP vendors need to prepare ex-post facto measures respectively. Users can take ex-post facto measures for the vulnerabilities, including gathering vulnerability information about the products being used and measures from the vendors, establishing the systems to support software updates and the usage procedure changes, and discussing response procedures for damages with personnel in charge, etc.

Examples of ex-post facto measures for the vulnerabilities that the providers of the products can take would be identifying the vulnerabilities and the report procedures, discussing the methods of reduction of damages and threats, discussing how to reflect that to products, and prioritizing measures.

[51] BMLinkS-JBMIA: Japan Business Machine and Information System Industries Association, The BMLinkS Project Committee http://bmlinks-committee.jbmia.or.jp/

3) Measures for the vulnerabilities of multiple protocol implementation

In circumstances in which there is no choice but to implement many protocols at the same time, designs to minimize the vulnerabilities of the MFPs and measures for developers can be referred to the widely disseminated "Security Engineering,"[52] "Secure Programming Course,"[53] and "Approaches for embedded system information security,"[54] etc., by IPA.

It is difficult that there are too many matters to discuss and too many testing items in the existing methods for these vulnerability measures to be implemented. Therefore, more examinations of some automated test tools and inspection methods may be necessary.

Test tools include tools to discover the vulnerabilities by examining source code,[55] fuzzing tools to comprehensively check by rewriting HTTP communications of the products, and the tools to discover the vulnerabilities by testing from outside in a black box manner, etc. IPA published materials that cover description of fuzzing and specific usage of the fuzzing tools.[56] Codenomicon, AppScan and Nessus, etc., are well-known products to examine vulnerabilities in a black box manner. For the evaluation procedures, including tests for these vulnerabilities, the product certification system, including vulnerability tests, which were performed at Windows Logo of Microsoft, can be referred.[57]

However, these tools can only apply to the standardized protocols for HTTP communications, and it should be noted that the manufacturing vulnerabilities that can be detected by manual checking cannot be detected on HTTP communications.

---

[52] "Security Engineering" by IPA – http://www.ipa.go.jp/security/awareness/vendor/software.html
[53] "Secure Programming Course" by IPA
http://www.ipa.go.jp/security/awareness/vendor/programming/
[54] "Approaches for embedded system information security"
http://www.ipa.go.jp/security/fy20/reports/emb_app/
[55] "Secure Programming Course C/C++Language" source code review by IPA
http://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/c103.html
[56] http://www.ipa.go.jp/security/vuln/fuzzing.html
[57] Windows Logo - http://www.microsoft.com/japan/whdc/winlogo/hwrequirements.mspx
Product certification examination system that is provided for Windows device driver

7.11.4 Measures

[Operation guide]

1) Disable all the functions that are not used while minimizing the functions used on the MFP.
2) Subscribe to the vulnerability measures information of the vendors or prepare to obtain it any time.
3) Regularly understand trends and security breaches obtained by the audit records, and take measures.
4) Have plans to take measures in cases that the vulnerabilities of the MFPs are found.
5) Have plans to take measures in cases of damage caused by the vulnerabilities.

[Development guide]

6) Manage the services that are implemented, but do not implement services no longer being used.
7) Clearly define and specify the communications that allow access to the protected assets. In some cases, implement the measures against attacks at the kernel level.
8) Measures against the vulnerabilities of the products should be addressed through product planning and development processes.
9) Consider tools likely to easily reflect the security policy for the MFP that can be applied in a usage environment of the MFP.
10) Consider using static analysis tools for source code, fuzzing tools and intrusion testing tools as vulnerability testing tools.
11) Have handling procedure plans ready to deal with situations in cases that vulnerabilities are found.

[Verification guide]

12) When examining a communications protocol that can access the protected assets, all parameters should be targets for inspection regardless of input availability for users.
13) Perform comprehensive inspections by understanding what can be examined and how much it can be examined by use of vulnerability assessment tools, and by using the source code review or manually to check the parts that cannot be examined.

7.11.5 References

Date of publication	Source
February 2002	IPA: Widespread vulnerabilities of SNMP http://www.ipa.go.jp/security/ciadr/20020213snmp.html Vulnerability information related to SNMPv1
2008	Information security measures for SE - vulnerability of HTTP http://www.chuu-information.com/security/fragile_6.html Points of vulnerabilities in the HTTP protocol are summarized
June 2008	JVNVU#878044 Vulnerabilities of authentication bypass due to improper HMAC processing under SNMPv3 implementation http://jvn.jp/cert/JVNVU878044/ Vulnerabilities that authentication is bypassed in SNMPv3 due to specific messages
July 2008	An Illustrated Guide to the Kaminsky DNS Vulnerability http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html Overview and handling of CACHE Poisoning by DKA

November 2010	IPA: Research Report on Known Vulnerabilities of TCP/IP Revised 5th Edition - http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html Vulnerability materials of detailed descriptions of TCP, ICMP, IPv4, and ARPs protocol
November 2010	IPA: Evaluation tool on Known Vulnerabilities of TCP/IP V5.0 http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html Compatible with TCP, ICMP, IPv4, ARP and some IPv6
November 2009	JVNVU#120541 Vulnerabilities of SSL and TLS protocols http://jvn.jp/cert/JVNVU120541/ Vulnerabilities of functions used to re-connect during the SSL/TLS communications
December 2009	CVE-2009-4537: r8169: straighten out overlength frame detection http://cve.mitre.org/cgi-bin/cvename.cgi? name=CVE-2009-4537 Failure of the frame length test that was included in the driver of Realtek Ethernet chip
July 2011	CVE-2011-1265 http://web.nvd.nist.gov/view/vuln/detail? vulnId=CVE-2011-1265 Vulnerability that the Microsoft products execute codes due to unauthorized Bluetooth packets
April 2012	CVE-2012-0475 http://web.nvd.nist.gov/view/vuln/detail? vulnId=CVE-2012-0475 Vulnerability that the access control list of IPv6 literals of Mozilla products is bypassed
May 2012	CVE-2011-2699 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-2699 Vulnerability of the impact of a DOS attack in an IPv6 implementation of Linux OS

7.11.6 Seriousness and attack potential evaluation (reference value)

[Attack assumptions]

Multiple protocols are introduced in this section, but it is assumed that the MFP services are stopped due to DOS attacks on the HTTP server inside the MFP using attack tools.

- It has to be the model that does not take the above measures in the operation guide.

[Scoring]

CVSS 2.0 Base value: 5.8 (Warning)

Attack source category	Possible attacks from neighboring networks
Complexity of attack criteria	Low
Pre-attack authentication Requirement	No authentication operation required
Confidentiality	No impact
Integrity	No impact
Availability	Overall impact

7.12 Concerning vulnerabilities of proprietary MFP protocols

This section explains proprietary protocols that are not included in the standardized protocols described in Section 7.11. Proprietary protocols refer to communications protocols developed or modified by vendors independently to provide communications services with other devices than the MFP. Vulnerabilities are not found by use of the inspection tools described in Section 7.11, unlike the standardized protocols. On the other hand, starting from the design and development stage, there may be bugs in the implementation leading to vulnerabilities, such as buffer overflow, etc., at unexpected locations. In this section, examples of the source code in the communications control are presented to show locations where leakage and bugs are likely to occur. These source code examples are for reference only, and are not the services implemented on the MFP.

7.12.1 [Attack methods and the impacts]

It is confirmed that some MFP vendors implement services that are assigned to ports other than general ports. Some only offer communications services with the standardized communications protocols via proprietary port numbers as listed in Section 7.11. However, some vendors implement their own proprietary services to provide additional services and cooperation devices provided by the vendors. In cases of the proprietary services by vendors, the specifications, such as the standardized communications protocols of well-known ports in RFC, etc., will not be published. In addition, unlike the services known to the general public, vulnerabilities are not identified. To put it better, they are unlikely to become targets of the attacks, and their vulnerabilities and attack methods are rarely published. On the other hand, it is possible that the vulnerabilities covered in well-known services may still exist.

Examples of the vulnerabilities of the protocols whose implementations have not been confirmed on the MFP are presented here, to describe the vulnerabilities that may occur at the time of implementation or in the specifications of proprietary protocols.

Vulnerabilities were published on July 7th, 2012, in the CVE of the references. Figure 7-10 is the source code of communications control for the well-known message exchange tool. This vulnerability is that the arbitrary code can be executed with buffer overflow triggered in the stack area by exploiting the regular inline images attached to the messages, in other words, the area of the size-defined icon (similar to pictogram used in the cell-phones).

```
void mxit_show_message( struct RXMsgData* mx )
  {
  char*             pos;
  int               start;
  unsigned int      end;
  int               emo_ofs;
  char              ii[128];
  char              tag[64];
  int*              img_id;

  if ( mx->got_img ) {
      while ( ( pos = strstr( mx->msg->str, MXIT_II_TAG ) ) ! = NULL ) {
          start = pos - mx->msg->str;
          emo_ofs = start + strlen( MXIT_II_TAG );
          end = emo_ofs + 1;

          while ( ( end < mx->msg->len ) && ( mx->msg->str[end] ! = '>' ) )
             end++;

          if ( end == mx->msg->len )     /* end of emoticon tag not found */
              break;

          memset( ii, 0x00, sizeof( ii ) );
          memcpy( ii, &mx->msg->str[emo_ofs], end - emo_ofs );

          /* remove inline image tag */
          g_string_erase( mx->msg, start, ( end - start ) + 1 );

          /* find the image entry */
          img_id = (int*) g_hash_table_lookup( mx->session->iimages, ii );
          if ( ! img_id ) {
              /* inline image not found, so we will just skip it */
              purple_debug_error( MXIT_PLUGIN_ID, "inline image NOT found (%s)¥n", ii );
          }
          else {
              /* insert img tag */
              g_snprintf( tag, sizeof( tag ), "<img id=¥"%i¥">", *img_id );
              g_string_insert( mx->msg, start, tag );
          }
      }
  }
```

Figure 7-10 Example of source code that performs vulnerable protocol processing

Lines in red are where problems reside. Large character strings of str [mem_ofs] can be input to the variable ii, which is ensured by a fixed 128 Bytes, so that it allows the overflow of the stack area to rewrite the return addresses. As a result, it makes it possible to run a shell with administrative privilege and arbitrary code. It is said that the seizure of the shell is difficult for some OS's that are installed on the MFP. There are some examples, however, that the OS vulnerabilities are actually applied to the MFP with a general-purpose OS installed, as described in Section 7.8.

Buffer overflow mechanisms and the attack code to run the shell using an implementation that can write any value to the stack area, as described above, are published on the IPA website.[58]

7.12.2 [Causes and discussion]

The cause of this vulnerability is that the function that triggers a buffer overflow has left unnoticed during development, and has been implemented. Inspections by the fuzzing tool after implementation may be effective if it is a general protocol port.[59] However, in the case of proprietary protocols, it is necessary to consider the design and inspection methods based on the property of the protocols being used.

Vulnerabilities at the implementation level, as described in Section 7.12.1, occur mainly for the reasons that coding rules are not coordinated in the development environment, or that a checking mechanism is not established as to whether the development is following the rules, etc. Deficiencies may be found at the time of the design or inspection, assuming the possibility that unauthorized values are input in the texts input by users or in the pull-down items to select. In this case, they may be missed from the targets of inspection, because they are processed inside the programs to handle the areas where the fixed images or the icons, etc., prepared by the vendors should be entered.

When it is programed with the fixed coding rules, design and inspection of the variable area and its manipulations should be carefully paid attention to. It is confirmed that the program listed as an example has been improved as follows when the current source code is downloaded:

```
:
int               emo_ofs;
char*             ii;
char              tag[64];
int*              img_id;
:
        if ( end == mx->msg->len )     /* end of emoticon tag not found */
            break;

        ii = g_strndup(&mx->msg->str[emo_ofs], end - emo_ofs);

        /* remove inline image tag */
        g_string_erase( mx->msg, start, ( end - start ) + 1 );
:
            g_snprintf( tag, sizeof( tag ), "<img id=¥"%i¥">", *img_id );
            g_string_insert( mx->msg, start, tag );
        }
        g_free(ii);
:
```

Figure 7-11 Improved source code that performs protocol processing

Using static analysis tools for source code is effective during development for the manipulations of variable area that is easily overlooked visually otherwise. In addition, measures of port scanning at the kernel level as described in Section 7.11 may be effective as a measure to interrupt with the presence detection of proprietary protocols that are breakthroughs of attacks.

---

[58] http://www.ipa.go.jp/security/awareness/vendor/programmingv1/b06_01.html

[59] The vulnerability created by session maintenance management, etc., cannot be detected in many cases, if inspections combined with a manual method are not conducted.

On the other hand, vulnerabilities cannot be found in many cases using the vulnerability inspection tools as described above, when evaluators conduct black-box testing of services using proprietary protocols that have been implemented on the MFP. Proprietary protocols are not examined using the inspection tools based on the databases of known vulnerabilities, such as Nessus, and automatic inspection tools for proprietary protocols do not exist. Some may be examined with fuzzing tools, if proprietary protocols have been extended from some standardized protocols, but the extended parts may not be examined in many cases. Therefore, when proprietary protocols are examined at the implementation level, it is necessary for the persons performing manual intrusion testing to search the parameter parts and to verify comprehensively that no overflow occurs by entering unauthorized values for the parameter.

In cases that the proprietary protocols are examined, it is realistic for the evaluators to ask developers to disclose the source code to review and confirm by using static analysis tools to perform analysis. In cases when the source code cannot be obtained, it is very difficult to debug, so attack code shall be created while checking the responses by entering unauthorized values into the parameter parts, after hearing the communications protocol specifications. Many examples of attack code that insert unauthorized code into the parameter parts are published in the Exploit Database of Metasploit.

7.12.3 Measures

[Operation guide]

1) Disable all the functions that are not used while minimizing the functions used on the MFP.
2) Subscribe to the vulnerability measures information of the vendors or prepare to obtain it any time.

[Development guide]

3) Manage the services that are implemented, but do not implement services no longer being used.
4) In cases when there is no impact on the other functions, consider the implementation of measures for the port scan.
5) Ensure that the source code is compliant with coding rules for all parameters of the protocol implemented.
6) Consider using static analysis tools of source code as vulnerability testing tools during development.
7) Have handling procedure plans ready to deal with situations in cases that vulnerabilities are found.

[Verification guide]

8) When examining a communications protocol that can access the protected assets, all parameters should be targets for inspection regardless of input availability for users.
9) Research if the vulnerability at the implementation level cannot indirectly access the protected assets.
10) Manually examine after checking the specifications of the proprietary protocol (using fuzzing tools, etc., if available). Examine by using static analysis tools and the source code review if the source code review is possible.

7.12.4 References

Date of publication	Source
July 2012	CVE-2012-3374 http://web.nvd.nist.gov/view/vuln/detail? vulnId=CVE-2012-3374 Vulnerability information of implementation leakage of message exchange software called Pidgin
September 2012 (Frequently updated)	Exploit Database of Metasploit http://www.metasploit.com/modules/ Code collection that will be helpful in creating such code associated with the overflow of proprietary protocols, etc.
March 2012	Guide for fuzzing usage http://www.ipa.go.jp/security/vuln/documents/fuzzing-guide.pdf Detailed description of fuzzing

7.12.5 Seriousness and attack potential evaluation (reference value)

[Attack assumptions]

The vulnerability described in this section is a bug that contains parameters, which can cause a buffer overflow in the proprietary protocol that the MFP has implemented. It is intended to obtain the authority to perform an OS command on the MFP by providing a backdoor by exploiting the parameters to execute arbitrary code. The scope of the impact is assumed to be that the protected assets can be manipulated completely from the OS command.

- It has to be the model that does not take the above measures in the development guide and verification guide.

[Scoring]

CVSS 2.0 Base value: 7.9 (Danger)

Attack source category	Possible attacks from neighboring networks
Complexity of attack criteria	Moderate
Pre-attack authentication requirement	No authentication operation required
Confidentiality	Overall impact
Integrity	Overall impact
Availability	Overall impact

7.13 Problems of intrusion via driver protocol

As shown in Table 7-2, many driver protocols are supported in the standards of the recent MFP to select and use freely in accordance with the usage.

Table 7-2 Major driver protocols used on the MFP

Driver protocols	Usage	Authentication procedure	Encryption procedure
LPR	Printing	-	-
raw9100	Printing	-	-
IPP	Printing	✓	✓
SMB	Printing and scanning	✓	✓
TWAIN	Scanning	✓	✓
FTP	Scanning	✓	✓
WebDAV	Scanning	✓	✓
SMTP	Faxing	✓	✓
POP3	Faxing	✓	✓
IMAP4	Faxing	✓	✓
WSD (Web Service Discovery)	Printing, scanning, and faxing	✓	✓
BMLinkS	Printing, scanning, and faxing	✓	✓

There are a number of vulnerabilities reported from clients in the implementation of the driver protocols to operate the MFP. By exploiting these vulnerabilities, various attacks are possible, such as unauthorized operations of the MFP (display screen spoofing and requests for unintended print processing, etc.), information leakage and data damage by unauthorized access to the stored protected assets, and instability on the MFP operations from system file damage, etc.

It is important for both developers and users to be aware of the vulnerabilities of the driver protocols and their impacts and to take necessary measures, because of the possible implementation (version) with remaining vulnerabilities to ensure compatibility with the devices connected to the MFP.

LPR as an example of vulnerability of driver protocols is discussed here.

7.13.1 [Attack methods and the impacts]

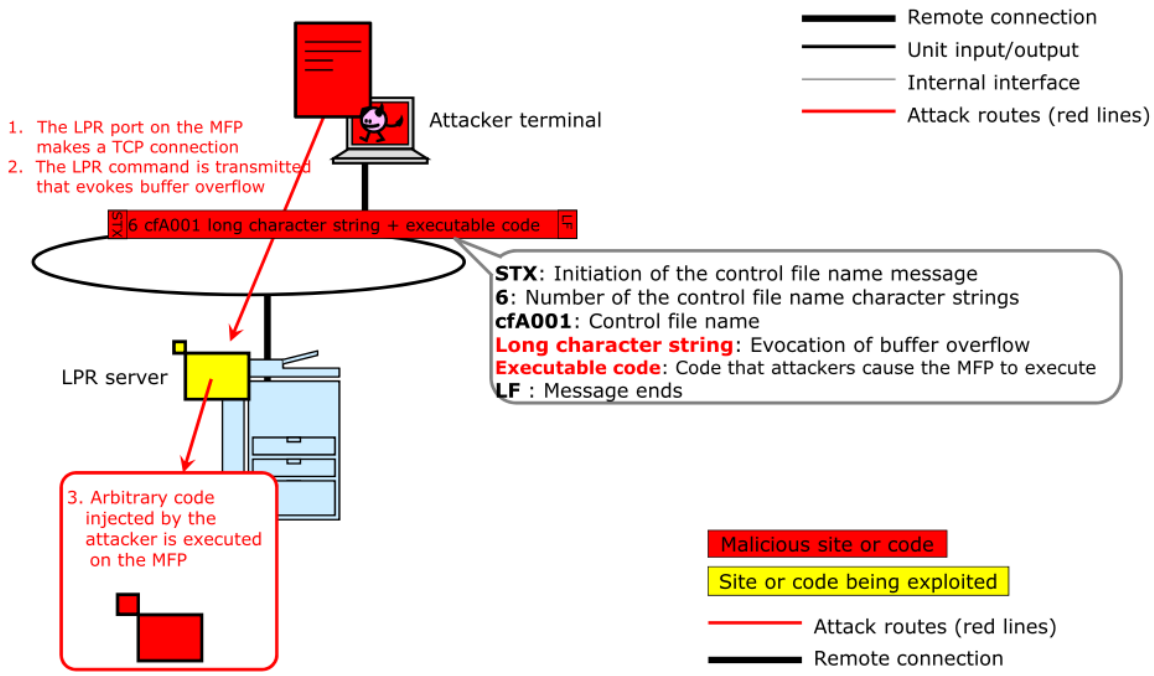


Figure 7-12 Example of intrusion via driver protocol LPR

First of all, an attacker establishes a TCP connection to TCP 515 port of the LPR server executed on the MFP. The attacker then sends an LPR command unconditionally to the LPR server on the MFP, because there is no procedure for user authentication of the LPR protocol.

Against the LPR server on the MFP, the attacker causes a buffer overflow by giving an unexpectedly long character string as a file name of the control file for printing. Followed by this very long character string, the attacker sends arbitrary executable code to the LPR server and sends the line feed code (LF: 0x0a) as an end-of-command to the LPR, and then, buffer overflow occurs in the LPR server so that the executable code sent by the attacker takes control.

Figure 7-13 below shows an example of a sequence of intrusion by the LPR command.

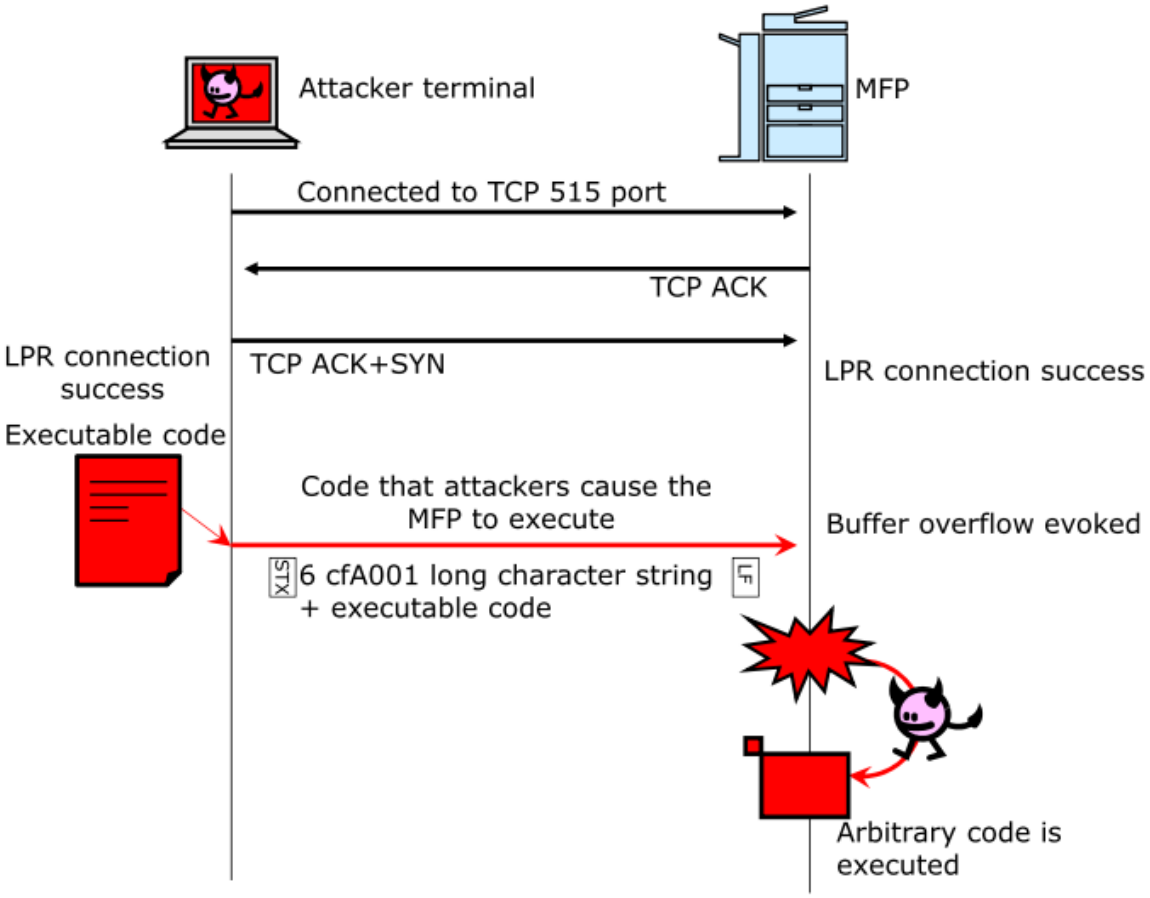


Figure 7-13 Example of a sequence of intrusion by driver protocol LPR command

As a result, arbitrary code is executed by the attacker in the execution environment where the LPR server is executed on the MFP. Once the attacker executes arbitrary code on the MFP, it is possible to execute another program on the MFP by introducing it, copy documents and job data handled by the MFP to the attacker's host, and attack another host from the MFP. Even if the attacker is unable to execute arbitrary code on the MFP, and if buffer overflow occurs on the LPR server on the MFP, that may stop the operations of the LPR server, or the LPR server or the MFP may re-start. As a result, the LPR server of the MFP or the MFP becomes temporarily unavailable.

7.13.2 [Causes and discussion]

In the LPR protocol, some commands are standardized to control the printing. However, there is no argument that indicates the length of the command string, and the character strings, which become arguments, are only separated by LF (Line Feed) code in the LPR protocol command. Besides, there is a command to specify the names of the job data files and job control files that are transferred, and arbitrary character string can be specified as a file name, but there is no argument to specify the character string length of the file name. In addition, both job control files and job data files have arguments that represent the length of the files in bytes, but they are specified by a number in text format with no limitation to the maximum length or number of digits indicating the length of the files.

In RFC 1179 where the LPR protocol specifications are standardized, the string length of the job data file names and the job control file names are about six characters. However, an unlimited number of characters can be sent, because there is no limit on the length of the string in the LPR protocol.

In addition, a heap memory overrun may occur when the unexpected scope is being specified in handling the numbers presented in the texts.

The “relaxed” protocol specifications by textual representation are common in procedures, such as HTTP, SMTP, and SIP. On the contrary, the receivers need detailed inspection due to the high flexibility instead of strict formats. Such inspection processing of the data received from the outside is called “verification of input values,” “sanitization of input data,” or “sanitization.” Refer to the “Secure Programming Course, C/C++ Language, Conspicuous vulnerability measures” by IPA for the vulnerabilities and measures for development, presented with image on the web.

The assumption for making this attack more successful is that the LPR server execution environment on the MFP should be a well-known OS, such as Linux, Windows, or VxWorks, and that the CPU or machine language used should also be well-known to operate the executable code injected as attackers intended. An environment to execute the machine language located on the stack memory or heap memory is also required.

Many protocols are supported for the MFP driver protocols, and there is a possibility that vulnerability, such as LPR, remains in other driver protocols as well. Developers of the MFPs need to confirm vulnerabilities for each driver protocol used on the MFP as shown in Table 7-2. In particular, lots of vulnerabilities are reported in the implementation of the driver protocols (LPR, IPP, or raw9100, etc.) operated on the MFP, as shown in the references. It is desirable to check the latest vulnerability information in the implementation of driver protocols used in the MFPs that are being developed, and it is also desirable either to publish patches and notify users on the product information sites, or to replace the firmware with a patch applied against the vulnerability on the basis of the maintenance contract, because the driver protocols may be used unintentionally with vulnerabilities remaining in the implementations for the purpose of assuring compatibility, etc., with the devices connected to the MFP. On the other hand, when MFP users are intended to ensure security, it is effective to close the unnecessary ports with the MFP settings by limiting the driver printer ports that are needed for use in the operational environment.

7.13.3 Measures

[Operation guide]

1) Specify servers used on the MFP, such as LPR, raw9100, IPP, SMB, SOAP, or WebDAV, to stop the listen ports for the services that are not used on the MFP. On that basis, check the vulnerability information of the MFP vendors to consider implementation of necessary measures, if necessary.
2) Use only specific print spool servers or gateway servers for scanning and faxing, as the host that can input job data for the MFP.

[Development guide]

3) Always check the latest vulnerability information for driver protocols implemented on the MFP, and notify users. In the case of vulnerabilities having an impact on the proprietary MFP, provide patches or firmware that correspond to the vulnerabilities, in addition to giving notice about them.

[Verification guide]

4) Check all driver protocols that are introduced on the MFP as to whether the known vulnerabilities of each protocol apply.
5) Check all driver protocols that are introduced on the MFP as to whether they are implemented correctly according to specifications, when vulnerabilities are handled by implementation.

7.13.4 References

Date of publication	Source
August 1990	RFC 1179 Line Printer Daemon Protocol http://tools.ietf.org/html/rfc1179 Protocol specifications of LPR by IETF
July 1998	What is LPR? http://support.apple.com/kb/TA21876? viewlocale=ja JP&locale=ja JP Support information from Apple Computer. The difference between the LPR and the PAP (Printer Access Protocol), a print job transmission procedure used on AppleTalk by Apple, is described.
October 2000	LPD Vulnerability Issues http://lpd.brooksnet.com/lpd-security.html Points and example measures on the print server are as follows: (1) Arbitrary file can be created on the print server via LPR. (2) Arbitrary file can be deleted on the print server via LPR. (3) Arbitrary command can be executed on the print server via LPR.
November 2001	CERT® Advisory CA-2001-30 Multiple Vulnerabilities in lpd http://www.cert.org/advisories/CA-2001-30.html Multiple vulnerabilities on the print server of the LPR (lpd) (1) Arbitrary code is executed by buffer overflow (2) Arbitrary options can be specified to the sendmail on the print server.
October 2006	The difference between LPR protocol and the standard TCP/IP port monitor http://www.atmarkit.co.jp/fwin2k/win2ktips/809stdprnprt/stdprnprt.html The difference between raw9100 and the LPR that are used on Microsoft Corporation's TCP/IP port monitor.
October 2007	US-Cert: Cisco IOS LPD buffer overflow vulnerability: VU#230505 https://www.kb.cert.org/vuls/id/230505 Buffer overflow occurs after the call of sprintf() on the LPD of Cisco IOS, if a host name that exceeds 99 characters is entered.
December 2007	US-Cert: CUPS buffer overflow vulnerability: VU#446897 http://www.kb.cert.org/vuls/id/446897 It has been reported that arbitrary code may be executed due to the vulnerability of buffer overflow in the "Common UNIX Printing System (CUPS)," the printing system of the UNIX OS.
April 2010	Mocha W32 LPD Remote Buffer Overflow Vulnerability http://www.securityfocus.com/bid/39498/info Vulnerability that arbitrary code is executed due to buffer overflow of the control file name character string by the control file incoming command of the LPR on the Mocha's LPR print server software for Windows. There is an exploit code for the procedure by Python script.

7.13.5 Seriousness and attack potential evaluation (reference value)

[Attack assumptions]

As an example of buffer overflow vulnerability of LPR protocol (arbitrary code is executed on the LPR server.), a backdoor is established by executing arbitrary code by exploiting the vulnerability, to obtain the authority to execute the OS command on the MFP. The scope of impact is assumed to be a case that the protected assets can be manipulated completely from the OS command.

- It has to be an environment that does not take the above measures.
- The LPR communications from the Internet are blocked by a firewall, etc.

[Scoring]

CVSS 2.0 Base value: 7.9 (Danger)

Attack source category	Possible attacks from neighboring networks
Complexity of attack criteria	Moderate
Pre-attack authentication Requirement	No authentication operation required
Confidentiality	Overall impact
Integrity	Overall impact
Availability	Overall impact

7.14 Problems due to vulnerabilities of page description language

Page description language is a language used to give instructions for output images, etc., when documents and images created on the client PC are printed by the MFP, etc., and to set up environments, and so on, and it includes PJL (Print Job Language), PCL (Printer Control Language), and PostScript. In general, it is possible to input a print job or deletion queue, etc., using page description language on the MFP. On the other hand, there may be exposure or data damage by unauthorized access to the data (protected assets) registered with printing jobs by attackers, or obtaining passwords by unauthorized access to the file system, etc. As an example of the page description language, PJL is discussed here.

7.14.1 [Attack methods and the impacts]

PJL specifications make it possible to perform MFP environment settings, job management preferences, or file system operations, etc., using the PJL command. The following show PJL commands related to file system operations:

Table 7-3 PJL commands related to file system operations

PJL commands	Details
FSAPPEND	A command to add data to files or to create a new file
FSDIRLIST	A command to display files and directories
FSDELETE	A command to delete files or empty directories
FSDOWNLOAD	A command to download files
FSINIT	A command to initialize file systems
FSMKDIR	A command to create directories
FSQUERY	A command to inquire about the entry
FSUPLOAD	A command to upload files

By exploiting PJL commands as shown above, there are possibilities of information leakage, data damage, or unauthorized access to the file system, etc., by obtaining the data (protected assets) registered by someone else.

The following example shows unauthorized access to the file system on the actual MFP by the directory traversal method, using the command (FSDIRLIST command) related to file system operations described above:

```
%-12345X@PJL INFO FILESYS
VOLUME    TOTAL SIZE        FREE SPACE        LOCATION LABEL    STATUS
0:        2929683456        2922577920        HDD               READ-WRITE

%-12345X@PJL FSDIRLIST NAME="0: ..¥..¥..¥..¥¥" ENTRY=1 COUNT=128
ENTRY=1
pjl TYPE=DIR
plwform TYPE=DIR
artform TYPE=DIR
seal TYPE=DIR
smb TYPE=DIR
jtpool TYPE=DIR
del TYPE=DIR

%-12345X@PJL FSDIRLIST NAME="0: ..¥..¥..¥..¥smb¥¥" ENTRY=1 COUNT=128
ENTRY=1
passwd.txt TYPE=FILE SIZE=243
share.txt TYPE=FILE SIZE=67
```

Figure 7-14 Attack using a PJL command (Directory traversal)

The above example shows attackers can obtain file system information by accessing raw9100 (9100/tcp) of the MFP, and access the directory configuration information or protected assets (passwd.txt, here), using the directory traversal methods based on the information obtained. It is possible to obtain, or tamper with, files using the PJL commands, if the protected assets are within the reach of access. It was actually confirmed that passwd.txt was obtained and tampered within this attack.

In the case that the page description language is exploited, it is sometimes possible to tamper with the MFP display (using RDYMSG commands) or with settings information, in addition to unauthorized access to the protected assets as described above. In addition, there is an attack reported that arbitrary code may be executed by triggering a buffer overflow using the INQUIRE command. Exposures or damage of the protected assets stored in the MFP, or destruction of the MFP itself, may be possible in some cases, using these attack methods.

Developers should develop while keeping the vulnerabilities of the page description language in mind, because PostScript, as shown in the references besides PJL, also has been reported to have vulnerabilities.

7.14.2 [Causes and discussion]

The causes for making unauthorized access to the file system on the MFP possible are the lack of support of developers for a directory traversal and the implementation of unnecessary PJL commands.

For the measures against the directory traversal, it is important to implement with limitations on access to files or directories that can be accessed using the PJL commands, assuming that attackers exist on the network that is accessible to the MFP. Additionally, it is effective to limit the PJL commands available on the MFP (or keep it unavailable) as a measure against vulnerabilities, such as the leakage of protected assets and settings information, as well as buffer overflow, etc.

7.14.3 Measures

[Operation guide]

1) Limit the host that can input job data for the MFP, such as to specific print spool servers or gateway servers for scanning and faxing, etc.
2) Confirm the lists of PJL commands that are available on the MFP with the developers, and contact them if there are any unnecessary commands.

[Development guide]

3) Limit access to files and directories accessible by PJL commands.
4) Limit PJL commands available on MFPs. (Limit the necessary functions for users)
5) Execute all available PJL commands, including information confirmation commands, to ensure that the behavior of the MFP or information that can be obtained do not have any problems.

[Verification guide]

6) Create valid attack code for inspection of the MFP to be examined, to confirm that there are no problems in the behavior or information that can be obtained, using the published references of attack codes by PJL commands, such as directory traversal and buffer overflow, etc.

7.14.4 References

Date of publication	Source
June 2003	HP PCL/PJL Reference (Printer Job Language Technical Reference Manual) http://h20000.www2.hp.com/bc/docs/support/SupportManual/bpl13208/bpl13208.pdf PCL/PJL specifications of HP
March 2010	CVE-2010-0619 http://cve.mitre.org/cgi-bin/cvename.cgi? name=CVE-2010-0619 Report of buffer overflow using PJL INQUIRE command
November 2010	HP LaserJet Directory Traversal on the PJL Interface http://www.exploit-db.com/exploits/15631/ Report on directory traversal using PJL commands
January 2012	Hacking MFPs PostScript(um–you've been hacked) http://andreicostin.com/papers/Conf%20-%2028C3%20-%20Hacking%20MFPs%20(part2)%20-%20PostScript_um%20you_ve%20been%20hacked%20-%20SRLabs%20-%20v2.pdf Report on the vulnerabilities of PostScript
February 2012	MULTIFUNCTION PRINTER VULNERABILITIES http://msisac.cisecurity.org/resources/reports/documents/A-0012-NCCIC-130020120223MFPVulnerability.pdf Vulnerabilities of MFPs are referred to extensively

7.14.5 Seriousness and attack potential evaluation (reference value)

[Attack assumptions]

An attack method to obtain protected assets using PJL commands by accessing the protected assets using directory traversal is discussed here. The following is an assumption:

- The MFP cannot be accessed directly from the networks outside of the companies

[Scoring]

CVSS 2.0 Base value: 5.8 (Warning)

Attack source category	Possible attacks from neighboring networks
Complexity of attack criteria	Low
Pre-attack authentication Requirement	No authentication operation required
Confidentiality	Partial impact
Integrity	Partial impact
Availability	Partial impact

7.15 Problems due to vulnerabilities of the web management console

It is common for MFPs in recent years that all types of security settings, etc., including MFP network and printer settings, status management of the print function, jobs and devices, as well as the backup function, have been performed using the web management console. Typically, the web management console provides functions corresponding to the user category, such as MFP administrators, general users, or maintenance personnel, etc. These functions are used by user category by performing user identity authentication and access control. Therefore, the web management console provided by the MFP is also required to take measures against common vulnerabilities as a general web application that includes web servers inside.

7.15.1 [Attack methods and the impacts]

Unlike websites on the Internet, the MFP is connected to the in-house LAN and is mainly set up and configured for the usage that is closed in the LAN. Therefore, it is usually difficult for attackers on the Internet to access the MFP web management console and attack by exploiting vulnerabilities. However, vulnerability measures on the MFP web management console are very important, in consideration of misuses of web applications and unauthorized accesses to the protected assets by insiders or attackers who intrude on internal networks, etc.

"How to Secure Your Web Site (5th Edition)," provided by IPA, categorizes issues (vulnerabilities) to be considered when constructing web applications as follows, and presents the measures.[60] These measures against the vulnerabilities of web applications are essential even for MFPs, and the development considering each vulnerability and to inform users of the appropriate usages required.

1) SQL injection

In the case that the MFP has a database server inside and manages the protected assets, the web applications on the MFP in collaboration with the database prepares SQL statements based on the input information. In the case that there is a problem with the preparations of the SQL statements, there is a possibility that unauthorized uses of the database are caused by attackers (e.g., unauthorized viewing of data, tampering and deletion of data, and unauthorized login by authentication bypass, etc.).

Measures against such attacks are as follows:

- Prepare all SQL statements by implementing placeholder.
- In the case that the SQL statement is prepared by character string consolidation, correctly configure the literals in the SQL statement using the API[61] of the database engine for escape processing, etc.
- Error message should not be returned as it is.
- Appropriate authority should be given to database accounts.[62]

2) OS command injection

While OS commands may be unique on the MFP in some cases, there is a possibility that unauthorized data viewing, tampering, deletion, or unauthorized system operations, etc., are performed by unauthorized executions of OS commands of the web server from outside,

[60] Vulnerabilities of mail header injection will not be mentioned, because they have less chance of being used on the web management console of the MFP.
[61] The same applies to the API provided by the framework and language being used in the applications.
[62] Sharing only one database account that has a universal type of authority used to update or delete all objects shall be avoided.

depending on languages that have developed web applications, if input parameter checks of web application are insufficient.

Measures against such attacks are as follows:

- Avoid using the language function that can start the shell.
- In the case that the language function that can start the shell is used, check all variables that compose the argument, and execute only the processing that was previously permitted.

3) Uncheck of path name parameter/directory traversal

It may be a part of the OS command injection, but in the case when there are web applications that directly specify the file name inside the web servers in the external parameters, there is a possibility that attackers can specify arbitrary files when there is a problem in the implementation of specifying the file names, and unintended processing may be performed by web applications.

Measures against such attacks are as follows:

- Avoid implementations that directly specify the file name inside the web servers in the external parameter.
- When a file is opened, specify a fixed directory, but the directory name should not be included in the file names.
- Appropriately manage the settings for access authority to the files on the web servers.
- Check file names.

4) Defects of session management

In the case when there are defects in the management and issuance of session IDs used for maintaining login status of administrators and users on web applications of the MFP, there is a possibility that attackers can illegally obtain session IDs of the administrators and users, who are logged in, to gain access by impersonating the users.

Measures against such attacks are as follows:

- Make session IDs difficult to predict.
- Do not store session IDs in the URL parameters.
- Add the secure attribute to the Cookie that is used for HTTPS communications.
- After a successful login, start a new session.
- After a successful login, issue the confidential information in addition to the existing session IDs to check its value for each page.
- Do not use the fixed values for session IDs.
- In the case when session IDs are set to Cookie, be careful with the setting of the expiration dates.

5) Cross-site scripting

If there is a problem with the output processing to a web page, there is a possibility that the website may be tampered with by embedding the script, etc., or that a Cookie stored by the user browser may be obtained, etc. As a result of this, for example, session information may be leaked.

Measures against such attacks are as follows:

- Perform the escape processing to all elements being output to web pages.
- When outputting the URL, permit only URLs that start with “http://” or “https://.”
- Do not dynamically generate the contents of the <script> ... </ script> elements.
- Make sure the style sheet is not captured from an arbitrary site.
- Check the contents of input values.

- Create a parse tree from the HTML text input, and extract only the necessary elements that do not include scripts.
- Eliminate the character strings that correspond to the scripts from the HTML text input.
- Specify the character encoding (charset) in the Content-Type field in the HTTP response header.
- Add the HttpOnly attribute to the Cookie being issued to disable the TRACE method as the prevention measures of Cookie information leakage.

6) CSRF (Cross site request forgeries)

In the case that there is no mechanism in the applications on the MFP web server to identify whether or not the requests from the users logged in are intended requests by the users, there is a possibility that malicious requests may be accepted via external sites. Having this structure of web applications, the users who logged in may perform unexpected processing (such as the execution of functions available only by the users logged in, or tampering with, and deletion of, the protected assets) by the traps prepared by attackers.

Measures against such attacks are as follows:

- Make the pages that execute processing accessible by the POST method, and automatically generate the previous page to insert the confidential information into the "hidden parameters," and execute processing only if the value is correct on the execution page.
- Ask for entering the password again on the page immediately before executing the processing, and execute the processing only if the password entered again is correct on the execution page.
- Check the Referer if the source link is correct, and execute the processing only when it is correct.
- When any important operation has been performed, automatically send to the email addresses that are registered.

7) HTTP header injection

In the web applications that dynamically generate the field values of the HTTP response header of output responses to requests, by using parameter values passed from the outside, there is a possibility that attackers will add an arbitrary header field to the responses, or create an arbitrary body, and conduct attacks that may create multiple responses, if there is a problem in output processing of the HTTP response headers.

Measures against such attacks are as follows:

- Do not directly output headers, but use the header output API that is provided in the language or execution environment of the web applications.
- In the case that the header output API that properly processes the line feed cannot be used, developers should implement the appropriate processing by themselves not to permit the use of the line feed.
- Delete the line feed for all the inputs from the outside.

8) Lack of access control and authorization control

In the case that there is a defect in access control and authorization control of the web pages that can only be accessed while users or administrators are logged in, for the applications on the MFP web servers, there is a possibility that attackers can impersonate users or make unauthorized accesses, etc., to the functions that are not permitted.

Measures against such attacks are as follows:

- The web pages that require defensive measures by the access control function should be provided with the authentication function that requires confidential information input, such as a password, etc.
- Implement the processing of authorization control in addition to the authentication function, and make logged-in users inaccessible by impersonating other users.

In addition to the above viewpoints, it is necessary to develop the web applications that have taken basic measures; for example, measures to avoid malfunctions caused by the input of unexpected values for parameters, such as unauthorized input of a value that is not in the radio button or list box; or measures to avoid including the information in the messages that respond to the errors that favor attackers, or to avoid outputting the trace information, etc.

As described in the references, the vulnerability that administrator authority can be obtained by authentication bypass was published on the web management screen of a domestic MFP vendor in 2012. The vulnerability of authentication CSRF is presented here as an example of the vulnerability that existed on the web management console:

<Overview of web management console>

In this web management console, user identity authentication (including administrators, etc.) and session management after login are appropriately performed at the top page, to provide various functions according to the user authority. It is possible to encrypt accesses to the web management console by SSL/TLS. However, it is difficult in general to obtain communications contents by wiretapping in this case.

<Main functions provided by the web management console>

- Users

  User information management function, inbox management function, etc.

- Administrators

  Network settings function, HDD encryption function, HDD bulk deletion function, backup and restore function, security mode settings function, etc.

- Maintenance personnel

  Firmware update function, HDD format function, password initialization function. etc.

As described above, identity authentication, session management, and encryption of communications have been properly performed for this web management console. However, there was a possibility that the various functions, which only administrators with identity authentication or authorized administrators could execute, may have been invoked and executed by attackers, because no measure was taken against vulnerabilities of CSRF as shown in Figure 7-15. In this case, instead of the CSRF method to create another website to make administrators conduct unauthorized acts, the attackers sent PDF files to administrators to make them perform arbitrary operations by exploiting the function of PDF viewer software, for which JavaScript is automatically executed when administrators view the PDF files.

By this attack, there was a possibility that all functions provided for the MFP in the web applications would have been executed by the attackers if certain conditions were met; for example, the leakage of user information, exposure or damage of registration data, unauthorized execution of administrator functions such as HDD bulk deletion, etc., security mode resetting, rewriting of unauthorized firmware, etc.

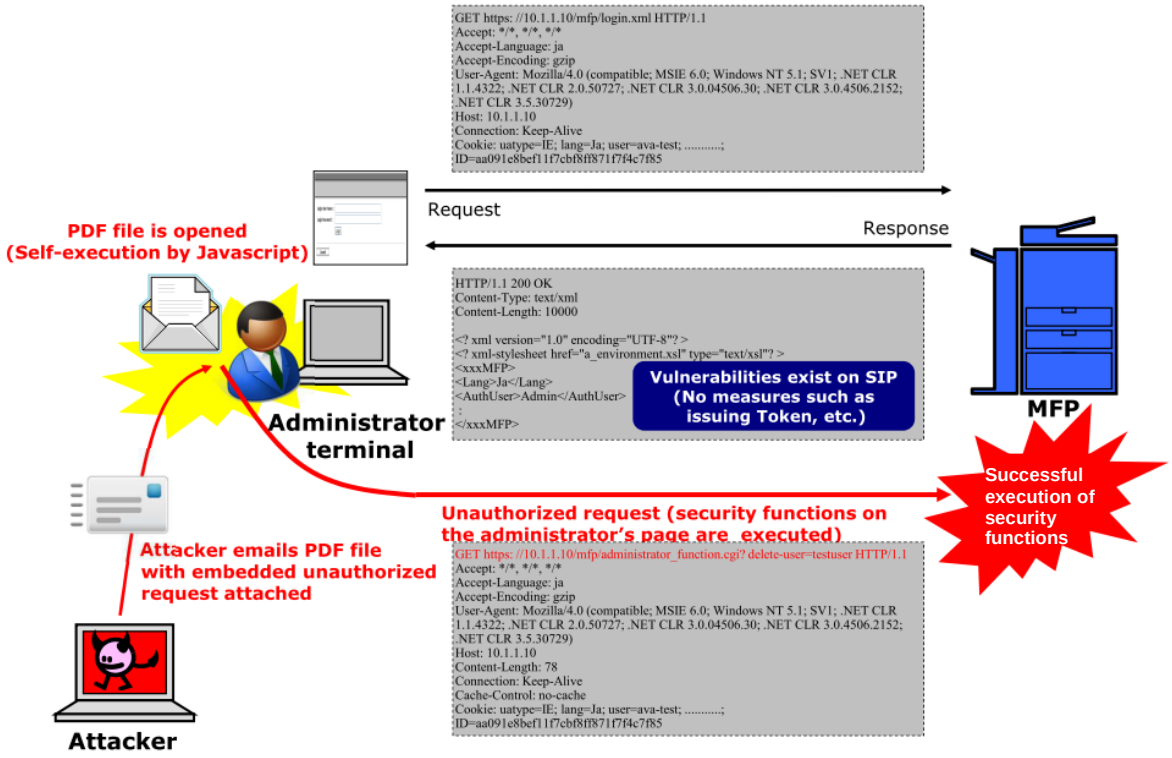


Figure 7-15 Example of attack by CSRF

7.15.2 [Causes and discussion]

The cause that makes the attack on the vulnerabilities of CSRF possible is that the measure against cross-site request forgery as described earlier is not performed (e.g.: verifying on the MFP using other identification ID than the session ID, such as Token, etc.). In the case when various functions, which only the users who are authorized or have identity authentication can execute, are provided, measures against vulnerabilities of CSRF are required.

The vulnerabilities, such as CSRF in the web applications that are described in this section, may be confirmed to some extent by vulnerability inspection tools for the general websites that are covered in Section 7.11.3. Since the session management mostly is not confirmed by the tools, it is necessary to ensure that the session value is actually checked by manual inspection and used, or that the implementation is not predictable or reusable with the session value, etc.

7.15.3 Measures

[Operation guide]

1) In the case that vulnerability information about the web management console is provided by vendors, etc., apply patches to the MFP provided or change the browser settings, etc., in consideration of the scope of the impact.
2) Access the web management console by encrypted communications, such as SSL/TLS, etc.
3) Follow the security guidelines of the MFP to setup the MFP on the network where the security can be ensured (in case there is a guideline).

[Development guide]

4) Develop web applications of the MFP, referring to the documents, etc., in the references.
5) Always check the latest vulnerability information related to the relevant applications, such as languages that are used in the web applications or on the web servers implemented on the MFP, and notify users. In the case of vulnerabilities having an impact on the proprietary MFP, provide patches or firmware that correspond to the vulnerabilities, in addition to giving notice about them.

[Verification guide]

6) Check with the web servers that are implemented on the MFP and script languages that are used in the web applications as to whether the known vulnerabilities apply.
7) Make sure there is no vulnerability in the web applications using the vulnerability inspection tools and manual inspections together.

7.15.4 References

Date of publication	Source
March 2012	IPA: How to Secure Your Web Site (Revised 5th Edition) http://www.ipa.go.jp/security/vuln/websecurity.html Notes for creating a secure web site and checklist for measures are summarized.
Frequently updated	OWASP (The Open Web Application Security Project) https://www.owasp.org/index.php/Category:OWASP Guide Project Guidelines with notes etc., for developing web applications. In addition to the above, more useful information, such as test guides, etc., is provided on this site.
Frequently updated	The Common Attack Pattern Enumeration and Classification (CAPEC) http://capec.mitre.org/index.html Various attack patterns are simply categorized and summarized.
April 2011	CVE-2011-1531 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1531 Vulnerabilities of EWS are reported.
April 2011	CVE-2011-1533 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1533 Vulnerabilities of Cross-Site scripting are reported.
April 2012	CVE-2012-1239 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1239 Vulnerabilities of possible authentication bypassing are reported.

7.15.5 Seriousness and attack potential evaluation (reference value)

[Attack assumptions]

Assuming that there is a vulnerability of CSRF in the session management of the management web applications, an attack in which attackers make administrators execute unauthorized instructions by using CSRF is discussed here. It is assumed that the confidentiality, integrity, and availability are impacted overall by making the administrators execute the backup and restore function on the MFP, including the protected assets.

[Scoring]

CVSS 2.0 Base value: 7.9 (Danger)

Attack source category	Possible attacks from neighboring networks
Complexity of attack criteria	Moderate
Pre-attack authentication requirement	No authentication operation required
Confidentiality	Overall impact
Integrity	Overall impact
Availability	Overall impact

7.16 Problems from the misuse of web-based maintenance functions

Attackers can illegally obtain the information inside the MFP and information of other systems related to the MFP, by exploiting these maintenance interfaces on some MFPs that provide web-based maintenance functions.

7.16.1 [Attack methods and the impacts]

The maintenance functions of the MFP include diagnosis of the remaining amount of toner and number of copies, diagnosis of failures, or replacement and repair of defective parts, in general. Among these functions, the following functions are used to replace a failed hard disk:[63]

1) The function to back up document files and address books in bulk inside of the MFP.
2) The function to overwrite document files and address books in bulk inside the MFP from certain files.
3) The function to delete and perform overwrite deletion of documents and address books in bulk inside the MFP.

The function to back up document files, described in 1), can retrieve documents in bulk that are stored on the hard disk inside the MFP to outside the MFP. This function is needed to replace with a new HDD when the HDD inside the MFP has failed.

The function that overwrites document files inside the MFP with certain files, described in 2), recovers the contents of the HDD using the backup data of the HDD saved in 1), and is called "restore."

The function to delete and perform overwrite deletion of documents and address books in bulk inside the MFP, described in 3), is used to delete the contents of the hard disk that needs to be replaced and disposed of. It is also used to prevent the information inside the MFP from leaking to third parties at the time of disposal of the MFP.

The interfaces inside the MFP as described above provide functions to perform maintenance remotely via networks, because they should be transferred to where the MFP is set up in order to perform the maintenance of the MFP.

In general, maintenance functions are executed from a terminal on the network in the organization as on a maintenance terminal shown at the top left in Figure 7-16. In the case of using the external maintenance services provided by developers or maintenance personnel, communications for remote maintenance through a network outside of the organization, such as in the upper-right corner of Figure 7-16 are performed. Maintenance interfaces directly connected to the main unit of the MFP may also be used in some cases.

[63] These functions are provided to users as administrator functions on some MFPs. However, it is assumed that these functions are implemented on the MFP as maintenance functions in this section.

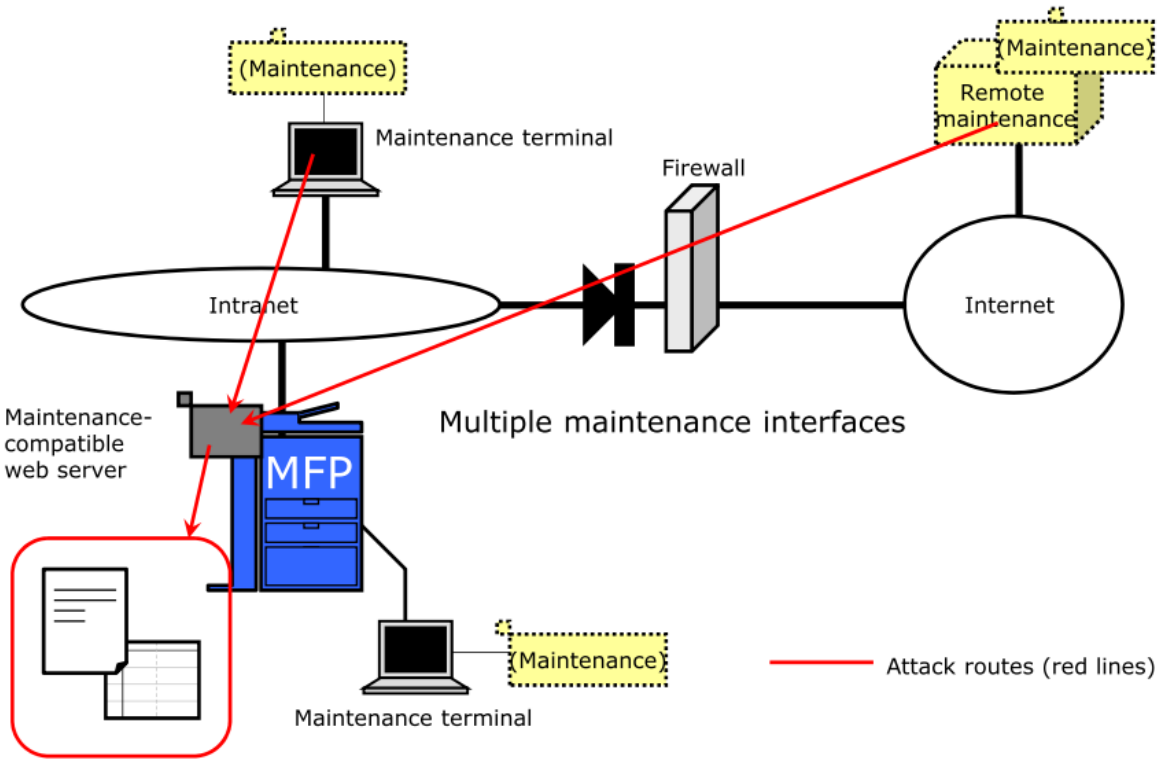


Figure 7-16 Example of method for accessing the maintenance interfaces (http)

As shown in the figure, there are multiple paths for the maintenance functions. Among these, it is assumed that the maintenance personnel use the web-based maintenance functions of the MFP in the users' intranet from a web browser on the maintenance terminal.

Figure 7-17 below shows an example of an attacker, who is a user, exploiting a maintenance person's session without authentication by performing CSRF against the web browser of the administrators, who uses the web-based maintenance functions, and making the maintenance person delete the data in the MFP.

The maintenance person opens a page of the maintenance functions after obtaining authentication on the maintenance website. Maintenance functions, such as data backups inside the MFP, can be executed without following the authentication procedure by injecting JavaScript code to open a specific URL on the administrators' browser as indicated in red lines, while the browser's maintenance function page is opened.

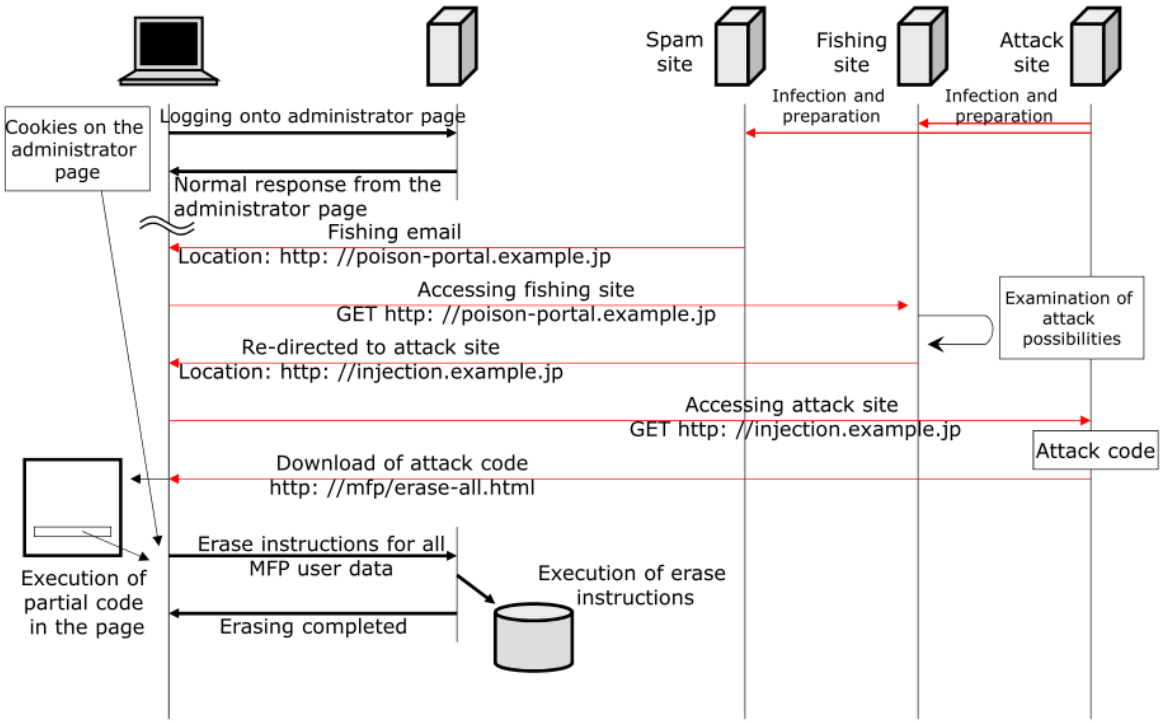


Figure 7-17 Example of a sequence for exploiting a maintenance interface using CSRF

The success of this attack method requires some conditions. A major assumption is that the session management function that can counter CSRF is not built into the maintenance website. Then, the page should remain open for use by maintenance personnel for maintenance functions, or there should be an insufficiency of the maintenance website, such as not managing logoffs, etc., to leave the session information on the maintenance terminal. On that basis, it is necessary to induce a browser on the maintenance terminal to a specific site to download the attack code. In addition, it is needed that the attacker is able to guess the command system of the maintenance website.

In terms of attack opportunities, it is even less than the CSRF to the users or administrators as described in Section 7.15. However, it cannot be said that there is no possibility that the conditions, behaviors or works of the maintenance personnel are visible.

In the maintenance works from a remote location, there are methods for the MFP to access the maintenance site to set up a dedicated connection, such as VPN, in a simple way. They are readily available on the user networks with IP address converting or firewall established.

7.16.2 [Causes and discussion]

When a defective part of the main unit of the MFP is replaced, maintenance interfaces of the main unit of the MFP perform important functions, such as backing up the internal information. Maintenance personnel of the MFP vendors or contractors perform maintenance works in general, but some maintenance functions may be disclosed to users for the convenience of users. In some cases, some dedicated maintenance software is disclosed to some users.

Although these maintenance functions are convenient, the functions for HDD replacement and disposal of the MFP are sometimes not clearly stated in the operation manuals of the MFP. Maintenance personnel of the MFP are responsible for parts replacement, but users need to back up the HDD contents when the HDD is replaced, because the users have responsibility over the HDD contents, including protected assets, etc. It is assumed, however, that the maintenance personnel may backup and restore the HDD contents upon replacement in this

research. In many cases, users do not have knowledge about the replacement of the HDD, or the methods or cautions for backup and restore, in general. It is a great benefit for users to have maintenance personnel take care of them.

In order to meet the needs of users who want high availability of the MFP, it is assumed that the maintenance functions may be opened outside via the networks. However, if the maintenance functions are exposed to the internal networks or to the outside, they would become targets for attackers. If they are the maintenance functions of the web applications as described in this section, they should be provided with a strong defense against much vulnerability that is described in Section 7.15.

If the convenience of the MFP increases in this way, threats also increase at the same time. The possibility to be intruded increases if the maintenance interfaces, in particular, are opened not only to the dedicated interfaces of the main unit of the MFP but also on the network. When third parties, such as maintenance personnel, take care of the HDD contents, the kinds of protection or measures that should be taken may become issues.

Not all MFP vendors are necessarily providing the backup function at this point. However, some measures to be taken are considered to use the backup function in order to continuously use the advanced MFP functions by shortening the service downtime for MFP users. The main measures include specifying the scope of access by function as of local maintenance functions, backup data protection by encryption, etc., for the important maintenance functions, such as backup and deletion.

7.16.3 Measures

[Operation guide]

1) Disable the maintenance functions from outside if they are not necessary, depending on the operating environment.
2) In cases when there are multiple maintenance functions, which are operable outside the maintenance functions using the web applications, disable the maintenance functions that are using the web applications.

[Development guide]

3) Dissemination of information to users of the risks due to enabling the maintenance functions externally.
4) Implementation of secure maintenance functions and the security default settings.

[Verification guide]

5) In case the maintenance interfaces are implemented by web servers, examine whether the measures against the vulnerabilities are implemented as described in Section 7.15, as with the case of the normal web console.

7.16.4 Reference

Date of publication	Source
June 2009	CWE-352 Cross site request forgeries http://jvndb.jvn.jp/ja/cwe/CWE-352.html

7.16.5 Seriousness and attack potential evaluation (reference value)

[Attack assumptions]

As assumed in this section, when the maintenance personnel use the web-based maintenance functions from the intranet, it is assumed that an attacker accesses all the protected assets on the MFP by executing functions, such as backup and restore by CSRF, together with the maintenance personnel.

- It should be the environment where the measures in the operation guide as above are not taken.
- It should be the environment where attackers can check the behaviors of the maintenance personnel.

[Scoring]

CVSS 2.0 Base value: 7.9 (Danger)

Attack source category	Possible attacks from neighboring networks
Complexity of attack criteria	Moderate
Pre-attack authentication requirement	No authentication operation required
Confidentiality	Overall impact
Integrity	Overall impact
Availability	Overall impact

7.17 Problems of using external authentication

In order to perform the appropriate access control for the protected assets inside the MFP, the MFP has a user identity authentication function. Some MFPs are implemented with the "external authentication" function to perform access control based on the results of the authentication function undertaken by the external authentication servers. In the case that the user identity authentication system is already configured in the office where the MFP is introduced, this external authentication function is considered to be used quite often from the viewpoint of convenience by the centralized user management. In this case, users are required to take measures, such as applying appropriate patches in accordance with the operational environment, etc., against several vulnerabilities[64] that exist in the external authentication servers. However, that is not the only viewpoint in terms of vulnerability. Vulnerability that exists inside the MFP mechanism itself, which uses the external authentication, should also be concerned.

7.17.1 [Attack methods and the impacts]

In this section, the mechanism using Microsoft Active Directory, which is implemented as many cooperation destinations of the external authentication of the MFP, is explained. Other than Active Directory, there are some external authentications of the MFP that can work with the NTLM,[65] which was used by Windows NT4.0 or earlier. However, the NTLM has old specifications, and they have been known to be vulnerable to man-in-the-middle attacks. This vulnerability can also be applied in the case that the NTLM is used for user authentication of the MFP. Therefore, an attack method in the case of using the authentication mechanism of the Active Directory, which have no problems in general use, is discussed in this section.

Supplement: Overview of Kerberos authentication

A mechanism called Kerberos is used for user authentication of Active Directory. As shown in Figure 7-18 "Kerberos authentication image," Kerberos consists of user terminals, servers that the users want to access, and KDC (Key Distribution Center). The KDC holds private keys to the user terminals (calculated from the password) and all private keys to the servers. Kerberos authentication using the KDC is applied as a means to share a session key for users to perform secure communications with the target servers. An overview of Kerberos authentication is described as follows:

[64] For example, vulnerability in the backdoor to Microsoft Active Directory is known. Directory server information is not necessarily reliable.

[65] Windows NT LAN Manager authentication

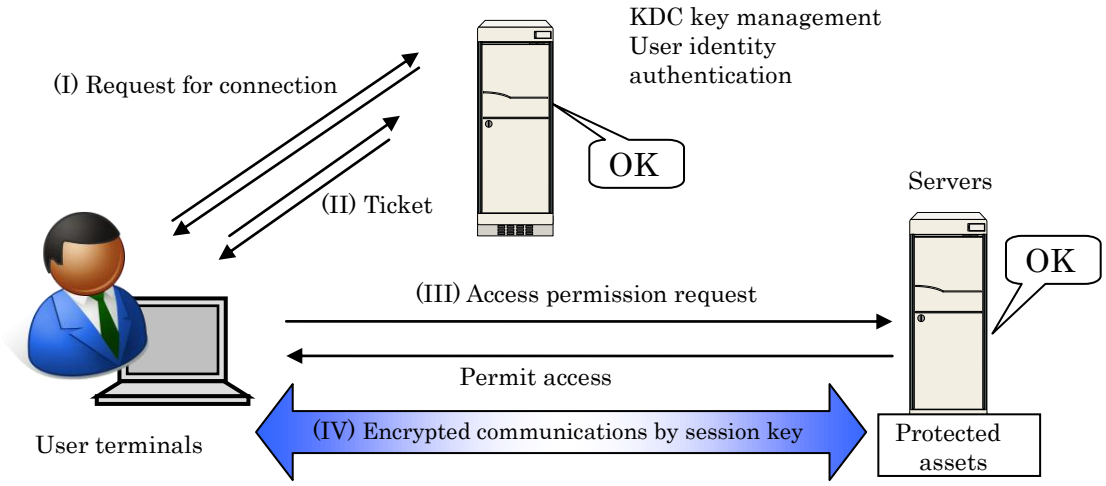


Figure 7-18 Kerberos authentication image

1) When a user wants to access the server from the user terminal, procedures give authentication to the user to ensure that the private key is recognized by both the KDC and the user terminal. The private key can be obtained by the calculation of the user's password at this time.
2) The KDC sends a ticket to interact with the server to the user terminal of the user who is authenticated. Encrypted information by the server key is added to the ticket.
3) The user terminal verifies and sends the ticket to the server. The server checks the ticket, determines that the user is given permission by the KDC by decrypting it with its own private key, and gives the user "access permission."
4) Then, encrypted communications between the user terminal and the server are performed by the session key, which was contained by encrypting in the ticket.

Unauthorized access to the protected assets of the MFP

In this mechanism, the attack on the authentication for MFP users is examined. As a result, the verification experiments confirmed that attackers can access the protected assets of the users, whom they are impersonating without knowing their passwords, if environments have access to the networks connected to the MFP.

This attack method is not publicly available at the moment. It is not really an unrealistic approach, and requires no special high attack potential.

Therefore, the details of the attack methods and their causes are omitted in this report due to the concerns of creating more opportunities for attacks by publishing such attack method details, in cases that there are vendors or models that do not take measures.

7.17.2 Measures

Although the details of the attack methods are omitted, the verification experiments confirmed that the attack would successfully gain unauthorized access to the protected assets if the "external authentication" mechanism on the MFP is used. When using the external authentication function, measures that should be considered to prevent such attacks are presented.

[Operation guide]

1) The MFP should be operated in an environment where monitoring of the existence of services running on the servers and monitoring of unauthorized ARP packets, etc., are available.
2) By checking the vulnerability information of the OS and services provided by the servers related to the external authentication, take measures as necessary, such as applying patches, etc.

[Development guide]

3) Security functions when accessing protected assets via the external authentication shall be added to ensure the security equivalent to the main unit authentication, even in case of using the external authentication.

[Verification guide]

4) Conduct intrusion tests if there is a possibility of attacks by comprehensively identifying attacks inside the MFP using an external environment to the MFP.

7.17.3 References

Date of publication	Source
January 2012	A Backdoor in the Next Generation Active Directory http://www.exploit-db.com/wp-content/themes/exploit/docs/18415.pdf The commentary article on the vulnerability of the backdoor hidden in Microsoft Active Directory
May 2004	NTLM authentication and the man-in-the-middle attack http://www.st.rim.or.jp/~shio/csm/ntlm/ Descriptions of the authentication servers by NTLM that can be easily impersonated
December 2011	CVE-2011-3406 Active Directory Buffer Overflow Vulnerability http://web.nvd.nist.gov/view/vuln/detail? vulnId=CVE-2011-3406 Vulnerability that authenticated users can execute arbitrary commands due to buffer overflow
June 2011	CVE-2011-1264 Active Directory Certificate Services Vulnerability http://web.nvd.nist.gov/view/vuln/detail? vulnId=CVE-2011-1264 Vulnerability related to XSS of Active Directory Certificate Services website
February 2011	CVE-2011-0040 Active Directory SPN Validation Vulnerability. http://web.nvd.nist.gov/view/vuln/detail? vulnId=CVE-2011-0040 Vulnerability of DOS by unauthorized requests

7.17.4 Seriousness and attack potential evaluation (reference value)

[Attack assumptions]

It is assumed that it is an environment where the details of the attack methods that are omitted are successfully conducted.

- It should be the environment where the measures in the operation guide as above are not taken.

[Scoring]

CVSS 2.0 Base value: 5.4 (Warning)

Attack source category	Possible attacks from neighboring networks
Complexity of attack criteria	Moderate
Pre-attack authentication requirement	No authentication operation required
Confidentiality	Partial impact
Integrity	Partial impact
Availability	Partial impact

7.18 Problems of malware infected files mixing into the MFP

Malware is a general term for a program, etc., that runs in a target device, and is created with the intention of producing actions that are unauthorized or that will cause harm. Malware, mentioned in this report, is a program that causes the unauthorized leakage and tampering of the protected assets against the infected MFPs and user terminals. A typical example of attack by malware against the MFP is uploading of unauthorized firmware with malware built-in, using the firmware update function as described in Section 7.7. Additionally, the propagation of malware to the user terminal connected to the running MFP that is infected is also assumed. The possibility of the malware stored in the MFP being propagated to the user terminals is discussed in this section.

7.18.1 [Attack methods and the impacts]

Possible methods of mixing the malware into the MFP are as follows:

- Upload firmware with malware built-in, using the firmware update function illegally. (Section 7.7)
- Upload programs with malware built-in, using the file update function by PJL described in Section 7.14.
- Upload any unauthorized programs using the maintenance interface function that is obtained by the methods described in Section 7.5.
- Save the malware inside the MFP by taking advantage of the vulnerable SDK described in Section 7.9.

It is assumed that the document files attached with malware are stored in the email queue to be sent to users by illegally operating the MFP by means of any of the above.

The method to propagate the malware stored in the queue to the user terminals uses general MFP functions. Recent MFPs have a function to attach images received via fax or scanned by the MFP to emails automatically, and to deliver to the user terminals.[66] Such functions can be executed as any users, or instructions can be executed directly using unauthorized methods. Buffer overflow, etc., can be used by the PJL of Section 7.14 for executing the instruction. In addition, instructions may be executed by the auto-run function using a USB that is modified illegally.

In order to guide users to execute the malware attached to emails, an attacker finds “Subject” or “Sender” trusted by the users, and adds them to create fake emails. If users are security-conscious, they can suspect fake emails from the subjects or the senders, and it is unlikely that they execute unauthorized attached files. However, in the case of receiving emails with familiar subjects and with file attachments from the normally-used MFP as a sender, users may open (execute) the attachment with relatively little suspicion.

[66] The MFPs of domestic vendors have deployed a function to distribute document data as email attachments, called Scan to Mail or Scan to E-Mail.

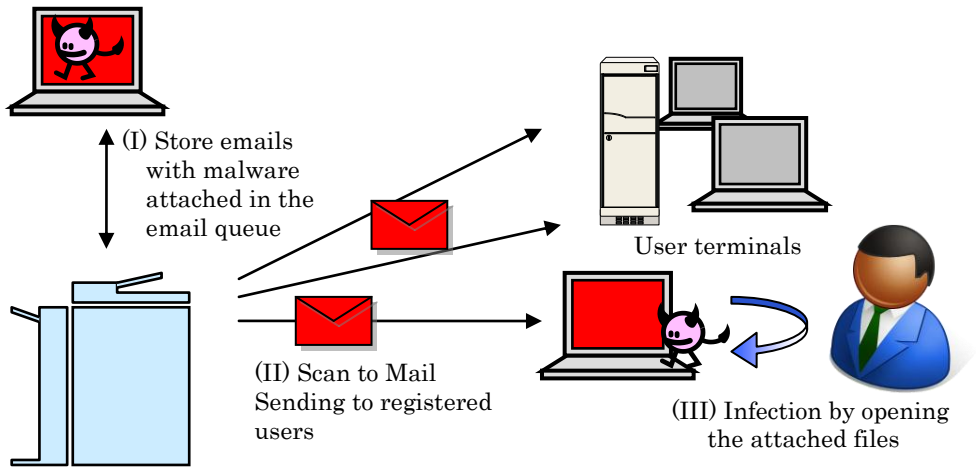


Figure 7-19 Image of malware propagation to the user terminals from the MFP

Supplement: Malware from which the MFP is impacted by attacks

While it is considered that there are attacks of malware propagation in the offices of the users having the MFP as a medium of infections as described in this section, there was a report that the MFP is impacted by unauthorized operations of user terminals, because the user terminals are infected with malware. In 2011, the American Chamber of Commerce became a target for targeted attack. In addition, a printer virus that prints a large volume on the MFP from the infected user terminal became well-known in the summer of 2012. It is generally difficult for the MFP functions to prevent such a case of impacts in the normal scope of operations of the MFP that is connected to the infected user terminal, by receiving a command for a large print job.

Supplement: Malware the main unit of the MFP is infected with

Next, there is also a possibility that MFPs themselves may be infected with malware that are mixed into the MFP (OS and firmware on the MFP are impacted). The MFPs may sometimes be infected with scripts that are attached to the documents, in addition to rewriting to the unauthorized firmware. In 2003, an MFP using a Windows-based embedded OS was infected with malware. In other words, the assumption that the MFPs are invisible from the external networks and that administrators do not perform unauthorized actions no longer holds, just for malware existing in one user terminal in the office.

Some public documents of MFP vendors that can be confirmed as of 2012, describe that the OS that is installed on the MFP is too minor to be infected with malware, as is shown in Figure 7-20 “Example of security concepts of MFP vendors” by some MFP vendors[67]

However, for example, in the case that a document attached with a script in which malware is embedded, is saved on the MFP, and the document is opened from the browser of the MFP panel, there is a possibility that the firmware or OS on the MFP may be impacted by malware if there is a vulnerability in the applications on the browser. Some MFPs are also confirmed to have had general-purpose embedded Linux as their OS in recent years. It may be desirable for developers to implement functional measures, such as script deletion from the document files, or not enabling it on the MFP, etc.

[67] A public document on the security concept of the MFP vendors is presented in the references.

> …since the majority of viruses and worms exploit vulnerabilities in Windows-based computers. **vendor name** **MFPs use non-standard operating systems** other than Windows. **Consequently, they are immune** to these viruses and worms.…

Figure 7-20 Example of security concepts of MFP vendors

7.18.2 [Causes and discussion]

Some MFPs have a function to save the data received as fax or scanned as PDF files, Microsoft Word, or Microsoft Excel formats, and to send them to users. By exploiting this function, it may be possible to send the documents with malware built-in in the form of attachments to emails to the user terminals. However, it is impossible to embed the script in the data converted into a PDF file, etc., to be saved, by using faxing or paper for inputting data in normal usage. In order to make this attack successful, it is assumed that the MFP should be already in an unauthorized condition; for example, a user who becomes an attacker should take procedures, such as saving the document data with a script directly into the email queue by using an unauthorized procedure that is prepared beforehand.

Measures that users should take are to maintain a policy that emails from the MFP which have unfamiliar files attached shall not be opened, and to make the policy known to everybody. As a measure in case the attached files have been opened, it is required to maintain applications, such as PDF reader, on the user terminal as versions without vulnerabilities all the time.

7.18.3 Measures

The function to send document files on the MFP automatically to a user terminal, etc., has the purpose of user convenience. This vulnerability does not depend on functional vulnerability of the MFP, but on the security policies and their operations in the offices of the users. Measures that users should take against the described attacks are explained here.

[Operation guide]

1) Operate a policy that emails even from reliable senders shall not be opened, if there is an unexpected attachment.
2) Maintain applications used in the offices of the users all the time as versions that do not have any problem using a reference to vulnerability information of the applications.
3) The formats that are not used to save the scanned or faxed images should be OFF in the MFP settings.

The development guide can suggest the implementation of the functions that the scripts embedded in the document data are automatically deleted, when sending the document data to the user terminals from the email queue on the MFP, but such functions could be disabled by rewriting the unauthorized firmware in some cases. As a supplement, the following measures can be taken against impacts on the MFP by malware. However, it is necessary to respond by taking functional measures described in each section, against malware mixing into the MFP through unauthorized procedures using the maintenance functions.

[Development guide]

4) Confirm that there are no vulnerabilities that have impacts from malware in the firmware or software that control communications of the MFP, using source code analysis tools, etc.
5) Make sure of the implementation that the scripts attached to the documents are not executed when verifying documents, etc., on the MFP operation panel.
6) Verify if the remodeling of published attack code has no impact on the OS that the MFP is implemented.

[Verification guide]

7) Examine the applications running on the MFP. For example, if the MFP has a browser installed on the panel, the browser or applications which operate by linking should be examined if they have no impact on the protected assets of the MFP by exploiting them.
8) Ecamine whether there is any impact on the MFP using the published attack code for the OS of the same systems.

7.18.4 References

Date of publication	Source
February 2012	MULTIFUNCTION PRINTER VULNERABILITIES http://msisac.cisecurity.org/resources/reports/documents/A-0012-NCCIC-130020120223MFPVulnerability.pdf Vulnerability report including malware mixing related to MFP
June 2012	Malware attack spread as email from your office's HP scanner http://nakedsecurity.sophos.com/2012/07/24/malware-hp-scanner/ Topic that malware is sent from the scanner to users
May 2012	PostScript: Danger Ahead? ! http://hackinparis.com/slides/hip2k12/Andrei-PostScript%20Danger%20Ahead.pdf Overview of methods to store malware on the MFP and propagate it
February 2011	Article about the attack via USB, which is published in BlackHat in 2005 http://news.mynavi.jp/articles/2005/08/03/blackhat4/index.html Methods which cause the USB to be mistaken as a device that automatically performs
December 2011	China Hackers Hit U.S. Chamber http://online.wsj.com/article/SB10001424052970204058404577110541568535300.html Article about the incident that U.S. Chamber of Commerce was attacked from China conducting unauthorized printing
June 2012	Printer virus http://blog.trendmicro.co.jp/archives/5415 Article about the printer virus that was epidemic in 2012
October 2007	Likewise, a “PDF virus” arose to a said vulnerability of Adobe http://itpro.nikkeibp.co.jp/article/NEWS/20071024/285333/ The file infection by attached files by taking advantage of the vulnerability of PDF
July 2010	The SHARP Security Suite http://files.sharpusa.com/Downloads/ForBusiness/DocumentSystems/MFPsPrinters/Security/copdow securitybro.pdf A claim that MFP OS is less likely to be susceptible to malware
July 2006	Comment on security by HP http://h20424.www2.hp.com/program/wdyhts/enterpriseprint/sg/en/pdfs/whitepaper/HP security solutions.pdf A claim that MFP OS is less likely to be susceptible to malware
February 2006	Lexmark technical white paper (Security) http://www.lexmark.com/vgn/images/portal/Security%20Features%20of%20Lexmark%20MFPs%20v1 1.pdf A claim that MFP OS is less likely to be susceptible to malware

April 2009	Samsung “MFP Security Overview” http://www.samsung.com/us/it_solutions/healthcare/_pdf/5_MFP%20Security%20Overview%20Rev0A.pdf A claim that MFP OS is less likely to be susceptible to malware
October 2003	Handling of vulnerabilities and computer viruses in Windows http://www.fujixerox.co.jp/company/news/release/2003/0919 msblast.html Example of the installed OS on the MFP that has been affected by malware

7.18.5 Seriousness and attack potential evaluation (reference value)

[Attack assumptions]

An attack on an MFP infected by malware described in the supplement is discussed here. It is assumed that the MFP is infected by putting malware on the office network, taking advantage of the vulnerability of any code that is executable on the embedded OS of the MFP, in the same manner as malware, in which the MFP with embedded Windows OS generated in 2003 has been affected. It is assumed that the malware that has a function to set up a backdoor using the vulnerability is published.

- It has to be an environment that does not take the above measures.

[Scoring]

CVSS 2.0 Base value: 8.3 (Danger)

Attack source category	Possible attacks from neighboring networks
Complexity of attack criteria	Low
Pre-attack authentication requirement	No authentication operation required
Confidentiality	Overall impact
Integrity	Overall impact
Availability	Overall impact

8. Other security measures

8.1 Problems of manufacture by developers and the time of delivery

For the attack methods against each vulnerability described in Chapter 7, the attacks on the MFP design assets or on the manufacturing and delivery process are based on the assumption that "the security in the manufacturing and delivery process are ensured by developers." Aspects of the attacks for these processes that should be ensured by the developers are explained here. If there is no sufficient security ensured in the manufacturing and delivery process by the developers, the attacks would succeed by an easier means without the attack procedures as described in Chapter 7. For example, for an attack that uploads unauthorized firmware from the maintenance interfaces of Section 7.7, reverse-engineering needs to be performed by using special hardware from the binary that is open to the public, because there is no source code of the firmware in the hands of an attacker. However, the attack will become much easier without reverse-engineering, if the attacker has directly obtained the source code by applying social engineering methods to the developers, removing design assets taking advantage of insufficient management, or exploiting the management system holes during the manufacturing and delivery process, etc. In addition to those, the leakage of internal documents with procedures for access to the confidential interfaces described in Section 7.5, may be possible during manufacturing and delivery process by the developers. In order to ensure security at the development sites as well as during the manufacturing and delivery process until MFPs are provided to users, the developers should be fully aware of the possibilities of the attacks during such procedures, and should ensure security by designing appropriate operation methods for each process.

8.2 Information provision to users through guidance

It is assumed that users may handle the vulnerabilities described in this section by the MFP settings, security policies, or a combination of both. In such case, developers shall provide precautions to users of more reliable ways, such as specifying in the guidance about the settings and operations in order to maintain the MFP in a secure condition; for example, cases when users should set up for the log records, or what users should observe to operate the MFP in secure conditions.

8.3 Outbound measures on the MFP

The outbound measures discussed in this section are measures against malware infection of client PCs and servers connected to the networks in the offices. Moreover, they are intended to prevent the malware infection from spreading from the office to the outside in case they are infected. As outbound measures, in addition to the malware expansion to the outside, the leakage of the protected assets to the outside, which is the ultimate goal of using malware, should be considered.

The 'Design and Operational Guide to Protect against "Advanced Persistent Threats," Revised 2nd Edition,'[68] by IPA suggests the measures and implementation methods for each point classified by performing the outbound measures mentioned above, from the viewpoint of detecting the backdoor and preventing malware from spreading as follows:

[68] http://www.ipa.go.jp/security/vuln/documents/newattack.pdf

1) Design of service communications path
   - Setup the cutoff rules for outward communications of the firewall.
   - Monitor the cutoff logs of the firewall.

2) Design an http communications detection function that imitates the communications patterns of browsers
   - Cut off the http method for usage of backdoor communications.

3) Design of sensor cutoff for the internal proxy communications (CONNECT connection) of RAT[69]
   - Monitor by the internal proxy log using the features of the establishment of the CONNECT communications of RAT.

4) Design of physical separation of direct internet connection at the most important points
   - Design VLAN, etc., so as not to directly connect to the internet at the most important points.

5) Protection of critical attack target servers
   - Protect the management segment to manage AD.
   - Apply patches for the AD services that are visible from users.

6) Design of VLAN network physical separation using switches, etc.
   - Design the user segment and the management segment separately.

7) Detection of infection activities due to capacitive load monitoring
   - Perform anomaly detection in log capacity or load on switches, etc., to cooperate with the security department.

8) Limited design of attainment scope of P2P
   - In addition to measures in 3) and 4), design the network for the purpose of eliminating unnecessary RPC[70] communications.

As described in Section 7.18, the MFP has a possibility of becoming a source of malware infection, and shall be managed by outbound measures as much as the other servers and client PCs in the offices. It also depends on the setup environments of the MFP, but some paths are directly connected to the external lines without a firewall, such as via fax line. The MFP that is infected with malware may transmit the protected assets to the outside by using those lines. In the case of performing outbound measures, such measures need to be taken to the lines that cannot be managed by a firewall, etc.

[69] Remote Access Trojan/Remote Administration Tool. It is a tool to remotely manipulate the systems that are intruded upon and used for incubation activities and theft activities, such as Poison ivy and Gh0st RAT, etc.

[70] Remote Procedure Call. It is a function to call the services that are running on a remote computer connected to the networks, to request processing. It has a function to assign a new port dynamically upon connecting to use it.

9. Discussion of the vulnerabilities related to new functions

In recent years, MFP vendors have developed new services, such as implementation of applications to smartphones and tablets, which were deployed initially to client terminal PCs, and seamless document management in conjunction with the cloud environment, etc. These services are intended to improve convenience for users, but are not intended to add new data workflows for the MFP usage described in Chapter 4. Smartphones and tablets are one of the user terminals, and the cloud computing is an extension of the communications system. However, for example, in addition to the external authentication in the cloud computing, authentication cooperation of the cloud service using the authentication information is performed. Therefore, the viewpoints regarding a new vulnerability in authentication cooperation are the focus in this chapter and are discussed, including the impacts of the deployment of the cloud environment. More specifically, the targets are the services that are developed for the corporations, and the services that securely store data in the cloud in coordination with authentication by Active Directory that is used in the external authentication described in Section 7.17, and output from the MFP at the company branches or other hubs, are the subject matter.

There is no vulnerability that the MFP can handle functionally, because this chapter is not a description of the attack procedures for the MFP provided by the vendors or the related client software. Attack procedures related to the authentication cooperation of Active Directory and the cloud services that are generated by the published implementation deficiencies of SAML are described as a reference when users consider the use of the MFP in coordination with the cloud environment.

9.1 Problems of the implementation deficiencies of SAML

There are two main technical points of view to ensure security in the cloud environment. One is to ensure the confidentiality and integrity of the protected assets stored in the storage on the cloud, and the other is the appropriate user authentication.

For the protected assets that are stored in the storage, it is common to use a method to realize the confidentiality and integrity well-balanced in such ways as ensuring the confidentiality by encryption, ensuring the integrity by redundant use of parity disks, and ensuring quantitative security using a secret distributing method. Actually, many cloud businesses accommodate services with such technical methods built-in.

For authentication, SAML[71] is well known as a technique to achieve cooperation with user authentication (single sign-on) by Active Directory that is operated in companies. In 2002, SAML 1.0 version was approved as an authentication cooperation technology, and is currently introduced in cloud businesses such as Google, etc.[72] Standard procedures of the authentication cooperation of SAML 2.0 are shown in Figure 9-1.

[71] Security Assertion Markup Language

[72] There are technologies, such as WS-Federation and OpenID for consumers as well, but they are not mentioned in this report.

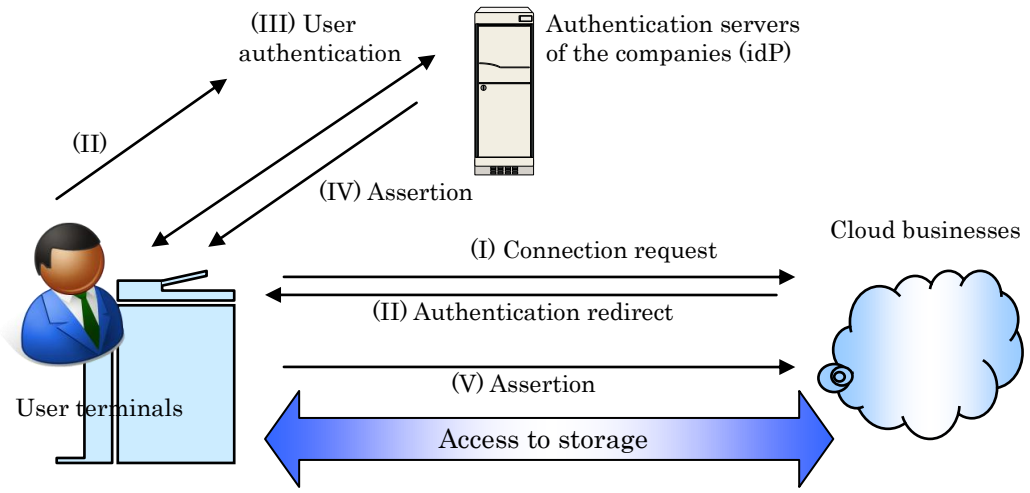


Figure 9-1 Image of authentication cooperation between Active Directory and cloud businesses

When a user accesses the protected assets on the cloud from a user terminal, the authentication request is redirected to the in-house authentication server (an authentication server called idP in coordination with Active Directory) during the access (from (I) to (II) in Figure 9-1). The authentication server issues the Assertion for the user (from (III) to (IV) in Figure 9-1). The user accesses the services on the cloud using the Assertion, which enables access to the protected assets as an authenticated user on the cloud through the verification of the Assertion ((V) in Figure 9-1).

9.1.1 [Attack methods and the impacts]

In this section, an explanation is given for an attack by an attacker who takes advantage of the vulnerability[73] of implementation deficiencies of SAML to access the protected assets of a user on the cloud by impersonating the user who performs authentication cooperation as described above. This attack uses the man-in-the-middle (MiM) attack at the network level. The attacker manipulates the packets, pretends to be a cloud to the user terminal, and obtains authentication as a user on the cloud by pretending to be the user towards communications from the cloud, so that he/she can access the protected assets of that user. Originally, SAML was a set of protocol specifications that can prevent MiM because an Assertion received from the idP and sent to the cloud in (IV) and (V) of Figure 9-2 includes identification information of the users and access points. Figure 9-2 However, this attack would be successful using SAML, which is implemented in the cloud services, because the measure taken against the MiM is incomplete as a result of the simplification. Because it is required to perform the MiM when arbitrary user is performing authentication works to access the protected assets on the cloud, there may be a small chance for attacks, but this attack itself is not difficult if scripts, etc., are prepared.

[73] http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-3891

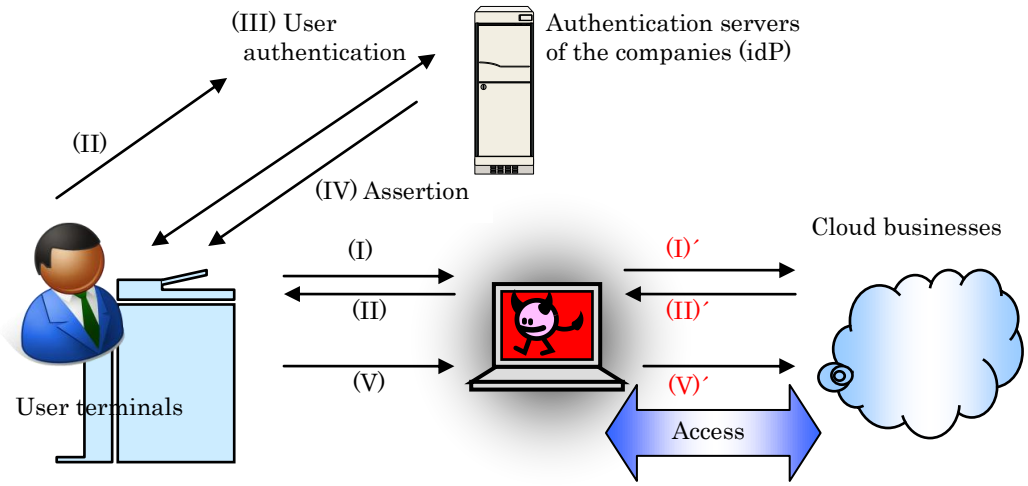


Figure 9-2 Image of unauthorized authentication by MiM

9.1.2 Measures

Measures that users should take against attacks described in this chapter are explained.

[Operation guide]

1) Confirm that the protected assets that are stored in the storage of cloud services are stored in a secure manner, such as with encryption and secret sharing.
2) Confirm that the data stored in the storage of cloud service is dispersion-managed, and is assured safety even at the time of failure.
3) Confirm that the cloud services are not providing an implementation that is vulnerable to attacks, such as MiM, in authentication cooperation between users and the cloud services.

Items that should be considered when using the cloud services are, for example, listed on the Open Government Cloud consortium website. When using the cloud services regardless of the cooperation with the MFP, it is desirable to read it in advance in order to understand the various risks due to the use of the cloud services.

9.1.3 References

Date of publication	Source
January 2012	SHARP CLOUD SOLUTION http://www.sharp.co.jp/print/solution/cloud/ List of services that provide printing on the MFP in the convenience stores, etc., from a variety of user terminals
April 2012	Article from PageScope Mobile of Konica Minolta http://www.konicaminolta.jp/about/release/2012/0403_02_01.html Article on the MFP driver and client software for smartphones and tablets
January 2011	Learning the authentication cooperation and account management technology required for the era of cloud computing http://enterprisezine.jp/iti/detail/2754 Article describing account management and single sign-on

November 2011	How to choose the cloud by learning from the security incidents of Dropbox and Google and cloud security guidelines http://web-tan.forum.impressrd.jp/e/2011/11/09/11249
Appropriately Updated	OASIS Security Services (SAML) TC https://www.oasis-open.org/committees/tc_home.php? wg_abbrev=security Website of SAML technical committee
October 2008	Formal Analysis of SAML 2.0 Web Browser Single Sign-On: Breaking the SAML-based Single Sign-On for Google Apps http://www.ai-lab.it/armando/pub/fmse9-armando.pdf

10. Conclusion

The MFP is one of the products that shall be considered of the numerous vulnerabilities in the usage in the offices where protected assets are handled. Protected assets stored on the HDD or SSD of the MFP should have the same level of security as file servers in the offices. Moreover, interfaces, including the websites that are provided to administrators and users, shall eliminate the possibility of attacks, such as buffer overflow and injection, etc. In that sense, the MFP is required to have security-conscious operations as much as the file servers and web servers in the offices, and should be installed with the appropriate functions to ensure the security that enables such operations.

This Research Report V2.0 explained specifically about the vulnerabilities that the MFP users, developers and evaluators, who evaluate security functions, should be aware of. This report covers aspects of all vulnerabilities since fiscal 2010 and later, that have been reported in the CVE with respect to printers and MFPs. This research found out that lots of vulnerabilities among these are discovered on the MFPs overseas, and MFPs in Japan which are used in a security-conscious environment as an assumption have reported almost no vulnerabilities.

However, some of the attack procedures described in this report have been used to make successful attacks against the MFPs of Japanese MFP vendors using the verification experiments, and it is confirmed that there are some vulnerabilities in the Japanese MFPs as well. These vulnerabilities may not be conspicuous in some forms of usage. When the users purchase the security-conscious MFPs, it is desirable to check with developers that there are no problems with vulnerabilities in view of the usage environment and security policies in the offices.

Due to new additional functions and cooperation with external services in the future, it is considered that new vulnerabilities of the MFP will be discovered, and that simple attack methods that seem to be unrealistic at this point will be published as well. In order for MFPs as security products representing Japan to continue to be used throughout the world, both users and the developers should continue to check vulnerability information and take measures respectively.

Research Report on the Security of MFPs V2.0

IT Security Center, Technology Headquarters, Information-technology Promotion Agency, Japan

March 2013