imagine. change.

MFP/Printer Security White Paper

Version 1.01 2023/9/29

Table of Contents

1. Introduction

Ricoh product safety and the importance of product security to the overall Ricoh Group

With the development of an information society, various threats such as frequent cyber attacks and unauthorized external access are all around us. In addition, as the scope of corporate response expands with the tightening/diversification of regulations in various countries, the emergence of geopolitical risks, and the like, companies are increasingly needing to promote security measures throughout the entire supply chain.

Ricoh regards “information security” as the scope of activities necessary to “safely and securely protect customer information from threats” and is implementing various measures to do so. This document introduces the functions and organization in that as activities to protect customer information handled by our products and services from attackers.

In order to ensure security, we ask that configuration and operation of security be done according to the customer's environment.
Ricoh communicates the importance of security to customers and helps them to make the right security settings.

Product security basic policy and concepts at Ricoh

This information security report provides an overview of the Ricoh Group’s information security initiatives. We encourage you to take a look.

Details can be seen on the Ricoh website.
URL：https://www.ricoh.com/security

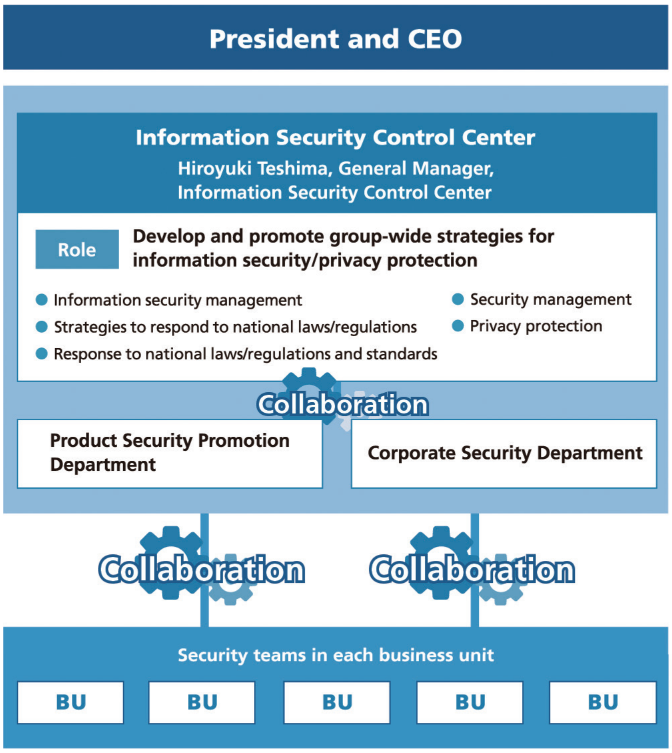
2. Information security management organization

Organization for achieving and maintaining product security

Based on international information security standards (ISO/IEC*1, NIST*2, etc.), we have established and strengthened an organization that is aware of information security for the entire supply chain of our group. We also appropriately anticipate security risks related to business systems in each process of planning, design, purchasing, production, and sales, and we continuously study and implement countermeasures.

The “Information Security Management Center” has been set up under the direct control of the CEO, and it is responsible for planning and promoting strategies of information security and privacy protection for the entire Group. The Information Security Management Center works with Product Security Promotion Department, which is responsible for product security, the Corporate Security Promotion Department, which is responsible for information security for the entire business, and security teams organized in each business unit to strengthen Group-wide activities.

*1)
ISO/IEC：International Organization of Standardization/International Electrotechnical Commission
*2)
NIST：National Institute of Standards and Technology



President and CEO

Information Security Control Center
Hiroyuki Teshima, General Manager,
Information Security Control Center

Role Develop and promote group-wide strategies for information security/privacy protection

- Information security management
- Strategies to respond to national laws/regulations
- Response to national laws/regulations and standards
- Security management
- Privacy protection

Collaboration

Product Security Promotion Department

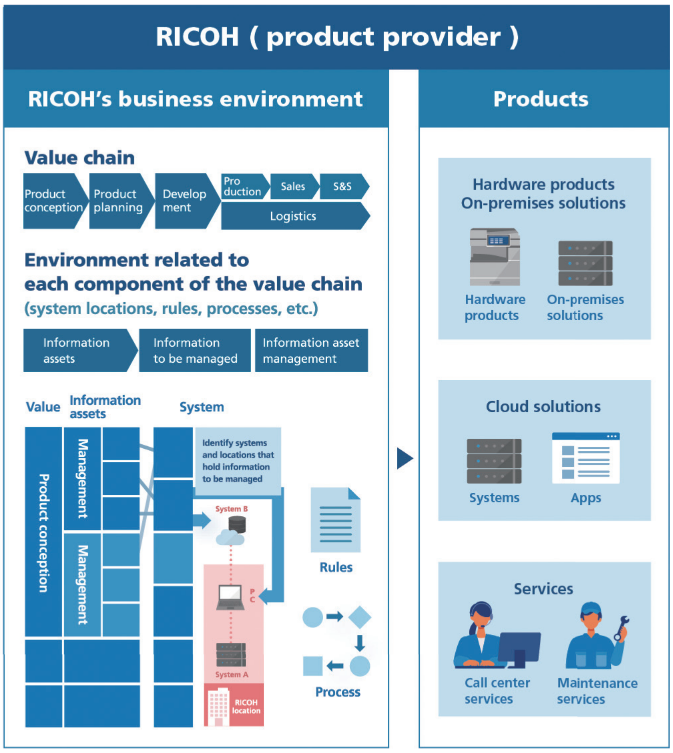
Corporate Security Department

Collaboration

Collaboration

Security teams in each business unit

BU BU BU BU BU



3. Security response policies for MFPs and printers

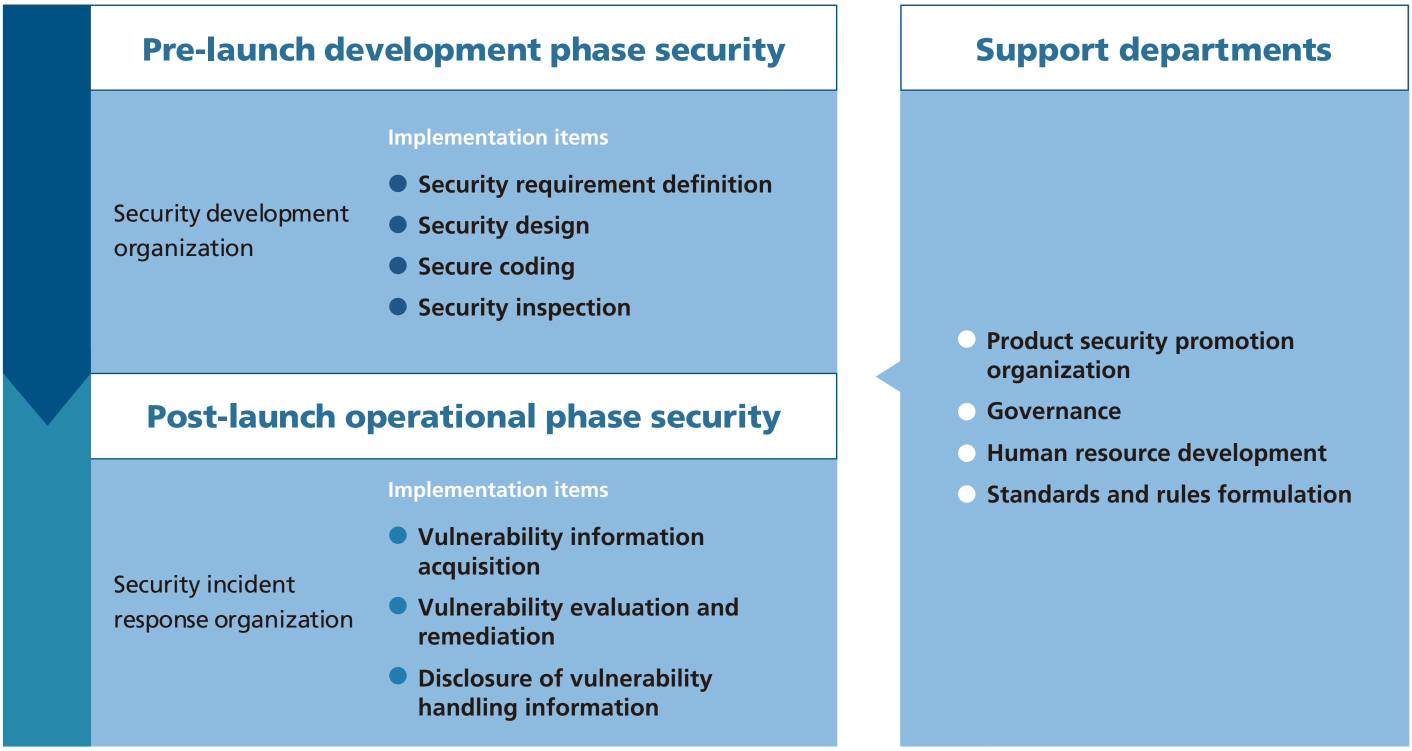
3 - 1 Organization separated into two phases

The digitalization of aspects of where we live and work has transformed us into an environment where many goods and services are connected, and cyber attacks are becoming increasingly advanced and sophisticated.

Against this backdrop, the Ricoh Group sets phases as those before and after launch based on the security response policy to ensure that customers can use our products and services with peace of mind. In the pre-launch development phase, a security development organization is formed to prevent the introduction and release of vulnerabilities. In the post-launch operational phase, a security incident organization is formed to detect and respond to vulnerabilities as early as possible.

〈 Security response policy 〉

- Acquire security technologies that keep pace with advances and innovations in digital technology.
- Establish an organization to implement product security.
- Strive to maintain quality related to security by establishing group-wide standards that comply with international standards.
- Develop security-conscious products and services and conduct security inspections to prevent introduction and release of vulnerabilities.
- Collect information on vulnerabilities and take appropriate action when it affects our products and services.
- Provide customers with useful information about the security of our products and services.



Pre-launch development phase security

Security development organization

Implementation items

- **Security requirement definition**
- **Security design**
- **Secure coding**
- **Security inspection**

Post-launch operational phase security

Security incident response organization

Implementation items

- **Vulnerability information acquisition**
- **Vulnerability evaluation and remediation**
- **Disclosure of vulnerability handling information**

Support departments

- **Product security promotion organization**
- **Governance**
- **Human resource development**
- **Standards and rules formulation**

3 - 2 Security policy and initiatives in the development phase

To ensure that customers and users of our products and services can use them with peace of mind, the Ricoh Group will practice security by design based on ISO/IEC 27034-1:2011（Application security — Part 1: Overview and concepts）, which considers security throughout the lifecycle of products and services from the planning and design stages.

3 - 2 - 1 Security development policy

The Ricoh Group will establish a security development organization and implement measures to prevent the introduction and release of vulnerabilities during the development of products and services.

Prevent introduction of vulnerabilities

We design security measures against product and service threats and implement security measures accurately and safely.

Prevent release of vulnerabilities

We conduct vulnerability assessments and take necessary countermeasures when vulnerabilities are found.

3 - 2 - 2 Action guidelines for security development

The Ricoh Group will practice and study the following items as Group regulations to prevent the introduction and release of vulnerabilities.

Definition of security requirements

We will determine the information and functions that need to be protected by security, the operational environment in which security measures are to be taken, and the target values for security risk reduction that are compatible with the characteristics of the product or service.

Security design

We will identify threats to information and functions that need to be protected and design security functions and secure operating environments/methods（security measures）to mitigate the occurrence of threats.

Moreover, we will design security functions that counter threats with a program structure and mechanism（security architecture）that does not cause disabling or performance degradation of the function itself.

Secure coding

To avoid introducing vulnerabilities during implementation, we confirm coding by static analysis.

Security inspection

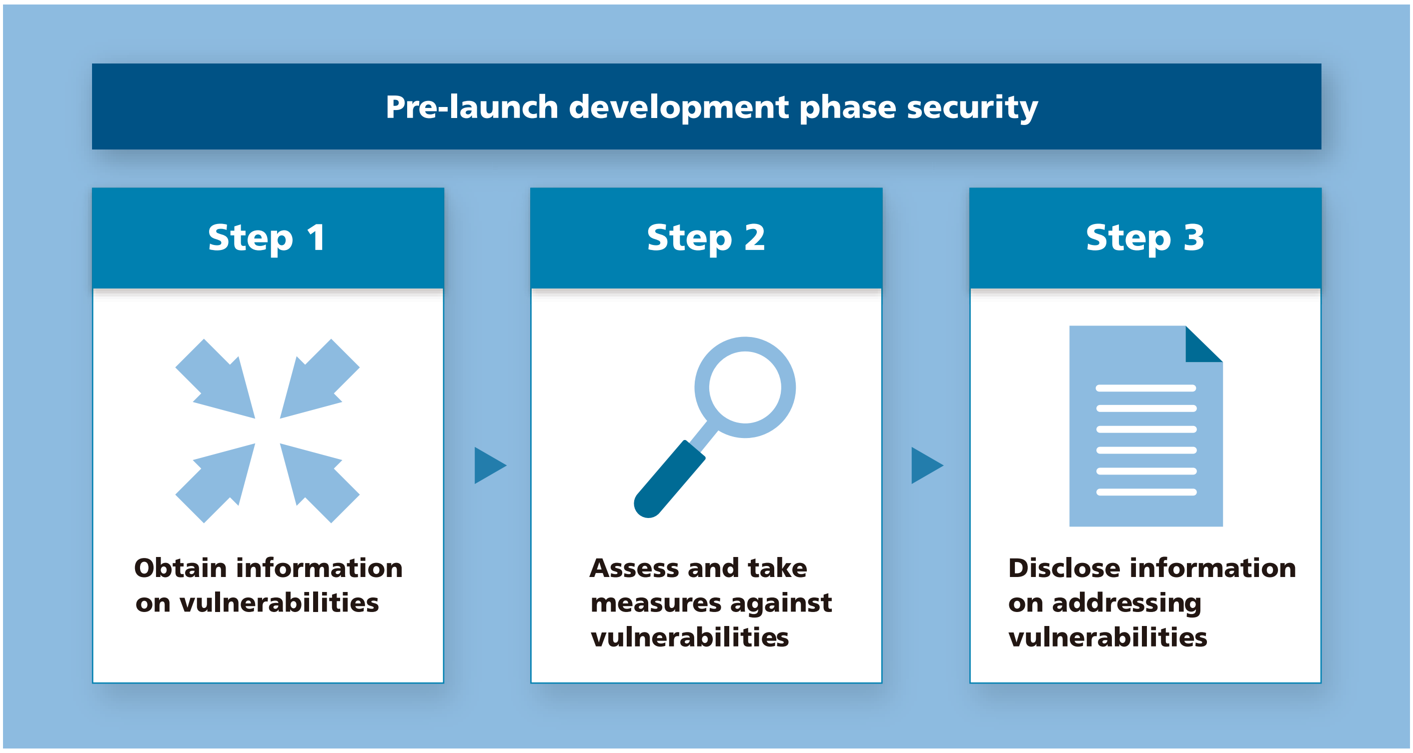
We conduct security inspections according to the characteristics of the products and services, and take necessary measures if vulnerabilities are found.

Security response policies for MFPs and printers

3 - 3 Security policy and initiatives in the operation phase

The Ricoh Group will respond to vulnerabilities based on “ISO/IEC 29147（Vulnerability Disclosure）” and “ISO/IEC 30111（Vulnerability Handling Processes）” for early detection and early response to vulnerabilities that may affect products and services after they are provided to the market. We also participate in the “Information Security Early Warning Partnership[*3]” to minimize damage caused by vulnerabilities.

[*3] Information Security Early Warning Partnership Guidelines（issued by Information-technology Promotion Agency, Japan（IPA)）



Pre-launch development phase security

Step 1 — Obtain information on vulnerabilities

Step 2 — Assess and take measures against vulnerabilities

Step 3 — Disclose information on addressing vulnerabilities

3 - 3 - 1 Vulnerability processing and disclosure policy

The Ricoh Group will establish a security incident response organization to ensure that users of our products and services can use those with peace of mind, and that organization will obtain information on vulnerabilities, assess and take measures against those, and disclose information on addressing vulnerabilities.

Obtain information on vulnerabilities

The Ricoh Group shall obtain information on vulnerabilities broadly and quickly from sources inside and outside the Group, and use a vulnerability management system[*4] to evaluate information on vulnerabilities and share that with the development department responsible for countermeasures against vulnerabilities of the product or service.

Obtain information on vulnerabilities in the Ricoh Group

We will continuously conduct security inspections throughout the lifecycle of products and services according to the characteristics of the products and services.

Obtain information on vulnerabilities outside the Ricoh Group

We will collect information on product vulnerabilities from users of our products and services, security researchers, and organizations that collect and distribute security-related information (such as JPCERT/CC[*5]).

[*4] The Ricoh Group’s internal system to manage vulnerabilities from obtaining information to completing countermeasures

[*5] Abbreviation for Japan Computer Emergency Response Team Coordination Center JPCERT/CC performs tasks such as collecting computer security information, supporting incident response, and disseminating computer security-related information.

Security response policies for MFPs and printers

Assess and take measures against vulnerabilities

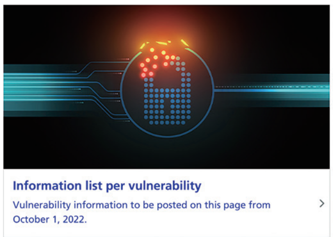
The product/service development department will evaluate the impact of the vulnerability received in the vulnerability management system on the product/service, and if it is confirmed that the vulnerability affects the product/service, the department will prepare information on and countermeasures against vulnerabilities as information on addressing vulnerabilities after implementing the necessary security measures.
To evaluate vulnerabilities from an objective viewpoint, we have established a Security Technology Committee as an organization to ensure that fair decisions are made.

Regarding the vulnerability response time, Ricoh sets deadlines for the implementation of countermeasures, aiming for a rapid response at the level of advanced security companies.
Furthermore, we will monitor and evaluate the status of implementation of measures against the set goals on a regular basis and make improvements in order to respond more promptly.

Disclose information on response to vulnerabilities.

The Ricoh Group will disclose as information on addressing vulnerabilities information on and countermeasures against vulnerabilities（including workarounds）to those who need such information at the appropriate time in accordance with the “principle of simultaneous disclosure of information on countermeasures[*6]” and the “principle of consistent disclosure date[*7].”
Information is disclosed per vulnerability on the Product Security page of the Ricoh website, viewable per product or service, allowing customers to quickly search and view the status of response for the models they are using.

For details, see the information to address vulnerabilities in products and services on the Product Security page.
URL：https://www.ricoh.com/security/products



Information list per vulnerability

Vulnerability information to be posted on this page from October 1, 2022.

Vulnerability information list per product/service

Vulnerabilities in Ricoh products and services discovered or fixed since October 1, 2022 can be searched by product or service

[*6] When information on a vulnerability is disclosed, information on countermeasures shall also be provided at the same time. If we disclose information about vulnerabilities before countermeasures are in place, there is a possibility that malicious third parties will develop and distribute attack code to exploit the vulnerabilities, which could then be used to launch cyber attacks against customers.

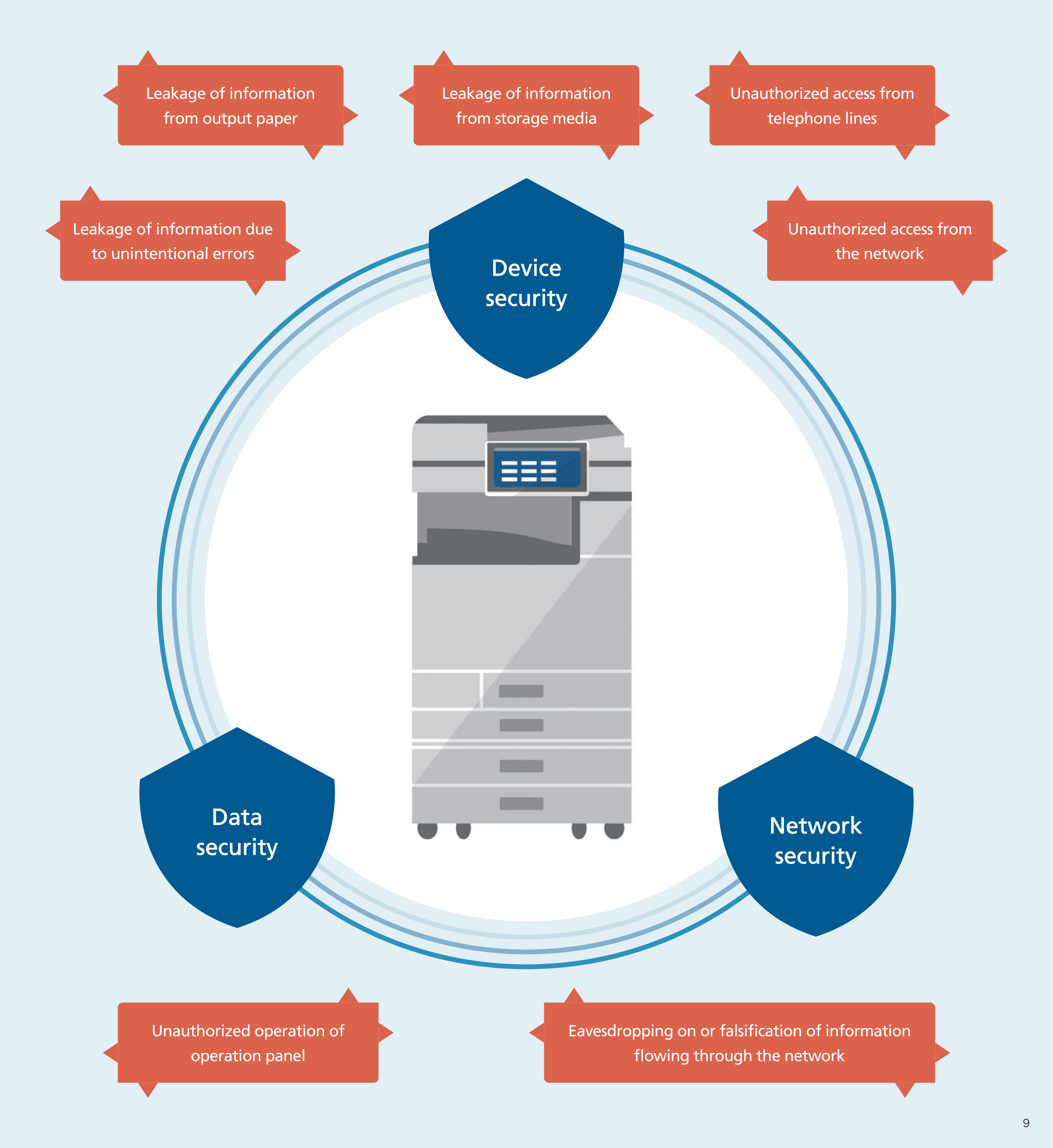
[*7] In the case of vulnerabilities that also affect the products and services of other companies, information disclosure shall be made with a certain level of coordination among the parties concerned. If we disclose information independently without waiting for the information disclosure date coordinated among concerned parties, that would expose customers who use other companies' products and services to the risk of cyber attacks.

4. Security threats for MFPs and printers and countermeasures against them

4 - 1 Overview of security functions for various threats

With the development of an information society, various threats such as computer viruses, leakage of personal information, and unauthorized external access are all around us.

In response to increasingly diverse threats, Ricoh is making various efforts as shown below, separated into three categories, to quickly focus on security measures for MFPs and assume various security threats to the extent possible.


Leakage of information from output paper
Leakage of information from storage media
Unauthorized access from telephone lines
Leakage of information due to unintentional errors
Unauthorized access from the network
Device security
Data security
Network security
Unauthorized operation of operation panel
Eavesdropping on or falsification of information flowing through the network

4 - 2 Device security

4 - 2 - 1 Firmware falsification prevention

MFPs and printers have built-in software called firmware that controls the operation of that device.
If this firmware is falsified by a person with malicious intent, it will not operate properly, and there are risks such as intrusion into the network using these devices as a stepping stone or destruction of the devices by unauthorized programs.
Devices designed by Ricoh are built with Trusted Platform Module (TPM) , and are designed not to start up if the firmware is falsified.

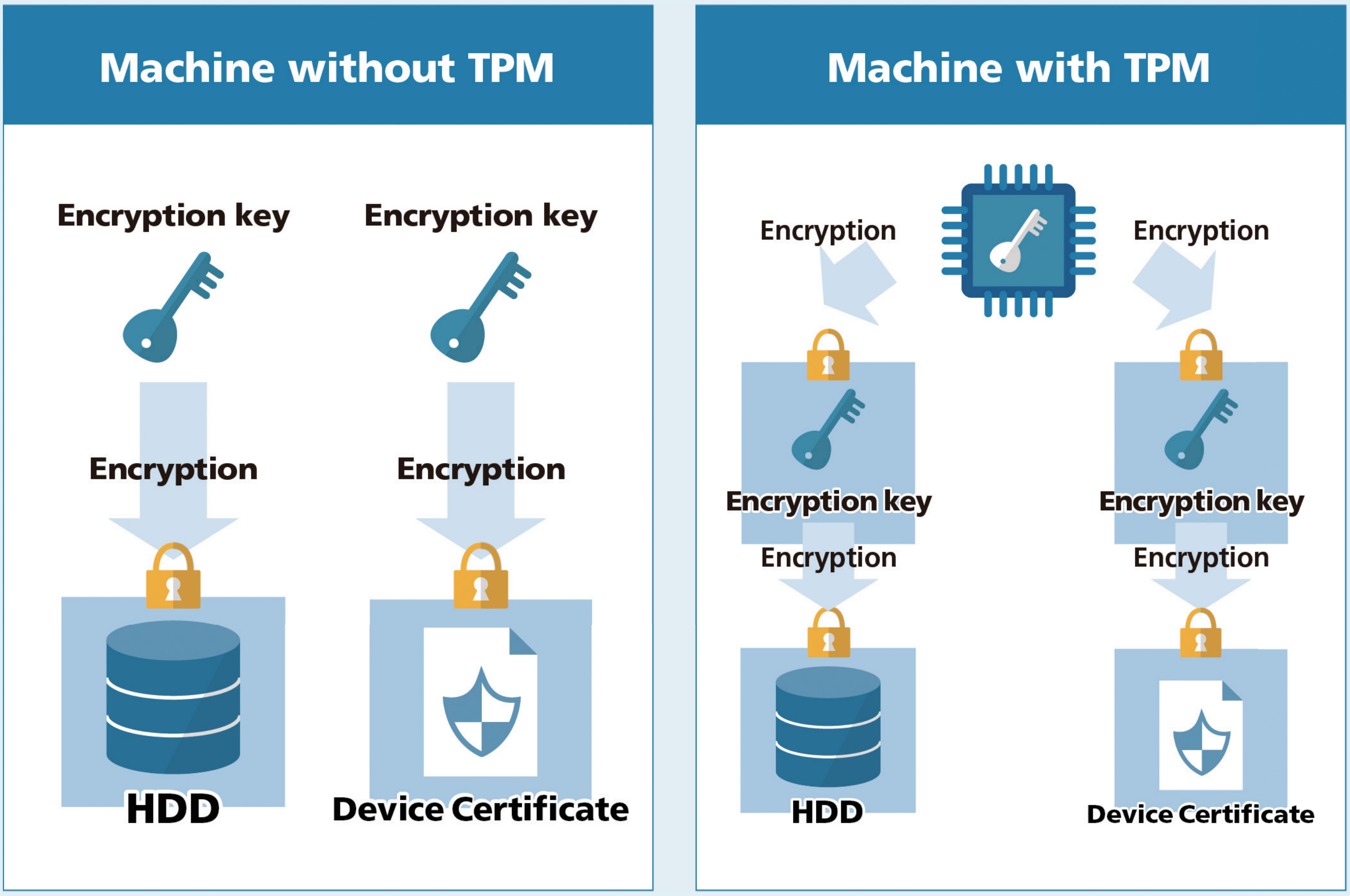
Moreover, the encryption keys used for hard disk encryption and device certificate encryption are further encrypted and protected by a root encryption key within this TPM.
The root encryption key cannot be read from outside the TPM, thus securing the information in the MFP.

RICOH IM C6010/C5510/C4510/C3510/C3010/C2510/C2010 support the most recent standard, TPM2.0.

A list of devices that support TPM can be seen on the Ricoh website.
URL：https://www.ricoh.com/products/security/mfp/function/tpmlist

If the encryption recording location is discovered, the encrypted data can be decrypted.

The root encryption key is held inside the TPM, so unauthorized reading cannot be done.



4 - 2 - 2 Sequential deletion of temporarily stored data*8

In situations such as when a document is read by a copier/scanner or output from a computer, some data may be temporarily stored on the hard disk drive or in memory.

This data includes image information, information input by the user, and device configuration information.

If this information is stolen in some way, information leaks may occur.

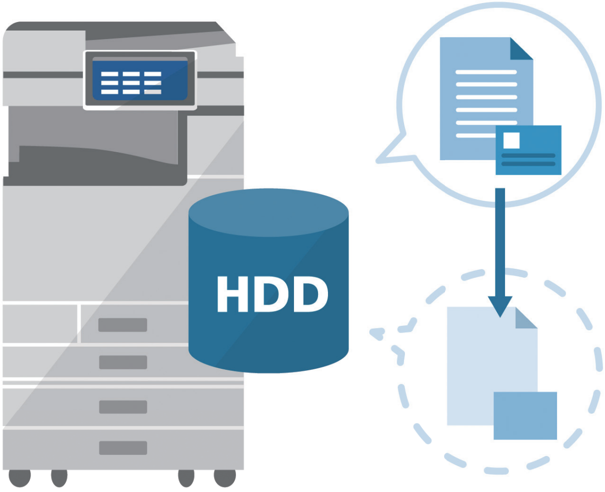
Ricoh MFPs erase temporary data stored on the hard disk drive by randomly overwriting it with 0s and 1s.

The image data stored in the MFP during copying and printing is sequentially deleted at each job execution.

- A method that complies with the U.S. National Security Agency (NSA) and U.S. Department of Defense (DoD) recommendations for the handling of classified information is employed.
- Repeatedly overwriting and deleting makes it virtually impossible to access temporary data (the number of overwrites can be selected from 1 to 9) .

Methods of sequential deletion

NSA	Data is overwritten twice with random numbers and once with zeros.
DoD	Data is overwritten the first time with random numbers, the second time with complements of the first time's random numbers, and the third time with random numbers.
Random Numbers	Data is overwritten with random numbers a specified number of times. The number of overwrites with random numbers can be selected from 1 to 9.



*8)
This function is available for models equipped with a hard disk drive for data storage.

4 - 2 - 3 Batch deletion of data

When an MFP is moved to another department or disposed of, user information and the like registered on the hard disk/SSD inside the device is batch deleted.

Batch deletion of data

NSA	Data is overwritten twice with random numbers and once with zeros.
DoD	Data is overwritten the first time with random numbers, the second time with complements of the first time's random numbers, and the third time with random numbers.
Random Numbers	Data is overwritten with random numbers a specified number of times. The number of overwrites with random numbers can be selected from 1 to 9.
BSI / VSITR	Data is overwritten with 0x00,0xFF,0x00,0xFF,0x00,0xFF,0xAA. It is overwritten a total of seven times.
Secure Erase	Data is overwritten and deleted using an algorithm built in to the hard disk.
Format	The hard disk is just formatted. Data is not overwritten, but this method is fast.

We support the above methods of deleting so customers can implement the method that best fits their internal policies. The effect of overwriting and deleting is equivalent, except for formatting.

4 - 2 - 4 Data theft prevention by storage encryption

Address book data, authentication information, stored documents and other data stored in the main unit of the MFP is encrypted when data is recorded. This prevents information leaks even if the storage is physically stolen.

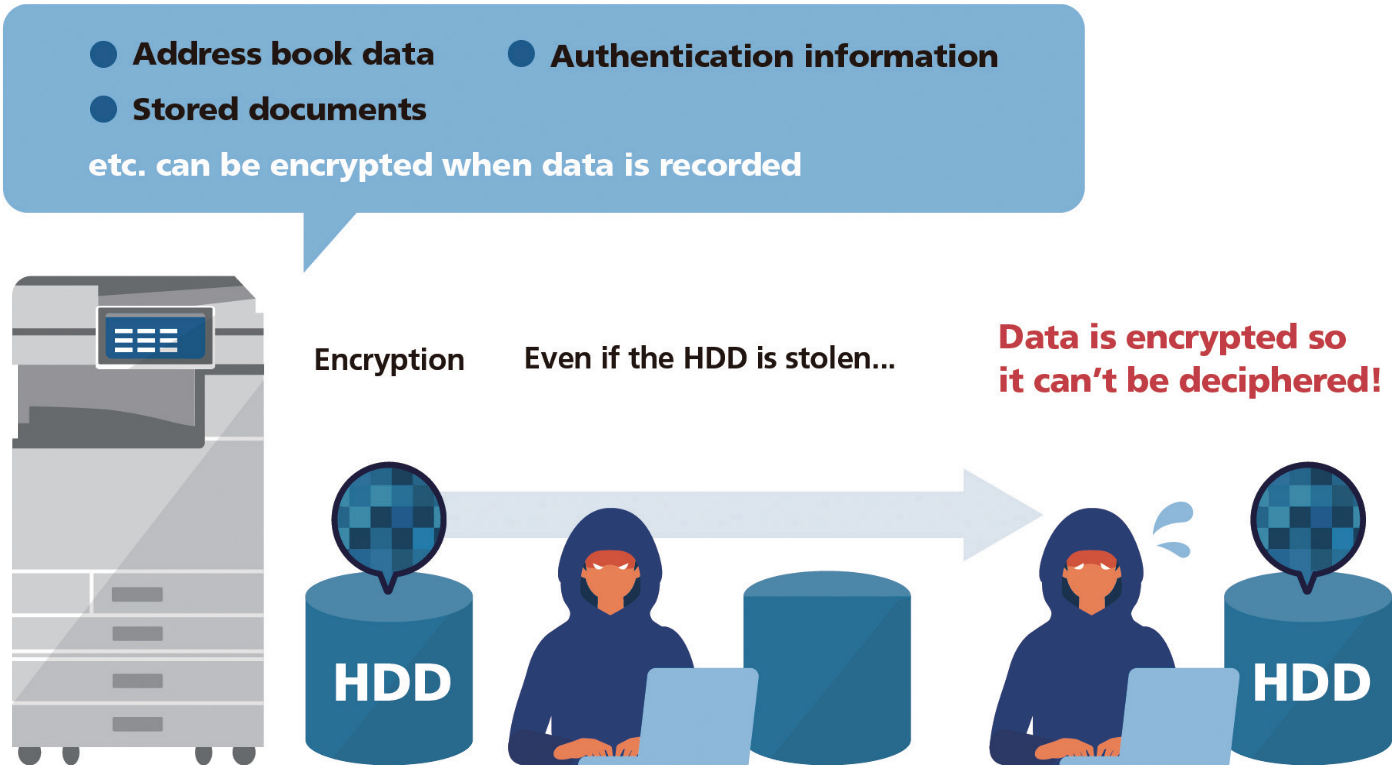
Enabling storage encryption not only protects MFP/printer data from theft, but also contributes to compliance with the organization's security policy.

Data to be encrypted

The following data stored in the main unit's onboard memory or storage, which retains data even after the power is turned off, is encrypted.

- Address book
- User authentication data
- Stored document data
- Temporarily stored document data
- Log
- Network interface settings information
- Device settings information

Ricoh provides Advanced Encryption Standard (AES) 256 bit storage encryption.


● Address book data ● Authentication information
● Stored documents
etc. can be encrypted when data is recorded
Encryption
Even if the HDD is stolen...
Data is encrypted so it can't be deciphered!
HDD
HDD

4 - 2 - 5 Fax line security

Since MFPs with fax functions are connected to the outside by a telephone line, unauthorized access from there must be prevented.
The software (process) in Ricoh MFPs cannot be linked to processes except other prescribed processes to achieve the desired function.
And the types of data handled are also restricted.
In other words, since data input from the fax line is not communicated to any process other than the one used to execute the fax operation, the MFP has a mechanism that prevents unauthorized access to the network through the fax line or unauthorized access to the device's internal programs.

4 - 2 - 6 Job log/access log management function

By collecting logs accumulated in devices such as MFPs, detailed information on the usage history of each function, error history, status of access to the device, and who accesses it can be confirmed. This functionality provides psychological restraint against information leaks and enables tracking in the event of a leak. The log information collected is as follows.

Job log

- Log information on all workflows related to user documents, such as copying, document storage in the document box, printer printing, fax transmission, and scanner delivery
- Printing of reports such as system setting lists output from the operation unit

Access log

- Authentication such as for login and logout
- Document operations such as creation, editing, and deletion of stored documents
- Service engineer operations such as hard disk initialization
- System operations for log forwarding results and at unauthorized copy reading
- Security actions such as encrypted communication, access attacks, lockouts, and firmware validation

4 - 3 Data security

Both digital data handled by MFPs and printers and documents output on paper have the potential to lead to serious security risks such as information leaks.

Ricoh products not only support corporate security policy compliance activities, but also provide features to prevent security incidents that may occur due to misuse or carelessness.

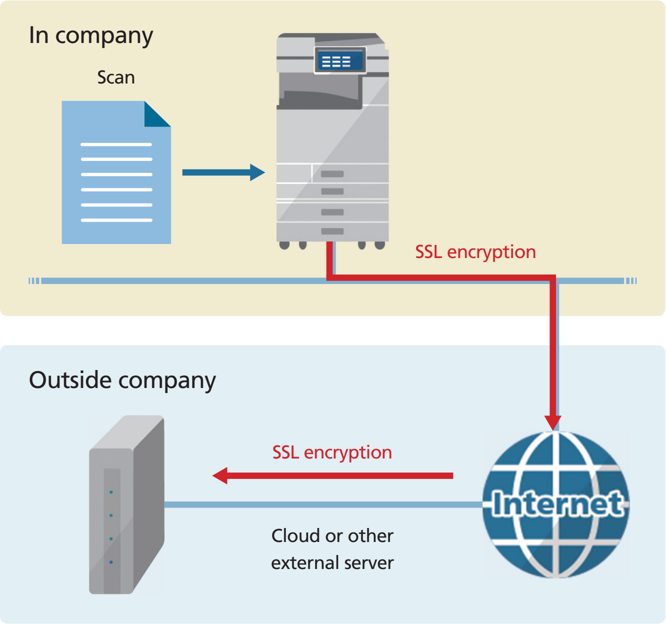
4 - 3 - 1 Scan functions

User permissions settings are useful for properly protecting the process of scanning and storing paper media information on a file server or sending it via e-mail.

Multiple authentication options, including user ID and password login and optional Kerberos authentication, can be used to restrict users who can use the scanning operation.

In addition, encrypting communications for sending scan data using SSL/TLS greatly reduces the risk of information leakage and falsification, which is a concern when using an SMTP server located outside the company.

Models released from the RICOH IM6000/5000/4000/3500/2500 support TLS1.3.



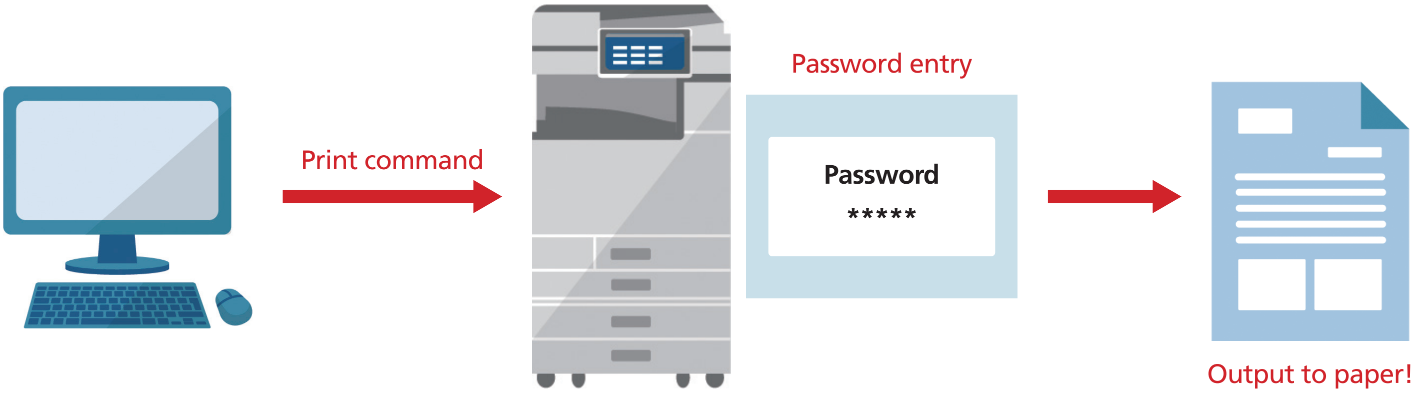
4 - 3 - 2 Locked print

Leaving printed documents after output leads to a major risk of information leakage. Confidential information may be visible to unauthorized persons or recovered and misused.

Documents printed can be stored in the storage of the MFP itself. With the Locked Print function, after printing with a password specified from a PC, the password must be entered on the operation panel of the MFP in order to output. Confidential documents can thus be output without being seen by others.

Prevent printed materials from being left out or taken home

If “Locked Print” is specified, the data will not be put on paper until a password is entered on the main unit.

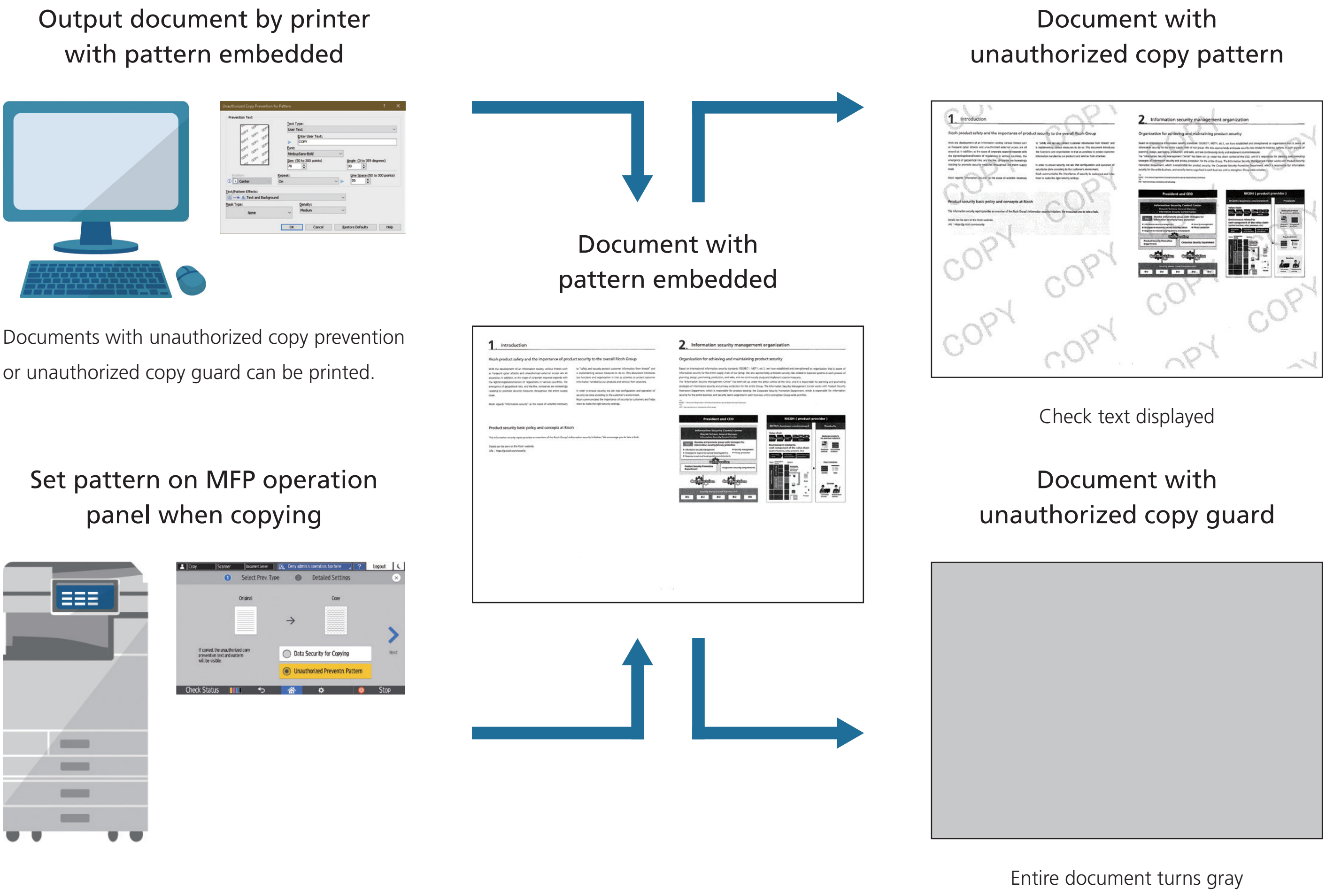


4 - 3 - 3 Unauthorized copy guard and pattern printing

Ricoh provides an unauthorized copy protection function that takes document security measures into consideration. A special pattern embedded throughout the document is printed when outputting or copying. When a document with an embedded pattern is copied, the embedded check text will appear. And if the pattern is detected, the image will be destroyed and the entire paper surface printed gray to deter information leaks. For example, when confidential information and the like must be output, this function can be used to prevent the spread of information through copying, thereby reducing information leaks.

Workflow for unauthorized copy prevention (image)

If "Locked Print" is specified, the data will not be put on paper until a password is entered on the main unit.



Output document by printer with pattern embedded

Unauthorized Copy Prevention for Pattern

Prevention Text

Text Type: User Text

Enter User Text: COPY

Font: NimbusSans-Bold

Size: (50 to 300 points) 70

Angle: (0 to 359 degrees) 30

Position: Center

Repeat: On

Line Space:(50 to 300 points) 70

Text/Pattern Effects: Text and Background

Mask Type: None

Density: Medium

Documents with unauthorized copy prevention or unauthorized copy guard can be printed.

Set pattern on MFP operation panel when copying

If copied, the unauthorized copy prevention text and pattern will be visible.

○ Data Security for Copying

● Unauthorized Preventn. Pattern

Document with pattern embedded

Document with unauthorized copy pattern

Check text displayed

Document with unauthorized copy guard

Entire document turns gray

4 - 3 - 4 Compulsory security printing

It is possible to add compulsory identifying information such as the name of the user who printed the document and when and from what device it was printed. This can be activated for copy, print, fax, and document server functions.

The type of information to be added can be selected from the list on the right.

- Date and time the document was printed
- Name or login user ID of the person who printed the document
- IP address and serial number of the device that printed the document

4 - 3 - 5 Restrictions on use of functions

Unauthorized use of MFPs or printers may lead to violations of company security policies.

Ricoh products can track usage by individuals.

It is also possible to restrict what functions are available and the print volume by user or department.

Security threats for MFPs and printers and countermeasures against them

4 - 4 Network security

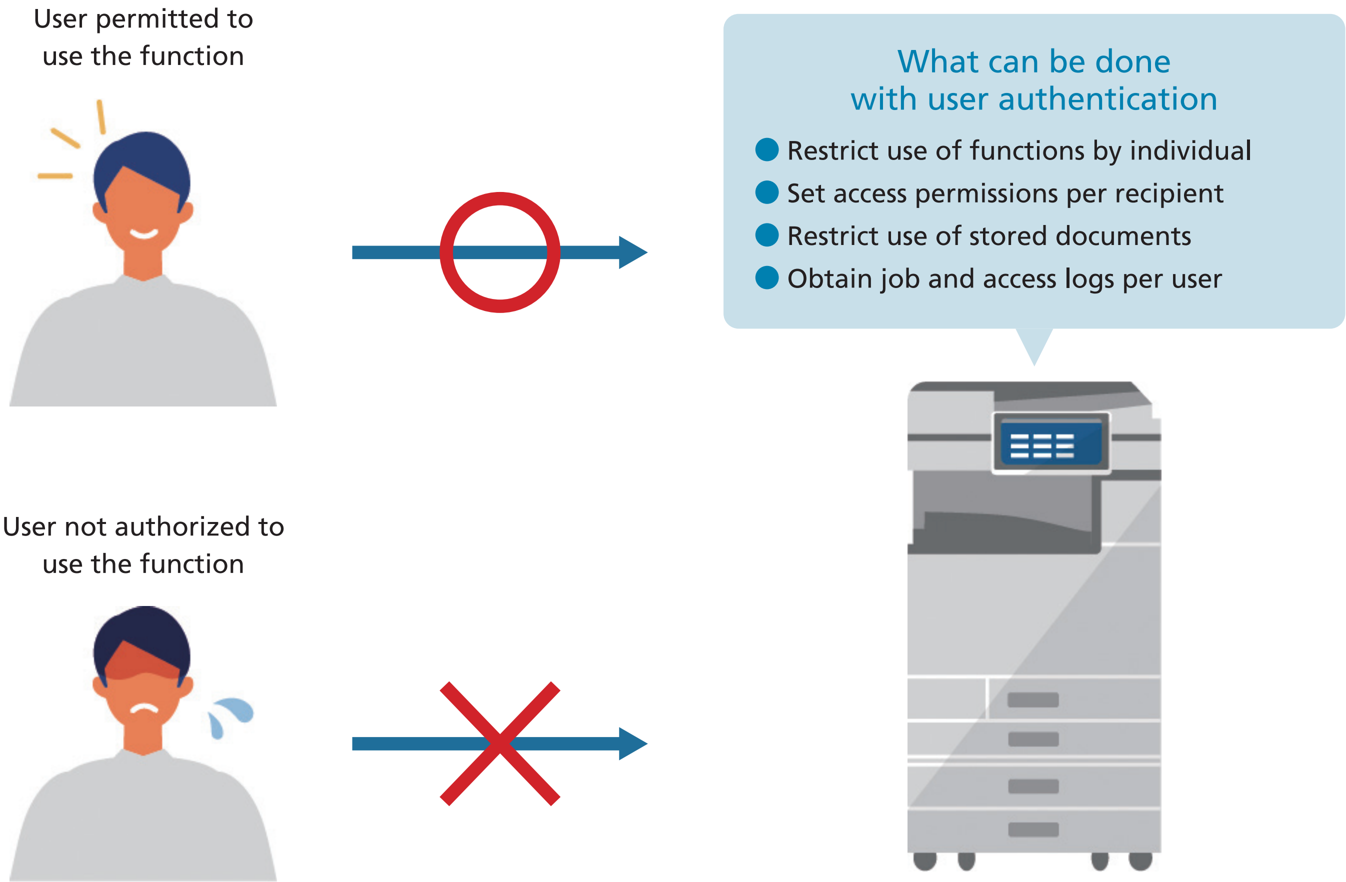
MFPs and printers perform communication with computers and servers over a network that contains critical information. If communication is not protected, critical information can be maliciously falsified or stolen.

Ricoh products and technologies provide functions to protect critical information from unauthorized access via the network.

4 - 4 - 1 User authentication

Devices are equipped with a user authentication system with login user name and password to enable identification of individuals. In addition, personal authentication through an existing authentication system is also possible by linking with a networked Windows domain controller or LDAP server.

The latest models can use multi-factor authentication by combining with an optional card reader.



User permitted to use the function

User not authorized to use the function

What can be done with user authentication

- ● Restrict use of functions by individual
- ● Set access permissions per recipient
- ● Restrict use of stored documents
- ● Obtain job and access logs per user

Authentication methods that can be selected

● Basic authentication ● Windows authentication ● LDAP authentication ● User code authentication ● Integration server authentication

4 - 4 - 2 Restrictions on unused ports

Leaving network ports of MFPs and printers open can lead to various threats such as destruction or falsification of stored data, denial of service (DOS attack), and intrusion by viruses and malware.

In addition to closing unused ports, Ricoh products can also disable certain protocols, such as SNMP and FTP, thereby blocking the risk of abuse.

4 - 4 - 3 Encryption of network communication

SSL/TLS

The administrator of the MFP can enable encrypted communication by setting SSL/TLS. This reduces the risk of data being intercepted, its content being analyzed, and it being falsified transmission.

Encryption algorithms (AES256bit and SHA-2) required by the U.S. National Institute of Standards and Technology (NIST) are standard on the latest Ricoh models with encryption communication functions. And by adopting an cryptographically secure pseudorandom number generation algorithm (HMAC_DRBG) to generate the cryptographic key, security of communication with the device and of processing within the device is increased.

For example, by encrypting communication for sending scan data using SSL/TLS, customers who have introduced e-mail servers and cloud services that utilize the Internet can greatly reduce the risk of information leakage and falsification that is a concern when using an SMTP server located outside the company. Communication between the RICOH Smart Device Connector app and an MFP too is protected with SSL/TLS.

SNMP

SNMP (Simple Network Management Protocol) is a protocol for monitoring and controlling network devices by collecting information such as total number of sheets printed and errors of network devices. Information is obtained from the Management Information Base (MIB), which describes the configuration of network devices, and that can be used to monitor service availability and otherwise assist equipment operations.

SNMP v3 incorporates user authentication functions, data encryption functions, and the like to protect customer data and network equipment information.

S/MIME

By registering the user's certificate in the address book of the MFP, messages can be sent using public key encryption, thereby deterring information leaks. In addition, by installing a device certificate in the main unit and attaching a digital signature using a private key, the risk of the sender being impersonated and of falsification of e-mail content can be reduced.

(Not available with W-NET FAX and direct SMTP.)

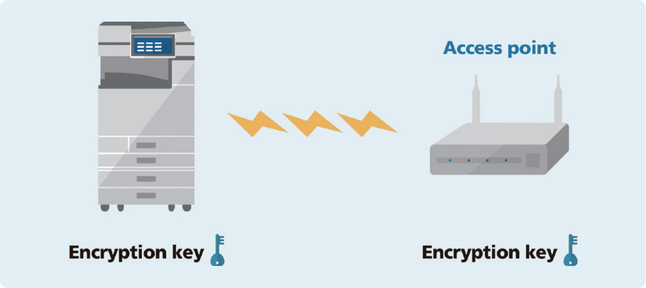
POP3/IMAP4 over SSL

Communication to receive e-mail from a server can be encrypted.

Wi-Fi®

WPA3™*9, WPA2™, and WPA2™-PSK using AES encryption (Wi-Fi Protected Access®) are supported for Wi-Fi® security.

*9)
Only supported with
RICOH IM C6010/C5510/C4510/C3510/C3010/C2510/C2010.



4 - 4 - 4 Print job data encryption

IPP over SSL/TLS

Interception of print job data can be dealt with by encryption using IPP over SSL/TLS.

Ricoh products encrypt Internet Printing Protocol (IPP) print data using Secure Sockets Layer/Transport Layer Security (SSL/TLS) to prevent interception of information on print job data in the communication path.

End-to-end encryption using drivers

End-to-end encryption of print data between user systems and Ricoh products is also possible. When confidential printing is performed with this setting enabled from the driver, the print job data is encrypted from the execution of the print instruction to just before printing. Decryption is not done until the password for confidential printing is entered.

5. Certification and evaluation

In order to enhance the security of documents, which are customers' information assets, Ricoh was one of the first to take security measures to prevent falsification and leakage of electronic and paper documents, and has focused on developing product security functions to address possible risks throughout the document lifecycle (from document generation through processing, storage, and destruction) .

In February 2010, Ricoh received CC certification conforming to IEEE 2600.1, the international standard for security functions that MFPs and printers should have, for the imagio MP 5000 SP/4000 SP (released in February 2008) . And in January 2020, the RICOH IM C6000/C5500/C4500/C3500/C3000/C2500/C2000 (released in January 2019) received CC certification conforming to the "Hardcopy Device (Digital MFP) Protection Profile (HCD PPv1.0) ."

To ensure that customers can use equipment with greater peace of mind, Ricoh offers a broad lineup of CC-certified products that conform to IEEE 2600.2 and HCD PPv1.0.

5 - 1 Security certification (CC certification)

Common Criteria (CC) is an international evaluation standard for information security that evaluates whether the security functions that IT products should have are properly developed.

When procuring IT products, customers can use the CC certification (ISO/IEC 15408) security standard to clearly communicate required specifications to product providers and compare the security features of different companies.

Currently, it is a government procurement standard in more than 25 countries around the world, and in recent years, MFP vendors in Japan and other countries have been actively seeking certification for their MFPs as well.

This system is also used by other industries to ensure competitiveness in the international market.

A list of certified devices that support TPM can be seen on the Ricoh website.

URL：https://www.ricoh.co.jp/mfp/security/cc/

5 - 1 - 1 Hardcopy Device Protection Profile（HCD PPv1.0）

The Hardcopy Device (MFP) Protection Profile v1.0 is a protection profile for MFPs that is a security requirement for government procurement led by Japanese and U.S. certification bodies and MFP manufacturers, including Ricoh. It came about through the establishment in 2012 of the Multifunction Printers Technical Community (MFP TC) at the Common Criteria Users Forum (CCUF) , an international user group for security evaluation and certification systems

Many of the MFPs in Ricoh's lineup have been evaluated based on HCD PP v1.0 in the areas listed at right.

- User identification and authentication systems
- Data encryption technology
- System firmware validation
- Separation of analog fax lines from copy/print/scan controllers
- Verification of data encryption algorithms
- Data overwriting processing

5 - 1 - 2 IEEE 2600.2

IEEE 2600 is an international standard established in 2003 by major MFP vendors and other companies in the industry to specify from a customer perspective the ideal form of CC certification functions of MFPs, which had hitherto been determined separately by the individual companies.

Ricoh has been active in IEEE working groups and contributed to the development of the Protection Profile (PP) .

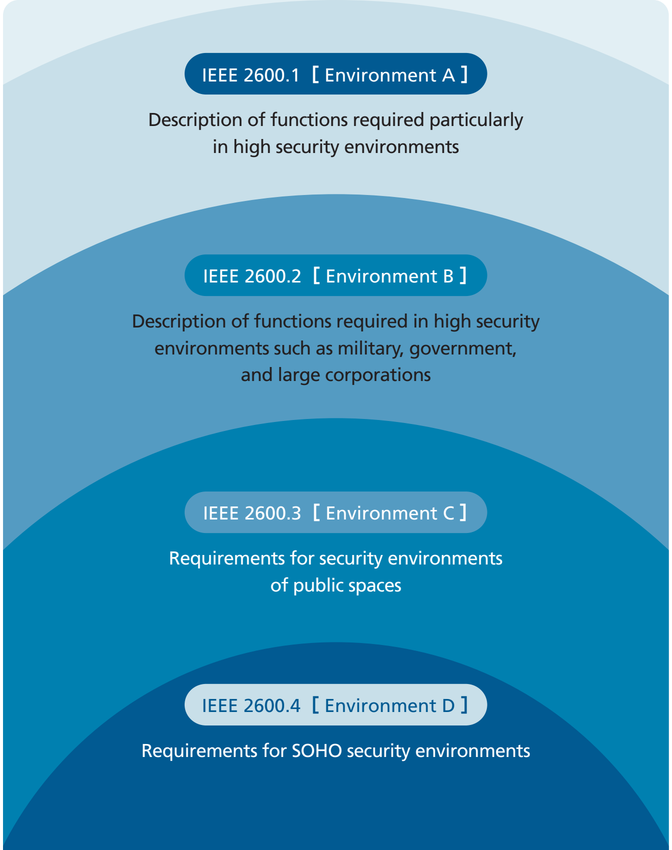
IEEE 2600 includes documents called PPs, which are created for different applications, such as for military and government, major corporations, public spaces, and SOHO.

The PP is used as a document that identifies the security functions/conditions, etc. to be evaluated for CC certification.

By incorporating this PP conformance into the "Security Target (ST) " and undergoing CC certification evaluation, PP conformance is acknowledged in CC certification.

If the products conform to the same PP of IEEE 2600, they will have the same level of security features.

IEEE 2600 PP documents include the following. PPs are defined per expected use environment.



IEEE 2600.1［Environment A］

Description of functions required particularly in high security environments

IEEE 2600.2［Environment B］

Description of functions required in high security environments such as military, government, and large corporations

IEEE 2600.3［Environment C］

Requirements for security environments of public spaces

IEEE 2600.4［Environment D］

Requirements for SOHO security environments

5 - 2 Penetration testing by Cisco

Penetration testing by Cisco was performed on RICOH IM C6010/C5510/C4510/C3510/C3010/C2510/C2010.
Resistance to malicious attacks is confirmed by passing tests on penetration attempts by white-hat hackers from security vendors with a wide range of expertise.

CISCO
Global footprint
Matured methodology
Support technology
Expertise
Operational excellence
Knowledge sharing initiatives

Global footprint

- Worldwide team with technical human resources concentrated in the U.S. and UK
- Excellent response operations in the U.S. and EMEA

Matured methodology

- Achievements in various industries

Support technology

- Significant investment in lab development
- Dedicated lab management
- IoT labs in Herndon, VA, Chicago, IL in the U.S. and Watford in the UK

Expertise

- Security expertise in hardware, chips, cloud technology, applications, and programs
- Expert practice management and technical leadership

Operational excellence

- Global collaboration mechanisms

Knowledge sharing initiatives

- Advisory accelerator provision and collaboration tools
- Custom Jira development
- Utilization of knowledge of internal and external experts

6. Conclusion

The growing need for information protection due to the increasing number of cyber attacks worldwide is now becoming universal and common knowledge. The constant struggle against attackers is likely to continue and not slow in the future. The Ricoh Group will continue to strengthen and improve our efforts in information security to ensure that we can respond flexibly as a digital services company. We will do that while keeping a close eye on changes in the external environment, such as the strengthening of security standards across industries and countries. And we will continue to strengthen our information security organization in order to achieve that goal.

RICOH
imagine. change.

https://www.ricoh.com/