# NEWS RELEASE

January 15, 2025

## Information Security Rating for Compliance with U.S. Security Standard NIST SP800-171/172 –FUJIFILM Business Innovation continues to be the first company in Japan to receive a AAA rating.

The Japan Security Rating Organization (JaSRO; Head Office: Chuo-ku, Tokyo; President: Soichiro Miyoshi) has assigned the highest information security rating of AAAis (*1) using the National Institute of Standards and Technology (NIST) criteria to digital multifunction devices and printers offered by FUJIFILM Business Innovation Corporation (Head Office: Minato-ku, Tokyo; President & CEO: Naoki Hama). The company was the first in Japan to receive the AAAis rating for its digital multifunction devices and printers last year, and has now received a new AAAis rating for its latest models this year.

FUJIFILM Business Innovation Corporation, which is engaged in product development and maintenance of digital multifunction devices and printers, is working to enhance information security and ensure quality by enhancing various security functions and addressing compromises in encryption algorithms in developing products to meet the information security needs of its users.

Within the scope of this rating, which is the development and maintenance of digital multifunction devices and printers offered to businesses using such devices in a NIST-compliant environment, the company continues to be the first in Japan to receive the rating of AAAis for incorporating the measures (identification, protection, detection, response and recovery control measures) required in terms of compliance with NIST SP800-171 and NIST SP800-172 at an exceptionally high standard.

<Rating>
Company: Fujifilm Business Innovation Corporation
Rating Classification: Information Security
Rating Type: NIST SP800-171/172 Compliance
Rating ID Code: 10000370402C2503
Rating Scope: Digital multifunction devices and printers offered to businesses using such devices in a NIST-compliant environment *2
Anticipated Risk: Information leakage
Rating: AAAis (Triple-A)*1
Direction of Rating: Positive
Period of Validity: From January 15, 2025, to January 14, 2026 (One year from the date of issuance)

*1: AAAis the highest of 17 ratings. The security level required for AAAis a condition of “extremely high-risk tolerance with many outstanding elements” and must meet the following two requirements:
Requirement 1: Responds quickly to new threats and maintains and develops a high level of control at all times.
Requirement 2: Appropriate measures consistent with SP800-171/172 are incorporated to an exceptionally high standard.

*2:
Apeos C7070 / C6570 / C5570 / C4570 / C3570 / C3070 / C2570
Apeos C8180 / C7580 / C6580
ApeosPro C810 / C750 / C650
Revoria Press E1136/ E1125 / E1110 / E1100
Revoria Press E1136P / E1125P / E1110P
Apeos 4570 / 3570
Apeos C2360 / C2060
Apeos 3060 / 2560 / 1860
Apeos C5240
Apeos 6340
ApeosPrint C5240
ApeosPrint 6340
ApeosPrint C5570 / C4570
Apeos 7580 / 6580 / 5580
ApeosPrint 4560 S / 3960 S / 3360 S
ApeosPrint C4030 / C3530
ApeosPrint 4830 / 4830 JM
Apeos C4030 / C3530
Apeos 5330
Apeos C7071 / C6571 / C5571 / C4571 / C3571 / C2571
Apeos C3061 / C2561 / C2061
Apeos C3067
(These models apply to the Japanese market only.)

As security threats and countermeasures for digital multifunction devices and printers, Fujifilm considers the following main items as security risks for digital multifunction devices and printers in offices in terms of information leakage, data falsification, and unauthorized access to information and has taken optimal countermeasures. Details of these measures are compiled in the Security White Paper for Fujifilm Digital

The news release and The Information Security Rating are the current views of JaSRO based on information obtained from relevant institutions and organizations and do not guarantee their accuracy, completeness, comprehensiveness, etc. for now and in future years. JaSRO shall not be liable for any claims, lawsuits, or other disputes related to the news release and The Information Security Rating, or for any damages, losses, or expenses that may be incurred by relevant institutions and organizations or any other third party.All copyrights and other intellectual property rights, trade secrets, know-how, and other rights and interests related to The Information Security Rating are reserved and belong exclusively to JaSRO.

Multifunction Devices (August 20, 2024: Version 2.4), which is disclosed on FUJIFILM Business Innovation's website as a downloadable document.

- Unauthorized operations by other users
- Eavesdropping and tampering of communication data
- Unauthorized access to administration functions
- Software tampering and destruction of digital multifunction devices and printer software
- Audit log tampering
- Breach of document data stored on digital multifunction devices and printers (at return after lease end or device disposal)
- Data breach caused by careless mistakes of system administrators or users

In addition, to ensure the reliability of its security, the company has obtained ISO/IEC27001 certification, an international standard for information security technology management systems, and has built on this effort to obtain ISO/IEC15408 (CC certification), an international standard for information technology security design and operation, etc. In addition, in order to respond to the recent increase in cyberattacks that take advantage of weaknesses in the supply chain of products, the company has established a process to ensure safety throughout the entire product lifecycle and obtained ISO/IEC20243 certification, an international standard for supply chain security.

An audit was conducted to comprehensively review the efforts of addressing information leakage, data falsification, attacks of unauthorized access to information, and acquisition, use, storage, transfer, and deletion of critical information in digital multifunction devices and printers provided to businesses using such devices in a NIST-compliant environment were reviewed from the standpoint of compliance with NIST SP800-171 and NIST SP800-172.

The major initiatives are as follows: High-level security features include tamper detection and automatic recovery at all processes when the multifunction device starts up, and support for ASLR (Address Space Layout Randomization), which randomizes the placement of data in memory so that even if a vulnerability were to occur, the same attack tool would not be able to attack multiple multifunction devices.

Regarding the acquisition and use of critical information, maintenance personnel (hereafter “customer engineers”) are restricted from accessing machine management functions without the user's permission. In addition, multi-factor authentication is implemented as the authentication method for machine administrators. In addition, it is possible to set up detailed authorization for each function, such as authorization holders who can change settings for network, security, and aggregate management functions, and authorization holders who can access audit logs, to enable the checks and balances function to work. The systems are designed to be further strengthened in accordance with the users' environment, for example, by linking with external authentication systems such as Active Directory operated by the user or with external log servers that support the Syslog protocol. In addition, to prevent users from unintentionally touching the start button on the operation panel and sending data, users must slide the start button to activate the system. Regarding the storage of critical information, critical information stored on digital multifunction devices/printers is encrypted, and measures are taken to prevent decryption even if the information is exported and installed on other devices. The root encryption key is stored in the TPM chip, and the use of TPM2.0 enables encryption of data communication between the controller and the TPM chip. For the transfer of critical information, all communication paths with digital multifunction devices/printers are compatible with TLS v1.3, the latest requirement of the new TLS encryption setting standards, and for wireless LAN connections, WPA3 support is implemented to strengthen network communication encryption and prevent information leaks and tampering, as well as eliminate the threat of information leaks due to unauthorized access by disabling connections to external networks via fax, digital multifunction device/printer management services (EP-BB), etc. In addition, even for analysis due to malfunctions, critical information is never brought out, but is instead handled entirely by the user.

Regarding the deletion of critical information, in cases where stored data in digital multifunction devices/printers is replaced or disposed of, sanitization is performed by the user using an overwrite-erase function, and if desired, the stored data is physically destroyed on the spot, among other measures (any storage is not reused).

Since the competence of customer engineers also plays a major role in ensuring the implementation of these measures, the company is strengthening its measures for human resources so that only those who have taken and passed NIST-compliant training courses, in addition to regular maintenance training, will be able to perform NIST-compliant maintenance.

Moreover, the following functions, which are further enhanced in addition to the previous measures, have been equipped, demonstrating the management policy to strengthen security as a concrete initiative.

(1) Enhanced tamper detection and recovery functions

With a boot-time tamper detection (secure-boot) function using the Root of Trust in hardware, tampering is made more difficult (almost impossible) by having the Root of Trust for secure-boot in hardware. In addition to the automatic recovery function when the Bootloader detects tampering, an OS and middleware/application tampering detection and automatic recovery function is implemented. In addition, it is possible to review whether tampering has been detected/recovered in the audit log.

(2) Enhanced audit log functionality

As part of cyber threat hunting, audit logs are sent to an external server using Syslog to enable monitoring, analysis, and reporting of audit logs. "Destination of scanned documents" and "Information that can identify multifunction devices" have been added to the items in the audit logs. The data format of the audit log is designed to be easily analyzed by Security Information and Event Management (SIEM) and other means.

(3) Support for SMB 3.1.1

SMB protocol (file sharing protocol) has added functions to support SMB 3.1.1 in Windows 10 and Windows 11 at scan sending (SMB) and job flow (SMB transfer). SMB 3.1.1 implements AES-GCM (Advanced

The news release and The Information Security Rating are the current views of JaSRO based on information obtained from relevant institutions and organizations and do not guarantee their accuracy, completeness, comprehensiveness, etc. for now and in future years. JaSRO shall not be liable for any claims, lawsuits, or other disputes related to the news release and The Information Security Rating, or for any damages, losses, or expenses that may be incurred by relevant institutions and organizations or any other third party.All copyrights and other intellectual property rights, trade secrets, know-how, and other rights and interests related to The Information Security Rating are reserved and belong exclusively to JaSRO.

Encryption Standard - Galois/Counter Mode), a function of SMB encryption, which is a common key cryptosystem that allows encryption and authentication to be performed simultaneously.

(4) Enhanced TLS communication security

A function has been added to enhance security by discontinuing the use of older cipher suites that have been identified as vulnerable. Specifically, the operation of not using cipher suites that do not have the characteristics of PFS (Perfect Forward Secrecy: a concept of key exchange in which both the encrypted communication and the secret key cannot be decrypted even if both are compromised) during TLS communication is applied to both TLS clients and TLS servers.

(5) Enhanced SSD management function

A function has been added that allows storage (SSD) information to be printed in the machine configuration column of the function setting list. By periodically outputting the function setting list, security can be enhanced so that even if a replacement is made, it can be noticed.

(6) Immediate reflection of settings when operating passwords

Passwords can be strengthened by specifying the minimum/maximum number of characters, and even for passwords registered before new conditions are implemented, users are prompted to change their passwords to new ones the next time they log in.

In addition, based on the idea of “easier to use”, frames will be added to icons displayed on the application screen. By giving the icons names that can display up to 7 half-size characters and 5 full-size characters of the authenticated user name, it is possible to identify who is logging in. Setting item names and setting values are displayed separately on the left and right in large font. The risk of operation errors has been reduced by improving operability based on customer feedback, such as by eliminating screen transitions and introducing a mini pop-up function to reduce the number of operation steps.

Comprehensively, in the development and maintenance of digital multifunction devices and printers offered to businesses using such devices in a NIST-compliant environment, the company incorporates the measures (identification, protection, detection, response and recovery control measures) required in terms of compliance with NIST SP800-171 at an exceptionally high standard.

In addition, to address NIST SP800-172, the implementation of a function to detect tampering in all processes at startup and enable automatic recovery, the implementation of a function to randomize the placement of data in memory, and evaluation by ISO/IEC 15408 (CC certification) have been incorporated to an exceptionally high standard.

In addition to compliance with NIST SP800-171/172, the company has also implemented compliance with NIST SP800-53, and is able to quickly address new threats, maintaining and developing a high level of management at all times, and has a high level of management maturity. We expect further implementation of planned enhancement measures.

In addition, in maintenance operations, as NIST-compliant services have only just been released, we expect the company to accumulate new know-how while utilizing the expertise it has accumulated over the years to further strengthen its operations.

○ Rating

Please refer to the JaSRO website (link below) for the rating of FUJIFILM Business Innovation Corporation.
https://jasro.org/client/index.html

○For details on Fujifilm Business Innovation's multifunction devices, please refer to the company website (link below).
https://www.fujifilm.com/fb/product/multifunction/promotion/security_measure

○Additional notes on rating definitions

The security rating system is a system devised through discussions at the Industrial Structure Council. The following are additional notes on the rating definitions that indicate compliance with NIST SP800-171/172.

The following are additional notes on the rating definitions that indicate compliance with NIST SP800-171/172.

| | |
|---|---|
| AAAis | (Requirement 1) Responds quickly to new threats and maintains and develops a high level of control at all times.<br>(Requirement 2) Appropriate measures consistent with SP800-171/172 are incorporated to an exceptionally high standard. |
| AAis | (Requirement 1) Possesses a continuous improvement process to maintain and develop a high standard of management.<br>(Requirement 2) Appropriate measures consistent with SP800-171/172 are comprehensively incorporated to a high standard. |
| Ais | (Requirement 1) Using verified processes, targets are managed and implemented with indicators.<br>(Requirement 2) In addition to reaching specified standards (ISO/IEC27001 standards), measures compliant with SP800-171/172 are partially incorporated. |
| BBBis | (Requirement 1) Systematically manages and executes procedures based on clearly defined protocols.<br>(Requirement 2) Preventive management measures (prevention in advance) of a certain standard (ISO/IEC27001 standards) are incorporated. |

| | |
|---|---|
| BBis | (Requirement 1) Procedures, etc. are not in place, but a certain level of control is in place.<br>(Requirement 2) Certain deterrent (to discourage behavior) and detective control measures are incorporated. |
| Bis | (Requirement 1) Informal management is carried out dependent on specific personnel.<br>(Requirement 2) Measures such as detective control measures (being able to detect the occurrence of incidents) are inadequate. |
| Cis | (Requirement 1) Processes have not been established and are inadequately managed.<br>(Requirement 2) Measures have not been taken, with a constant exposure to threats. |

<Contact>
Planning Department,
Japan Security Rating Organization
E-mail: info@jasro.org

JaSRO is the world's first third-party information security rating agency.

- *We are working to create a social system in which the level of information management measures is verified by the security rating system.*
- *We provide support for the establishment and internal audit in compliance with Information system Security Management and Assessment Program of Japanese government (ISMAP).*