Nomura Research Institute Group

NEWS RELEASE

Jan. 25, 2024

NRI SecureTechnologies, Ltd.

NRI Secure Conducts "2023 Fact-Finding Survey on Information Security in Companies" in Japan, the US, and Australia

— Less than 20% of Japanese companies have adopted Generative AI services versus an approximately 70% adoption rate in US & Australia —

NRI SecureTechnologies, Ltd. (Headquarters: Chiyoda Ward, Tokyo; President: Shunichi Tatewaki; "NRI Secure"), a leading global provider of cybersecurity services, conducted a fact-finding survey on information security from August to September 2023, covering a total of 2,783 companies located in Japan, the US, and Australia. NRI Secure has conducted the survey annually since FY2002, and this year marks the 21st installment.

The main findings are as follows.

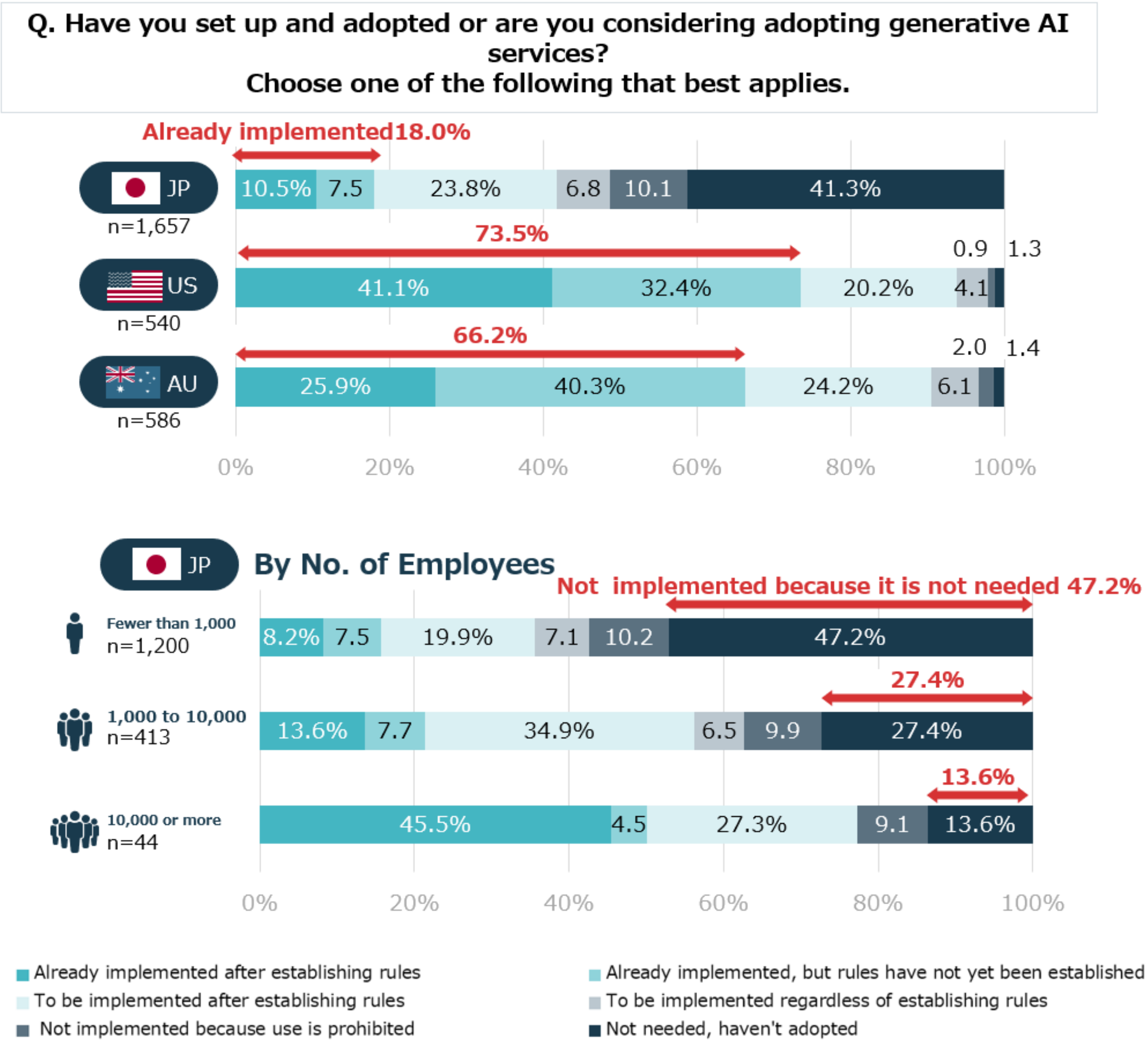
■ Only around 20% of Japanese companies have adopted generative AI services

1. Adoption rate

With regard to the rate at which generative AI services have been adopted, a total of 18.0% of Japanese companies responded that they had "Already implemented after establishing rules" or "Already implemented, but rules have not yet been established" security rules (or 50% of Japanese companies with at least 10,000 employees). Given the same response choices, 73.5% of companies in the US and 66.2% of companies in Australia gave these answers, making it clear that companies in both countries had adopted generative AI services at higher rates compared to their Japanese counterparts (Fig. 1).

In addition, around 10% of companies in Japan regardless of employee scale responded that they "Not implemented because use is prohibited", a far higher percentage than that among companies in the US (0.9%) or Australia (2.0%), which revealed a more cautious stance on adopting generative AI services among Japanese firms. Moreover, nearly half of companies with fewer than 1,000 employees responded "Not implemented because it is not needed", indicating the prevalence of Japanese companies that do not see any need for generative AI services.

Fig.1: Generative AI Service Rule Setup/Adoption Status (By Country and By Employee Scale at Japanese Companies)

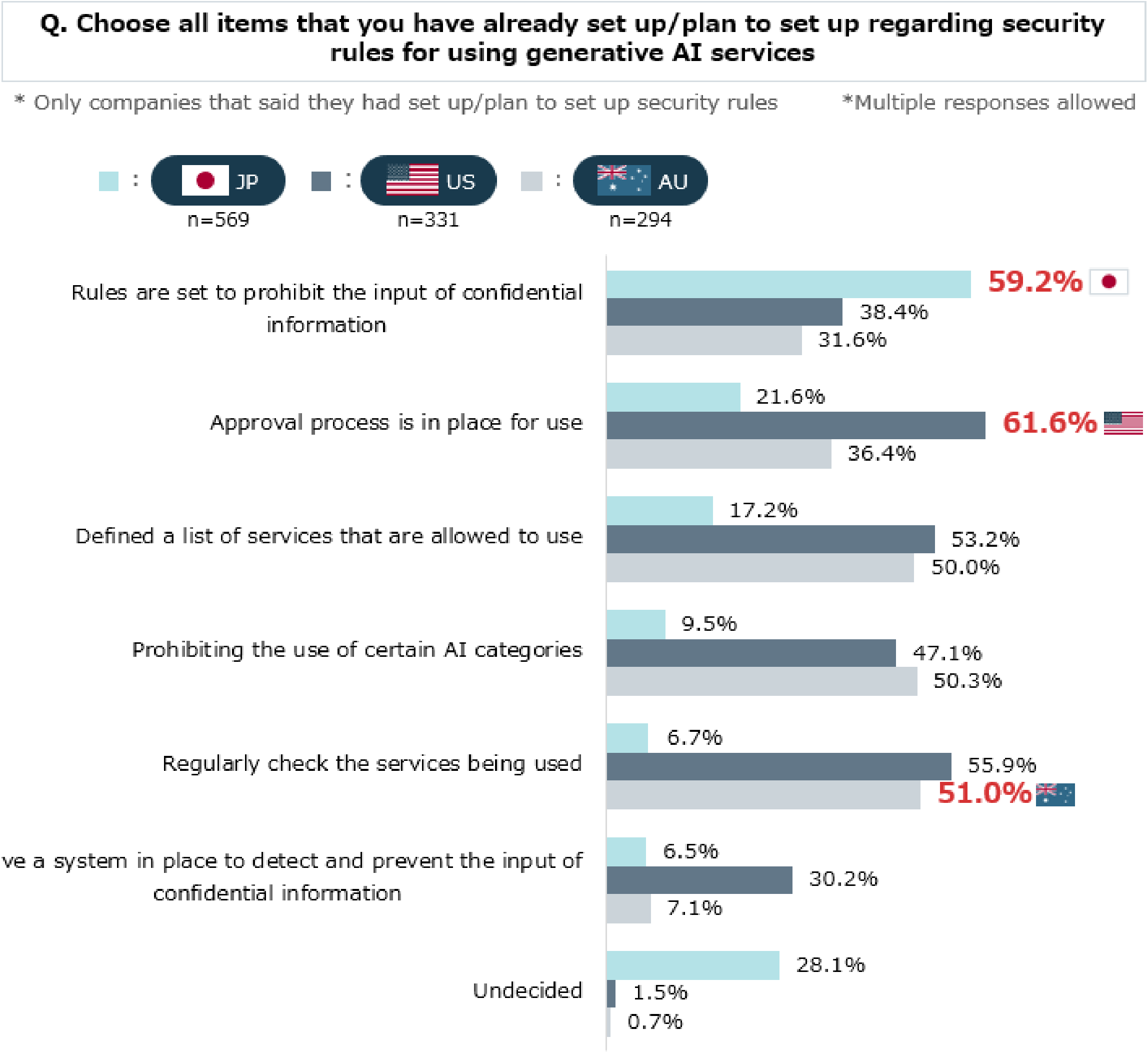


2. Security rules for the use of generative AI services

Those companies that said they had “Already implemented after establishing rules” or were “To be implemented after establishing rules” security rules on the use of generative AI services were then asked a follow-up question, namely what sort of rules they had set up or were planning to set up, with multiple responses possible. In Japan, the response “Rules are set to prohibit the input of confidential information” was given by 59.2% of companies, which was higher compared to 38.4% of companies in the US and 31.6% of companies in Australia (Fig. 2).

Meanwhile, the most given response in the US was “Approval process is in place for use” (61.6%), while in Australia it was “Regularly check the services being used” (51.0%). Regarding the use of generative AI services, which is expected to become more widespread going forward, it's important not only to put rules in place which rely on users' judgment, but also to establish a use environment involving the use of monitoring and control systems or other such mechanisms.

Fig. 2: Security Rules Already Set Up/To Be Set Up for Use of Generative AI Services (By Country)



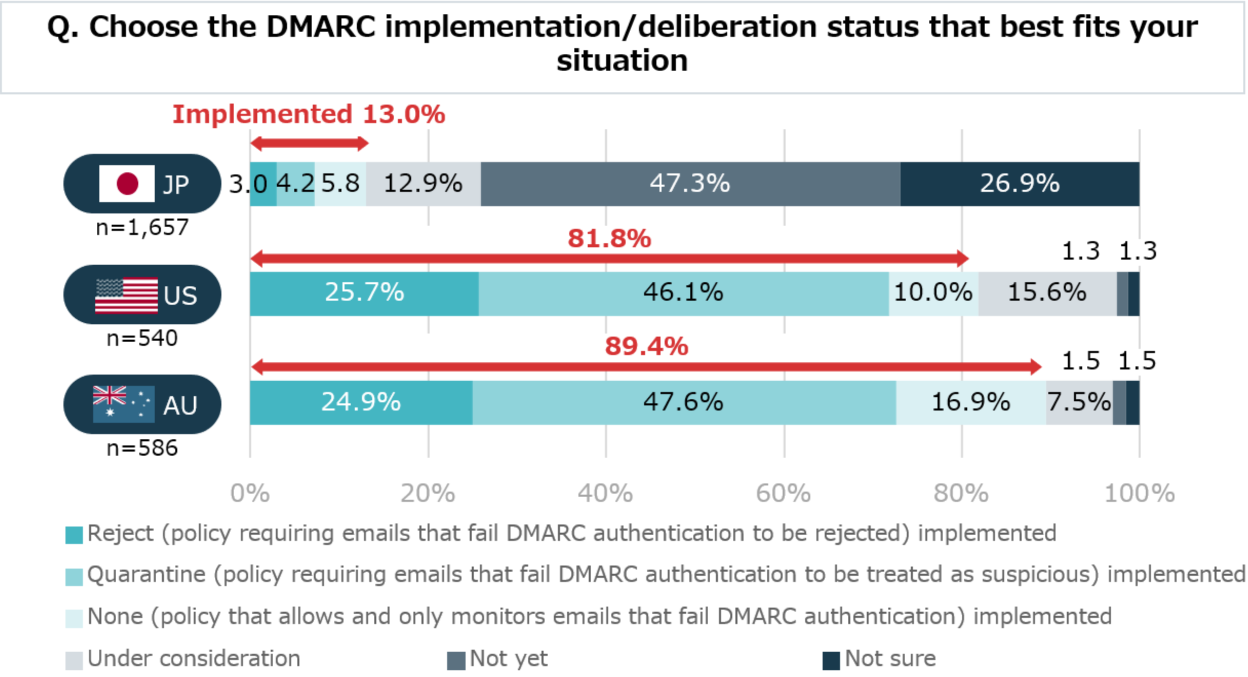
■ Implementation rate of "DMARC", a measure to combat spoof emails, is approximately 10% in Japan versus around 80% in US, Australia

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a technology used to verify whether an email was legitimately sent based on the email sender's domain, its purpose being to protect recipients from malicious emails involving fake in-house domains, and it is becoming broadly adopted around the world.

In this survey, DMARC implementation was categorized into three stages, these being "Reject", "Quarantine", and "None", with the respondents being asked about their "DMARC implementation/deliberation status". According to the results, 13% of Japanese companies, 81.8% of US companies, and 89.4% of Australian companies said they had "Already implemented" some form of DMARC, the responses indicating that the prevalence of DMARC implementation among Japanese companies is significantly lower (Fig. 3).

In the US and Australia, where high percentages of companies have implemented DMARC, those implementation efforts have been promoted under government leadership. In Japan as well, the Ministry of Economy, Trade and Industry, the National Police Agency, and the Ministry of Internal Affairs and Communications called on credit card companies in February 2023 to implement DMARC[1], and in July of that same year, the "Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies"[2] clearly specified DMARC as a measure for combatting spoof emails. Furthermore, as seen from the "Email Sender Guidelines" released by Google in November 2023 which require business operators that send emails to use DMARC authentication, the implementation of DMARC can be also expected to spread in Japan going forward.

Fig. 3: DMARC Implementation/Discussion Status (By Country)

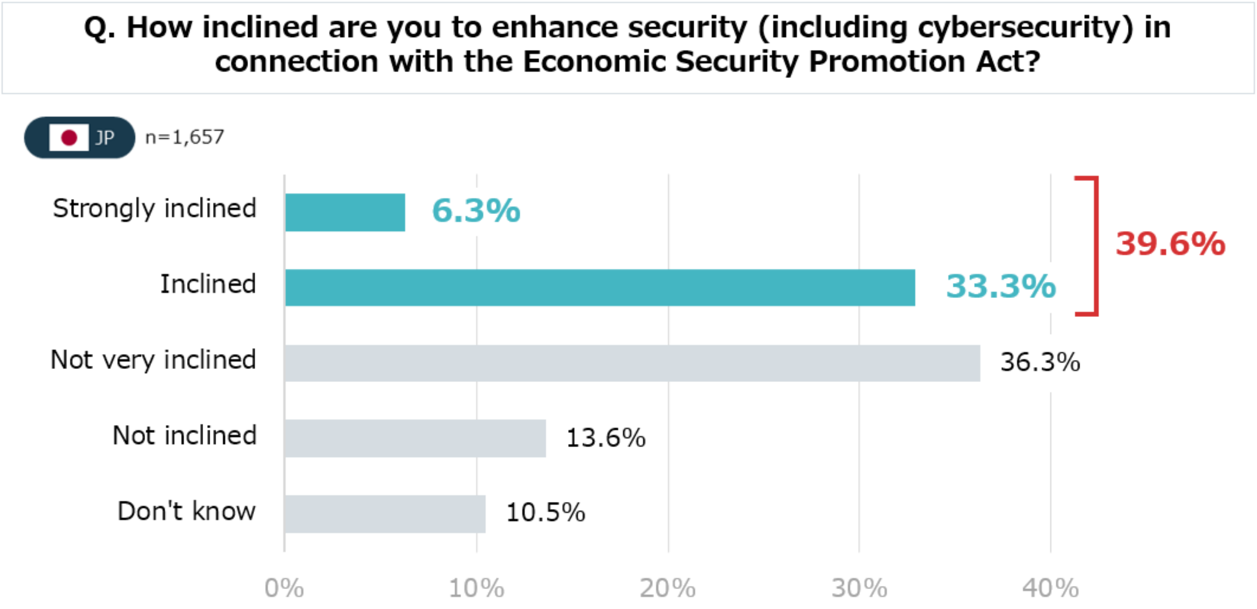


■ More than just specified social infrastructure business operators: some 40% of Japanese companies are inclined to enhance their security in response to the Economic Security Promotion Act

We asked Japanese companies whether they were inclined to enhance their security measures (including in the cyber domain) in connection with the Economic Security Promotion Act that was established in Japan in 2022[3], with a total of 39.6% of respondents saying they were “strongly inclined” or “inclined” (Fig. 4).

If we narrow those companies down to only those designated as “specified social infrastructure business operators” which provide services that are the foundation for public life or economic activity, 88.2% of companies (15 out of 17) replied that they were “strongly inclined” or “inclined” to enhance security. Compared to the overall trends, specified social infrastructure business operators are more highly aware when it comes to security enhancements in connection with the Economic Security Promotion Act.

Fig. 4: Percentage of Japanese Companies Inclined to Enhance Security (Including in the Cyber Domain) in Connection with the Economic Security Promotion Act



A detailed report on the “2023 Fact-Finding Survey on Information Security in Companies” (Japanese only) is available at the following website.

https://www.nri-secure.co.jp/download/insight2023-report

This year’s survey highlighted how when compared with their US and Australian counterparts in fields such as generative AI security and DMARC, Japanese companies are conspicuously lagging behind in their adoption efforts. Considering these survey findings, NRI Secure will continue to support companies and organizations with their information security measures, to better contribute to a safe and secure information systems environment and society.

[1] Considering the rise of phishing which can lead to unauthorized use of credit card numbers and other personal information, the Ministry of Economy, Trade and Industry, the National Police Agency, and the Ministry of Internal Affairs requested that credit card companies etc. adopt sender domain authentication technology (DMARC) and take other anti-phishing measures (Source: METI, “Request to Credit Card Companies, etc. to Bolster Anti-Phishing Measures” Feb. 1, 2023).

[2] Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies: The Cybersecurity Strategic Headquarters, which was established under the Cabinet pursuant to the Basic Act on Cybersecurity, released the 2023 edition of the “Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies” on July 4, 2023.

[3] Economic Security Promotion Act: A law enacted in May 2022 considering the increasing complexity of global conditions and changes in the world’s socioeconomic structure, established as an economic measure enabling the government to formulate basic policies related to the promotion of national security through integrated implementation of economic policies, thereby better ensuring national security. It consists of four main pillars: (1) ensure the stable supply of essential goods; (2) ensure the stable provision of critical infrastructure services; (3) assist the development of advanced critical technologies; and (4) non-disclosure of patent applications.

Inquiries about this news release:
Public Relations, NRI SecureTechnologies, Ltd.
TEL：03-6706-0622　E-mail：info@nri-secure.co.jp

Reference

■ Survey Overview

Survey name	“2023 Fact-Finding Survey on Information Security in Companies”
Survey purpose	To clarify the information security-related initiatives being taken by companies in Japan, the US, and Australia, and to provide useful reference information to persons engaged in operations relating to corporate information systems and information security.
Survey period	• Japan: August 1, 2023 to September 29, 2023 • US, Australia: September 8, 2023 to September 29, 2023
Survey method	Web questionnaire
No. of respondents and breakdown by employee scale	• Japan: 1,657 (less than 1,000: 72.4%; 1,000 to 5,000: 21.3%; 5,000 or more: 6.3%) • US: 540 (less than 1,000: 70.9%; 1,000 to 5,000: 20.9%; 5,000 or more: 8.1%) • Australia: 586 (less than 1,000: 65.5%; 1,000 to 5,000: 26.4%; 5,000 or more: 8.0%)

* Single-answer percentages may not sum up to 100% for all choices due to rounding.