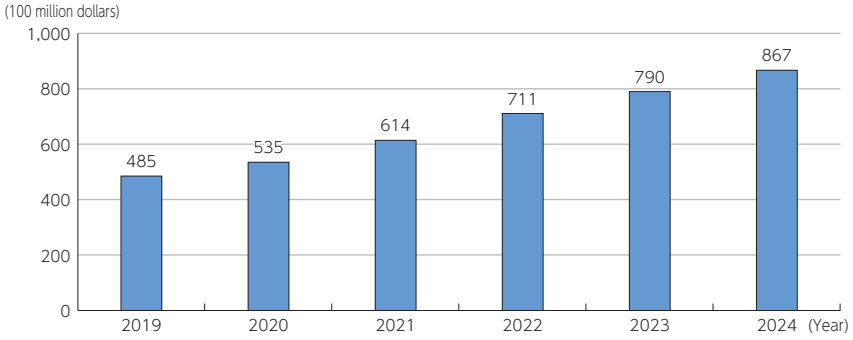
Section 10 Trends of cybersecurity

1. Market overview

The global market for cybersecurity has remained robust, reaching 86.7 billion dollars in 2024, representing a 9.7% increase from the previous year (**Figure 2-1-10-1**).

Figure 2-1-10-1 Changes in the global cybersecurity market size



(Source) Prepared based on Canalys data

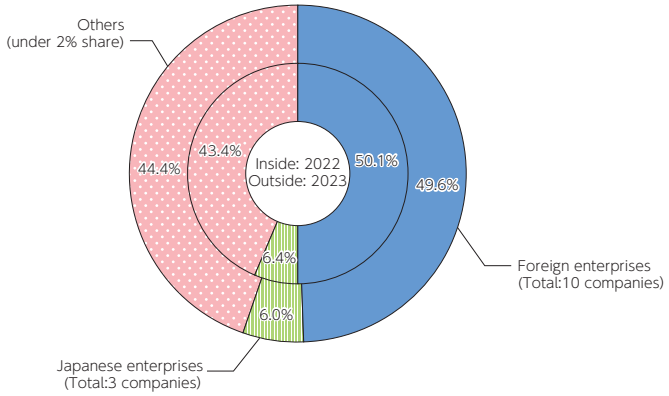
As for the major players in the cybersecurity market, Palo Alto Networks, Cisco, and Fortinet held the top three global market shares since 2019, however, as of the second quarter of 2024, Microsoft has replaced Cisco and entered the top three. In recent years, Palo Alto Networks, which holds the top share, has been expanding its market share, approaching 10%. Microsoft has also been rapidly expanding its share in recent years, and is gaining recognition in this field, for features such as the ease of implementation, as it offers advanced security features such as Microsoft 365 E5 Security as part of its Microsoft 365 series.

Figure (related data) Major global cybersecurity companies
Source: Prepared based on Canalys data
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/datashu.html#f00277
(Data collection)

In 2023, the domestic market for information security products (sales) in Japan reached 557.404 billion yen, a 12.0% increase from the previous year. By functional market segments of security products, the sales of security software, including endpoint security software and network security software, accounted for 89.1% of the total market at 496.511 billion yen in 2023, while security appliances, including content management, UTM, and VPN, accounted for 10.9% at 60.893 billion yen.

Furthermore, the domestic market share of information security product vendors (sales) in 2022 and 2023 was categorized into "Foreign Companies" and "Domestic Companies" for those with a market share of 2% or more, and the sales amounts of those companies were calculated for 2022 and 2023.The results showed that foreign companies held a share of over 50% for both years, indicating that a significant portion of Japan's cybersecurity products rely on overseas sources (**Figure 2-1-10-2**).

Figure 2-1-10-2 Domestic information security products market share (sales) (2022 and 2023)



(Source) Prepared based on IDC Japan, April 2025 "Japan IT Security Products Market Shares in the 1st Half of 2024: The Growing SaaS Security Market" (JPJ50704524)

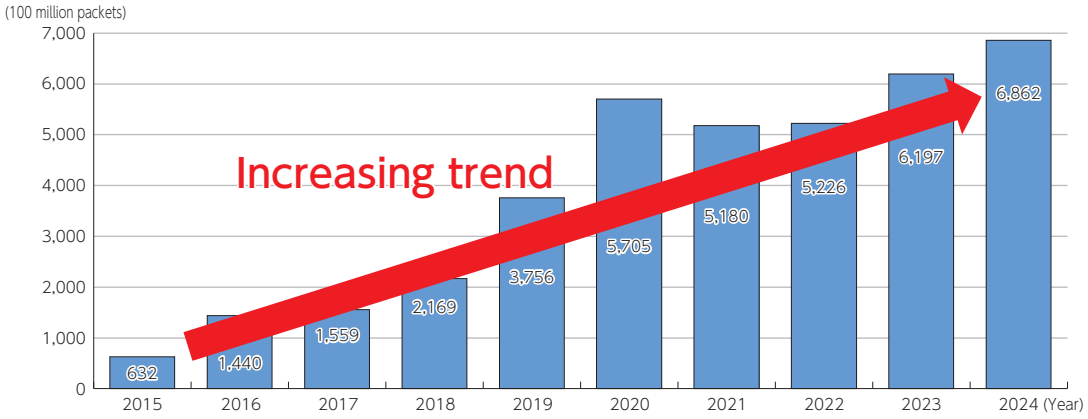
2. Current status of cybersecurity

(1) The increasing threat of cybersecurity

The large-scale cyberattack observation network (NICTER), which is operated by the NICT, observed a total of approximately 686.2 billion packets through darknet monitoring in 2024, a 10.86-fold increase compared with 2015 (approximately 63.2 billion packets). This indicates that a significant number of observation packets are still being received. (**Figure 2-1-10-3**). In addition, the total observed packet count in 2024 corresponds to an observation occurring approximately every 13 seconds for each IP address.

It should be noted that 2024 has recorded the highest number of observations to date, and the observation packets flying around the Internet are even more active compared with 2023.

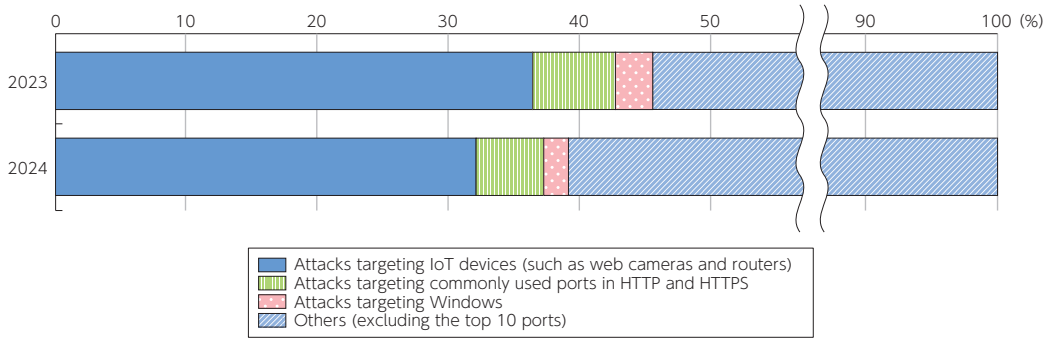
Figure 2-1-10-3 Changes in the number of cyberattack-related communications detected by NICTER



(Source) Prepared based on NICT "NICTER Observation Report 2024"

Furthermore, the observed communications related to cyberattacks in NICTER shows that, similar to 2023, communications targeting IoT devices were most frequently observed, accounting for about 30% of all cyberattack-related communications. The next most frequently observed attacks were on ports used by HTTP and HTTPS (**Figure 2-1-10-4**).

Figure 2-1-10-4 Targets of cyberattack-related communications detected by NICTER



(Source) Prepared based on NICT "NICTER Observation Report 2024"

In 2024, there were 563 cases of violations of the Act on Prohibition of Unauthorized Computer Access (hereinafter referred to as the "Unauthorized Computer Access Prohibition Act"), an increase of 42 cases from the previous year.

Figure (related data) Changes in arrests for violation of the Unauthorized Computer Access Prohibition Act
Source: Prepared based on the National Police Agency, the MIC and the METI "Status of Unauthorized Access Activities and Research and Development of Access Control Technology",
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/datashu.html#f00283
(Data collection)

(2) Economic losses caused by cybersecurity issues

Various organizations have conducted research and analysis on the economic losses caused by cybersecurity issues (**Figure 2-1-10-5**). The numerical values vary depending on the scope of the losses, but for example, according to a survey conducted by Trend Micro in 2024, the average cumulative damage caused by cyberattacks experienced by corporate organizations over the past three years was approximately 171 million yen.

Figure 2-1-10-5 Economic losses caused by cybersecurity issues

Investigation/ analysis entity	Target area	Period covered	Overview of economic loss	Amount of loss
Trend Micro	Japan	2024 [research period]	Average cumulative damage amount for corporate organizations thatexperienced damage from cyber attacks in the past three years	171 million yen (an increase of approximately 4.6 million yen from the previous year)
National Police Agency	Japan	First half of 2024	Total investigation and recovery costs associated with ransomware damage	25%: <1 million yen 21%: 1 million to <5 million yen 8%: 5 million to <10 million yen 27%: 10 million to <50 million yen 19%: ≧ 50 million yen or more
FBI	The U.S.	2023	Total amount of reported damage by cybercrime incidents	12.5 billion dollars (a 22% increase from the previous year)
Sophos	14 countries (North America, Central and South America, Europe, Asia Pacific)	2024	Ransom paid per organization to recover from a ransomware attack	・Average: Approximately 3.96 million dollars (a 2.6-fold increase from the previous year) ・Median: 2 million dollars (a 5-fold increase from the previous year)
			Average annual cost per organization to recover from a ransomware attack (excluding ransom payment)	2.73 million dollars
IBM	World	2024	Global average cost of single data breach for an organization	4.88 million dollars
Statista	World	2018 - 2029	Estimated global cost of cybercrime	9.22 trillion dollars in 2024 15.63 trillion dollars in 2029

(Source) Prepared based on published materials

(3) Trends in wireless LAN security

According to a survey conducted by the MIC[1] in November 2024 to understand the security awareness among wireless LAN users, the recognition of public wireless LAN is high (approximately 92%), but only about half of the respondents actually use it. The most common reason for not using public wireless LAN is "Security Concerns", cited by about 60% of respondents. Among users of public wireless LAN, nearly 90% feel "Security Concerns", with many users citing information theft and unauthorized access from outside as their particular concerns.

Public Wi-Fi that supports OpenRoaming[2] uses technology to encrypt communications and prevent connections to fake public Wi-Fi, allowing users to safely use public Wi-Fi. In addition, once a user registers to use OpenRoaming, the user can use any public Wi-Fi that supports OpenRoaming around the world without any additional settings. In Japan, OpenRoaming is being introduced in urban areas such as Tokyo and Osaka, and the number of public Wi-Fi networks that support OpenRoaming is expected to expand gradually.

(4) Adoption status of sender domain authentication technologies

As of September 2024, the adoption status of sender domain authentication technologies in the JP domain for preventing spoofed emails is approximately 88.4% for SPF and approximately 32.6% for DMARC, both showing an increase.

Figure (related data) Adoption status of sender domain authentication technologies in the JP domain
Source: Compiled by the MIC with the cooperation of four telecommunications companies
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/datashu.html#f00283
(Data collection)

[1] https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/
[2] An international Wi-Fi Roaming platform supported by the Wireless Broadband Alliance, a global organization that introduces and promotes the latest Wi-Fi technologies and services.