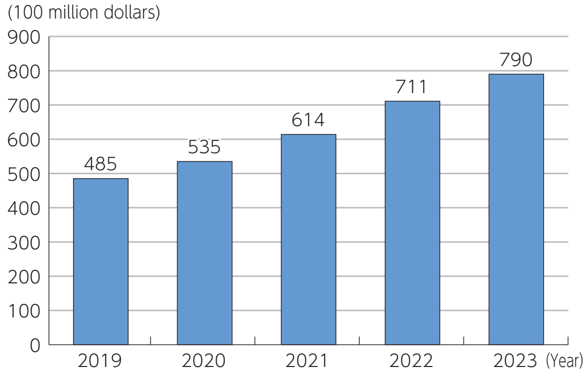
Section 10 Trends of cybersecurity

1. Market overview

The global market for cybersecurity is expected to remain robust, reaching 79 billion dollars in 2023, representing an 11.1% increase from the previous year **(Figure 2-1-10-1)**.

As for the major players in the cybersecurity market, Cisco, Palo Alto Networks, Check Point, Symantec, and Fortinet held the top 5 market shares from 2018 to 2019. However, starting in 2020, Trellix emerged as a replacement for Symantec, and by 2022, it had captured a 3.1% share. Nevertheless, as of 2023, Microsoft and Crowd Strike had replaced Check Point and Trellix in the top 5. Additionally, the market share of the leading player, Palo Alto Networks, has been expanding in recent years.

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



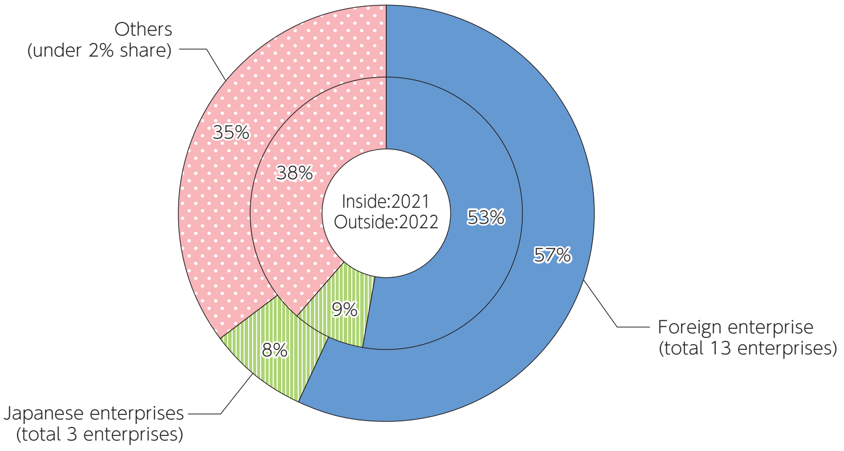
(Source) Prepared based on Canalys data

Figure (related data) Major global cybersecurity companies
Source: Prepared based on Canalys data
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/html/datashu.html#f00294
(Data collection)

In 2022, the domestic market for information security products in Japan reached 525.454 billion yen, a 19.8% increase from the previous year. Within the security product functional market segments, the sales of security software, including endpoint security software and network security software, accounted for 81.3% of the total market at 427.42 billion yen, while security appliances, including content management, UTM, and VPN, accounted for 18.7% at 98.051 billion yen.

Furthermore, the market share of information security product vendors (sales) in 2021 and 2022 was categorized into "Foreign Companies" and "Domestic Companies" for those with a share of 2% or more in the overall market. The results showed that both foreign companies held a share of over 50%, 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)



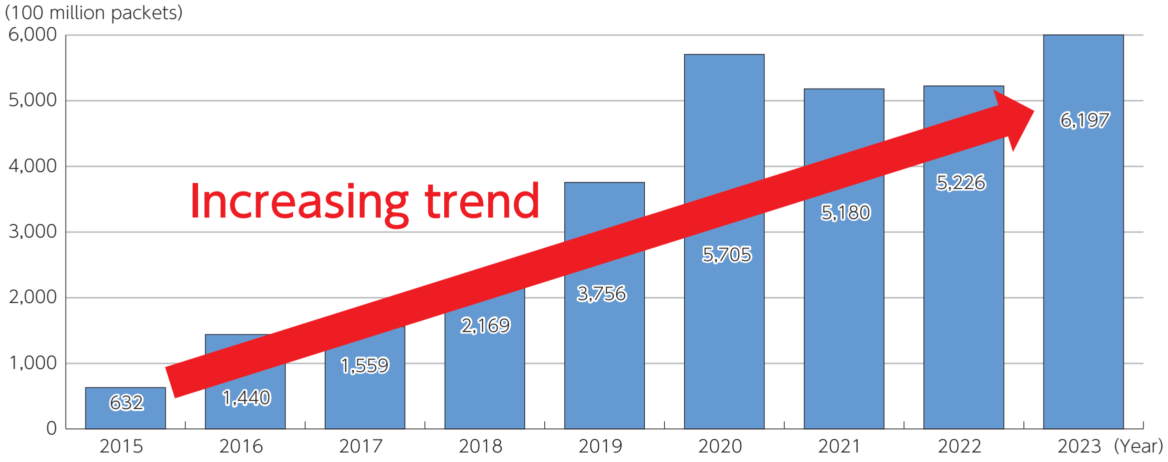
(Source) IDC Japan, August 2023 "Japan IT Security Products Market Shares, 2022: Progress of Security Platform"(JPJ49213223)

2. Current status of cybersecurity

(1) The increasing threat of cybersecurity

The NICT operates the large-scale cyberattack observation network (NICTER), which has observed a total of approximately 619.7 billion packets in 2023, a 9.8-fold increase compared to 2015 (approximately 63.2 billion packets) **(Figure 2-1-10-3)**. This indicates that a significant number of observation packets are still being received. In addition, the total observed packet count in 2023 corresponds to an observation occurring approximately every 14 seconds for each IP address. It should be noted that 2023 has recorded the highest number of observations to date, and the observation packets flying around the internet are even more active compared to 2022.

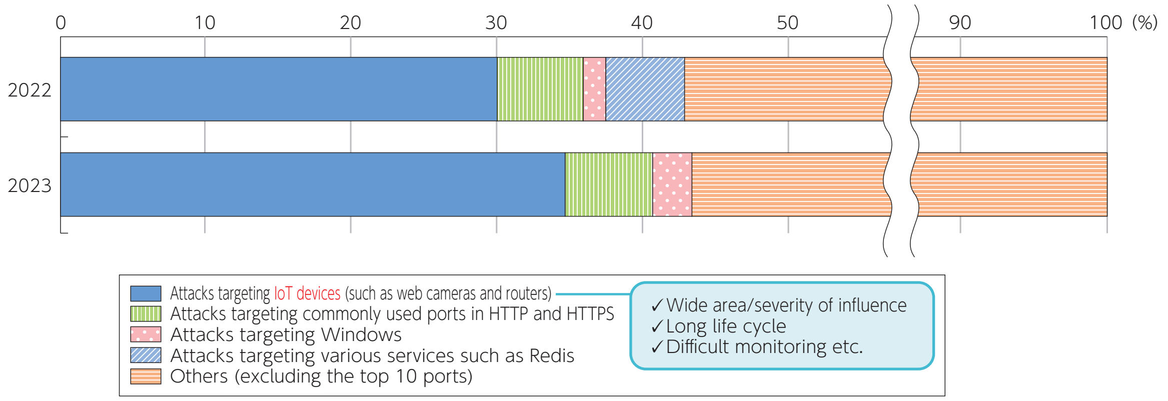
Figure 2-1-10-3 Changes in the number of cyberattack-related communications detected by NICTER



(Source) Prepared based on NICT "NICTER Observation Report 2023"

Furthermore, the observed communication related to cyberattacks in NICTER shows that, similar to 2022, a large number of communications targeting IoT devices were observed, accounting for about 30% of all cyberattack-related communications. Attacks on ports used by HTTP and HTTPS were also observed at a similar rate **(Figure 2-1-10-4)**.

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



* This is an analysis of top 10 ports in what observed by NICTER in 2022 and 2023.

(Source) Prepared based on NICT "NICTER Observation Report 2023"

In 2023, there were 521 cases of violations of the Act on Prohibition of Unauthorized Computer Access (Act No. 128 of 1999, hereinafter referred to as the "Unauthorized Computer Access Prohibition Act"), which was one case fewer than 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/r06/html/datashu.html#f00300
(Data collection)

In recent years, ransomware cyberattacks have continued to affect various companies and medical institutions both domestically and internationally, leading to impacts on people's lives and the socio-economic landscape. Additionally, the resumption of "Emotet" activity was confirmed in March 2023, prompting cautionary measures from the Independent Administrative Institution Information-technology Promotion Agency, Japan (IPA) and JPCERT/CC. There have also been cases of DDoS attacks targeting websites of Japanese government agencies, local governments, and companies, affecting business continuity and raising concerns about cyberattacks for the general public.

Given this challenging situation, in April 2023, the METI, the MIC, the National Police Agency, and the National center of Incident readiness and Strategy for Cybersecurity (NISC) issued cautionary measures for the risks posed by the Golden Week holiday on cybersecurity.

(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 2023, the average cumulative damage caused by cyberattacks experienced by corporate organizations over the past three years was approximately 125.28 million yen.

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

Investigation/ analysis entity	Target area	Period coverd	Overview of economic loss	Amount of loss
Trend Micro	Japan	2023 [research period]	Average cumulative damage amount for corporate organizations that experienced damage from cyber attacks in the past three years	125.28 million yen
National Police Agency	Japan	First half of 2023	Total investigation and recovery conts associated with ransomware damage	26%: <1 million yen 19%: 1 million to <5 million yen 25%: 5 million to <10 million yen 23%: 10 million to <50 million yen 8%: ≧ 50 million yen or more
FBI	The U.S.	2022	Total amount of reported damage by cybercrime incidents	10.2 billion dollars
NFIB	The UK	2023	Total amount of reported damage by cybercrimes	5.6 million pounds
Sophos	14 countries	2023	Average annual cost per organization to recover from most recent ransomware attackト	1.82 million dollars
IBM	16 countries	2023	Global average cost of single data breach for an organization	4.45 million dollars
Cybersecurity Ventures	World	2025 [Prediction]	Cost by cybercrimes	10.5 trillion dollars
Fastl	North America, Europe, Asia, Pacific area	2023	Loss of companies which had cyberattacks	9% of income in the past 12 months

(Source) Prepared based on published materials

(3) Trends in wireless LAN security

According to a survey conducted by the MIC in March 2024 to understand the security awareness of wireless LAN users, the awareness of public wireless LAN is high (approximately 94%), 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 70% of respondents. Among users of public wireless LAN, about 90% feel "Security Concerns", with approximately 40% expressing a "Vague Sense of Unease".

(4) Adoption status of sender domain authentication technologies

As of December 2023, the adoption status of sender domain authentication technologies for preventing spoofed emails in the JP domain is approximately 82.9% for SPF and approximately 10.2% for DMARC, both showing a slight increase.

Figure (related data) Status of introduction of sender domain authentication technologies for JP domains
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/html/datashu.html#f00307
(Data collection)