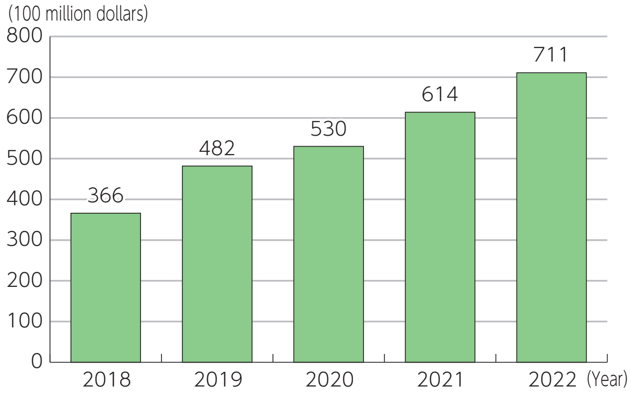
Section 10 Cybersecurity Trends

1. Market overview

The global cybersecurity market (sales) continues to be strong and is expected to grow by 9.3495 trillion yen (38.7% increase) in 2022 (**Figure 4-10-1-1**). By security product category, network security spending was the highest as of the fourth quarter of 2022, accounting for 27.6% of total spending.

Figure 4-10-1-1 Changes in global cybersecurity market size (sales)



(Source) Based on Canalys estimates[1]

Figure (related data) Global cybersecurity market size (by product category)
Source: Based on Canalys "Strong channel sales propel the cybersecurity market to US$20 billion in Q4 2022"
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2023/data_collection.html#f00263
(Data collection)

Cisco, Palo Alto Networks, Check Point, Symantec, and Fortinet were the top five companies in the cybersecurity market in the world from 2018 to 2019, but Trellix replaced Symantec in 2020 and took 3.1% of the market in 2022. Palo Alto Networks has the largest share at only 8.2% of the market, and its share of the global cybersecurity market remains dispersed.

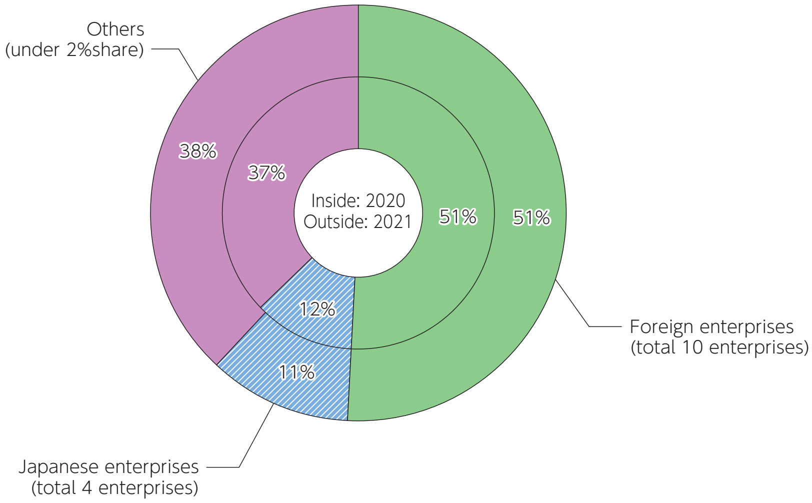
Figure (related data) Major global cybersecurity companies
Source: Based on Canalys data
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2023/data_collection.html#f00264
(Data collection)

In 2021, the domestic information security products market (sales) increased 16% from the previous year to 436.015 billion yen. By security product function market segment, the security software market (which includes endpoint security software and network security software) accounted for 84.1% of the total sales at 315.942 billion yen in 2021, while the security appliance market (which includes content management, UTM, and VPN) accounted for 15.9% of the total at 349 million yen.

We divided enterprises with over 2% share (in sales) in the domestic information security products market in 2021 into foreign enterprises and domestic enterprises, and totalized their sales in 2020 and 2021. Foreign enterprises account for more than 50% of sales both in 2020 and 2021. Japan continues to heavily rely on overseas enterprises for cybersecurity products **(Figure 4-10-1-2)**.

[1] https://www.canalys.com/newsroom/cybersecurity-market-grows-9-in-2018-to-reach-us37-billion
https://canalys.com/newsroom/cybersecurity-investment-2020
https://canalys.com/newsroom/cybersecurity-market-2022

Figure 4-10-1-2 Domestic information security products market share (sales), 2020-2021



(Source) Based on IDC Japan, July 2022 "Japan IT Security Products Market Shares, 2021: External Threat Measures and Internal Threat Measures" (JPJ47880222)

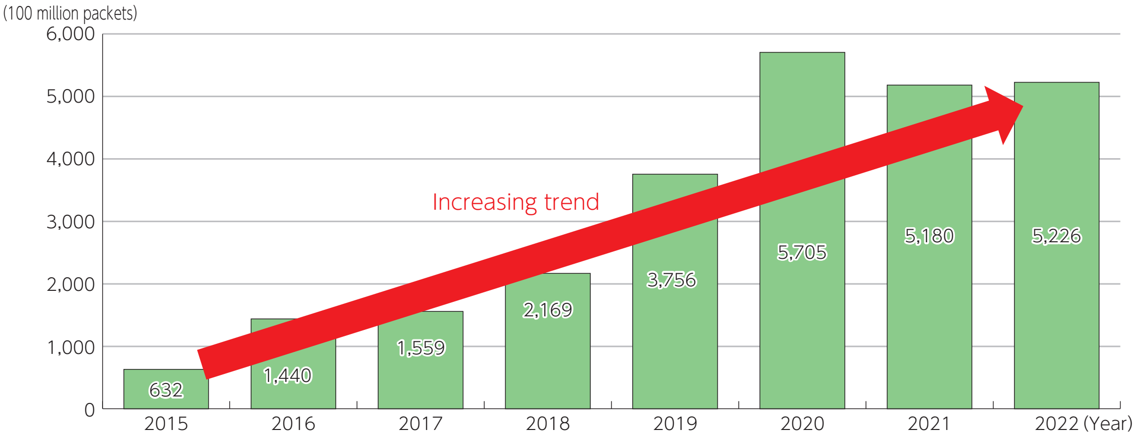
2. State of cybersecurity

(1) Increasing threat to cybersecurity

The number of cyberattack-related communications (about 522.6 billion packets) observed by the Network Incident analysis Center for Tactical Emergency Response (NICTER) operated by NICT in 2022 was 8.3 times higher than in 2015 (about 63.2 billion packets), and many attack-related communications are still being observed (**Figure 4-10-2-1**). The number of cyberattack-related communications observed in 2022 is equivalent to one attack per 17 seconds on each IP address.

The number observed decreased from 2020. The factors include the absence of specific phenomena (large-scale backscatter[2] and a huge quantity of concentrated communications that is thought to be sent from specific senders for the purpose of survey) found in 2022.

Figure 4-10-2-1 Changes in the number of cyberattack-related communications detected by NICTER

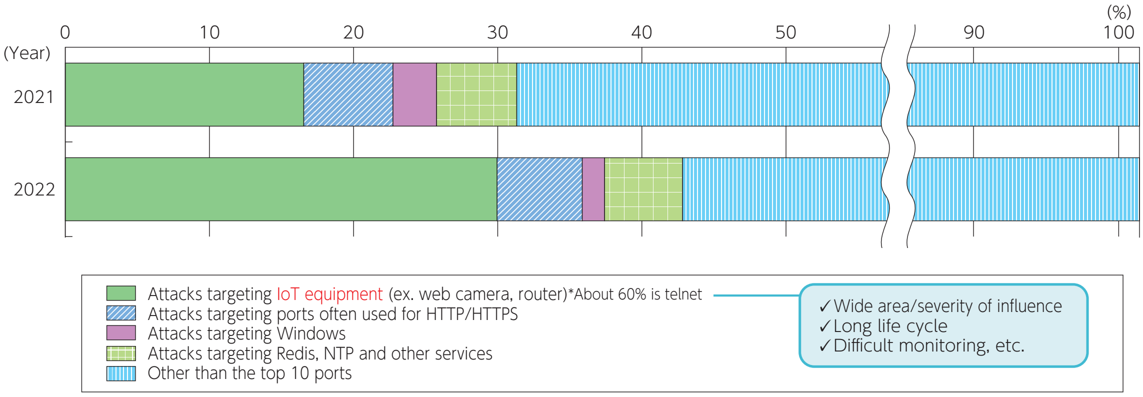


(Source) Based on NICT "NICTER Observation Report 2022"

With regard to cyberattack-related communications in NICTER, communications targeting IoT devices increased significantly from 2021, accounting for 30% of all cyberattack-related communications. Attacks on ports used for HTTP and HTTPS have been observed at a similar rate to last year **(Figure 4-10-2-2)**.

[2] An answer (SYN-ACK) packet from a server that is under DoS attack (SYN-flood attack) with a spoofed send-side IP address. Because a large quantity of response packets reaches the darknet from the servers targeted by DoS attack if IP addresses are randomly spoofed, the DoS attack can be detected.

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



(Source) Based on "NICTER Observation Report 2022" of National Institute of Information and Communications Technology

There were 522 arrests for violation of the Act on Prohibition of Unauthorized Computer Access (hereinafter referred to as "Unauthorized Access Prohibition Act") in 2022, an increase of 93 compared with the previous year.

Figure (related data) Changes in arrests for violation of the Unauthorized Access Prohibition Act
Source: Based on NPA/MIC/METI "Unauthorized Access Activities and Status of Research and Development of Access Control Technology"
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2023/data_collection.html#f00270
(Data collection)

In recent years, cyberattacks caused by ransomware have continued to target various companies and medical institutions in Japan and overseas, affecting people's lives and the social economy. In March 2023, the resumption of Emotet activities was confirmed, and in the same month, the Information-Technology Promotion Agency (IPA) and JPCERT/CC issued an alert. Recently, DDoS attacks targeting the websites of Japanese government agencies, local governments, and companies have had an impact on business continuity. Everyone is now facing concerns with cyberattacks.

In light of the cybersecurity risks posed by major holidays, METI, MIC, the NPA, and NISC issued a warning in April 2023 about the measures they would like to see implemented in preparation for the spring holidays.

(2) Economic losses caused by cybersecurity issues

Various organizations have published studies and analyses of the economic losses caused by cybersecurity issues (**Figure 4-10-2-3**). The figures vary depending on the scope of losses considered. For example, according to a survey conducted by Trend Micro, the average annual damage per organization caused by security incidents in Japan over the course of fiscal 2021 is estimated to be approximately 328.5 million yen.

Figure 4-10-2-3 Economic losses caused by cybersecurity issues

Investigation/ analysis entity	Target area	Period covered	Overview of economic loss	Loss amount
Trend Micro	Japan	Fiscal 2021	Average annual damage per organization resulting from security incidents	328.5 million yen
National Police Agency	Japan	First half of 2022	Total investigation and recovery costs associated with ransomware damage	20%: < 1 million yen 14%: 1 million to < 5 million yen 10%: 5 million to < 10 million yen 37%: 10 million yen to < 50 million yen 18%: 50 million yen or more
FBI	U.S.	2021	Total amount of damage reported for cybercrime incidents	$6.9 billion
NFIB	UK	2022	Total amount of damage reported for cybercrime	£6.3 million
Sophos	31 countries	2021	Average annual cost per organization to recover from most recent ransomware attack	$1.4 million
IBM	World	2022	Global average cost of single data breach for an organization	$4.35 million
Cybersecurity Ventures	World	2023 [expected]	Cost of cybercrime	$8 trillion
McAfee, CSIS	World	2020	Cost of cybercrime	$945 billion

(Source) Based on the published materials of each company

(3) Wireless LAN security trends

According to an attitude survey conducted by MIC in November 2022 to understand the security awareness of wireless LAN users, most respondents are aware of the existence of public wireless LAN (approximately 94%), but only about half of them are actually using it. "Security concerns" was the leading reason for not using public wireless LAN far ahead of other reasons. About 90% of public wireless LAN users feel anxiety about security, but half of them answered that they feel a "vague sense of unease."

(4) Introduction of sender domain authentication technologies

With regard to introducing sender domain authentication technologies for preventing spoofed emails in JP domains, SPF and DMARC accounted for approximately 77.2% and 2.7% of technologies introduced, respectively, as of December 2022, and both of them are slightly increasing.

Figure (related data) Introduction of sender domain authentication technologies for JP domains
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2023/data_collection.html#f00277
(Data collection)