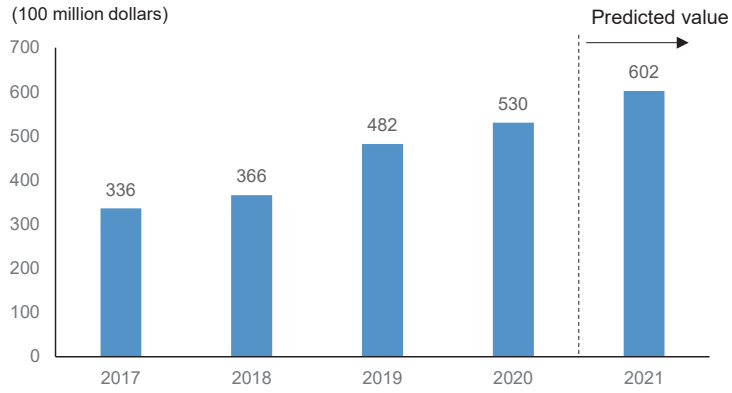
Section 7 Cyber Security Trends

1. Overall condition of the global market

Due to the rapid increase of targeted cyber-attacks including ransomware and other factors, the global cyber security market increased to 5.6591 trillion yen in 2020 and is expected to reach 6.6072 trillion yen in 2021 (16.8% increase year-on-year) (**Figure 3-7-1-1**).

Figure 3-7-1-1 Changes and forecasts for the size of the global cyber security market



(Source) Prepared from Estimation by Canalys[83]

Five major players - Cisco, Palo Alto Networks, Check Point, Symantec and Fortinet – have been ranked high in market share since 2017 (**Figure 3-7-1-2**). However, the top share of Cisco is around 10%. Shares are dispersed in the global cyber security market.

Figure 3-7-1-2 Major global cyber security operator

Operators	Global market share			
	2017	2018	2019 (Q1)	2020 (Q1)
Cisco	9.4%	9.9%	10%	9.1%
Palo Alto Networks	5.9%	6.9%	7%	7.8%
Check Point	6.4%	6.1%	6%	5.4%
Symantec	7.5%	6.1%	6%	4.7%
Fortinet	5.1%	5.5%	5%	5.9%

(Source) Prepared from Estimation by Canalys[84]

[83] 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/canalys-cybersecurity-2021-forecast

[84] https://www.canalys.com/newsroom/cybersecurity-market-grows-9-in-2018-to-reach-us37-billion
https://www.canalys.com/newsroom/cybersecurity-market-q1-2019
https://www.canalys.com/newsroom/canalys-cybersecurity-market-q1-2020

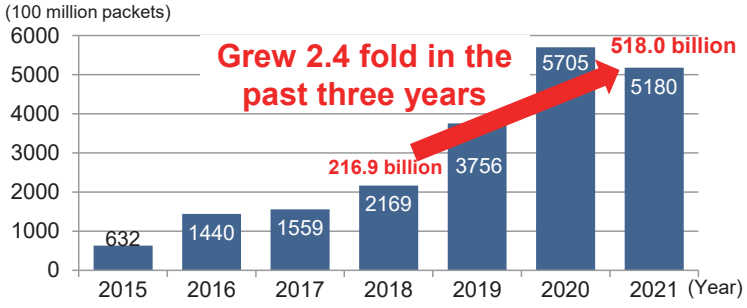
2. Present state of cyber security in Japan

i Increasing threat to cyber security

The number of cyber-attack-related communications (approximately 518.0 billion packets) as observed by Network Incident analysis Center for Tactical Emergency Response (NICTER) that is operated by NICT increased 2.4-fold in 2021 compared with three years ago (216.9 billion packets in 2018), and 3.7-fold compared with five years ago (144.0 billion packets in 2016). Huge quantities of cyber-attack-related communications are still observed (**Figure 3-7-2-1**). The number of cyber-attack-related communications observed in 2021 is equivalent to one attack per 18 seconds on each IP address.

The number decreased from 2020 to 2021. The factors include the absence of specific phenomena (large-scale backscatter[85] and a huge quantity of concentrated communications that is thought to be sent from specific senders for the purpose of survey) found in 2020.

Figure 3-7-2-1 Changes in the number of cyber-attack-related communications detected by NICTER



(Source) NICT, NICTER Observation Report 2021

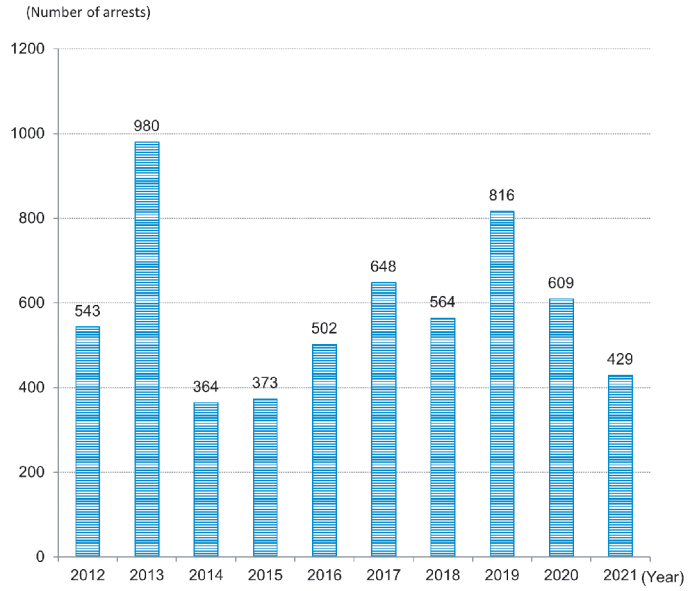
By content of cyber-attack-related communications detected by NICTER, communications targeting IoT equipment account for the largest part. The ratio of the attacks targeting Windows that was second last year decreased, while the ratio of communications to ports used for various services, which were not in the top places last year, and the ratio of other increased. Targets of attacks continued to diversify.

Related data
Targets of cyber-attack-related communications detected by NICTER
Source: Prepared from the National Institute of Information and Communications Technology, "NICTER Observation Report 2021"
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2022/data_collection.pdf#3-7-4 (Data Collection)

The number of arrests for violation of the Act on Prohibition of Unauthorized Computer Access (hereinafter "Unauthorized Access Prohibition Act") was 429, decreasing 180 compared with the previous year (**Figure 3-7-2-2**).

[85] Refers to answer (SYN-ACK) packet from a server that is under DoS attack (SYN-flood attack) with 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 3-7-2-2 Changes in the number of arrests for violation of the Unauthorized Access Prohibition Act



(Source) Prepared from NPA/MIC/METI,
"State of Occurrence of Unauthorized Access and R&D of Technologies related to Access Control Functions"

Since November 2021, there have been signs of resumption of Emotet attack activities. In February 2022, in response to its rapid spread, the Information-technology Promotion Agency (IPA) and JPCERT/CC called attention to the attack.

Considering the increased risk of cyber-attack cases, an alert calling for strengthening of cyber security measures was sent out by METI on February 23, 2022, by METI, MIC, MHLW, MLIT, NPA and Cabinet Secretariat Center for CyberSecurity (NISC) on March 1, 2022, and by METI MIC, NPA and NISC on March 24. On April 25 of the same year, METI, MIC, NPA and NISC advised to take countermeasures toward the long vacation.

ii Wireless LAN security trends

According to an attitude survey conducted by MIC in March 2021 to understand security awareness of wireless LAN users, most respondents know the existence of public wireless LAN (approx. 96%), but only about half of them are actually using it. "Security concern" is the top reason for not using public wireless LAN, way ahead of other reasons. About 90% of public wireless LAN users feel anxiety about security, but half of them answered that this is "vague sense of unease."

iii Introduction state of sender domain authentication technologies

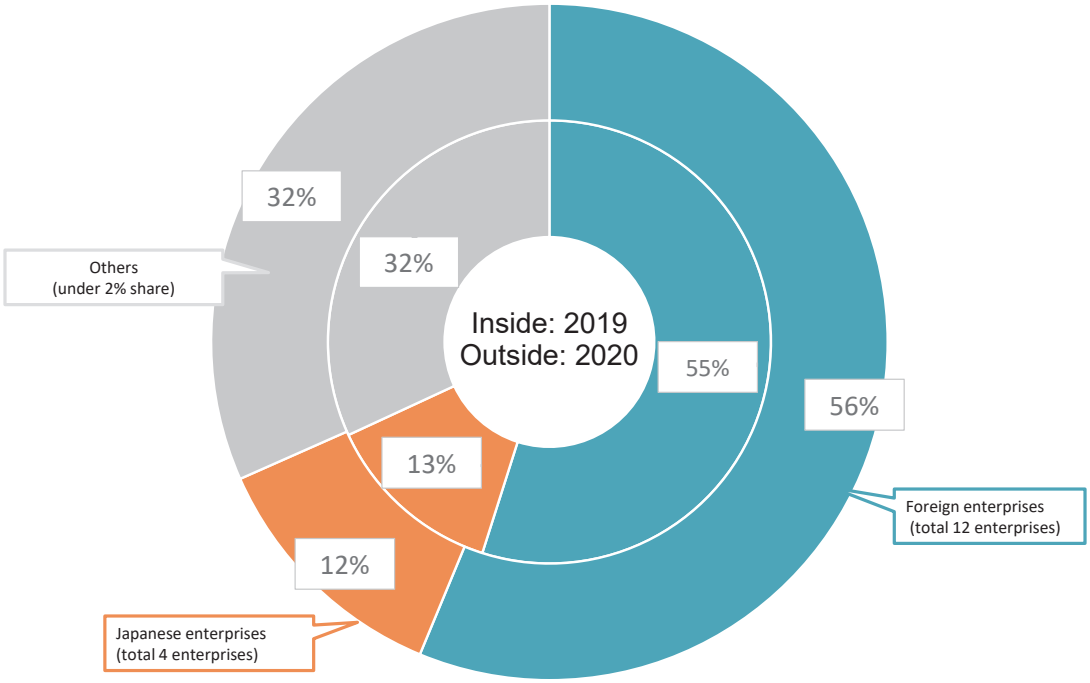
Introduction rate of "sender domain authentication technologies" to prevent spoofed e-mails is slightly increasing: about 67.5% for SPF and about 2.1% for DMARC in December 2021.

Related data
State of introduction of sender domain authentication technologies to IP domains
Source: MIC, "State of setting sender domain authentication technology in IP domain names
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2022/data_collection.pdf#3-7-13 (Data Collection)

iv Dependence on overseas cyber-security products

We divided enterprises with over 2% share (in sales) in the domestic information security product market in 2020 into foreign enterprises and domestic enterprises, and totalized their sales in 2019 and 2020. Foreign enterprises have a large share of sales both in 2019 and 2020. Japan continues to heavily rely on overseas operators for cyber-security products (**Figure 3-7-2-3**).

Figure 3-7-2-3 Domestic information security product market share (sales) (2019 to 2020)



(Source) Prepared from IDC Japan, July 2021, "Japan IT Security Products Market Shares, 2020: External Threat Measures and Internal Threat Measures Drive the Market" (JPJ46567421)