Overview of Threats in Cyberspace 2023

Public Security Intelligence Agency

Preface

The Public Security Intelligence Agency (PSIA) is tasked with ensuring public security in Japan in accordance with the Subversive Activities Prevention Act and the Act on the Control of Organizations, and as a core member of Japan's intelligence community, collects and analyzes information on domestic and international trends that may affect public security in Japan, including not only cyberattacks but also international terrorism, the situation of neighboring countries and trends of domestic organizations, and provides this information to the relevant organizations in a timely and appropriate manner, thereby contributing to the promotion of government measures to ensure a safe and secure society.

In 2020, the PSIA published the "Current Status of Cyberattacks 2020" in order to raise awareness of the growing threats in cyberspace. After the year 2021, the report was renamed "Overview of Threats in Cyberspace," going through editions, to provide a more comprehensive description of threats in cyberspace, and now the 2023 edition has been prepared.

Threats in cyberspace continue to be serious, and attention to influence operations in cyberspace, including the spread of disinformation, has expanded the areas of cyberspace that need to be monitored.

Responding to this situation, this booklet provides an overview of threats in cyberspace in 2022, including threats posed by the activities of non-state actors and the proliferation of disinformation, as well as a special feature on the growing threats posed by the expansion of cyberspace into the space and marine fields.

In addition, this booklet provides an overview of cyberattacks with the involvement or support of states and other entities and public attribution by European countries, the US, etc., as well as basic measures against cyberattacks and the latest cybersecurity concepts under the heading of "Cyberattack Techniques and Countermeasures."

We hope that this booklet, which is available on the PSIA's website, will help the public understand the threats in cyberspace.

※Terms marked with 🔑 are explained as "**KEYWORD**" at the bottom of each page.

Growing Threats in Cyberspace

Cyberattacks aimed at stealing confidential information, acquiring money, and disrupting business operations have become commonplace both in Japan and abroad, and **the methods used for such attacks have also become more sophisticated.** In addition, as cyberspace expands and penetrates further into the real world due to technological progress and changes in social structure, the activities of malicious actors in cyberspace pose **a serious threat** to the sustainable development of society and economy as well as to the safety and security of people's lives.

Furthermore, the threat of cyberattacks is becoming more serious from a national security perspective, as states are believed to be strengthening their cyber warfare capabilities, such as **information theft and destruction of critical infrastructure**, to achieve their political, economic, and military purpose.

Major cyberattacks and related incidents in recent years

December 2015

Massive power outage in Ukraine

A cyberattack on a Ukrainian electric power company resulted in the unauthorized operation of its control system, causing hours-long power outages in western Ukraine and affecting approximately 225,000 people.

November 2016

Russian interference in the US presidential election

According to the US government, Russia worked to influence the 2016 US presidential election through the publication and dissemination of hacked and stolen emails, disinformation, and operations on social media sites (→ see p.8).

May 2017

Ransomware "WannaCry" incident

"WannaCry" ransomware spread worldwide, causing infection damage to government agencies, medical institutions, and businesses in about 150 countries, including Japan (→ see p.12).

December 2020

Attacks uncovered that exploit IT management tool update programs

A large-scale cyberattack occurred, triggered by an attack that exploited an update for an IT management tool manufactured by SolarWinds, a US information and telecommunications company. The US Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive instructing federal agencies to immediately stop using the tool (→ see p.11).

May 2021

Cyberattacks uncovered on information sharing tools provided by a major Japanese information and telecommunications company

A cyberattack on an information sharing tool provided by a major Japanese information and telecommunications company was uncovered. It was later revealed that data including personal information was stolen from 100 or more organizations that used the tool.

February 2022

Cyberattack on satellite communications networks just prior to invasion of Ukraine

According to the US and British governments, Russia attacked the satellite communications networks operated by the US communications company "Viasat" just prior to its invasion of Ukraine in order to disrupt Ukrainian command and control. Communications of several thousand customers in Ukraine and tens of thousands of customers in Europe were suspended (→ see p.6).

KEYWORD **Ransomware** : malware that renders a computer unusable and demands a "ransom" in return for recovery

Diversifying activities of non-state actors

In 2022, cyberattacks by non-state actors operating in connection with international events occurred.

Screenshot of a video posted by “Killnet” declaring war on Japan

(Photo: Jiji)

In the wake of the invasion of Ukraine, media reporting indicated that some 200 groups and individuals, either pro-Russian or pro-Ukrainian, have emerged in cyberspace in disarray. Among them, a hacker group calling itself "Killnet" that supports Russia reportedly carried out DDoS attacks 🔑 on the websites of government agencies and critical infrastructure companies of the US and its allies in March, and in May, named Ukraine and NATO member countries as targets of cyberattacks. Also in September, the websites of Japanese government agencies and railroad companies were temporarily disturbed. "Killnet" has admitted to some of the crimes and has since continued to carry out DDoS attacks against organizations around the world.

Furthermore, there were groups claiming to have conducted cyberattacks against the Russian government, including some from the international hacker group “Anonymous.”

US House Speaker Pelosi visiting Taiwan and President Tsai Ing-wen

(Photo: Â©Chien chih-Hung / Taiwan Presigent / Planet Pix via ZUMA Press Wire / Kyodo News Images)

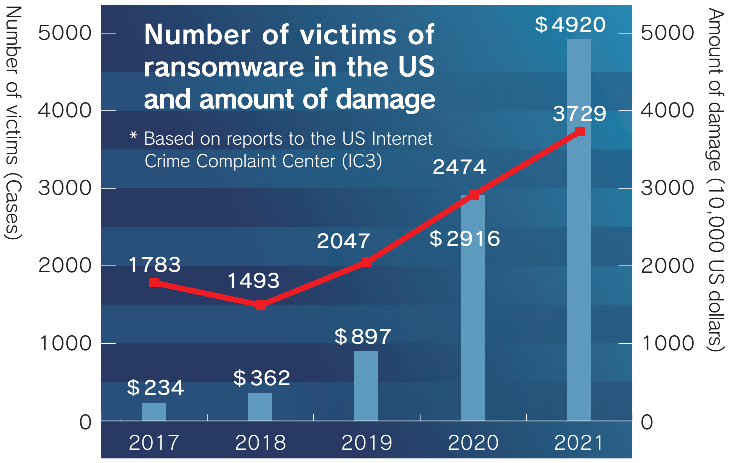
Also in August, just prior to the arrival of US House Speaker Pelosi in Taiwan, DDoS attacks were launched against a number of websites in Taiwan, including the Presidential Office, and TV monitors were hacked in various locations, including train stations and convenience stores, displaying messages critical of the Speaker. Subsequently, a Chinese patriotic hacker group calling itself "27Attack" claimed to have conducted a cyber operation against the Presidential Office and others.

KEYWORD 🔑 **DDoS attack** : A cyberattack in which a large number of terminals send numerous processing requests to take down servers.

Numerous ransomware attacks occurred in Japan and abroad

The threat of ransomware attacks, which disable data by encrypting it and demanding money in exchange for its restoration, has continued to grow in recent years both in Japan and abroad, and in 2022, there was another wave of related damage.

At the end of February, a major Japanese auto parts manufacturer temporarily halted production at its plant in Japan due to a system failure caused by unauthorized access from an external party at one of its suppliers. It was later reported that this may have been a ransomware attack.
In addition, several ransomware attacks against automobile-related companies and their overseas offices were uncovered in February and March.



(Based on the US Federal Bureau of Investigation "IC3 Annual Report")

Ransomware attacks have also occurred against medical institutions. A US study noted that the number of ransomware attacks against medical institutions in the country doubled between 2016 and 2021. The US Federal Bureau of Investigation (FBI) also reported that the medical and public health sectors had the highest number of ransomware attacks among critical infrastructure sectors that were confirmed to have been hit by ransomware in 2021.

Likewise in Japan, a medical institution in Tokushima Prefecture suffered a cyberattack by a cybercrime group using "LockBit 2.0" ransomware in June, which disabled the electronic medical record and in-hospital LAN. In addition, a ransomware attack on a medical institution in Osaka in October caused damage that required more than a month to resume normal medical services due to the impact of the failure of the electronic medical record system.

Reception machines for outpatients with "out of service" tags attached due to a system failure at a medical institution in Osaka

(Photo: Jiji)

In response to this situation, international efforts are being made to combat ransomware. The "NO MORE RANSOM" project, led by Europol and involving law enforcement agencies and private security companies from various countries, identifies ransomware and provides decryption tools through its website. Following the international conference on counter ransomware held in November, led by the US and attended by 37 countries and organizations including Japan, the "International Counter Ransomware Task Force" was established in January 2023, led by Australia as the chair to promote international cooperation in the areas of threat information sharing, countering illicit finance, and holding ransomware actors accountable.

Threat posed by the spread of disinformation

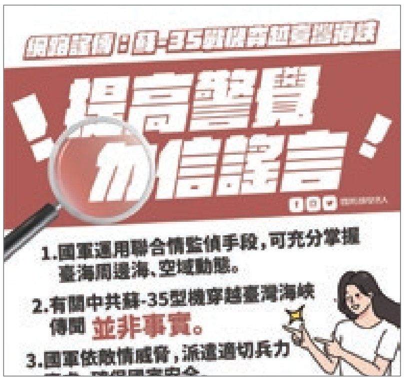
Disinformation can cause confusion by exploiting social unrest and influencing people's perceptions, decision-making, and behavior.

The year 2022 was marked by disinformation circulated in connection with international events.

For example, during the Russian invasion of Ukraine, a Russian Foreign Ministry spokesperson claimed in March to “have obtained evidence that Ukraine was developing biological and chemical weapons near its border with Russia,” which was denied by the White House Press Secretary. Also in April, it was reported that "the body of a foreign mercenary carrying a US passport was found during a raid on a Ukrainian militia stronghold" (Komsomolskaya Pravda, a Russian newspaper, dated April 17), but The Washington Post interviewed the holder of the passport and reported that the Russian paper's report was incorrect.

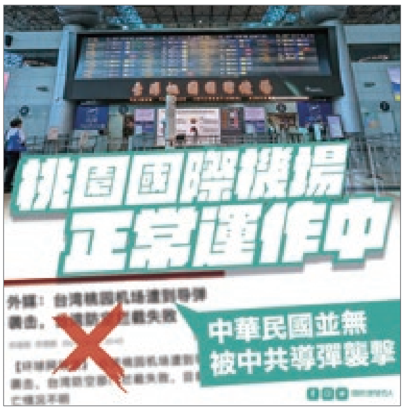
Also, on the occasion of the visit of US House Speaker Pelosi to Taiwan (August 2-3), a reporter from the Chinese state-run media CCTV posted on blog that "Chinese military aircraft crossed the Taiwan Strait," which was spread by the same media and others, but Taiwan's Ministry of National Defense has denied the report (see the upper right figure).

In addition, Taiwan's Ministry of National Defense called for the attention of Taiwanese citizens to the fact that social networking posts such as "Taiwan's Taoyuan International Airport was attacked by missiles from the Chinese People's Liberation Army" and "Chinese military aircraft shot down a Taiwanese military plane" are disinformation (see the lower right figure).
In Japan, too, at around the same time, a post was confirmed on Twitter saying that an aircraft with Speaker Pelosi on board had been shot down, but the post was made by an account posing as a news site of “Yahoo! JAPAN” and there was no such post on the official account, and the news site urged people to be careful of information from fake accounts.


網路謠傳：殲-35戰機穿越臺灣海峽
提高警覺 勿信謠言！
1.國軍運用聯合情監偵手段，可充分掌握臺海周邊海、空域動態。
2.有關中共殲-35型機穿越臺灣海峽傳聞 並非事實。
3.國軍依敵情威脅，派遣適切兵力

Taiwan's Ministry of National Defense calls the posting of "Chinese military aircraft crossed the Taiwan Strait" as "disinformation."

(Photo: Taiwan's Ministry of National Defense website https://air.mnd.gov.tw)



Taiwan's Ministry of National Defense announces that "Taoyuan Airport is functioning normally."

(Photo: Taiwan's Ministry of National Defense Facebook https://www.facebook.com/MilitarySpokesman)

Cyberattacks on the space and maritime sectors

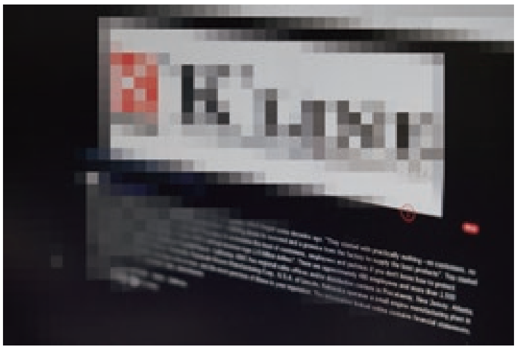
Cyberspace continues to expand in the space and maritime fields due to the increase in the number of satellites in operation and their expanded use, as well as the IT-oriented maritime industry with the introduction of navigation systems, engine control systems, etc., and space and maritime-related cyberattacks are reportedly on the rise accordingly.

In the space sector, in February 2022, one hour before Russia invaded Ukraine, a cyberattack on the satellite communications networks operated by "Viasat," a US communications company, disrupted communications services for several thousand customers in Ukraine and tens of thousands of customers across Europe, and in Germany, the remote monitoring of thousands of wind turbines was disrupted.

Major space-related cyberattacks

Announcement	Occurrence	Factual summary
November 2017	US	Cyberattacks on manufacturers of measuring instruments and others resulted in the theft of trade secrets, including a global navigation satellite systems technology.
February 2020	Japan	An aerial surveying company handling satellite imagery suffered a cyberattack and confirmed unauthorized access to its internal network terminals.
September 2020	5 countries including US	Hackers, backed by Iran's Islamic Revolutionary Guard Corps, sent malware via spear phishing emails to infiltrate satellite-related companies' systems.
July 2021	South Korea	The Korea Aerospace Research Institute (KARI) was cyberattacked by a North Korean cyber threat actor, and information was leaked.
February 2022	Europe including Ukraine	DoS attacks and malware distribution on the ground modems of "KA-SAT," a communications satellite operated by "Viasat," a US communications company, caused satellite communications services to be suspended. In Europe, Internet service providers in France, Germany, and the Czech Republic shut down service.

In the maritime sector, in February 2019, cyberattacks on ships' operational technology systems occurred, including a computer system on a ship sailing to ports such as New York in the US that was infected with malware and its functionality was significantly degraded. In 2021, a Japanese shipping company received unauthorized access and the possibility of information leakage was confirmed, and in 2022, port facilities in Germany, Belgium, and the Netherlands suffered a series of cyberattacks. In addition, a cyberattack in a port in India that appeared to have been carried out using ransomware caused the management system of certain terminals to be shut down.


A site on the dark web that claims to be selling data from a Japanese shipping company whose internal information may have been leaked in a cyberattack
(Photo: Jiji)

In early January 2023, a ransomware attack on the servers of ship management software operated by "DNV," a European ship inspection agency, affected approximately 1,000 vessels equipped with the software.

Unlawful Activities in Cyberspace 1

Information theft and cyber espionage

These activities are aimed at infiltrating the information systems of government agencies and private companies, as well as personal PCs and smartphones, in order to steal important internal information and secretly monitor the movements of individuals. As part of espionage activities, a wide range of fields are targeted for attacks, including politics, economy, diplomacy, and national security.

Leak of 1.25 million cases of personal information at Japan Pension Service (announced in 2015)

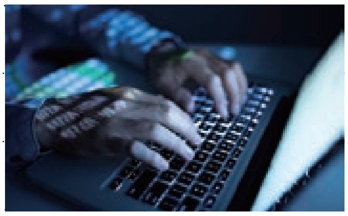
As a result of an employee of the Japan Pension Service opening a file with malware attached to an email, a PC terminal was remotely controlled from the outside, resulting in the leak of approximately 1.25 million personal information of subscribers.

Possible leak of data files with potential security implications (announced in 2021)

Regarding a cyberattack (in 2019) against a major Japanese electronics manufacturer, it was found that out of approximately 20,000 data files containing defense-related information that may have been leaked to outside parties as a result of the attack, there were 59 data files that may have had an impact on national security.

Unlawful Activities in Cyberspace 2

Destruction or interference with the functioning of information systems



These activities are aimed at causing information systems to stop or malfunction. DDoS attacks and malware are used to cause relatively minor damage such as website tampering and browsing problems, while some attacks can cause serious damage such as the shutdown of critical infrastructure.

Large-scale power outage in India (in 2020)

A large-scale power outage occurred in Mumbai, India, which resulted in the suspension of train services and hospitals switching to emergency power. This incident occurred amidst a military conflict between India and China, and rising tensions between the two countries. A US security firm released a report claiming that a cyberattack by China was the cause.

Cyberattacks against Ukrainian financial institutions (in 2022)

The US and the UK announced that Russian military intelligence was involved in DDoS attacks on Ukrainian financial institutions and others that reportedly disrupted online payments and banking applications.

Unlawful acquisition of money

These activities are aimed at fraudulently acquiring bank deposits, crypto-assets, etc. Breaking into the systems of banks and crypto-asset exchanges to send money to external parties, ransomware, cryptojacking 🔑 and other methods are used.

Unauthorized withdrawals from ATMs by hacking (announced in 2018 and 2020)

According to US government announcements, North Korean cyber threat actors have hacked into financial institutions' systems to make unauthorized withdrawals of large amounts of cash from ATMs located in dozens of countries since 2015.

Fraudulent remittance incident in a blockchain game (announced in 2022)

A blockchain game developed by a Vietnamese company received unauthorized access from an external party, resulting in the unauthorized transfer of approximately $600 million worth of crypto-assets.

Online influence operations

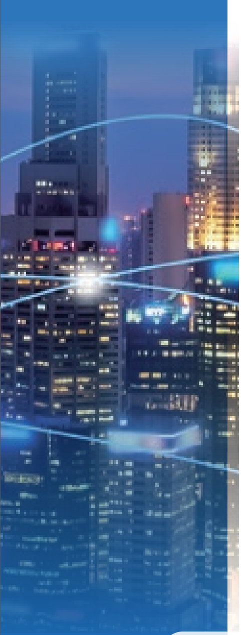
These are activities aimed at influencing people's perceptions, decision-makings, and actions through the intentional use of information. In Western countries, there is growing concern that foreign governments are interfering with public opinion during elections by disseminating stolen information or disinformation online, thereby threatening the foundations of democracy.

Russian interference in the 2016 US presidential election (announced in 2019)

According to US government announcements, on the occasion of the 2016 US presidential election, (1) Russian military officials hacked and stole emails and other information from Democratic candidate Clinton's campaign, and published and disseminated them online, and (2) companies close to the Russian government spread disinformation and engaged in manipulative activities on social media sites.

Russian interference in the 2019 UK general election (announced in 2020)

According to UK government announcements, on the occasion of the 2019 UK general election, confidential government documents relating to the US-UK Free Trade Agreement were illegally obtained and disseminated online through the social media site "Reddit." The UK government concluded that it is almost certain that Russian actors attempted to interfere in the election, in which the issue was the UK's withdrawal from the EU.



KEYWORD 🔑 **Cryptojacking** : The act of allowing a program that "mines" crypto-assets to run on another person's PC or other devices without permission so that the third party can unlawfully obtain financial gain

Threat Actors and Attribution in Cyberspace

Threat actors (cyber attackers) include a wide variety of actors, such as hacktivist groups, money-grubbing criminals, and criminals who commit a crime to see people's reactions, as well as cyberattack groups with the involvement or support of states and other entities. Of particular concern as a serious threat are advanced cyberattack groups with the involvement or support of states and other entities, which are generally characterized as follows.

- **Execute attacks as military or intelligence operations to achieve politico-military national goals, such as the destruction of critical infrastructure, information manipulation, and espionage**
- **Continue persistent attacks without regard to the cost to accomplish the mission**
- **In some cases, criminals or private hackers are used as outside collaborators or agents.**

Cyber threat actors that conduct sophisticated attacks against specific targets in a persistent manner, where the involvement or support of states and other entities is assumed, are referred to as APTs (Advanced Persistent Threats).

Overview of cyberattacks with the involvement or support of states and other entities

China	Attacking actor	The main players are the People's Liberation Army (Strategic Support Force), the Ministry of State Security, and companies, cyber criminals, etc. commissioned by these organizations.
	Features	It is pointed out that information theft is mainly targeted at the 10 key industries identified as key sectors in "Made in China 2025" (next-generation information and communications technology, aerospace equipment, marine construction equipment and high-tech vessels, energy-saving and new energy cars, etc.).
Russia	Attacking actor	Main Intelligence Directorate of the General Staff of the Armed Forces of Russia (GRU), Foreign Intelligence Service (SVR), Federal Security Service (FSB), and others (cyber criminals, companies, etc.)
	Features	Cyber warfare is positioned as a part of "information warfare" and aims for: ● Information theft, manipulation, and exposure to grasp the internal situation of the enemy and to secure its own superiority. ● Destroying the military, administrative, and industrial systems of the enemy and inducing disruption.
North Korea	Attacking actor	The main players are the General Reconnaissance Bureau and its subordinate organizations.
	Features	Acquisition of foreign currency to help the country's economy, theft of information, and provocation and retaliation through sabotage, etc.

KEYWORD

Hacktivist group : An individual or organization that conducts cyberattacks for the purpose of social or political advocacy. A term coined by combining the words "hack," meaning "unauthorized intrusion into a computer system, etc." and "activist," meaning "a person of action."

1 China

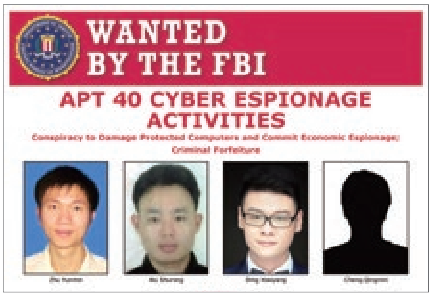
Recent major public attributions

July 2021

The US, UK, and other governments issued a statement that a Chinese cyber threat actor called "APT40" threatens the security of cyberspace.

The Japanese government (Ministry of Foreign Affairs Statement by Press Secretary) also supports the attribution by the US, UK, and other governments, noting that it is highly likely that the Chinese government is behind "APT40."

The US Department of Justice also announced the indictment of a total of four "APT40" personnel, including three employees of the Hainan Provincial State Security Department, on charges of conspiracy to commit computer fraud and economic espionage for their involvement in a global cyberattack campaign aimed at stealing intellectual property and trade secrets.


WANTED
BY THE FBI
APT 40 CYBER ESPIONAGE
ACTIVITIES
Conspiracy to Damage Protected Computers and Commit Economic Espionage;
Criminal Forfeiture

FBI's APT40 Wanted List

(Photo: FBI website https://www.fbi.gov)

July 2022

The Director of the US Federal Bureau of Investigation (FBI) and the Director General of the UK Security Service (MI5) held a joint address on threats from the Chinese government and the Chinese Communist Party, noting that attacks by state-sponsored cyber threat actors against the government and private sector have been observed and their activities are becoming larger and more sophisticated.

MI5 Director General McCallum (left) and FBI Director Wray (right) at a joint address

(Photo: MI5 website https://www.mi5.gov.uk)

KEYWORD

Public Attribution : Efforts by governments, etc., as part of their efforts to deter and respond to cyberattacks, to identify the attackers, such as APT groups, and the state or other organizations behind the attack, and to publicly name and blame the country in question.

2 Russia

Recent major public attributions

October 2020

The US and UK governments determined that the Main Intelligence Directorate of the General Staff of the Armed Forces of Russia (GRU) carried out a cyberattack disguised as an attack by North Korea in order to disrupt the Pyeongchang Winter Olympic Games.

The US Department of Justice announced the indictment of six GRU members.

April 2021

The US Department of the Treasury designated for sanctions 16 organizations and 16 individuals for their alleged involvement in meddling in the 2020 presidential election, as well as six Russian companies for their alleged support of the cyber activities of Russian intelligence agencies.

President Biden also condemned the large-scale cyberattacks stemming from the supply chain attack on "SolarWinds" products, which he said were likely carried out by a cyber threat actor backed by the Russian Foreign Intelligence Service (SVR) known as "APT29" (also known as "Cozy Bear"), and announced the expulsion of 10 Russian diplomats stationed in Washington, D.C.

March 2022

A US federal grand jury in the District of Columbia announced an indictment charging an employee of a research institute affiliated with the Russian Ministry of Defense for infecting a control system used in a foreign refinery with malware "TRITON" between May and September 2017, causing shutdowns of the refinery's operations.

May 2022

The UK Foreign, Commonwealth and Development Office issued an assessment that the Russian Military Intelligence was almost certainly involved in the defacements of Ukrainian government websites and the deployment of "WhisperGate" destructive malware, carried out on January 13, prior to Russia's invasion of Ukraine.

3 North Korea

Recent major public attributions

▼

July 2020

The European Council announced the imposition of the first sanctions against organizations and individuals involved in cyberattacks. In the same announcement, the Council noted that the attack using the "WannaCry" ransomware was carried out by a North Korean cyber threat actor known as "Lazarus" (also known as "APT38").

February 2021

The US Department of Justice announced the indictment of three hackers belonging to the General Reconnaissance Bureau of North Korea for their involvement in disruptive cyberattacks and cyber financial crimes (such as theft of money and crypto-assets, ransomware and cyber-enabled extortion, and creation and development of malicious crypto-asset applications).

Three North Korean defendants announced by the US Department of Justice

(Photo: FBI website https://www.fbi.gov)

April 2022

The US Federal Bureau of Investigation (FBI) announced that a cyberattack on a blockchain game network developed by a Vietnamese company to steal crypto-assets was carried out by a North Korean cyber threat actor known as "Lazarus" and other names. The US Treasury Department has added the North Korean crypto wallet used in the case to its sanctions list.

October 2022

The Panel of Experts of the UN Security Council Sanctions Committee on North Korea released its midterm report for the year 2022 (dated September 7). It noted that North Korean cyber threat actors stole crypto-assets worth hundreds of millions of US dollars during 2022 and continued cyberactivity focusing on stealing information.

Attribution Trends in Japan

In October 2022, Japan's Financial Services Agency, National Police Agency, and the National center of Incident readiness and Strategy for Cybersecurity issued an alert to individuals and businesses involved in crypto-asset transactions regarding cyberattacks by North Korea. Also, in December of the same year, the Ministry of Foreign Affairs, the Ministry of Finance, and the Ministry of Economy, Trade and Industry of Japan announced that the "Lazarus Group," a North Korean cyber threat entity, would be added to the list of parties subject to measures such as asset freezes.

Cyberattack Techniques

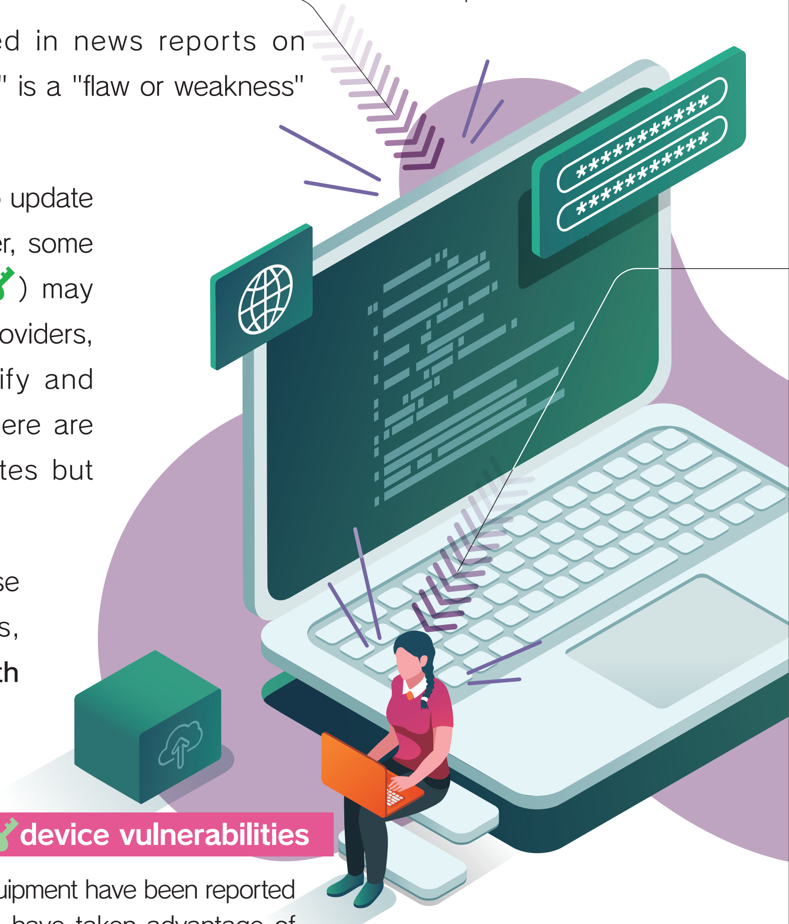
Attacks that exploit weaknesses in the system

→ See P.15 for examples of countermeasures

The term "vulnerability" is often used in news reports on cyberattacks. In a nutshell, a "vulnerability" is a "flaw or weakness" in a computer system.

System providers are constantly working to update their systems to fix vulnerabilities. However, some vulnerabilities (zero-day vulnerabilities) may not even be noticed by developers or providers, making it virtually impossible to identify and address all vulnerabilities. In addition, there are cases where companies provide updates but users do not apply them.

Attackers attempt to achieve their purpose by damaging or manipulating systems, **primarily by exploiting vulnerabilities with malware.**



Example Attacks that exploit VPN device vulnerabilities

In recent years, vulnerabilities in multiple VPN equipment have been reported one after another, and attacks that appear to have taken advantage of these vulnerabilities to steal and abuse authentication information have occurred.
At the end of October 2021, a cybercrime group using "LockBit 2.0" ransomware attacked a public hospital in Japan. Electronic medical records were encrypted, and hospital systems were downed. The attack appears to have targeted a vulnerability in the VPN equipment used by the hospital.

Example Cloud Service Vulnerability

Cloud service is a service that provides data, software, servers, etc., to users via a network, and its use by companies as a means of managing information assets is increasing every year due to its convenience and the introduction of remote working. On the other hand, the cloud service has become an intrusion route for cyberattacks and can be a major target in cases where vulnerabilities are inherent due to human misconfiguration, as well as for attackers who distribute malware that mines crypto-assets.
In January 2022, "Lapsus$," a cybercrime group reportedly based in South America, infiltrated the system of a US company that provides authentication services in the cloud through an outsourced service provider. Hundreds of customer data may have been viewed or manipulated. Also, in May 2022, a cloud service network device of a Japanese company received unauthorized access by exploiting a vulnerability, and it was pointed out that, combined with the inadequate settings of the information security system, authentication information of some customers may have been stolen. According to an Israeli security firm, the number of cyberattacks against cloud services per organization in 2022 was about 50% higher than in 2021, making cyberattacks against cloud services a major threat.
When using cloud services, it is necessary to confirm that information security measures such as physical information security measures at the data center, data backup, vulnerability countermeasures for OS and software, prevention of unauthorized access, access log management, communication encryption, and hardware device failure countermeasures are properly implemented by the service provider.

KEYWORD

Zero-day vulnerabilities：Unknown vulnerabilities before their existence is publicized or before a security update program is provided.
VPN：A virtual dedicated line built on the Internet for secure communications between locations.

Cyberattack Techniques

Attacks that exploit gaps in the human mind

→ See P.16 for examples of countermeasures

Attackers take advantage of not only vulnerabilities in the system. Attackers use "social engineering " to exploit gaps in the human mind to gain unlawful access to systems by deceiving or misleading the users.

The best example of **a cyberattack that takes advantage of human psychology** is a targeted attack (spear phishing) (see KEYWORD on p. 5). It uses themes that attract the attention of email recipients, or it uses text from previous emails to induce recipients to enter information or click on malicious attachments or URLs.

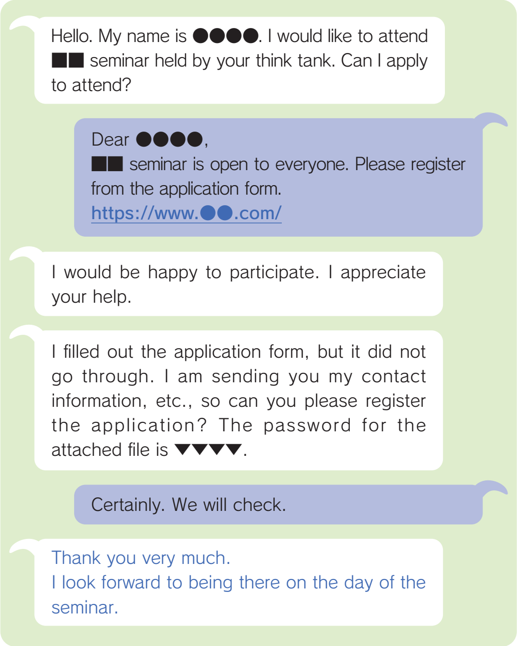
In addition to "phishing attacks," which use email and websites, attackers are also targeting gaps in the human mind of targets in various ways, including "vishing attacks," which use voice communications, and "smishing attacks," which use SMS and other text messages, to steal personal information.

Example Targeted attacks using email and social media

Attackers gather information in advance through various means, including social media, and then send messages that do not arouse suspicion by posing as human resources personnel of major companies or employees of business partners.

Among the actual cases of targeted emails, there was a case in which a fake social media account posing as a human resources representative was used to send false job information to employees of a target company, infecting them with malware. Another case was confirmed in which someone pretended to be a fake employee of a business partner company and sent an email with a false bank transfer address when communicating via email with a real employee of the company to purchase a product, suggesting that he or she kept track of the email correspondence.

In addition, a number of cyberattacks have been confirmed in recent years against academics, think tank researchers, and members of the media, in which attackers pretend to be employees or staff of real organizations and send them emails requesting lectures or interviews, materials, etc. to have them execute malicious programs in an attempt to steal information, and the National Police Agency and the National center of Incident readiness and Strategy for Cybersecurity have issued an alert. In a similar case, a file containing malware was sent under the guise of participation in an actually scheduled seminar.



Hello. My name is ●●●●. I would like to attend ■■ seminar held by your think tank. Can I apply to attend?

Dear ●●●●,
■■ seminar is open to everyone. Please register from the application form.
https://www.●●.com/

I would be happy to participate. I appreciate your help.

I filled out the application form, but it did not go through. I am sending you my contact information, etc., so can you please register the application? The password for the attached file is ▼▼▼▼.

Certainly. We will check.

Thank you very much.
I look forward to being there on the day of the seminar.

The attacker (left) pretended to attend a seminar and sent a file containing malware to the victim (right) under the false pretense that an error had occurred (Based on an actual case).

KEYWORD

Social engineering : a means of stealing information or inducing a specific behavior by exploiting gaps in human psychology and behavior

Targeted Attack (Spear Phishing) : An act of sending emails, etc. to a target pretending to be a person related to the target in order to unlawfully obtain personal information.

Countermeasures against attacks on systems

- Understand the status of PCs, smartphones, and other devices in use, as well as their software and app versions, and update them to the latest versions as soon as possible

【Reference】

The Information-technology Promotion Agency (IPA) of Japan, the Cybersecurity and Infrastructure Security Agency (CISA) of the US, the National Institute of Standards and Technology (NIST) of the US, and others publish vulnerability information.

- IPA https://www.ipa.go.jp
- CISA https://www.cisa.gov
- NIST database of vulnerabilities https://nvd.nist.gov

- Administrators should implement multi-factor authentication, and users should not use the same passwords, set passwords with long characters that are difficult to guess and manage them appropriately.

【Reference】

Multi-factor authentication is an authentication method that combines two or more of the three authentication factors (knowledge information, possession information, and biometric information), and the following are specific examples:

- Knowledge information (PIN) + possession information (e.g., one-time password authentication by phone, SMS, apps, etc.)
- Knowledge information (password) + biometric information (vein authentication, fingerprint authentication, etc.)

- Check cybersecurity firms and other information dissemination to understand the latest TTP of attackers and implement appropriate countermeasures

"EDR" attracts attention as a next-generation security product.

In recent years, the sophistication and ingenuity of APT and other targeted cyberattacks have led to an increase in the number of attacks that cannot be detected by antivirus software. In addition, with the spread of cloud services and the diversification of work styles, including remote working, traditional "perimeter security," which monitors only communications from outside the organization's network, is no longer sufficient to deal with threats.
One security product that is being deployed as a response to this situation is "EDR" (Endpoint Detection and Response). Based on the concept of "zero trust," EDR monitors the behavior and operations of endpoints (PCs, servers, mobile devices, etc.) in an organization's network and detects attacks based on suspicious behavior, thereby enabling rapid initial response (shutting down the network or stopping processes) and is also effective against unknown malware.

KEYWORD

TTP : The attacker's modus operandi, such as tactics, techniques, and procedures
Zero Trust : The idea is that all communications are considered equally "untrustworthy" regardless of whether they are inside or outside the organization's network, and all communications are detected and authenticated on the assumption that the system is infiltrated.

Countermeasures against gaps in the human mind

- If you feel something is strange, do not click on attachments or URLs in emails, SMS, etc., and take careful measures by calling or otherwise confirming with the person you believe to be the genuine sender or by contacting the person in charge of the system.

【Reference】

The malware "Emotet," which has reportedly resumed its activities, extracts information such as address books and email sending/receiving history and uses this information to send emails infected with "Emotet" to business partners and customers as legitimate senders, increasing the risk that recipients will trust the sender's information and open attached files based on the sender's information.

In addition, targeted email attacks are also being carried out using the contents of past correspondence, making it difficult to discern the authenticity of emails.

More attention to the following points will increase the likelihood of preventing suspicious file executions or clicks on URLs.

- Even if the title of the email is related to oneself, isn't the sender of the email an unknown person?
- Isn't the email sent from a free email address?
- Doesn't the body of the email contain unnatural Japanese or kanji characters that are not used in Japanese?
- Aren't there any suspicious features, such as an attached file being an executable file (e.g., exe) or in a compressed format (e.g., rar) that is not commonly used in Japan?

- Do not carelessly post your address, phone number, or email address on social media sites, and be aware that posts about your hobbies, work, or friendships can be used for social engineering (→ see p.14).
- Implement appropriate technical measures, including the introduction of software applications that enable the detection of suspicious emails.

Isn't "Telling users not to click on bad links" enough?

To counter cyberattacks that exploit our weaknesses, it is of course necessary on an individual level to avoid clicking on suspicious email attachments and URLs. However, a blog post published by the UK's National Cyber Security Centre (NCSC) points out that such warnings are not enough to counter cyberattacks in an organization.

The article points out that, in a situation where business operations frequently require clicking on links from unfamiliar domains, and where it is advantageous for attackers to only need to successfully fool one person to break into a system, it is necessary to take appropriate technical measures, such as those described on the left page, to protect an organization from cyberattacks. It also suggests that individual awareness-raising and training are not meaningless, and it is also important to build an organizational culture and work environment that enables early response to incidents, such as prompt reporting to security personnel without fear of reprimand or penalty if a malicious link is clicked.

Functions of the PSIA as a Government Agency

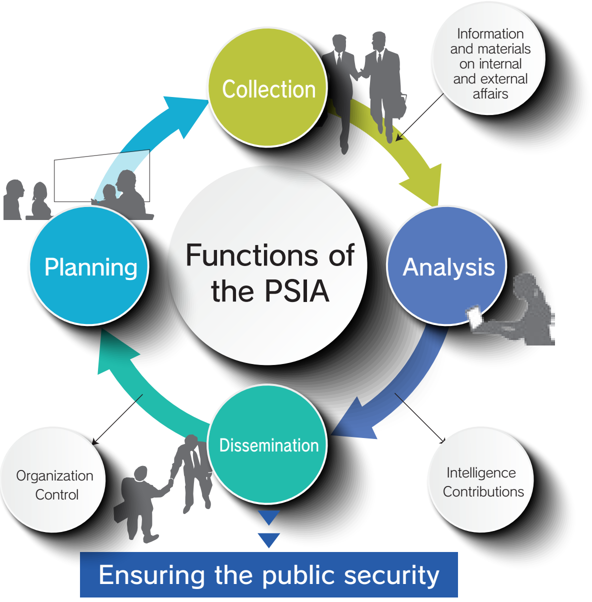
The Public Security Intelligence Agency (PSIA) investigates subversive organizations, etc., and when the PSIA finds that an organization should be subject to controls, it submits a request to the Public Security Examination Commission to designate that the activities of the said organization be restricted, or that it be disbanded.
In addition, as a core member of the intelligence community consisting of Japan's intelligence organizations, the PSIA provides relevant organizations including the Office of the Prime Minister and the Cabinet Secretariat with intelligence that contributes to the promotion of government policies on a daily basis.

Organization Control

- Investigates organizations that could engage in violent subversive activities
- Submits a request to the Public Security Examination Commission to designate that the activities be restricted or that it be disbanded
- Conducts control measures with respect to organizations placed under surveillance disposition

Intelligence Contributions

- As a core member of Japan's intelligence community, provides relevant organizations with intelligence that contributes to government policies.

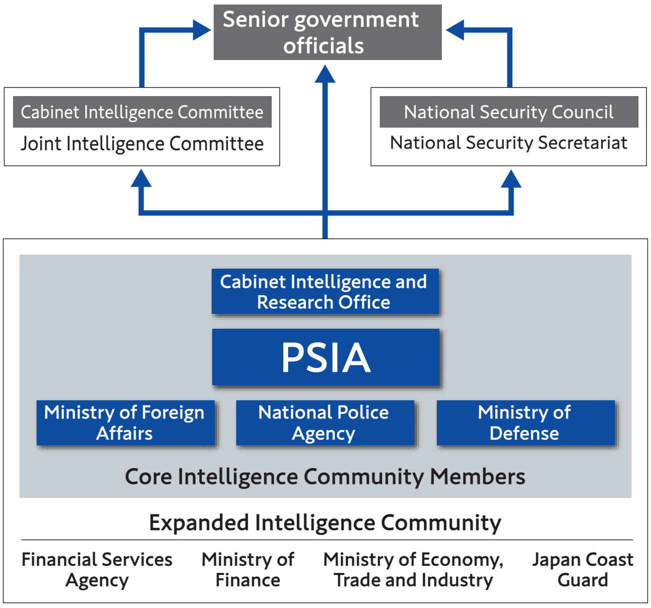

Collection
Information and materials on internal and external affairs
Analysis
Functions of the PSIA
Planning
Dissemination
Organization Control
Intelligence Contributions
Ensuring the public security

Promoting Investigation on Cybersecurity

The PSIA collects and analyzes information on cyberspace and provides this to relevant organizations.

《Functions of the PSIA in Cybersecurity Policy》

The latest annual plan "Cybersecurity 2022" based on the Japanese government's "Cybersecurity Strategy" (cabinet decision, September 2021) states the role of the PSIA that "in order to promote investigations related to cyberspace, the Public Security Intelligence Agency promotes efforts to contribute to cyber-intelligence countermeasures such as strengthening systems of collecting and analyzing HUMINT information and providing it to relevant agencies and organizations in a timely and appropriate manner."

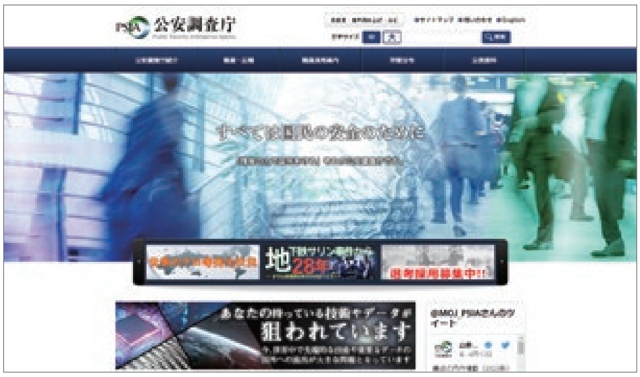

Senior government officials
Cabinet Intelligence Committee
Joint Intelligence Committee
National Security Council
National Security Secretariat
Cabinet Intelligence and Research Office
PSIA
Ministry of Foreign Affairs
National Police Agency
Ministry of Defense
Core Intelligence Community Members
Expanded Intelligence Community
Financial Services Agency
Ministry of Finance
Ministry of Economy, Trade and Industry
Japan Coast Guard

Information Dissemination and Publication from the PSIA

PSIA Website

https://www.moj.go.jp/psia/

The web pages of the PSIA post related laws and regulations under the PSIA's jurisdiction, its history and tasks, and show situations at home and abroad in each of the following categories: "Information on Aum Shinrikyo," "Situations occurring tied to terrorism and relevant affairs in the world," and "Recent Domestic and International Situations."


公安調査庁

あなたの持っている技術やデータが

狙われています

PSIA Official SNS Accounts

The PSIA's official Twitter account and YouTube channel "PSIAchannel" contain information about the PSIA's measures and initiatives, and are used to distribute information that the PSIA wants to announce. We hope you will view this information, together with the information available on the PSIA's website.

Twitter

「@MOJ_PSIA」

PSIA

公安調査庁

フォロー

公安調査庁

フォロー

ツイート

メディア

いいね

YouTube

「PSIAchannel」

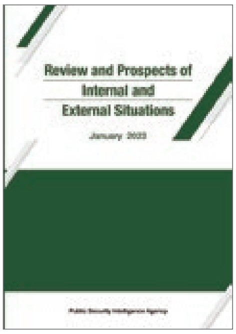
公安調査庁

PSIAchannel

Review and Prospects of Internal and External Situations

In January of each year, the PSIA publishes a "Review and Prospects of Internal and External Situations" report on domestic and international developments related to public security in the previous year.

The latest edition and past editions are available on the PSIA's website.


Review and Prospects of Internal and External Situations

January 2023

Public Security Intelligence Agency

Handbook of International Terrorism

Since 1993, the PSIA has published the "Handbook of International Terrorism," which summarizes trends in international terrorism.

In addition, the handbook is posted on the PSIA's website in an easy-to-understand format to make it more widely known to the public.

国際テロリズム要覧

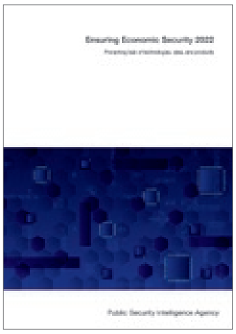
2022

公安調査庁

Economic Security Pamphlet

This pamphlet summarizes the current situation that should be kept in mind from the viewpoint of economic security. Please use this pamphlet for company or academic training, etc.

Please also refer to the Economic Security special page on the PSIA's website.


Ensuring Economic Security 2022

Public Security Intelligence Agency

Protecting the People with the Power of Intelligence

PSIA 公安調査庁
PUBLIC SECURITY INTELLIGENCE AGENCY

Overview of Threats in Cyberspace 2023