Overview of Threats in Cyberspace

2022

Public Security Intelligence Agency
Introduction

As a core member of Japan’s intelligence community, the Public Security Intelligence Agency collects and analyzes information on domestic and international trends that may affect Japan’s public security, including not only cyberattacks but also international terrorism, the situation in neighboring countries and trends in domestic organizations, and provides this information to relevant organizations in a timely and appropriate manner, thereby contributing to the promotion of government measures for a safe and secure society.

The domestic and international situation surrounding Japan is changing at a dizzying pace on a daily basis, and the international order is becoming more unstable due to the prolonged impact of the new coronavirus infection and the growing geopolitical tensions, including the relationship between the US and China. In line with this situation in cyberspace as well, various malicious entities are becoming more active, and the threat is becoming more serious in Japan.

In response to this situation, we have prepared this booklet, "Overview of Threats in Cyberspace 2022," as we did the year before last and last year. We hope that this booklet will help the public understand the threats in cyberspace.

WADA Masaki, Director-General of the Public Security Intelligence Agency
Cyberattacks aimed at disrupting business operations, stealing confidential information, and acquiring money have become commonplace in Japan and abroad, and their methods 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.

### Growing Threats in Cyberspace

- **Massive power outage in Ukraine**
  - December 2015
  - 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 (→ see p.6).

- **Russian interference in the US presidential election**
  - November 2016
  - 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).

- **Ransomware "WannaCry" incident**
  - May 2017
  - "WannaCry" ransomware spread worldwide, causing infection damage to government agencies, medical institutions, and businesses in about 150 countries, including Japan (→ see p.6, 12).

- **Stealing of personal information from US company Equifax uncovered**
  - September 2017
  - Equifax, a US credit information company, was discovered to have received unauthorized access, resulting in the theft of personal information (names, dates of birth, and social security numbers) of approximately 145 million US citizens.

- **Attacks uncovered that exploit IT management tool update programs**
  - December 2020
  - 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).

- **Cyberattacks uncovered on information sharing tools provided by a major Japanese information and telecommunications company**
  - May 2021
  - 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.

---

**Keyword**

Ransomware: malware that renders a computer unusable and demands a “ransom” in return for recovery.
A series of attacks targeting overseas offices of Japanese companies uncovered

In 2021, a series of cyberattacks targeting overseas offices of Japanese companies were uncovered.

In March, in a case of unauthorized access to a major electrical equipment manufacturer (announced in November 2020), it was discovered that unauthorized access to the company’s overseas subsidiary had led to unauthorized access to cloud services contracted by the company. In July, it was also discovered that an overseas subsidiary of a major pharmaceutical manufacturer suffered an external cyberattack (in October 2020), resulting in the leak of some information.

Furthermore, in August, it was discovered that an overseas group company of a major insurance company had suffered a ransomware attack, and in October, an overseas subsidiary of a major automobile manufacturer suffered unauthorized access, causing some of its plants to suspend operations. In November, unauthorized access to the network of a major electrical equipment manufacturer was discovered, and it was later revealed that the attack was via the server of the company’s overseas subsidiary.

These attacks targeted overseas offices, where security tends to be relatively weak, and some of them used overseas offices as stepping stones to gain unauthorized access to domestic servers, requiring continued vigilance.

Examples of cyberattacks targeting overseas offices of Japanese companies

**March 2021**
Unauthorized access to a major electrical equipment manufacturer (announced in November 2020) was found to have been triggered by unauthorized access to an overseas subsidiary of the company.

**August**
While an overseas group company of a major insurance company was attacked by ransomware, leak of confidential information, etc. was unconfirmed.

**October**
An overseas subsidiary of a major automobile manufacturer received unauthorized access to its network, causing a partial shutdown of its production system. Operations were suspended for two days at a portion of the plant.

**October**
A major pharmaceutical manufacturer’s overseas subsidiary suffered a cyber attack from an outside party and it was found that employee information had been posted on the dark web.

**November**
It was discovered that the network of a major electrical equipment manufacturer had been unlawfully accessed, and part of the data on a file server had been read.

It was later discovered that a file server located in Japan was also unlawfully accessed via a server of an overseas subsidiary.
Numerous ransomware attacks occur in Japan and abroad

The year 2021 saw a renewed focus on the use of ransomware in response to the growing damage caused by ransomware attacks worldwide.

The ransomware attack on US petroleum products pipeline operator "Colonial" in May, which forced the operator to shut down its pipeline for five days, caused a tremendous impact, including panic hoarding and a series of gasoline sellouts on the East Coast.

In Japan, a ransomware attack on a chemical manufacturer uncovered in June required approximately two weeks to restore normal operations. In addition, a ransomware attack on a food company discovered in July revealed the possibility of partial leak of corporate and personal information, and the damage to the financial system caused delays in the submission of financial reports.

Furthermore, a ransomware attack on a medical institution that was discovered in October resulted in the unavailability of electronic medical records, and it took several months to restore them, seriously affecting the hospital's operations and ultimately the lives of the citizens who used the hospital.

In addition to the above, several ransomware attacks against overseas offices of Japanese companies were also discovered.

With ransomware attacks on the rise, we must continue to be vigilant against ransomware attacks against Japanese companies and other organizations.

Number of victims of ransomware in the US and amount of damage

Based on reports to the US Internet Crime Complaint Center (IC3)

(Source: US Federal Bureau of Investigation, "IC3 Annual Report")
Expansion of online influence operations

In March, the US Office of the Director of National Intelligence (ODNI) released the assessment, "Foreign Threats to the 2020 US Federal Elections." The assessment concluded that foreign powers, including Russia, interfered in the 2020 presidential election, although they did not influence the outcome of the election.

Also in September, Germany protested to Russia over repeated cyberattacks, including targeted attacks against the country’s politicians, ahead of the German federal parliamentary elections.

Furthermore, in June, in connection with the new coronavirus infection, Taiwan's Ministry of Justice Investigation Bureau announced that it had launched an investigation into the spread of false information from mainland China that Taiwan’s medical system had collapsed.

These possibly state-involved and state-supported online influence operations may threaten the foundations of democracy, including electoral systems and may cause further confusion by influencing people’s perceptions, decision-making, and behavior through disinformation that takes advantage of social unrest caused by new coronavirus infections and other factors.

**Key points of the assessment released by ODNI**

- "We have no indications that any foreign actor attempted to alter any technical aspect of the voting process in the 2020 US [federal] elections, including voter registration, casting ballots, vote tabulation, or reporting results."

- "We assess that Russian president Putin authorized, and a range of Russian government organizations conducted, influence operations aimed at denigrating President Biden’s candidacy and the Democratic Party, supporting former President Trump, undermining public confidence in the electoral process, and exacerbating sociopolitical divisions in the US. Unlike in 2016, we did not see persistent Russian cyber efforts to gain access to election infrastructure."

- "We assess that Iran carried out a multi-pronged covert influence campaign intended to undercut former President Trump’s reelection prospects[,] ... undermine public confidence in the electoral process[,] ... and sow division and exacerbate societal tensions in the US. ... We assess that Supreme Leader Khamenei authorized the campaign[.]

- "We assess that China … considered but did not deploy influence efforts intended to change the outcome of the US Presidential election. ... China sought stability in its relationship with the United States, [and] did not view either election outcome as being advantageous enough for China to risk getting caught meddling[,]"

- "We assess that a range of additional foreign actors—including Lebanese Hizballah, Cuba, and Venezuela—took some steps to attempt to influence the election. ... [W]e assess that they were smaller in scale than the influence efforts conducted by other actors this election cycle. Cybercriminals disrupted some election preparations; we judge their activities probably were driven by financial motivations."
Critical infrastructure, which is essential for maintaining social life, is the target of various cyberattacks, ranging from cyber warfare by states to terrorist organizations and cyber criminals with pecuniary motives, due to the large impact if its functions are disrupted.

Outside of Japan, in February 2021, a cyberattack occurred at a water treatment plant in Florida, US, attempting to raise the concentration of sodium hydroxide in tap water to about 100 times the normal level, and in September, a cyberattack targeting financial institutions and postal service providers in New Zealand caused connection problems to some websites.

Also in May, a ransomware attack against a US petroleum products pipeline operator caused a significant impact (see p. 4). Regarding this incident, the Russian hacker group “DarkSide” admitted its involvement and apologized for the impact it had on society. At the subsequent US-Russia summit, President Biden presented President Putin with 16 sectors of critical infrastructure (chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services <police, fire, ambulance, etc.>, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, nuclear materials and nuclear waste, transportation systems, and water and wastewater systems) where attacks are not tolerated and asked him to take action.

### Cyberattacks on Critical Infrastructure

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2013</td>
<td>South Korea</td>
<td>Simultaneous system failures due to malware infection occurred at financial institutions and broadcasting stations, disrupting ATM use and some broadcasting operations.</td>
</tr>
<tr>
<td>April 2015</td>
<td>France</td>
<td>A cyberattack by a hacker group calling itself the “Cyber Caliphate,” believed to be affiliated with ISIL, caused a temporary suspension of broadcasts by an international broadcaster in France.</td>
</tr>
<tr>
<td>December 2015</td>
<td>Ukraine</td>
<td>A cyberattack on a power company resulted in the unauthorized manipulation of its control system, causing hours-long power outages in the western part of the country and affecting approximately 225,000 people.</td>
</tr>
<tr>
<td>May 2017</td>
<td>Approximately 150 countries including Japan</td>
<td>A large-scale ransomware attack occurred in about 150 countries around the world, including Japan, infecting about 300,000 terminals of government agencies, medical institutions, financial institutions, and others. Systems were shut down, with a significant impact on business operations.</td>
</tr>
<tr>
<td>October 2020</td>
<td>India</td>
<td>A cyberattack on the central power supply command center, port facilities and other facilities caused a major power outage in Mumbai.</td>
</tr>
<tr>
<td>May 2021</td>
<td>US</td>
<td>The largest petroleum product pipeline operator in the US was hit by a ransomware attack, shutting down operations for five days. A number of gasoline sellouts occurred due to panic hoarding.</td>
</tr>
</tbody>
</table>
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 (published 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.

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.

Major cyberattack incident in Georgia (in 2019)

A cyberattack in Georgia defaced and shut down government websites and disrupted the country’s national broadcasting service. The US, UK, and Georgian governments later attributed the incident to the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU).

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.
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.

Fraudulent remittance incident at Central Bank of Bangladesh (in 2016)

The Central Bank of Bangladesh received a targeted email attack in which the Central Bank sent unauthorized money transfer instructions to the Federal Reserve Bank of New York via the Society for Worldwide Interbank Financial Telecommunications (SWIFT) system, resulting in unauthorized transfers from an account held by the Central Bank at the Federal Reserve Bank to accounts held by private organizations, etc. in other Asian countries. The amount of damage was estimated to be approximately $81 million.

Fraudulent remittance incident at a crypto asset exchange (in 2018)

As a result of unauthorized external access to the system of a crypto asset exchange operated by a Japanese company, crypto assets worth approximately 58 billion yen were unlawfully transferred.

Online influence operations

These are activities aimed at influencing people’s perceptions, decision-making, 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 or false information 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.

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 (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 state-involved and state-supported cyberattack groups. Of particular concern as a serious threat are state-involved and state-supported advanced cyberattack groups, 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 hackers are used as outside collaborators or agents.

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

In addition, cyberattacks are highly anonymous and secretive in nature, and the source of the attack is not self-evident. Therefore, even if an attack is carried out with the involvement and support of a state, the perpetrating state can easily deny it, making it more difficult to deter than traditional military threats.

Under these circumstances, the US, UK, and other governments are stepping up efforts in what is called “public attribution” to deter and respond to cyberattacks by identifying attackers such as APT groups and the state actors behind them, and then publicly naming and shaming the countries concerned.

<table>
<thead>
<tr>
<th>Distinguished name of APT (Examples of aliases in parentheses)</th>
<th>Relevant state institutions based on US and European government pronouncements</th>
<th>Examples of cyberattack incidents and targets involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>APT1 (Comment Panda)</td>
<td>People’s Liberation Army of China</td>
<td>Information theft from six organizations in the US, including atomic power manufacturers (2006 - 2014)</td>
</tr>
<tr>
<td>APT41 (Wicked Panda)</td>
<td>Ministry of State Security of China</td>
<td>Attacks for money targeting online gaming companies (circa 2009 - 2015)</td>
</tr>
</tbody>
</table>
The US, UK, and other governments have been more active than ever in public attribution to deter unlawful state cyber activity, pointing to state involvement by China, Russia, and North Korea, as follows.

**China**

Military and intelligence agencies' involvement in cyberattacks and cooperation with cybercriminals has been pointed out

**Recent major public attributions**

July 2021

The US, UK, and other governments issued a statement regarding a cyber threat actor called "APT40" which the Chinese government is behind, saying that China's malicious activities threaten cyberspace security. 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.

**Cyberattack case against JAXA, etc.**

In April 2021, the Metropolitan Police Department referred a Chinese Communist Party member, who was in Japan at the time of the contract, to the Tokyo District Public Prosecutors Office on suspicion of unauthorized creation and use of private electronic or magnetic records for having contracted under a false name for a rental server used in a cyberattack against the Japan Aerospace Exploration Agency (JAXA) and others. During the course of the investigation, it was pointed out that the case was found to be likely to involve "Tick," a Chinese cyber threat actor with the support of the Unit 61419 of the Chinese People's Liberation Army.

**Japan's "Cybersecurity Strategy"**

The Japanese government's "Cybersecurity Strategy" decided by the Cabinet in September 2021 named China, Russia, and North Korea as cyberattack threat actors for the first time, stated that "it is observed that China, Russia, and North Korea are continuing to build the cyber capabilities" and pointed out the possibility of them conducting cyberattacks in an attempt to steal information, etc.
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.

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 reiterated his condemnation of 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.

The G7 issued a joint statement calling on Russia to hold to account those within its borders who conduct ransomware attacks and other cybercrimes.

The European Council issued a statement condemning the Russian government for its involvement in a malicious cyber activity called as "Ghostwriter." The statement noted that "Ghostwriter" targeted numerous members of Parliaments, government officials, politicians, and members of the press and civil society in the EU in an attempt to steal data and undermine democratic institutions and processes, including by enabling disinformation and information manipulation, and it urged Russia to adhere to the norms of responsible state behaviour in cyberspace.
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”).

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 cryptocurrency, ransomware and cyber-enabled extortion, and creation and development of malicious cryptocurrency applications).

According to an announcement by members of the ruling and opposition parties belonging to the National Assembly Intelligence Committee of South Korea, the National Intelligence Service of South Korea reported to the Committee that North Korea had attempted to steal technology information from South Korea, including vaccines and medicines for new coronavirus infections. The Service also reported cases by North Korea of hacking to steal money, ransomware attacks targeting businesses, and phishing e-mails sent to approximately 100 South Korean VIPs.

The Panel of Experts of the UN Security Council’s North Korea Sanctions Committee released its midterm report (dated September 8) for FY2021. The report notes the activities of cyber threat actors (“Lazarus,” “Kimsuky,” etc.) under the General Reconnaissance Bureau of North Korea, including attacks against Germany’s defense industry and the theft of information from pharmaceutical companies developing Covid-19 vaccines.
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 2019, a number of VPN equipment vulnerabilities were reported one after another, and soon after, attacks were confirmed that appeared to have taken advantage of these vulnerabilities to steal and abuse authentication information. Although the manufacturers of these devices provided fixes for the vulnerabilities, it was pointed out that VPN devices with unfixed vulnerabilities could still be targeted, and that authentication information stolen before the fixes were made could still be used for malicious purposes.

**Example: Attacks using vulnerabilities in the remote working environment**

While the number of companies introducing remote working in Japan has been increasing due to the recent reform of work styles and the spread of the new coronavirus infection, because of the urgent establishment of remote working environments, cyberattack cases due to the use of old VPN equipment with vulnerabilities left unattended, cyberattack cases against private terminals used for business purposes and cases of hijacking of web conferencing systems have been observed.

**Example: "Apache Log4j" vulnerability**

In 2021, a vulnerability was discovered in "Apache Log4j," software used to output application logs, which could be manipulated by an external third party (execution or termination of programs, alteration, deletion, or leak of data stored on the server, etc.). Since the software is widely used in Internet servers around the world, a large number of devices could be affected, and The Apache Software Foundation, the developer of the software, has rated its severity as the highest level (Critical). It has also been pointed out that there have been confirmed attempts by concerned countries to exploit the vulnerability.
Cyberattack Techniques

Attacks that exploit gaps in the human mind

Attacks 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 e-mail recipients, or it uses text from previous e-mails to induce recipients to enter information or click on malicious attachments or URLs.

In addition to "phishing attacks," which use e-mail 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 e-mail

A number of targeted e-mail attacks aiming to infect users with the "LODEINFO" malware have been confirmed in Japan. The malware has been updated frequently, and its functions have been continuously extended, including new screen capture and ransomware functions. Malicious document files are attached to attack e-mails. The body of the e-mail and attached files were found to be disguised as content related to new coronavirus infections, diplomacy, security, etc.

Example Targeted attacks using social media

Attackers actively use social media by searching for self-introductions, posts, images, etc. on social media to gather information in order to select targets in line with their objectives, contact, and attack the targets.

In actual social media cases, false social media accounts posing as human resources (HR) representatives of major companies were used to send false job postings to employees of targeted companies, infecting them with malware. Other methods were also observed, such as using voice and video calls to continue communication, gaining trust, and then sending malware.

Recently, a new attack method that exploits file-sharing services such as cloud storage to induce users to download malware from a URL pasted in a message has been confirmed, and it appears that attackers are also continuing to devise new attack methods.
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 United States, the National Institute of Standards and Technology (NIST) of the United States, and others publish vulnerability information.

- Information-technology Promotion Agency, Japan (IPA)
  https://www.ipa.go.jp
- US Cybersecurity and Infrastructure Security Agency (CISA)
  https://www.cisa.gov
- US National Institute of Standards and Technology (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.

**Next-generation "Zero-Trust Security" Approach Drawing Attention**

Recently, in response to the spread of cloud services and the need for countermeasures against sophisticated targeted attacks that infiltrate organizational networks for long periods of time and in secret, the concept of "zero-trust" next-generation security measures has been attracting attention as an alternative to the current "perimeter security."

The "Zero Trust" system considers all communications equally "untrustworthy" regardless of whether they are inside or outside the organization and ensures security through accurate identification of users/devices and constant monitoring/confirmation by a) setting access privileges to the minimum necessary and evaluating the trustworthiness of each access on a case-by-case basis, b) implementing comprehensive authentication by combining multiple factors, and c) stopping even authorized access privileges when the possibility of impersonation is high.

**KEYWORD**

TTP: The attacker’s modus operandi, such as tactics, techniques, and procedures.
If you feel something is strange, do not click on attachments or URLs in e-mails, SMS, social media, 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 e-mail attacks are also being carried out using the contents of past correspondence, making it difficult to discern the authenticity of e-mails.

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 e-mail is related to oneself, isn’t the sender of the e-mail an unknown person?
- Isn’t the email sent from a free email address?
- Doesn’t the body of the e-mail contain unnatural Japanese or kanji characters that are not used in Japanese (e.g., simplified characters)?
- 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.

Implement appropriate technical measures, including the introduction of software applications that enable the detection of suspicious e-mails.

**The De-PPAP Movement**
When exchanging files, the method of sending a zip file with a password attached followed by an e-mail containing the password to the file is generally described as "PPAP." This method was widely used as a security measure. However, sending the password in the same way as the file and using the zip file for encryption in the first place are not considered effective as a security measure, and there is now a widespread movement in the public and private sectors to abolish "PPAP."
Functions of the Public Security Intelligence Agency as a Government Agency

The Public Security Intelligence Agency investigates subversive organizations, etc., and when the Agency 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 Public Security Intelligence Agency 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.

Promoting Investigation on Cybersecurity

The Public Security Intelligence Agency also collects and analyzes information on cyberspace and provides this to relevant organizations in a timely and appropriate manner.

《Functions of the Public Security Intelligence Agency in Cybersecurity Policy》

The latest annual plan “Cybersecurity 2021” based on the Japanese government’s “Cybersecurity Strategy” (cabinet decision, September 2021) states the role of the Public Security Intelligence Agency 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.”
Website of the Public Security Intelligence Agency

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

The web pages of the Public Security Intelligence Agency post related laws and regulations under the Agency’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.”

Official SNS Accounts of the Public Safety Intelligence Agency

The official Twitter account of the Public Security Intelligence Agency and the Agency’s official YouTube channel “PSIAchannel” contain information about the Agency’s measures and initiatives, and are used to distribute information that the Agency wants to announce. We hope you will view this information, together with the information available on the Agency’s website.

Twitter
「@MOJ_PSIA」

YouTube
「PSIAchannel」

Review and Prospects of Internal and External Situations

In January of each year, the Public Security Intelligence Agency 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 of “Review and Prospects of Internal and External Situations” are available on the Public Security Intelligence Agency’s website.

Handbook of International Terrorism

Since 1993, the Public Security Intelligence Agency has published the “Handbook of International Terrorism,” which summarizes trends in international terrorism.

In addition, the 2022 edition of the “Handbook of International Terrorism” is posted on the Public Security Intelligence Agency’s website in an easy-to-understand format to make it more widely known to the public.

Economic Security Leaflet

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

Please also refer to the Economic Security special page on the Public Security Intelligence Agency’s website.
Protecting the People with the Power of Intelligence