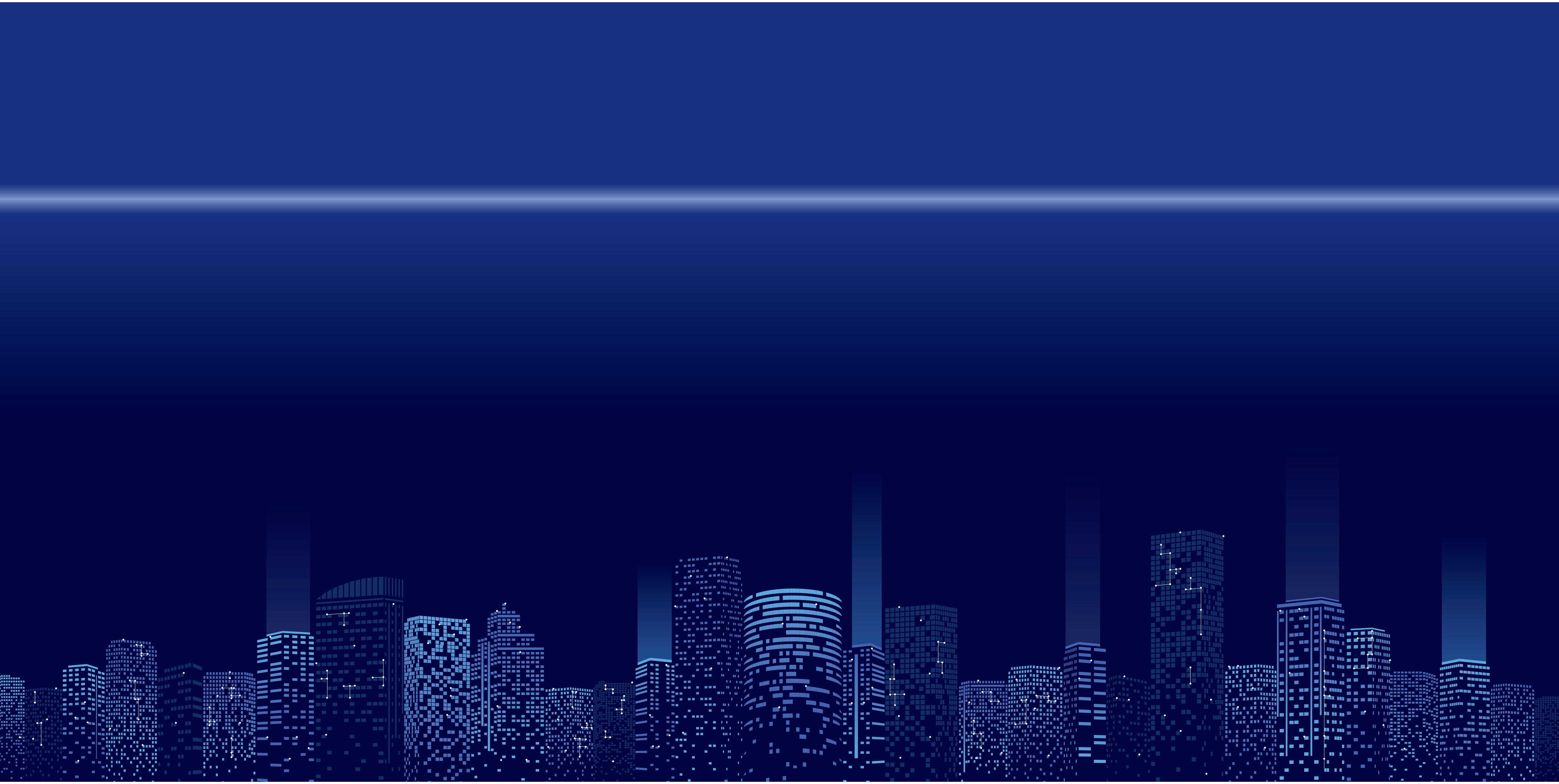


Ensuring Economic Security 2023

Preventing leak of technologies, data, and products

Protecting the People with the Power of Intelligence

PSIA 公安調査庁
PUBLIC SECURITY INTELLIGENCE AGENCY

Public Security Intelligence Agency

2023.07

Introduction

Amid growing global trends to strengthen economic security, cases have been observed in which states, organizations, and individuals seeking to improperly obtain Japan's "advantages" in technologies, data, and products (hereinafter referred to as "entities of concern") attempt to leak sensitive technologies, data, and products by offering transactions and exchanges under the guise of seemingly harmless economic, academic, and other activities.

The unintentional leak of technologies, data, and products from Japan could result in the loss of its international competitiveness and novelty in research, as well as threaten the security of the nation and its people by being diverted to research and development of weapons of mass destruction and the like. Therefore, it is of utmost importance that the public and private sectors work together to strengthen efforts to ensure economic security and preemptively prevent the leak of technologies, data, and products, based on an accurate understanding of these risks.

This pamphlet has been prepared to inform the public about the current situation, which should be kept in mind from the viewpoint of economic security. We hope that it will help your understanding.

Contents

Current Situation Surrounding Japan

The Increasingly Tense US-China Conflict

European Union (EU)

"EU Foreign Direct Investment Screening Regulation"—October 2020

- Screening of foreign direct investment in sensitive technologies and critical infrastructure

New EU industrial strategy "Open Strategic Autonomy"—May 2021

- Identification of products that are highly import-dependent and for which it is difficult to diversify procurement sources or substitute within the region, and strengthening of cooperation in areas of strategic importance

Proposal for an "EU chips act"—February 2022

- Breaking away from dependence on Asian semiconductors, and strengthening research and development, and production in the EU

Canada

Update to the "Guidelines on the National Security Review of Investments"—March 2021

- Identification of areas that could present national security concerns in foreign investment and review of foreign investment in these areas

Release of "National Security Guidelines for Research Partnerships"—July 2021

- Protection of domestic intellectual property from espionage and other activities

Enactment of "Regulations on the Unreliable Entity List"—September 2020

- Creating lists of foreign organizations and individuals that threaten China's sovereignty, security, and interests, and restriction or prohibition of their import, export, investment, entry into China, etc.

Enactment of "Rules on Countering the Unjustified Extraterritorial Application of Foreign Legislations and Order Measures"—January 2021

- Prevention of the application of foreign regulatory laws and regulations in China

Enactment of "Anti-Foreign Sanctions Law"—June 2021

- Allowing for countermeasures at the legal level against "discriminatory restrictive measures" by foreign countries (In February 2022, China announced countermeasures against two US companies)

Restrictions on entry of Chinese researchers and students—June 2018 onwards

- Stricter visa issuance for Chinese students of science and engineering

Posting of Chinese companies on the Entity List based on the "National Defense Authorization Act for 2019"—May 2019 onwards

- In December 2022, major Chinese semiconductor companies were added to the Entity List

(Note: The Entity List includes organizations and individuals involved in activities subject to US sanctions or contrary to the US national security or foreign policy interests. Exports to those on this list are restricted.)

Exclusion of China from the supply chain of critical technologies and products under the "Executive Order on America's Supply Chains"—February 2021 onwards

- Restrictions on the procurement and use of information and telecommunications equipment, etc. made by Chinese companies

Strengthening export control of semiconductor-related products—October 2022 onwards

- Restrictions on the export of semiconductors, semiconductor manufacturing equipment, etc. to China and the export to semiconductor manufacturing facilities for China

United Kingdom

"National Security and Investment Act"—January 2022

- Granting the government the authority to scrutinize and intervene in foreign investment, etc.

Germany

Amendment to the "Foreign Trade and Payments Act"—July 2020

- Expanding the scope of notification requirements for investments by non-EU companies

Amendment to the "IT Security Act"—May 2021

- Strengthening the functions of the Federal Office for Information Security
- Prohibiting the use of components in critical infrastructures if they undermine public security

France

Amendment to the "Code of Post and Electronic Communications"—August 2019

- Requiring communications carriers to undergo prior review when using hardware and software related to wireless communications networks for 5G and beyond

Extension of special measures to regulate foreign investment—December 2022

- Extending special measures to protect companies in strategic sectors from acquisition by foreign capital (until the end of December 2023)

Australia

Amendment to the "Foreign Acquisitions and Takeovers Act"—January 2021

- Mandating government review of foreign investment in land and business sensitive to national security, regardless of the amount of investment

Amendment to the "Security of Critical Infrastructure Act"—December 2021

- Expansion of the scope of foreign investment examination from four to 11 sectors

Economic Security Situation Surrounding Russia’s Aggression in Ukraine

While Western countries are implementing strict sanctions, Russia is believed to be procuring Western products through third countries while taking various countermeasures. A British think tank has pointed out that many Western products, including semiconductors, are being used in Russian military equipment, and engines and cameras made in Japan are among them.

Developments concerning sanctions against Russia

- Freezing of assets of government officials, oligarchs, etc.
- Exclusion of certain banks from SWIFT
- Establishment of ceiling prices for crude oil and petroleum products
- Prohibition of the export of luxury goods, etc.
- Prohibition or restrictions of new investment
- Restrictions and bans on import
- Tighter export controls on key technologies and products

etc.

- Export ban on certain products from Russia
- Restrictions on port calls
- Ban on transporting leased aircraft out of Russia
- Non-payment of compensation for patent use
- Mandatory donations by foreign companies withdrawing from Russia
- Restructuring of the “Sakhalin I and II” operating entities
- Procurement of products through third countries

etc.

Numerous Western products are mounted on Russian military equipment

In a report titled “SILICON LIFELINE: WESTERN ELECTRONICS AT THE HEART OF RUSSIA’S WAR MACHINE” in August 2022, the Royal United Services Institute (RUSI), a British think tank, pointed out that semiconductors and electronic components from many Western countries and regions, including Japan, are used in Russian military weapons.

In a report titled “THE ORLAN COMPLEX: TRACKING THE SUPPLY CHAINS OF RUSSIA’S MOST SUCCESSFUL UAV” in December of the same year, RUSI noted that Western products used in Russian military unmanned aerial vehicles are procured through Hong Kong-based and other companies.

Parts and country/ region of manufacture (examples)

Sensors (US)	Cameras (Japan)	Communication components (Switzerland)
Engines (Japan)	Electronic components (US, Germany)	Semiconductors (US)

Mounted on

Orlan-10 unmanned aircraft (photo courtesy of Sputnik/ Kyodo News Images)

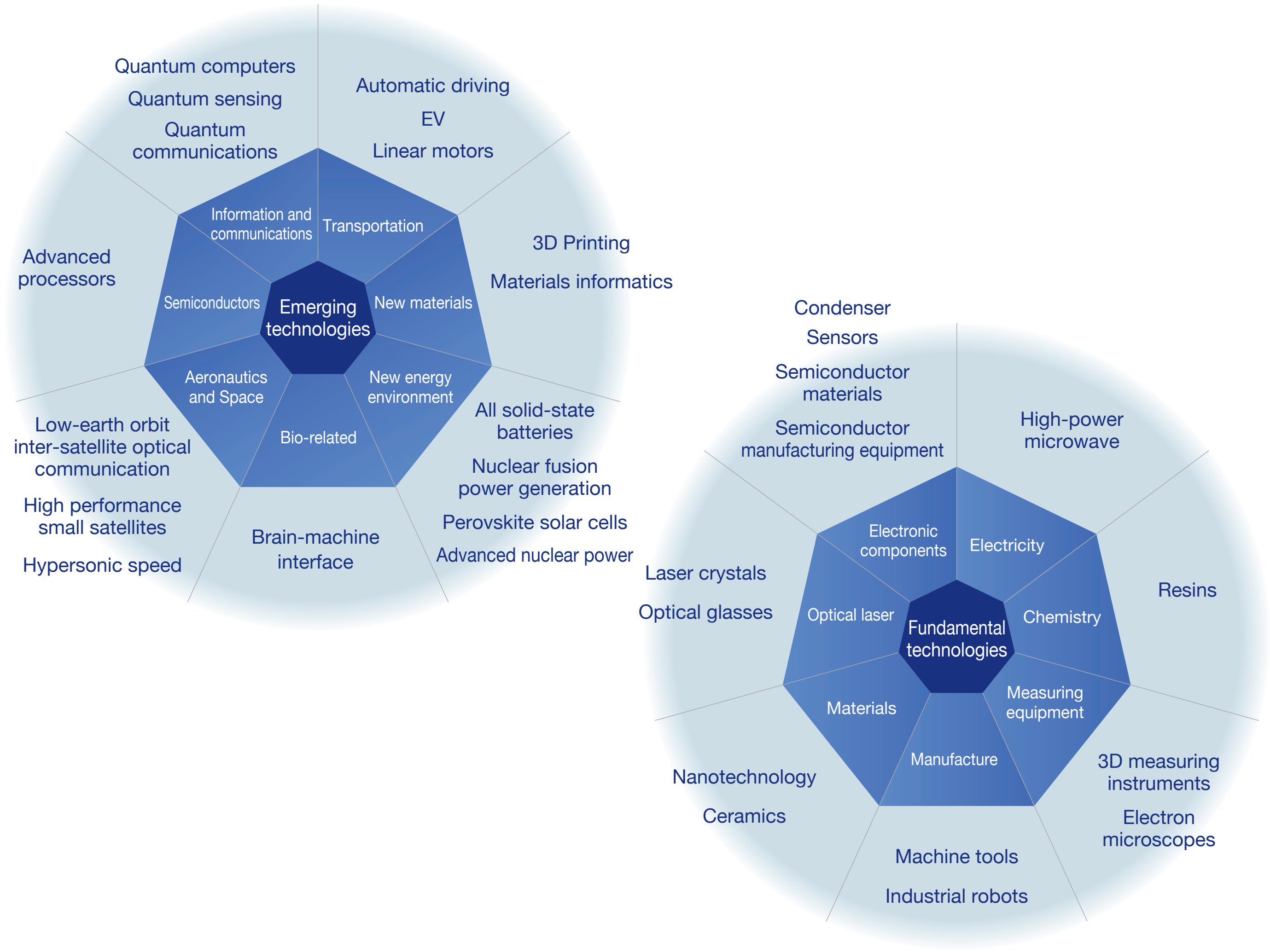
Technologies in the Spotlight

In recent years, there have been moves to strengthen military power and industrial competitiveness by promoting the mutual transfer of civilian and military technologies, as well as to acquire necessary technologies and human talents through legal and illegal means. In response to this situation, emerging technologies, such as AI and quantum technologies, that could be a “game changer” in both the military and civilian sectors, as well as fundamental technologies, such as those related to semiconductors, that are essential for the development and manufacturing of emerging technologies, are attracting attention in major countries from the viewpoint of economic security.

In Japan, export control measures have long been implemented in accordance with the international framework (multilateral export control regime) and relevant domestic laws and regulations to prevent the diversion of technologies and products to the development of weapons of mass destruction by countries of concern.

In addition, it has been pointed out that today, in order to “know” the “advantages (strengths)” and “choke points (weaknesses)” of one's own country’s technologies and products, and to “protect” those technologies and products, it is necessary to further strengthen export control measures as well as to strengthen the supply chain of products and materials, and to properly control technologies and data in academia, such as universities and research institutions.

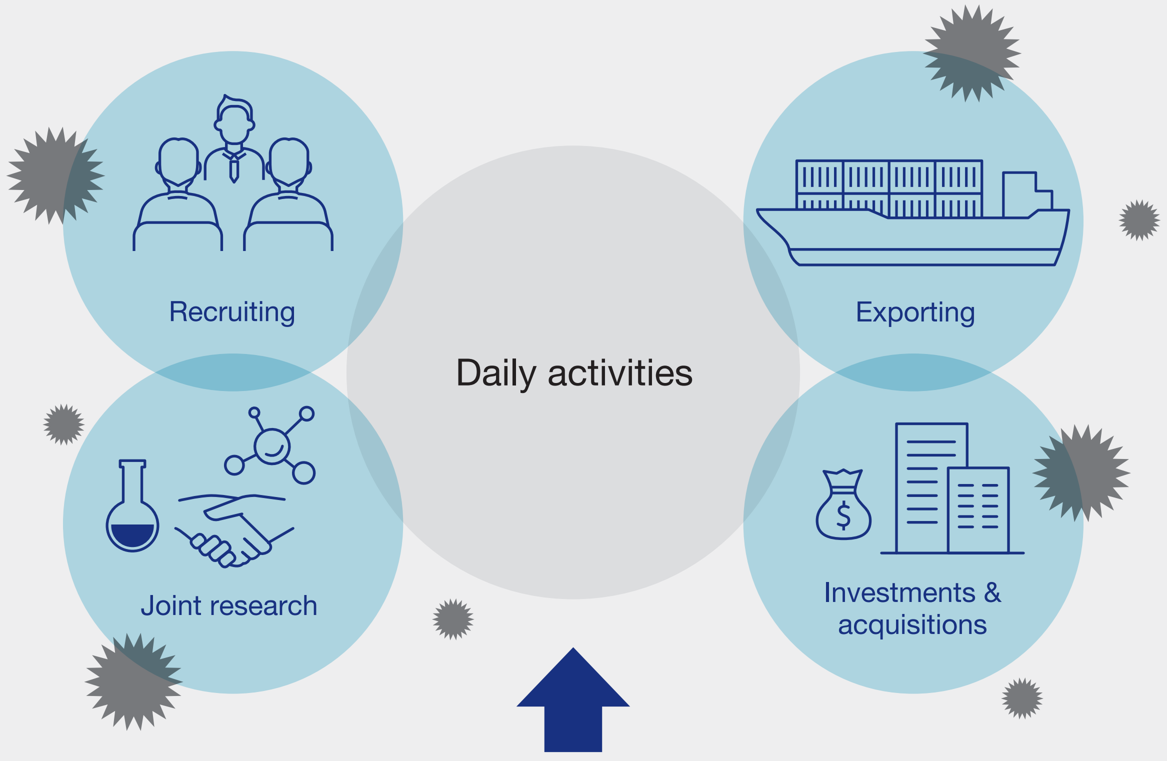
In order for Japan to maintain its strong presence in the fields of industry, science, and technology in the future, it is necessary to pass on the industrial, scientific, and technological infrastructure to the next generation. To this end, it is necessary to “nurture” new industries and technologies, while at the same time preventing the unintended leak of technologies.



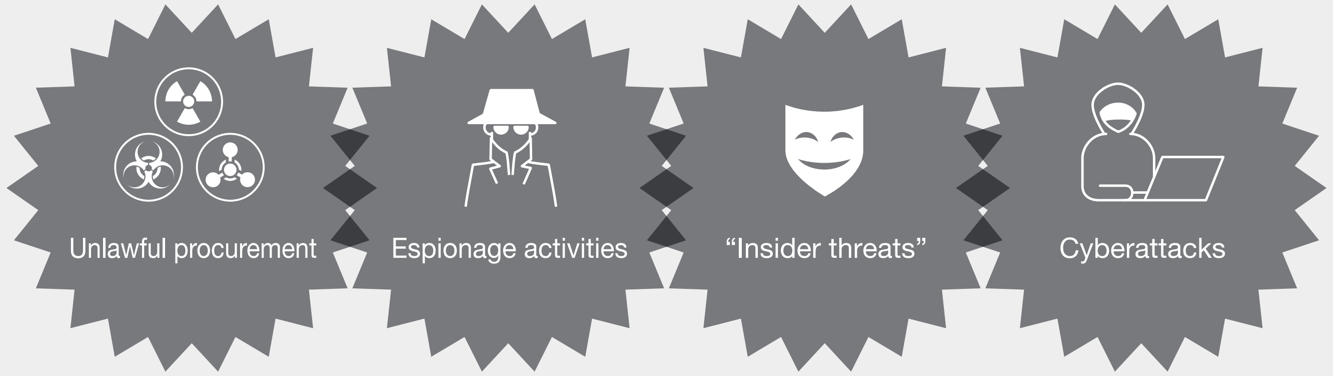
This diagram is a visualization by PSIA of technologies that have attracted attention based on publicly available information and is not an exhaustive list of technologies in general.

Approaches by Entities of Concern

Some of Japan's companies, universities, and other institutions possess world-class technologies, data, and products. What methods do the entities of concern use to try to acquire such technologies, data, and products from us? A close examination of past cases has revealed the reality that daily economic and academic activities are being misused to siphon off technologies, data, and products.



They may be the targets of entities of concern before one knows it



Worst-case scenario

There is no reservation on the part of entities of concern.
If we do not take action, these risks may befall us.

- Leak of sensitive products, technologies, etc.
- Military diversion of proprietary technologies
- Loss of technological superiority
- Administrative disposition and prosecution for violation of the Foreign Exchange and Foreign Trade Act
- Sanctions by the US, the UN, etc.
- Guidance from regulatory authorities
- Deterioration of reputation
- Loss of pioneering status and impact of research
- Loss of opportunities for industry-academia collaboration
- Unreasonable intervention in research
- Overheated media reporting, "flaming" on social media
- Criticisms of screening and guidance systems
- Prejudice and discrimination against foreign students
- Leak of personal information

To reduce risks

What can we do?

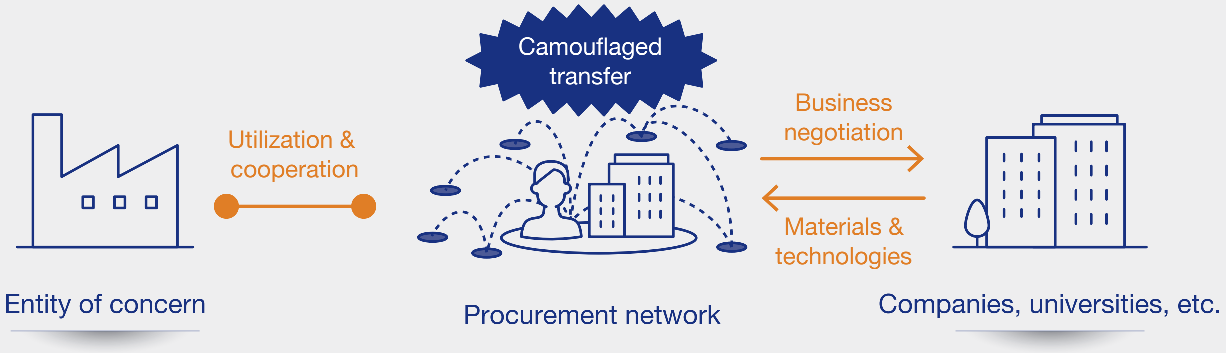
The following pages provide pointers on how to recognize a dubious approach and overseas pointers on specific countermeasures. All of the information was compiled from publicly available information from government agencies and think tanks in the US, the UK, Germany, Sweden, Canada, and South Korea.

Let's consider what can be done based on actual cases.

Even if the following conditions are met, it does not mean that we can immediately conclude that there is a concern.

1 Unlawful procurement

An entity of concern will try to involve you in unlawful procurement activities through deceptive means. There may be an entity of concern lurking behind any inquiry or negotiation that gives you an unnatural impression, given your past business practices and experiences.



Findings in recent years

A dual Iranian/US national procured electronic equipment and other goods from US companies and exported them to Iran without authorization for several years until 2021, after painting a company in the United Arab Emirates (UAE) as a false end-user. The person was found to have been operating under the direction of the Central Bank of Iran.

A North Korean diplomat stationed in Russia plotted to procure, through Russian companies, aramid fibers, winders, and other materials that could be used in ballistic missiles for several years until 2020. In the course of the transactions, it was found that the North Korean diplomat misrepresented these materials as “clothing equipment,” “textile machines,” and other such items.

In Japan

Cases were observed in which entities of concern procured materials and technologies from overseas by disguising their business names and contact information.

Cases were observed in which a company, regardless of the size of the business, continues to conduct business while being aware of suspicious explanations and documents of the counterparty, and was involved in suspicious procurement activities.

Indicators

Isn’t this the kind of party you deal with?

- ✓ Its trade name or location is similar to the sanctioned target
- ✓ It has little product knowledge or business experience
- ✓ Its online presence is excessively low
- ✓ The description of its website differs depending on the version of the language, etc.
- ✓ It does not try to bargain, even though it is a large deal
- ✓ It attempts to purchase regulated products under the guise of “use for academic purposes”
- ✓ It tries to hand-carry merchandise
- ✓ There is a separate company with the same employees, location, and contact information

Aren't there any of these characteristics in your transactions?

- ✓ The end user is not clear, and changes frequently
- ✓ Information needed for the transaction is insufficient
- ✓ Requests for support come from a non-destination location
- ✓ Frequent inquiries without regard to cost
- ✓ The final consignee/end-user is a shipping company
- ✓ A detour route that is expensive and time-consuming to transport is designated
- ✓ Frequent inquiries for the exact same product
- ✓ The product specifications do not match the intended use in the application

Isn't it an unnatural settlement?

- ✓ Sticking to cash settlements
- ✓ Trying to pay from a personal account instead of a corporate account
- ✓ Trying to buy at a price abnormally higher than the market price
- ✓ Sending money repeatedly in a short period of time without regard to commissions
- ✓ A third party attempts to pay for the transaction

Examples of countermeasures employed in other countries

Gather specific information

- Do not hesitate to inquire about ambiguities with the other party
- If the reason for the feeling of “unnaturalness” or “discomfort” cannot be explained rationally, collect further information
- Include the information you collect in your decision-making process even if it is unfavorable to the business deal or transaction you want to proceed with

Understanding and support from management

- Explicitly encourage due diligence
- Allocate adequate resources to the department in charge
- Support education and training of personnel
- Conduct frequent risk assessments of transaction management systems
- Prepare manuals for procedures of approving transactions

Overseas offices can be targeted

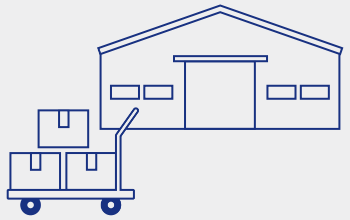
- Build strong and friendly relationships with overseas offices
- Maintain frequent communication with overseas offices to ensure that instructions and requests from the head office are thoroughly understood and executed

The role of financial institutions is also important

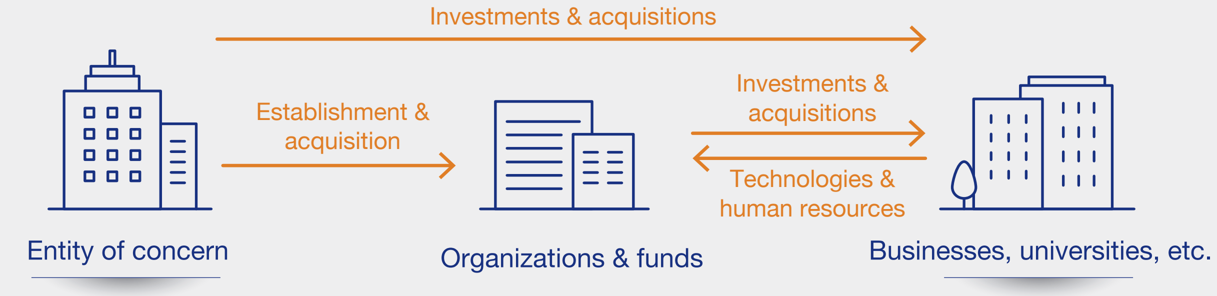
- Obtain additional information if there is any uncertainty about its customer, substantially controlling entity, business relationships, or sources of funding
- Proactively engage with customers and strengthen monitoring of transactions
- If you feel that a transaction is not in line with your customers, obtain evidence to support it
- Provide training for contact and sales personnel on the types of proliferation finance, risks, and how to deal with them

Realization made only possible by the transportation industry

- Check the container for any signs that it has been opened unnaturally
- Conduct more careful due diligence than usual on new customers and customers who bring in a large number of shipments, such as by confirming the existence of such customers
- If there are irrational points in the transportation route or a sudden increase in transportation volume in a short period of time, ask the shipper to explain the background of the transaction
- If necessary, ask for an explanation from the shipper without hesitation



Investments & acquisitions


Investments & acquisitions
Establishment & acquisition
Investments & acquisitions
Technologies & human resources
Entity of concern
Organizations & funds
Businesses, universities, etc.

Findings in recent years

A Chinese state-owned company was found to have acquired ownership of a major Ukrainian company that manufactures aircraft engines and other products in an attempt to take the company's assets overseas. In 2021, the Ukrainian authorities imposed sanctions on the Chinese company to counter the takeover.

A Chinese company acquired a British semiconductor manufacturer through its subsidiary Dutch company. In 2022, the British government ordered the Dutch company to sell most of the shares it had acquired, citing technical and geographical risks to national security.

It was discovered that a Chinese company was planning to acquire a factory of a German semiconductor-related company through its subsidiary in Sweden. The German government decided to prohibit the acquisition in 2022 on the grounds that it threatens public order and security in Germany.

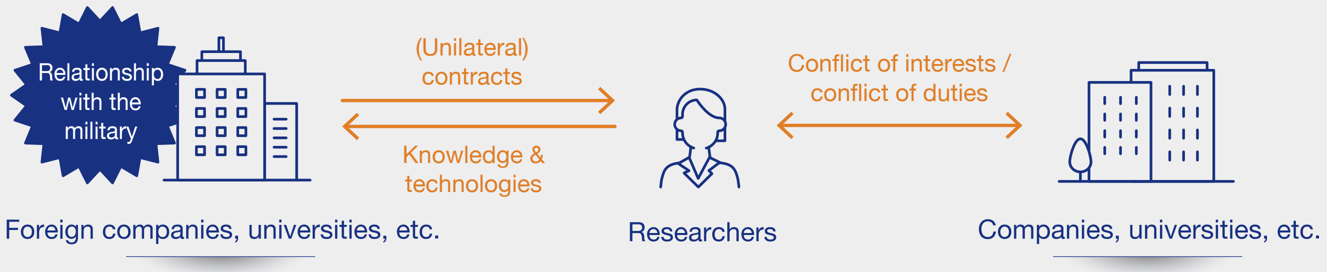
In Japan

There is a possibility that Japan's sensitive technologies, data, and products are unintentionally leaked in the event of a takeover of a company of economic security importance by an entity of concern.

Note that venture/start-up financing and business succession by small and medium-sized enterprises (SMEs) can be used by entities of concern to exert influence.

Joint research and projects

Japan has prospered while reaping the tremendous benefits of science, technology, and innovation. As Japan continues to strengthen its international exchanges, we must avoid a situation in which new discoveries and research results are unintentionally leaked to the outside world, reducing the novelty and competitiveness of our research.


Relationship with the military
(Unilateral) contracts
Knowledge & technologies
Conflict of interests / conflict of duties
Foreign companies, universities, etc.
Researchers
Companies, universities, etc.

Findings in recent years

A Chinese professor working at a state university in the US was found to have been a co-inventor of 24 patents filed in China, but had concealed this fact from his employer and others. He also failed to report the fact that he had received awards related to the “Thousand Talents Plan.”

Some Chinese universities are directly contributing to the People’s Liberation Army’s cyberattack and defense capabilities through joint research and research grants, embodying a military-civilian fusion approach.

In Japan

As joint research is promoted with open science as the main principle, it is important to build a research environment that is trusted internationally.

Some of the joint research proposed by the entities of concern require the participants to forcibly transfer intellectual property (IP) or impose secrecy on them.

When conducting joint research or projects with external parties, it is important to scrutinize the source of funds and the content of the contract, and to confirm a conflict of interests and a conflict of duties.

Indicators

Watch out for this kind of joint research!

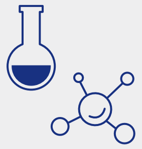
- ✓ The other party tries to buy your IP with a hard bargain
- ✓ The source of the research funds is unknown
- ✓ You are asked to withhold some or all of their activities from your organization
- ✓ You are asked not to follow the policies and practices of your organization
- ✓ Personally attempting to pursue joint research with a foreign government or university without the permission of his/her affiliation
- ✓ Attempting to forcibly transfer the results of joint research
- ✓ The other party seeks to file a patent application independently for a product or technology jointly developed by the two parties

Don’t you see this kind of behavior?

- ✓ Attempting to take another person’s private property or materials without permission
- ✓ Attempting to obtain information/data that is not relevant to the person
- ✓ Unnecessary copying of confidential information and trade secrets
- ✓ Repeated unnatural overtime, work on holidays, and foreign business trips
- ✓ Attempting to remotely access the organization's network during extended vacations, sick leave, or unnatural hours

Examples of countermeasures employed in other countries

Review of research fields



- Does the research field pose a threat or actual harm to public health or public security if misused by a third party?
- How resistant is the research content and data to misuse, theft, or cyberattacks by third parties?
- Are there any laws or regulations in the research field that apply to the provision of information to outside parties? What are they?

Get to know your research partner

- What background does the person have?
- Does he/she have any contacts with foreign military or military-related institutions?
- Does he/she have a track record of collaboration with other universities or research institutions?
- Does he/she have a track record of receiving/managing external funds?
- What does he/she intend to use the results of the joint research for and what kind of profit does he/she intend to make from it?
- Does he/she understand a conflict of interests/conflict of duties?

Check the contract details

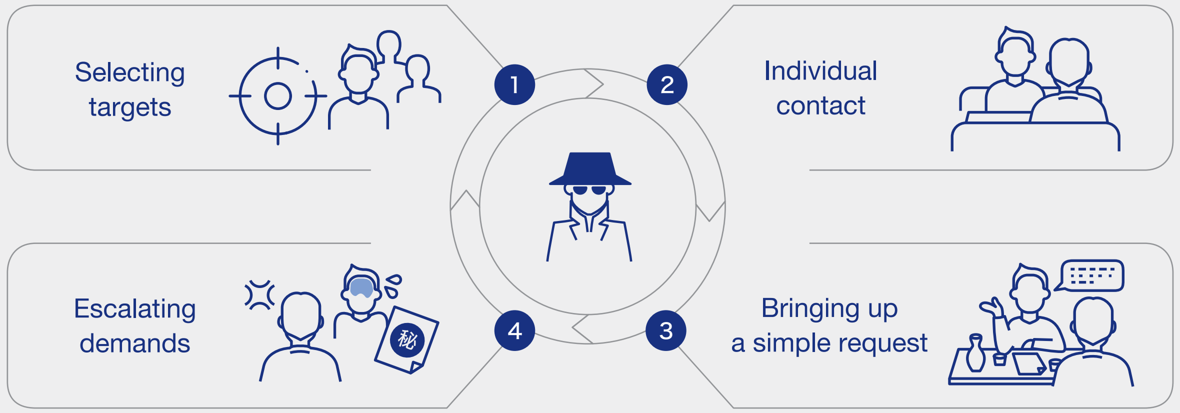
- Are the study locations and participating members clear?
- Are the scope and duration of secrecy and the scope of access clear?
- Is the attribution of research results clear?
- Is the source of funds clear?
- Does it include a clause that allows the collaboration to be terminated without legal liability if problems/risks arise?

Share information related to progress and background

- Share information obtained by the administration with faculty and researchers, and information obtained by faculty and researchers with the administration whenever possible
- Share within the university measures that can be taken to reduce risk, as well as contact information in case assistance is needed

2 Espionage activities

Foreign intelligence officers are one of the typical entities of concern. It is said that there are those in Japan who collect sensitive information by impersonating diplomats or civilians, or by employing a variety of collaborators.



Findings in recent years

A Russian national working at a German university was found to have illegally provided information pertaining to the development stage of European rocket "Ariane" in return for cash payments from a Russian intelligence officer, and was convicted in 2022 with a suspended sentence.

An officer belonging to China's intelligence agency, the Ministry of State Security, was found to have been plotting to recruit university professors and others to obtain sensitive fingerprint identification technology in the US between 2008 and 2018, claiming to be affiliated with Institute for International Studies of Ocean University of China.

In Japan

It is important to recognize that "everyone can be a target."

Intelligence officers use exhibitions, lectures, conferences, and other occasions to contact potentially exploitable persons.

Be wary if an "acquaintance" you have met in person or online offers you a "part-time job" or expresses interest in the nature and sensitivity of your work. It is important to respond in an organizational manner.

What is a foreign intelligence agency?

- Often part of a foreign government agency or military, it collects and analyzes "information" that is of value to its own country. It may also disseminate disinformation.
- It works with the goal of benefiting its own country politically, militarily, and economically.
- Employees of intelligence agencies who have received special training in intelligence collection and analysis are sometimes referred to as "intelligence officers."

What is the aim?

- Primarily, it is "information." They contact those who have access to "information" up front and build relationships over a period of years.
- Foreign intelligence officers, basically, do not like to stand out. They tend to call out to the target at industrial exhibitions, academic conferences, and other places where large number of people come and go, and try to make individual contact with the target.

What kind of conversational techniques do they use?

- Foreign intelligence officers, for example, use a conversational technique called "elicitation" to extract information without alerting their targets.
- The techniques vary from posing as an expert, using sycophancy, bringing up common ground, and daring to criticize.
- It is important to note that even a "small chat" with a stranger may be an inducement in a subtle way.
- In some authoritarian countries, government officials may make TV phone calls to people from these countries residing in Japan, citing their relatives and other reasons to pressure them to cooperate in espionage activities.

They might talk to you

It is not only technicians or experts in a particular field that intelligence officers are interested in. To "price" you out, they may, for example, try to elicit information such as those listed at right.

- Information that could serve as an excuse to contact you again
- Information that could be used to bring you in
- Your hobbies, interests, and family structure
- Whether you have been granted access to sensitive information

Why would you end up cooperating?

- Various studies have been conducted in the US and elsewhere on the motivations that drive people to engage in espionage activities.
- "MICE" is one of the theoretical models that became famous during the Cold War, and is an acronym for the right.
- There is a wide range of debate over MICE's validity and other issues. For example, some say that disgruntlement, ingratiation, thrills and other factors should be included in the motive.

Money
Ideology
Compromise
Ego

Indicators

Is there anyone like this?

- ✓ A person who attempts to take another person's private property or materials without permission
- ✓ A person who tries to obtain information/data that is not relevant to him/her
- ✓ A person who unnecessarily copies confidential information and trade secrets
- ✓ A person who disposes of sensitive documents without authorization
- ✓ A person who repeatedly works unnatural overtime, works on holidays, or goes on foreign business trips
- ✓ A person who attempts to remotely access the network to which he/she belongs while on extended vacation, sick leave, or at unnatural hours
- ✓ A person who purchases expensive items that are out of reach for his/her household income
- ✓ A person with profligate spending habits and excessive debts
- ✓ A person who shows an unusual interest in a colleague's personal life, finances, or relationships

Examples of countermeasures employed in other countries

Preparing for "the moment"

- Prepare simple, safe answers in case an outsider asks you about yourself or your business
- Think of a way to answer probing questions with ease
- Do not try to get the attention of people you are meeting for the first time. Be especially careful when talking about yourself, your colleagues, or your work
- Be wary of people who try to elicit individual and specific information
- Never give individual or specific information to someone who do not need to know these information, regardless of the appearance and demeanor of a person who speaks to you or atmosphere of the place

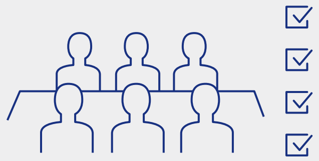
When you want to avoid answering a question

- Do not think, "It's rude not to answer"
- Tell them to refer to websites and other publicly available information
- Change the subject without regard to the content or flow of the conversation
- Dodge the other person's question by asking a counter-question
- Limit yourself to mundane/vague answers
- Answer, "I don't know," "I have no idea," or "I can't talk about it"
- Tell them, "I'm going to talk to the security officer at my workplace"

When you are asked for dubious cooperation

- Check the person's identity and be mindful of what he/she says
- Clearly state, "Absolutely not"
- Do not withhold answers, do not make fun of, and do not be modest
- Tell them, "I'll report to the security officer at my workplace"
- Refuse personal contact or communication
- Do not mention duties or place of employment

Responding in an organizational manner



- Determine and publicize the contact person/persons in charge of handling the situation
- Enhance security education for employees, faculty and staff
- Be as specific as possible when reporting suspicious approaches from outside sources to the workplace
- Actively share information within the workplace

Various events

Industry exhibitions, international conferences, and academic meetings may be frequented by people who are not in line with the purpose of the event, such as foreign intelligence officers and their collaborators. They may be targeting not only a particular product or technology, but also "you."

Information like these is targeted

- Specifications and images of exhibits
- Information on the latest and emerging technologies
- Information that could serve as an excuse to contact you again
- Information that could be used to bring you in
- Your hobbies, interests, and family structure
- Whether you have been granted access to sensitive information

In a foreign country, there are added risks

- Surveillance of behavior by authorities
- Interception of conversations and emails
- Search and seizure of documents and electronic equipment
- Installation of malware on PCs and other devices
- Entering hotel rooms and searching luggage

Indicators

Is there anyone like this?

- ✓ A person who attempts to take back exhibits or imitations of exhibits
- ✓ A person who tries to take more photos of exhibits than necessary
- ✓ A person who tries to get the same information from different personnel at the exhibit booth
- ✓ A person who returns to the exhibit booth repeatedly and tries to talk to a different personnel than the previous one
- ✓ A person who tries to establish a personal relationship with you even though you do not know each other at all

International conferences and academic conferences can be an opportunity

- ✓ Trying to elicit information that is not relevant to the meeting agenda
- ✓ Trying to find out about job duties and access rights to sensitive information
- ✓ Trying to maintain the connection in an unnatural way, such as persistently contacting you after the event

Examples of countermeasures employed in other countries

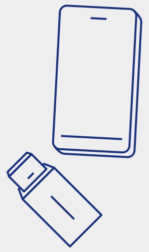
Prepare before the event

- Install a model in the exhibition booth, not the actual machine
- Verify that exhibits are properly protected
- Consider in advance the extent to which information will be shared
- Confirm with the person in charge at your organization that the compensation you receive for attending international conferences/academic conferences does not constitute a conflict of interests or breach of contract
- Be careful not to use your own, colleagues', or acquaintances' character flaws, financial problems, or struggles as fodder for chit-chat
- If you receive a suspicious approach from a stranger, report it to your organization

Be attentive to information dissemination

- Do not disclose travel dates
- Consider whether your activities in a foreign country may be considered a "threat" by the authorities of the destination country
- When traveling to a destination, try not to attract more attention than necessary
- Do not post on social media that you are traveling or upload photos
- Keep sensitive products and documents under control at all times and take them back unless they can be disposed of in an appropriate manner

Cell phones and other electronic devices are a "treasure trove"



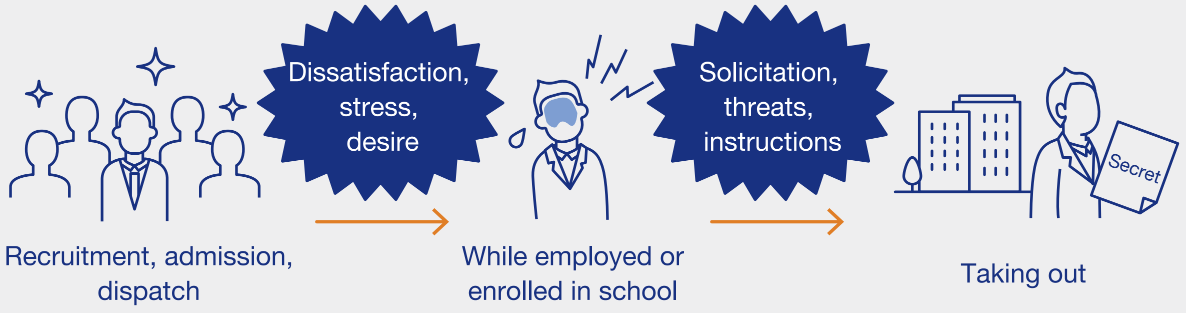
- Leave behind unneeded electronic devices
- Delete sensitive contact information, research data, and intellectual property information from all electronic devices you carry before you travel
- Do not leave electronic devices unattended in hotels and other places, and always carry them with you
- Do not use computers or fax machines installed in overseas hotels or business centers
- When using a provided computer, avoid sensitive interactions and delete search and browsing history and cache each time you use it
- Use USB memory sticks and other devices given to you at your destination only after consulting with security personnel
- Upon returning home, check for viruses on any electronic devices you carried and change passwords

3 “Insider threats”

Not only current home-grown employees and staff, but also temporary employees from outside the company and retirees may intentionally or unintentionally leak secrets and become an “insider threat” to the company.

What is an “insider threat?”

- In general, it refers to employees and staff with access to information, data, networks, facilities, equipment, and personnel within an organization, regardless of their job title, who misuse their authority and knowledge to cause damage to the organization in question.
- Insider threats can take many forms, including information leaks, intellectual property theft, cyberattacks, business sabotage, and acts of violence.



Recruitment, admission, dispatch → Dissatisfaction, stress, desire → While employed or enrolled in school → Solicitation, threats, instructions → Taking out

Findings in recent years

In 2016, a former employee of a major South Korean company took internal company documents with him as he retired and leaked them to the research team of a new company he founded. It was also discovered that he had leaked semiconductor cleaning equipment technology to China.

In 2022, an employee with systems-related knowledge at the US National Security Agency (NSA) obtained excerpts from secret documents and sent them to an outside party via encrypted email. It was discovered that the individual was in need of money and requested that cryptocurrency be provided in return for the information.

In Japan

Cases were observed in which trade secrets and other confidential information were leaked due to dissatisfaction with the company, stress, financial needs, and other reasons.

There is also a risk of being used by outside parties, such as foreign intelligence officers or their collaborators.

While there is no uniform motive for taking out confidential technologies and data, it is important to create a system that allows flexible information sharing among human resources, technology, and security divisions.

Indicators

Beware of workplaces like this

- ✓ High-stress environment
- ✓ Lack of fairness and transparency
- ✓ Inconsistent operation of rules
- ✓ Not addressing complaints, threats, or risks even when aware of them
- ✓ Vertically divided, and information is not shared
- ✓ Overwork is the norm
- ✓ No gratitude to employees
- ✓ Shortly after the merger
- ✓ No defined procedures for risk assessment
- ✓ Staff not receiving required training

Do you know anyone like this?

- ✓ Excessive stress
- ✓ Financial problems
- ✓ Unexplainably large income
- ✓ Excessive gambling habits, sexual misconduct, drug or alcohol abuse, and criminal behavior
- ✓ Tries to erase the “confidential” label on documents
- ✓ Feeling dissatisfied with coworkers because of “unfairness” in relation to his/her own treatment and evaluation
- ✓ Refusing to follow workplace rules and procedures
- ✓ Unusually large amount of overtime work for uncertain reasons
- ✓ Working late at night or other unnatural hours without reasonable cause
- ✓ Bringing personal equipment into sensitive areas
- ✓ Storing sensitive documents and data at home or elsewhere
- ✓ Using external media without authorization
- ✓ Communicating with other companies in the industry or outside parties without authorization
- ✓ Repeating short-term, unnatural overseas travel
- ✓ Failing to comply with requests to report overseas travel or contact with foreign nationals

Examples of countermeasures employed in other countries

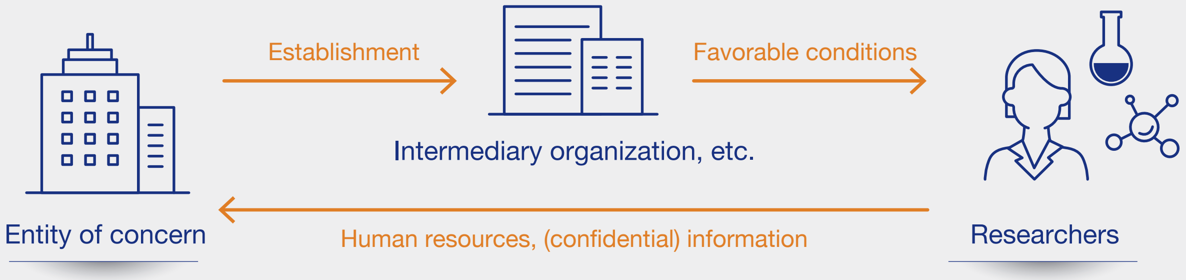
Protecting the “assets” of your organization

- Determine what constitutes an “insider threat” and how to deal with it, based on the business type, organizational culture, and other factors
- The “insider threat” should be addressed jointly by various departments, including HR, IT, legal, and security, in addition to executives
- Ensure that information related to IP is properly protected
- Ensure that new employees are properly screened before they are hired
- Periodically check for suspicious activities on the computer network

Organization-wide response

- Make it known what behaviors of co-workers to watch out for, whom to inform, and how to notify them
- Regularly conduct security-related training
- Create an environment and system that allow employees to easily and readily report suspicious activities when they become aware of them

Recruiting



Entity of concern

Establishment

Intermediary organization, etc.

Favorable conditions

Researchers

Human resources, (confidential) information

Findings in recent years

A Chinese manufacturer poached several employees from a US company and instructed them to take intellectual property and trade secrets related to the company’s digital communication technology without authorization. It was found that between 2007 and 2020, the manufacturer used the trade secrets stolen from the US company for product development, employee training, and other purposes.

A Chinese company lobbied several R&D personnel belonging to a Taiwanese manufacturer to take out a large amount of data, including trade secrets, in exchange for a huge salary and executive posts. It was discovered that the company actually poached all of them and tried to use the stolen trade secrets to establish a new factory.

A Korean recruited by a Chinese manufacturer pulled out several researchers who belonged to separate Korean companies. It was discovered that each of them had taken trade secrets held by the company they worked for by photographing them with cell phones.

In Japan

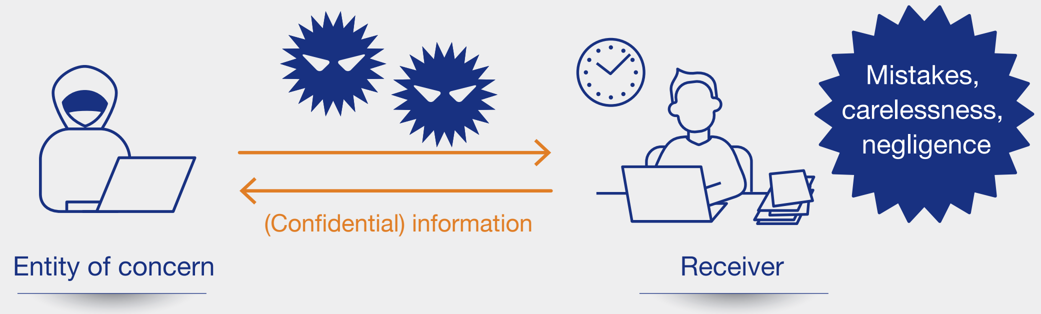
International human resource exchange is an extremely important factor for the development of Japanese companies and universities.

On the other hand, employees’ taking out of secrets is one of the main causes of information leak.

It is important to prepare for unnecessary information leak by concluding nondisclosure agreements and managing access rights to databases.

4 Cyberattacks

Cyberattacks aimed at stealing confidential information, stealing money, or disrupting business operations have become common both in Japan and abroad, and their methods have also become more sophisticated. In particular, cyberattacks by sophisticated cyberattack groups, such as those involving or sponsored by states, tend to continue without regard to cost as part of operations of military and intelligence agencies, requiring vigilance.


Mistakes, carelessness, negligence
(Confidential) information
Entity of concern
Receiver

Findings in recent years

An actor operating in China was found to have exploited a Microsoft product vulnerability to launch a cyberattack on the Norwegian Parliament's email system. A senior Norwegian government official named and accused China of its involvement in 2021.

Tortoiseshell, an Iranian hacker group, was found to have targeted US military personnel and the defense and aviation industries, among others, and then spied on them by contacting online and sending malware* to their devices.

*Malicious program

It is found to be "almost certain" that the Russian military intelligence agency defaced Ukrainian government websites and sent destructive malware in 2022, in advance of the invasion of Ukraine.

In Japan

Incidents have occurred in which information is stolen from companies, universities, and other institutions that possess sensitive technologies and data through cyberattacks.

Cases of advanced cyberattacks involving or sponsored by states were observed in which they can remain in hiding for a long period of time from the time of intrusion to the time of detection, and therefore special attention is required.

Methods of cyberattacks

! Attacks exploiting weaknesses in the system

- Cyberattacks exploit vulnerabilities ("flaws" and "weaknesses") in computer systems. Attackers achieve their objectives by stealing data or disrupting the user's use of the system through malware or other means.
- Some of the vulnerabilities may not even be noticed by the developer or providing company (zero-day vulnerabilities).
- Attacks have also occurred by exploiting VPN equipment and router vulnerabilities.

! Attacks by "social engineering"

- Attackers use "social engineering"* to gain unauthorized access. There are various forms of "social engineering" attacks.

*Means of stealing information or inducing a specific action by exploiting gaps in human psychology or behavior.

- Targeted attacks (spear phishing) use topics of interest to email recipients, such as recent events or financial documents, to induce them to click on malicious attachments or URLs.
- Phishing attacks using email and websites, vishing attacks using voice communications, and smishing attacks using SMS and other text messages are also types of "social engineering" attacks.

Indicators

When “phishing attacks” are suspected

- ✓ The email address is very similar to that of a trusted company
- ✓ Addressee is inclusive rather than a specific individual's name
- ✓ Contact information is not provided in the signature line
- ✓ There is a spelling error
- ✓ Poor grammar and syntax are observed
- ✓ An email from an unknown sender asking you to download or open an attachment or click on a link

Examples of countermeasures employed in other countries

Countermeasures against attacks on systems

- Update the OS, software, and applications of the PC or smartphone to the latest version
- Enable antivirus software and update it daily to the latest version
- Use two-factor authentication (e.g. login with a password set by the user + password notified to the user's cell phone or other devices).
- Set complex passwords and do not use the same password repeatedly. Also, manage passwords appropriately, such as by not leaving paper with the password written on it near equipment

Countermeasures against “social engineering” attacks

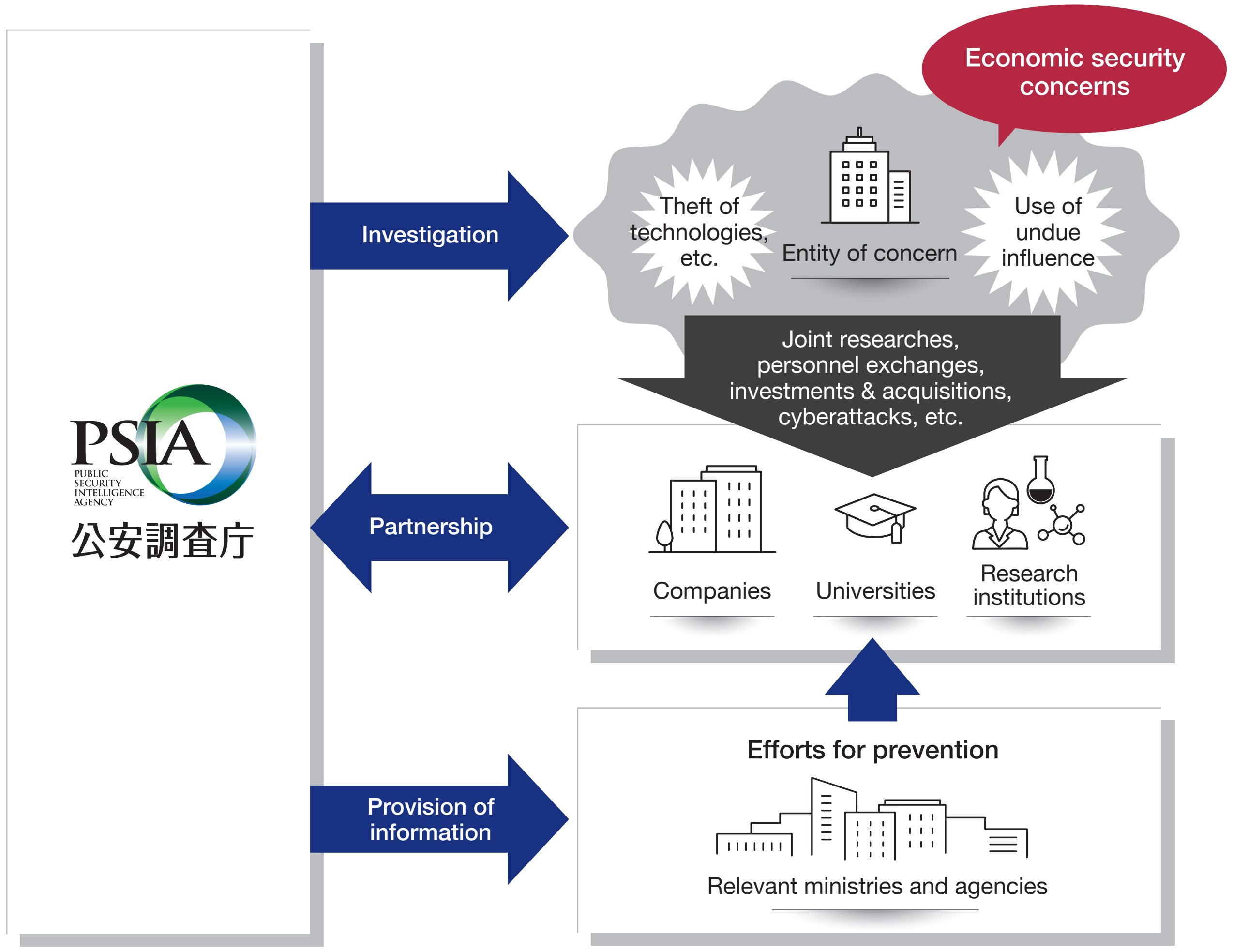
- Do not open attachments or click on links in the body of emails sent by strangers
- Check for information about yourself online whether it is the information necessary to be disclosed online, as it can be used for “social engineering” purposes. Also, be aware of online references to yourself by friends, family, colleagues, and other acquaintances
- Use anti-phishing measures provided by your email software or web browser
- When transmitting sensitive information online, check the security of the website. For example, look for URLs that begin with “https” indicating that the website is secure

Public Security Intelligence Agency’s Efforts

Japan has been making efforts to ensure economic security, and in May 2022, the “Act on the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures (Economic Security Promotion Act)” was enacted. The Act establishes four systems related to (1) ensuring stable supply of critical products, (2) ensuring stable provision of essential infrastructure services, (3) enhancing the development of specified critical technologies, and (4) non-disclosure of selected patent applications, to be implemented in stages within six months to two years from promulgation. In August 2022, the parts of the provisions of this law pertaining to (1) and (3), in addition to the general provisions part, came into effect.

As an intelligence agency, the Public Security Intelligence Agency (PSIA) collects and analyzes information on (1) the theft of technologies, data and products, (2) the use of undue influence, among others, by entities of concern, and further provides information to relevant organizations and conducts public-private partnerships with companies, universities, and other institutions to contribute to policy making on economic security and the prevention of leak of technologies, data, and products.

By providing information, PSIA contributes to policy making on economic security and the prevention of leak of technologies, data, and products



PSIA
PUBLIC SECURITY INTELLIGENCE AGENCY
公安調査庁
Investigation
Partnership
Provision of information
Economic security concerns
Theft of technologies, etc.
Entity of concern
Use of undue influence
Joint researches, personnel exchanges, investments & acquisitions, cyberattacks, etc.
Companies
Universities
Research institutions
Efforts for prevention
Relevant ministries and agencies

Public-Private Partnership and Information Dissemination

Public-private partnership

In order to prevent the leak of technologies, data, and products, it is important for companies, universities, research and other institutions, which can be the target of technology theft, to properly understand the risks and avoid being involved in technology theft by entities of concern.

The Public Security Intelligence Agency (PSIA) shares its knowledge on specific cases of technology leaks, tactics used by entities of concern, and responses to suspicious approaches through exchanges of opinions and lectures with companies, universities, and other institutions. If you have any individual consultation, requests for lectures, or provision of information on technology, data, or product leaks, please contact the "Contact Point for Consultation and Requests for Lectures on Economic Security" below.

Contact Point for Consultation and Requests for Lectures on Economic Security

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

E-mail **psia-es@i.moj.go.jp**

Past lectures

- ●Symposium on economic security co-hosted by the Japan Business Federation and the Public Security Intelligence Agency (June 2022)
  Federal Bureau of Investigation (FBI) Legal Attache delivered a keynote address titled "ECONOMIC SECURITY: The FBI and Preventing Technology Leaks"
- ●Seminar hosted by the Tokyo Chamber of Commerce and Industry (July 2022)
- ●Vacuum Show 2022, hosted by the Japan Vacuum Industry Association (October 2022)
- ●Lecture for startups hosted by the Japan Business Federation (October 2022)
- ●Forum on economic security hosted by the Aichi Prefectural Government (November 2022)

In addition, we have held many other lectures for individual companies and universities

We have received comments from companies such as, "We were able to avoid problems," "We would like to create guidelines for information security based on the lecture," and "After listening to the lecture, some executives immediately came (to the department in charge) to discuss business policies."

Symposium on economic security

Past contributions

- ●The Japan Business Federation "Gekkan Keidanren (Monthly Keidanren)" (December issue, 2022)
- ●Monthly newsletter of the Japan Federation of Certified Administrative Procedures Legal Specialists Associations (February issue, 2023)

In addition, we have contributed to magazines of industry associations and local chambers of commerce and industry

Information dissemination

あなたの持っている技術やデータが
狙われています
今、世界中で先端的な技術や重要なデータの
国外への流出が大きな問題となっています

The Public Security Intelligence Agency has established a special feature page on economic security on its website, where this pamphlet, educational videos, and an overview of the above symposiums are available. In addition, it regularly publishes reports on global economic security trends. If you wish to make use of the pamphlet and videos or share the reports within your company, please contact the above Contact Point.

Other publications

Review and Prospects of Internal and External Situations

This is a review of situations concerning public security both in Japan and abroad over the past year, as well as an outlook on the future.

Review and Prospects of Internal and External Situations (January 2023)

Handbook of International Terrorism

This is a summary of current trends in international terrorism, profiles of international terrorist organizations and their moves, and the state of terrorism by region.

Handbook of International Terrorism 2022

Overview of Threats in Cyberspace

This is a summary of threats posed by cyberattacks in recent years, their patterns, actors, modus operandi, and countermeasures.

Overview of Threats in Cyberspace 2023

Website of the Public Security Intelligence Agency

The website of the Public Security Intelligence Agency shows related laws and regulations under the Agency's jurisdiction, its history, and tasks, as well as shows situations at home and abroad in each of the following categories: "Economic Security Trends," "Aum Shinrikyo,"and "Situations on terrorism and relevant affairs in the world." It also notifies recruitment information and event information on job fairs for new recruits, which are conducted nationwide.

https://www.moj.go.jp/psia/ Public Security Intelligence Agency Search

Official SNS Accounts of the Public Security Intelligence Agency

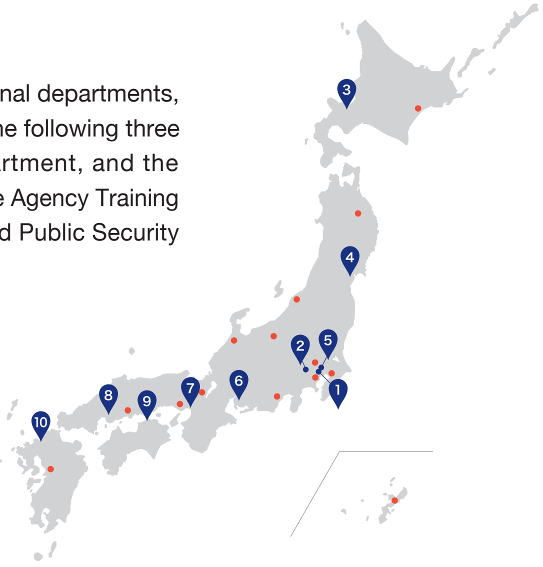
The official Twitter account of the Public Security Intelligence Agency and the Agency's official YouTube channel contain information about the Agency's measures and initiatives, and are used to distribute information that the Agency wants to announce.

Official Twitter account **@MOJ_PSIA**	Offcial Twitter account (for recruitment) **@PSIA_recruit**
Official YouTube channel	**PSIAchannel**

Organization and Network

The organization of the Public Security Intelligence Agency consists of its internal departments, an affiliated organ, and regional bureaus. The internal departments comprise the following three departments: the General Affairs Department, the First Intelligence Department, and the Second Intelligence Department. The agency has the Public Security Intelligence Agency Training Institute as its affiliated organ, and the Public Security Intelligence Bureaus and Public Security Intelligence Offices comprising the regional branches across Japan.

1 Public Security Intelligence Agency (Headquarters)
2 Public Security Intelligence Agency Training Institute
3 Hokkaido Public Security Intelligence Bureau
4 Tohoku Public Security Intelligence Bureau
5 Kanto Public Security Intelligence Bureau
6 Chubu Public Security Intelligence Bureau
7 Kinki Public Security Intelligence Bureau
8 Chugoku Public Security Intelligence Bureau
9 Shikoku Public Security Intelligence Bureau
10 Kyushu Public Security Intelligence Bureau
● …Public Security Intelligence Offices



Public Security Intelligence Agency

Central Government Building No.6 1-1-1 Kasumigaseki, Chiyoda-ku, Tokyo 100-0013 TEL: 03-3592-5711 (main)