Preventing Technology Leaks

警察庁

National Police Agency

Economic Security Office, Foreign Affairs Division,
Foreign Affairs and Intelligence Department, Security Bureau
(Courtesy:the Ministry of Economy, Trade and Industry)

Introduction

In recent years, the security landscape has expanded into the economic and technological domains, driven by increasingly complex international circumstances, the emergence of innovative technologies such as AI and quantum technology, and the rise of new security arenas including outer space, cyberspace, and the electromagnetic spectrum.

Under these circumstances, many countries are advancing economic security measures, including support to strengthen their industries, preventing the outflow of critical technologies, and strengthening export controls.

In Japan as well, all provisions of the Economic Security Promotion Act—which establishes the necessary systems as economic measures to ensure national security—had come into effect by May 2024.

In addition, all provisions of the Act on the Protection and Utilization of Critical Economic Security Information came into effect by May 2025. The Act establishes key systems—often referred to as a security clearance framework for economic security—such as designating critical economic security information, setting rules on who can handle it, and allowing its provision to business operators that contribute to ensuring Japan's national security. And Japan is also working to strengthen its economic structure and ensure its technologies remain both advanced and essential, with the aim of protecting public safety and peace of mind.

In this context, preventing the outflow of technology has also become an important issue for economic security.

Japan hosts many companies and academic institutions with advanced technologies. Some technology and research could be diverted for military use, and if such information leaks overseas, it could not only weaken these organizations' global competitiveness but also seriously threaten Japan's national security.

To address this issue, the police are promoting outreach activities to support companies and academic institutions in preventing technology leaks by providing information on specific methods used to obtain technology and measures to counter them.
To address the imminent risks, proactive efforts are needed not only by the police but also by all of you.

This pamphlet is part of our outreach efforts and is intended for managers, employees, and researchers in companies and academia. It aims to present common patterns of technology leakage risks and key points for each individual to be aware of, to support voluntary preventive measures.
We would greatly appreciate it if you could refer to this pamphlet alongside the measures currently in place, so we can work together to protect your critical technologies.

Contents

Preventing Technology Leakage

To prevent technology leakage, it is essential to understand the current situation, cases, and countermeasures.

Current Situation

What Is Happening Now?

Geopolitical risks have been increasing, and global industrial competition is intensifying.
Japan has many companies and academic institutions with advanced technologies, regardless of their size. As a result, these technologies are increasingly targeted by foreign entities seeking to strengthen their own industries or to use them for military purposes.

Preventing technology leakage is now a major economic security issue.

Cases

How Does Technology Leakage Occur?

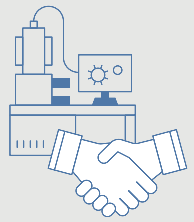
The risks of foreign entities targeting technologies at companies and academic institutions can be grouped into three main patterns.

Patterns of Technology Leakage Risks

Technology leakage through cyber attacks

Technology leakage through espionage

Technology leakage through economic and academic activities



How Does Technology Leakage Occur?

Let's look at cases where technology leakage has been exposed, as well as situations where the risk of leakage tends to increase.

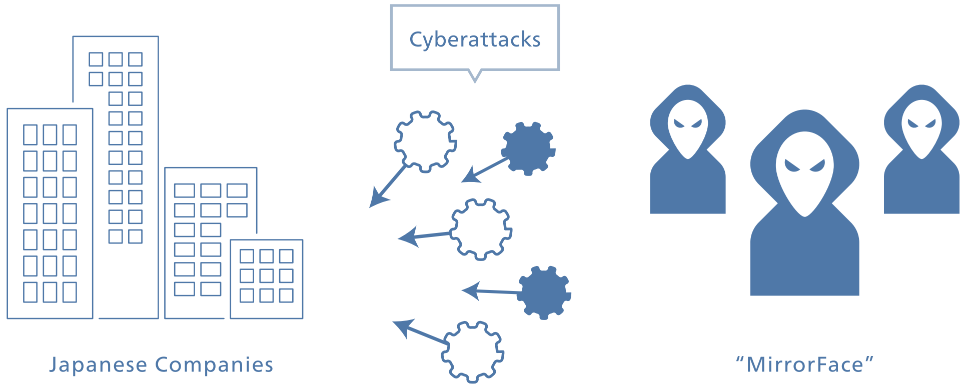
Technology Leakage Through Cyberattacks

Cyberattacks targeting government agencies and critical infrastructure operators in Japan and abroad are becoming more severe. As digital transformation progresses across all industries, the risk of information theft through cyberattacks or unauthorized access is also rising.

CASE 1

It has been confirmed that since around 2019, a cyberattack group known as MirrorFace has been targeting domestic organizations, businesses, and individuals in Japan.

These attacks include phishing emails with malware attachments or links that trigger malware downloads, as well as intrusions into targeted networks—especially by exploiting vulnerabilities in network equipment, such as VPN devices—to steal information. These cyberattacks are assessed as organized operations suspected to have connection to China.

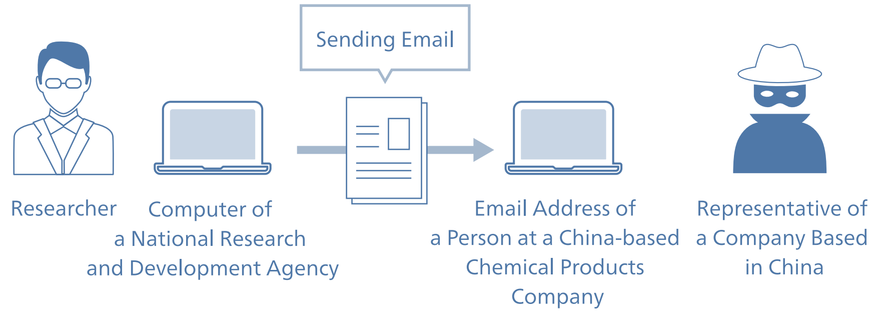


Technology Leakage Through Espionage

We must be prepared not only for cyber risks but also for the theft of information through people. In such cases, foreign entities may recruit individuals as spies to gain easier access to company information and steal it.

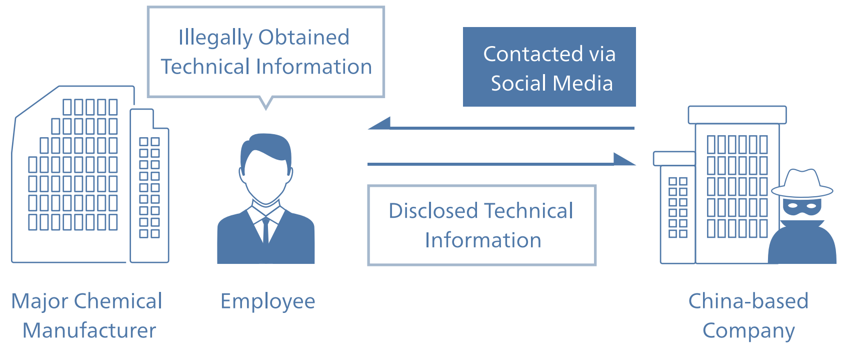
CASE 1

In April 2018, a foreign researcher at a national research and development institute sent research data on the synthesis of fluorinated compounds—a trade secret of the institute—to an email address associated with a company in China. In June 2023, the National Police Agency arrested the researcher on charges of violating the Unfair Competition Prevention Act.


Sending Email
Researcher
Computer of a National Research and Development Agency
Email Address of a Person at a China-based Chemical Products Company
Representative of a Company Based in China

CASE 2

The Osaka Prefectural Police arrested an employee of a major chemical manufacturer in October 2020 for violating the Unfair Competition Prevention Act. Between 2018 and 2019, the employee illegally acquired technical information related to the company's LCD technology (a trade secret) and disclosed it to a company located in China. It is reported that the Chinese firm contacted the employee via a business-oriented social networking service.


Illegally Obtained Technical Information
Contacted via Social Media
Disclosed Technical Information
Major Chemical Manufacturer
Employee
China-based Company

Technology Leakage Through Economic and Academic Activities

As business activities become more global and research more open and international, there is an increasing risk that information could be targeted even during legitimate economic and academic efforts—such as joint ventures, corporate acquisitions, and collaborative research—when these efforts are used as cover.

CASE 1

When the CEO of a space-related R&D startup attended a business event, he was approached by a man who claimed to be a Chinese-American employee of a U.S. government agency. They exchanged contact details. Later, the man asked for a one-on-one meeting, saying there was a joint space development project involving the United States, Japan, China, and Russia, and that he wanted to discuss it over a meal, requesting that the CEO come alone. However, after checking, the CEO found out that the man had no link to the claimed government agency, revealing he had approached under a false identity.

CASE 2

A foreign company asked a Japanese university to provide test cells created using advanced technology. While following proper procedures after obtaining an export license, the foreign customs authority claimed there were issues with export procedures and demanded additional submissions of the cell production method and research materials—information that should not have been required. Concerned about the risk of technology leakage, the university halted the transaction. The university believes the customs authority intervened to obtain related technology after becoming aware of the transaction with the foreign company.

Countermeasures

What Should We Do?

Each of us needs to understand the risks and methods of technology leakage and take basic preventive measures. The following pages summarize key tips and essentials. Please stay aware that "this could happen to me" and apply these insights in your daily activities.

What You Should Do First

Identifying and Managing Confidential Information

Preventing technology leakage involves understanding and following these three steps.

Step 1

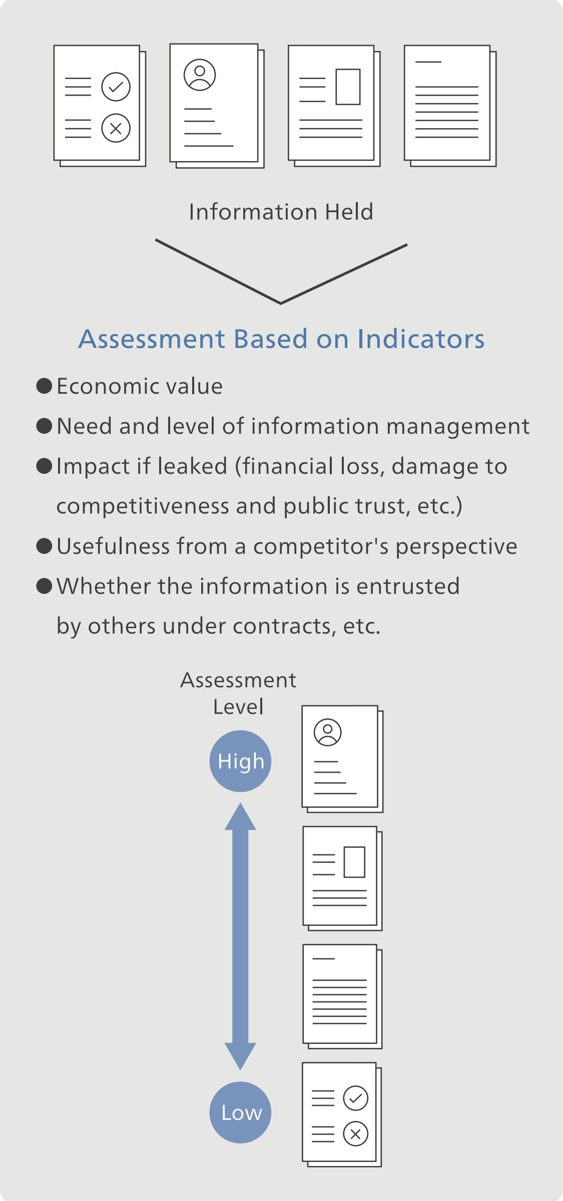
Identify and assess the information you hold, and determine confidential information.

[1] Understand the Full Scope of Information Held by Your Company

Start by identifying all the information your company possesses. Information may exist not only in written form or as electronic data on servers and computers, but also in employees' memories—such as manufacturing know-how—which is not documented or visible. Be careful to account for all such information to prevent any omissions.

[2] Evaluate the Information You Hold

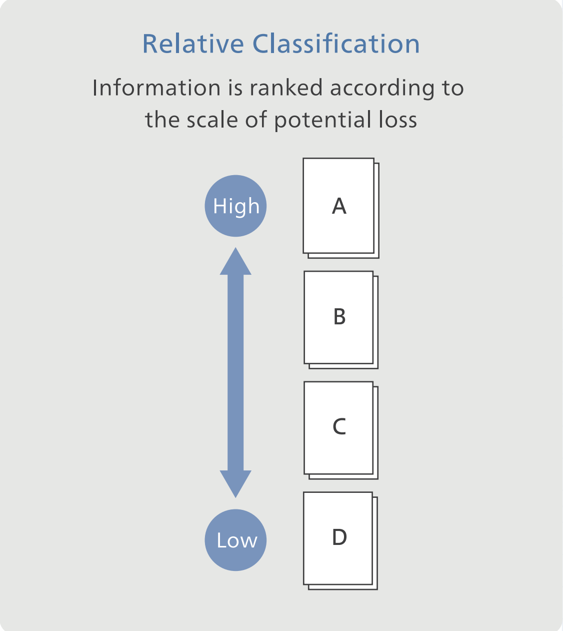
Assess the information you have identified using indicators such as its economic value and the potential loss in the event of a leak.



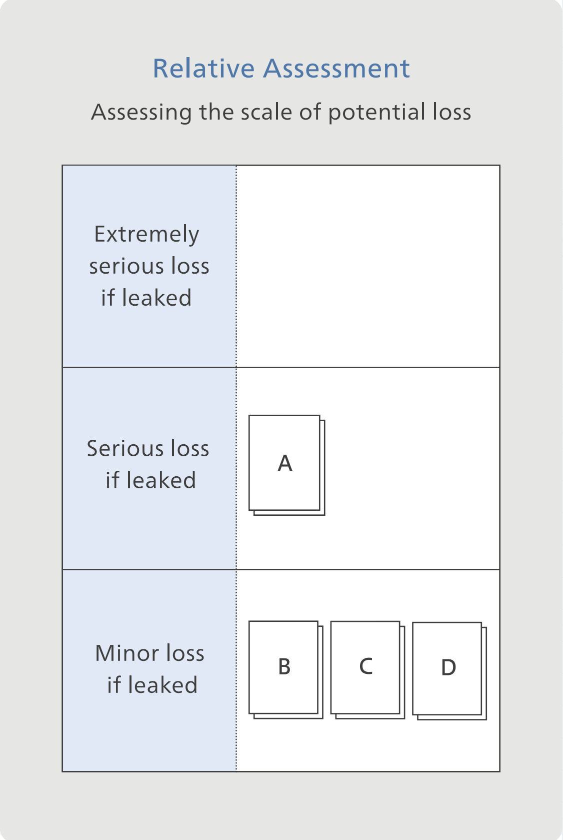
- Economic value
- Need and level of information management
- Impact if leaked (financial loss, damage to competitiveness and public trust, etc.)
- Usefulness from a competitor's perspective
- Whether the information is entrusted by others under contracts, etc.

[3] Determine What Constitutes Confidential Information

Based on the evaluation, decide whether the information requires protection. Consider management and litigation costs, as well as potential losses if the information were leaked, and make a comprehensive judgment.


Relative Classification

Information is ranked according to the scale of potential loss


Relative Assessment

Assessing the scale of potential loss

Extremely serious loss if leaked	
Serious loss if leaked	A
Minor loss if leaked	B C D

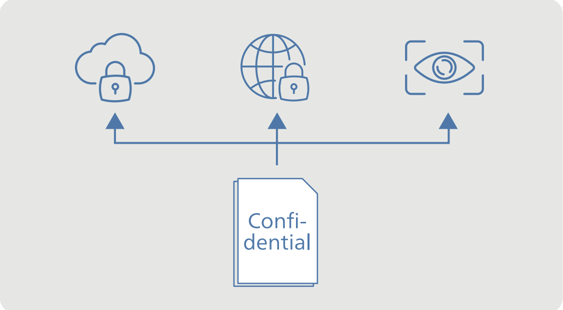
Step 2

Classify confidential information

Confidential information should be classified based on factors such as its content and nature, the level of its assessed value, how it is used, and the management measures available within the company. It is important to strike a balance between protecting information and maintaining convenience for day-to-day operations.

Step 3

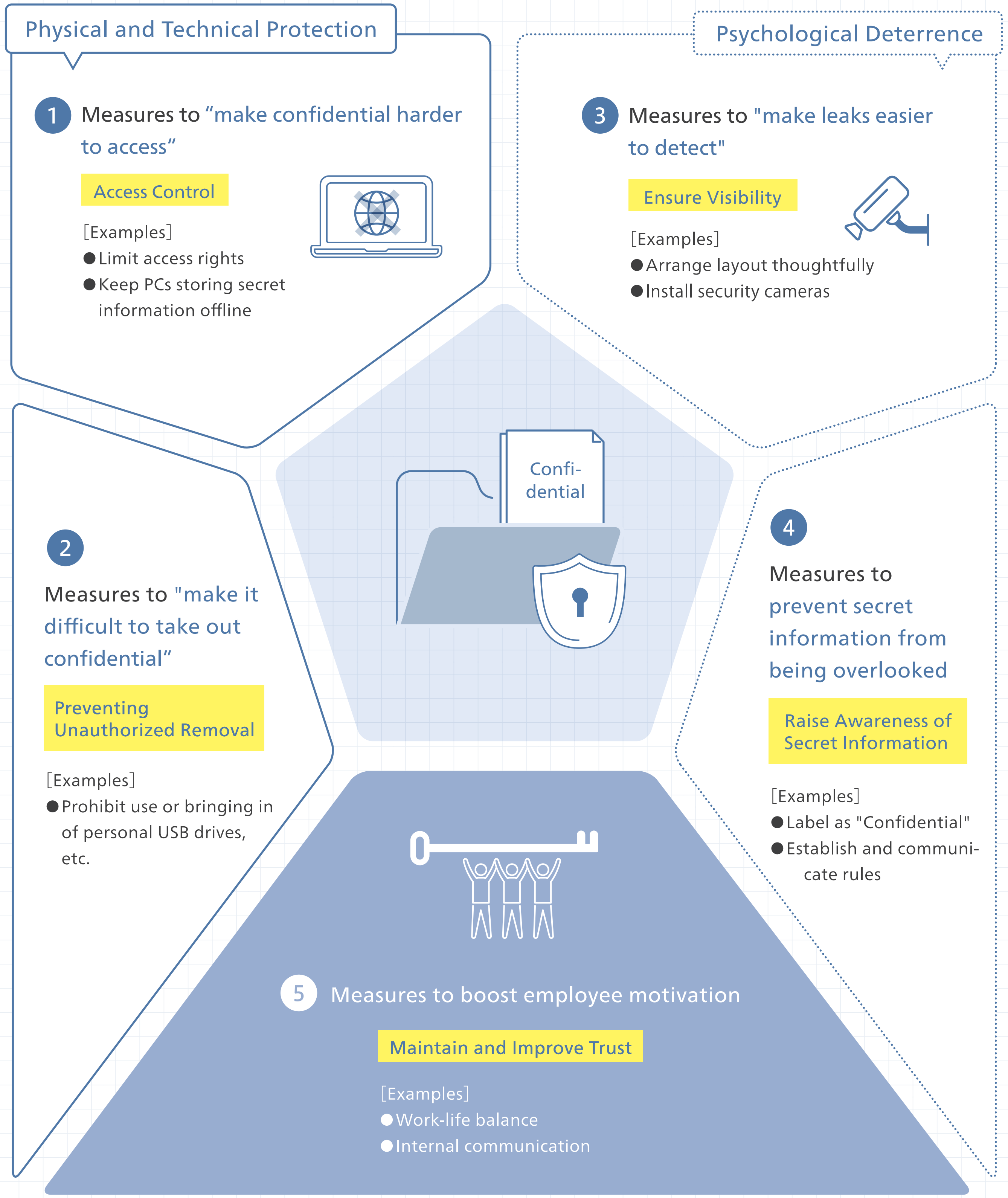
Select Measures Based on the Classification of Confidential Information.



For each classification of confidential information, determine specific measures to prevent data leakage. The most effective measures depend on factors such as for whom measures need to be taken, how the information is stored, and the methods and motives for potential leakage. Considerations may also vary based on circumstances, such as whether remote work is utilized, so measures should be tailored to each company's specific needs.

Five Measures to Prevent Leakage

There are five main measures to prevent technology leakage.
Understand the purpose of each measure and ensure they are implemented thoroughly within your organization.



Physical and Technical Protection

1 Measures to “make confidential harder to access“

Access Control

[Examples]
- ●Limit access rights
- ●Keep PCs storing secret information offline

Psychological Deterrence

3 Measures to "make leaks easier to detect"

Ensure Visibility

[Examples]
- ●Arrange layout thoughtfully
- ●Install security cameras

2 Measures to "make it difficult to take out confidential”

Preventing Unauthorized Removal

[Examples]
- ●Prohibit use or bringing in of personal USB drives, etc.

4 Measures to prevent secret information from being overlooked

Raise Awareness of Secret Information

[Examples]
- ●Label as "Confidential"
- ●Establish and communicate rules

5 Measures to boost employee motivation

Maintain and Improve Trust

[Examples]
- ●Work-life balance
- ●Internal communication

Source: Ministry of Economy, Trade and Industry, Confidential Information Protection Handbook

Measure ①

Preparing for Cyberattacks

Three Basic Countermeasures

1 Measures to Reduce Risks

- Strengthen authentication by making passwords complex, reviewing access permissions, implementing multi-factor authentication, and removing unnecessary accounts.
- Take stock of all information assets, including IoT devices. As vulnerabilities in inter-connected equipment like VPNs and gateways, could be exploited for Cyberattacks, apply security patches promptly.
- Ensure that the organization is aware of safe practices, including avoiding careless opening of email attachments, refraining from clicking on unknown URLs, and promptly reporting or seeking advice when necessary.

2 Early Detection of Incidents

- Review various logs on servers and other systems.
- Monitor and analyze communications, and re-examine access controls.

3 Appropriate Response and Recovery in Case of an Incident

- Prepare for potential data loss by performing regular data backups and confirming recovery procedures.
- Establish procedures for responding when an incident is detected, and prepare external communication and internal response.

Utilizing the “Cybersecurity Management Guidelines”

The Cybersecurity Management Guidelines Version 3.0 by the Ministry of Economy, Trade and Industry outlines principles and actions that executives should be aware of and implement, such as establishing a risk management framework. Additionally, the Practices for Implementing Cybersecurity Management Guidelines Version 3.0, 4th Edition, by the Information-Technology Promotion Agency (IPA) provides practical examples and addresses common concerns of security personnel.

These guidelines can serve as references for implementing cybersecurity measures. Please use them alongside the three basic countermeasures introduced earlier.

Executive Awareness and Framework Establishment

This section outlines the mindset executives should have and the important organizational framework to establish for cybersecurity measures.

Source: Ministry of Economy, Trade and Industry, Cybersecurity Management Guidelines Ver. 3.0

Specific Measures

Provides detailed guidance on the measures to take in response to common concerns.

Source: Information-Technology Promotion Agency (IPA), Practices for Implementing Cybersecurity Management Guidelines Ver. 3.0, 4th Edition

Measure ②

Protection Against Espionage

Contact with unfamiliar parties such as receiving messages from unfamiliar foreigners or gifts from foreign companies can carry the risk of espionage.

See : Observe the Person Carefully

When you meet someone in private settings or on social media—situations different from your usual business environment—check their affiliation and contact information.

- Anyone can be at risk of being approached by someone with malicious intent.
- Some individuals may research you beforehand, then approach you as if by coincidence, inviting you to meals to gather information.
- Check for inconsistencies between what they say and their profile, and confirm that the company they claim to represent actually exists.

Stop : Pause and Think

When posting personal information on social media or other platforms visible to many people, pause and be cautious.

Social media is a useful tool, but malicious actors might use it to collect personal information about their targets, creating opportunities to approach or even coerce them.

Take a moment to be cautious when receiving gifts from others.

Gifts or treats from someone may put you in a situation where it is difficult to refuse, potentially creating an opportunity for them to later request information from you. Consider calmly why they are giving a personal gift and what it might mean.

Share : Communicate and Consult

Share and consult with your supervisor or colleagues, even about minor concerns. If something seems suspicious, you can also contact the police.

- Malicious actors may secretly target individuals. Consulting others when approached by strangers or encountering suspicious behavior helps you stay calm, and sharing information can help prevent those around you from becoming targets as well.
- If you are asked to provide information, do not take it lightly by thinking, "It's just a small amount." or "They seem like a good person." Doing so could not only result in the leakage of valuable technology but also put you at risk of legal violations.

3Ss Everyone Should Keep in Mind

See	Carefully observe people and documents
Stop	Pause and consider; assess the risks
Share	Share information; consult with others

Measure ③

Preparation in Business and Academic Activities

Establishing joint ventures or conducting collaborative research with foreign companies can be a valuable opportunity to enhance corporate value. However, such collaborations also carry the risk of unintended or unexpected technology leakage.

See : Observe the Person Carefully

Carefully check the foreign companies you are doing business with.

- The goal is not to restrict joint ventures, acquisitions, or collaborative research with foreign companies, but to be aware of potential risks of technology leakage that may exist in the background.
- It can also be effective to have experts verify the other party's actual status.

Recognize the Risks of Technology Leakage

- Carefully review the contents of contracts and other documents.
- Trusting the other party without verification may result in essential clauses, such as "export control" provisions, being removed without explanation. It is also effective to have the relevant department or experts review these documents.

Stop : Pause and Assess the Risks

When engaging in activities that could lead to the provision of technology to foreign parties, pause and carefully consider the associated risks.

- There have been cases in which foreign companies identified issues with equipment just before a contract was finalized, requesting access to design drawings or prototypes. Providing such items could result in the theft of technology.
- Risk assessments should cover not only expansion into foreign markets or the establishment of joint ventures, but also withdrawal from foreign markets or the dissolution of joint ventures.
- Exchanging information within the industry can also help in understanding relevant laws and risk cases in that country.

Share : Communicate and Consult

For transactions involving sensitive technology, share information and consult with the relevant departments in advance.

Focusing solely on completing a deal can lead to neglecting export controls or trade secret management, potentially resulting in violations of applicable laws.

If you notice any suspicious behavior, consult with the appropriate authorities or the police.

- Once technology information is leaked, it cannot be recovered.
- To prevent leakage, always consult with relevant authorities or the police if you have any doubts about providing technology to foreign parties.

National Police Agency website “Preventing Technology Leaks“
https://www.npa.go.jp/bureau/security/economic-security/index.html

Economic Security Office, Foreign Affairs Division,
Foreign Affairs and Intelligence Department, Security Bureau
keizaianpo110@npa.go.jp