METI
Ministry of Economy, Trade and Industry

Handbook for Protection of Confidential Information

～Improving Corporate Value～

December, 2020

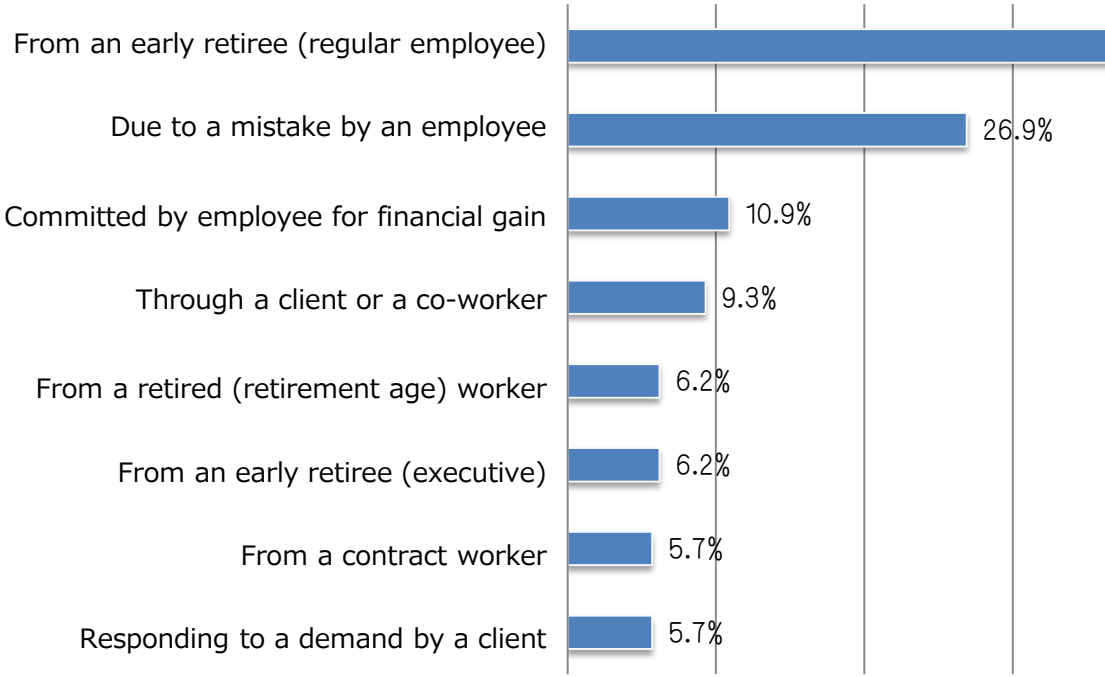
IP Policy Office

METI, Japan

Introduction

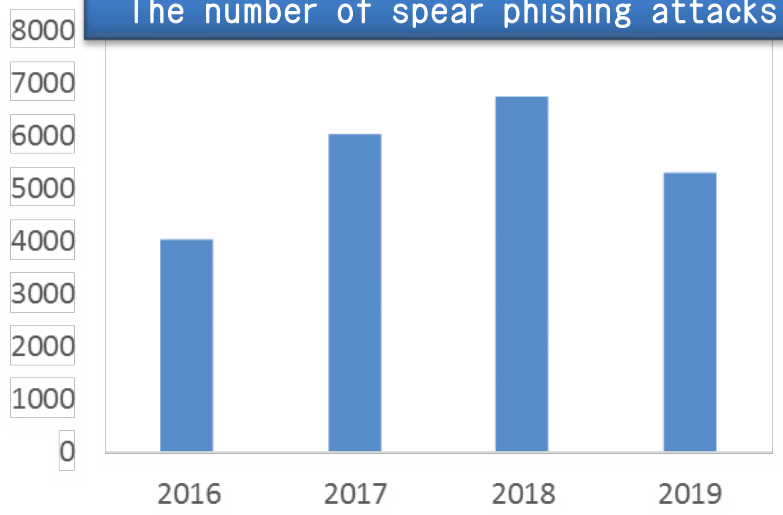
Route of information leakage and Cyber attacks

Route of Information leakage



(Source) METI's questionnaire survey (3,000 answered) "2012FY Information leakage through human resources"

The number of spear phishing attacks



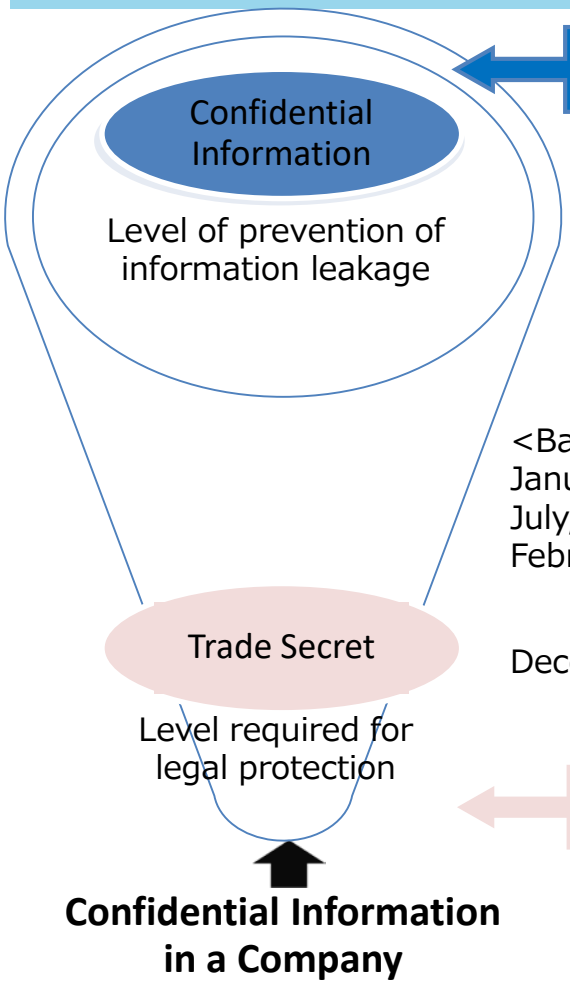
(Source) NPA "Threats in Cyberspace in 2019"

Confidential information that companies have is in danger of leaking both from the inside and the outside.
It is therefore necessary to take appropriate respective measures to protect the information.

1. Background of “Handbook for Protection of Confidential Information”

The Government will develop the “Manual for Trade Secret Protection” (provisional name) with comprehensive (including preventive) measures against trade secret leaks and advanced measures recommended to be taken in the event of such a leak.

Intellectual Property Strategy Program 2015 (June 19th, 2015)



Handbook for Protection of Confidential Information

The Handbook introduces the following comprehensive measures for reference, or to allow companies that want to implement better measures to select such measures based on their actual situations:

- ○ Measures against confidential information leakage
- ○ Measures in cases where information has been leaked
- ○ Templates for various provisions and contracts, etc., consulting desks

<Background>

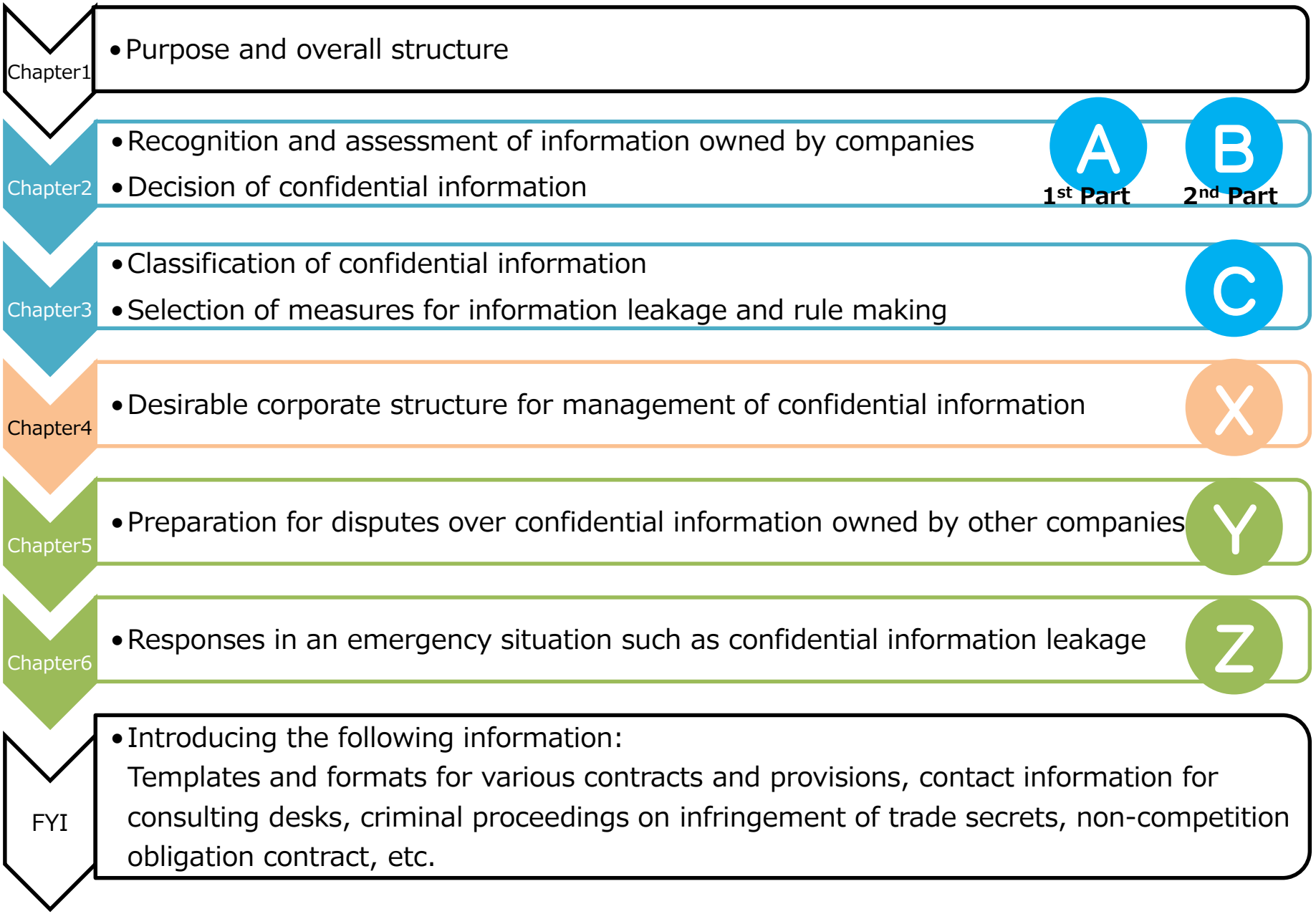
January, 2015	Complete revision of “Management Guidelines for trade secrets”
July, 2015	Amendment of the UCPA (This became effective on Jan. 1st, 2016)
February, 2016	Formulation and announcement of “Handbook for protection of confidential information” (http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html#handbook)
December, 2016	Formulation and announcement of “Guidance of Handbook for protection of confidential information” (http://www.meti.go.jp/policy/economy/chizai/chiteki/2016_11_29_12_08_41/index.html)

Management Guidelines for trade secrets (Jan. 2015)

This shows the lowest level necessary to receive legal protection as trade secrets.

(FYI) Contents of the handbook※

※Only available in Japanese



2. Points of the Handbook

Responses based on routes of leakage

① Employees, etc. ② Retired persons, etc. ③ Client companies, etc. ④ External

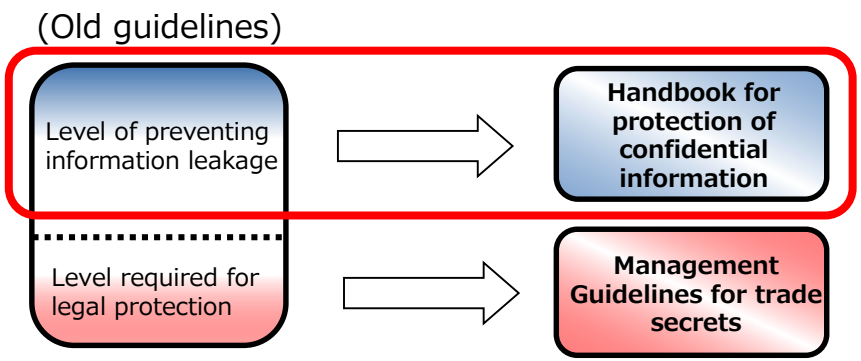
It is necessary to take measures that are appropriate to the route of leakage.

Introducing concepts that companies can refer to

- Balance between “management” and “effective use”
- Introducing “five categories of measures” for efficiently dealing with situations

(FYI) Points of the Handbook

Positioning of the Handbook



Introducing comprehensive measures that might be effective in preventing information leakage and are recommended when a leak has occurred.

Revised completely to show the lowest level of measures that are necessary to receive legal protection as trade secrets

Newly added content

- Preparation for lawsuits filed by other companies
- Responses in emergency situations

(FYI) Overview of trade secrets (Three requirements for trade secrets)

Unfair Competition Prevention Act (Article 2, Paragraph 6)

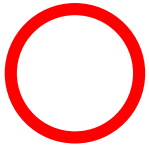
"Trade secret" means technical or business information useful for commercial activities such as manufacturing or marketing methods that is kept secret and that is not publicly known.

[Secrecy management]

For secrecy management requirements to legally satisfy the definition, it is necessary that the intent to maintain confidentiality within a specific company regarding a specific, legally owned trade secret, has been clarified to its employees by using appropriate confidentiality measures, thereby allowing the employees to recognize the said intention of confidentiality.

[Usefulness]

For "usefulness" to be recognized, the specific information should be objectively useful for business activities. It does not need to be actually used in business activities in order to satisfy the requirements.

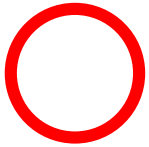


- Drawing, manufacturing know-how
- Customer lists
- Sales manuals etc.

- Information about tax evasion, careless release of harmful substances, and other illegal or antisocial conduct

[Not publicly known]

No such information is generally available from any source other than the information under the control of the owner.



- if a third party other than the owner develops a similar trade secret of the same kind independently, and if the said third party keeps it a secret, then it remains within the "non-public" domain.

- Information published in any publication
- Information published as a patent

3. Measures against information leakage in the Handbook ~Overall image~

Measures focused on Information

A **See Chapter 2 in the Handbook**
Determine what kind of information your company has.

B **See Chapter 2 in the Handbook**
Determine how important the information is, and decide which information to be kept secret.

C **See Chapter 3 in the Handbook**
Determine the measures to be taken according to the importance of the information in terms of balancing secrecy management and utilization of the information.

- An example of information assets that are strengths of the company

Technical Information	✓ Experimental data ✓ Design drawing ✓ Manufacturing process
Commercial Information	✓ Customer list ✓ Market analysis information ✓ Trade prices

- An example of information utilization for a manufacturer

Make public	Keep secret
✓ Method for performance evaluation	✓ Manufacturing process ✓ Material combination

Measures addressing accidents

Y. **See Chapter 5 in the Handbook**
Protecting other companies' information

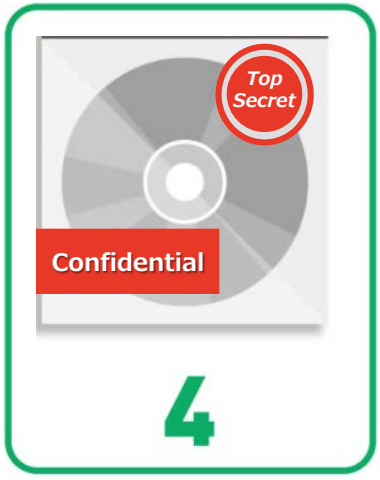
Z. **See Chapter 6 in the Handbook**
If an information leak has happened…

Measures focused on Corporate Structure

X. **See Chapter 4 in the Handbook**
Establishing desirable corporate structure for management of confidential information

3. Measures against information leakage in the Handbook ~Five categories of measures for efficient implementation~

- Setting five “categories of measures” based on leakage factors.
- Based on each company’s situation, they can select appropriate measures.

Physical and Technical measures		Psychological measures		Work environment
Restriction of access	Difficulty of removal	Ensuring visibility	Increasing recognition of confidentiality	Maintenance and enhancement of loyalty
				
Measures to prevent access to confidential information	Measures making removal of confidential information difficult	Measures that make discovering information leakage easier	Measures that make confidentiality of information recognizable	Measures that motivate employees to make stealing information unthinkable
Concrete measures				
◘ Setting access rights ◘ Not connecting PCs with confidential information to external networks ◘ Restricting routes in companies ◘ Entry and exit measures ◘ Separating folders ◘ Paperless ◘ Introducing firewalls, etc.	◘ Prohibiting the use of or possession of personal USB devices in the workplace ◘ Collect all meeting documentation after a meeting ◘ Encrypting electronic data ◘ Restricting external uploads, etc.	◘ Designing seat arrangement and layout ◘ Installing security cameras ◘ Cleaning up work place ◘ Installing “No entry” signs ◘ Saving PC logs ◘ Recording work operations, etc.	◘ Clearly display confidentiality indicators ◘ Establishing and enforcing rules ◘ Signing NDAs ◘ Utilizing “Unauthorized removal prohibited” signs and other indicators ◘ Implementing training, etc.	◘ Promoting work-life balance ◘ Promoting communication ◘ Company awards ◘ Raising awareness of leakage cases, etc.

(FYI) Five categories of measures preventing confidential information leakage ~Select measures based on stage of criminal action~

Have malice ↓ Decision ↓ Start implementing ↓ Accomplish the goal (Removal)

Measures for enhancing employee loyalty
[Maintenance and enhancement of loyalty] ⑤
(Ex. Work-life balance, Internal communication)

Measures against ignorance of confidentiality (employees do not realize confidentiality)
[Raising awareness of confidential information] ④
(Ex. Indicating confidentiality, establishing and enforcing rules and provisions, implementing training)

Measures for an environment that is easy to find a leakage
[Ensuring visibility] ③
(Ex. Designing layout (seat arrangement), installing security cameras, maintaining access logs)

Measures making it harder to access confidential information
[Restrict access] ①
(Ex. Limiting access rights, not connecting PC with confidential information to internet)

Measures making it difficult to remove confidential information
[Difficulty of removal] ②
(Ex. Prohibit use or possession of personal USB device in the workplace)

Avoidance/Abandonment/Failure of theft

[How to select measures]
- "Ensuring visibility" and "Difficulty of taking out" are effective measures in cases where many people can access the information.
- The greater the diversity of employees, the more difficult it is to maintain and enhance loyalty.

3. Measures against information leakage in the Handbook ~Measures focused on Corporate Structure~

- Establishing desirable “corporate structure” for effective management of confidential information

Item X, See Chapter 4 in the Handbook

Involvement by managers

It shows importance of manager involvement in management of confidential information in terms of leadership and supervision of implementation.
Ex.) Managers participate in and supervise the employees' implementation of the system.

Roles of various departments

Provides examples that companies can refer to in deciding roles of each department

3. Measures against information leakage in the Handbook ~Measures addressing Accidents ①~

- Protecting information owned by other companies (to prevent from being sued)

Item Y, See Chapter 5 in the Handbook

- It introduces methods of preventing disputes and of preparing for a defense in cases where companies are unintentionally involved in disputes. These preparations can lead to enhanced trust and the acquisition of various human resources from other companies.

Substantiation of unique ownership of companies' information

It is important to regularly, objectively substantiate that the information is unique information owned by the company to prepare for instances of other companies initiating litigation based on infringements of confidential information. (Ex. Preservation of documents)

Prevention of infringing on confidential information owned by other companies

(i) In employing people from such potential companies
Ex. Check contracts of previous employers

(ii) In Joint research and development
Ex. Store confidential information owned by other companies separately

(iii) In receiving confidential information in a deal
Ex. Check documents in receiving samples etc.

(iv) In selling confidential information
Ex. Check contracts on source of the information

Prevention of disputes related to items created by infringement of trade secrets

It is necessary to take adequate measures to substantiate that due attention was paid in suspicious situations.

3. Measures against information leakage in the Handbook ~Measures addressing Accidents ②~

- If information leakage has occurred,

Item Z, See Chapter 6 in the Handbook

- It is difficult to completely prevent information leakage even if companies manage information appropriately.
- Therefore, the Handbook introduces procedures so that companies can deal with an emergency situation quickly if information leakage has occurred.

Recognizing and checking signs

(i) Recognition of leakage signs
(ii) Investigate suspicion of leakage

First action

(i) In-house investigation, recognition of accurate status and investigation of the cause
(ii) Investigation of damage
(iii) Perspective on first action
(iv) Establish an emergency response team, etc.

Pursuing liabilities

(i) Criminal measures
(ii) Civil measures
(iii) Disciplinary action

Preservation and collection of proof

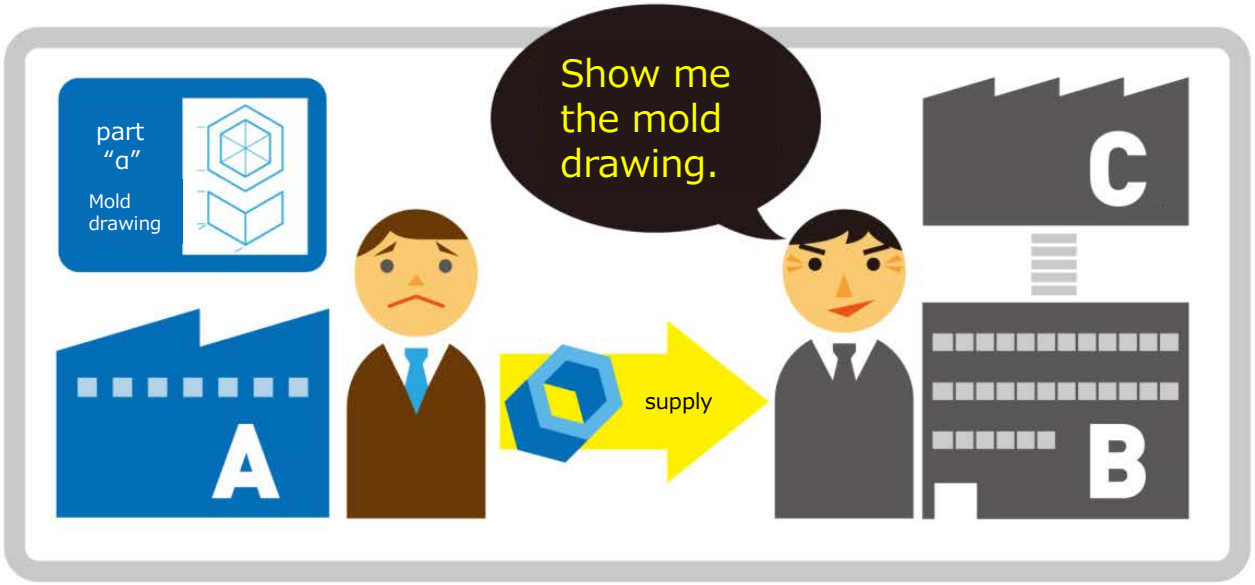
4. This actually happened!? Cases and measures

Case 1. Company A - a component supplier

[Measures against client company] Company A was asked to provide mold drawing to the client, but…

- Part α, which Company A developed individually and provided to Client B, is popular with clients because of its accuracy.
- One day, Client B asked Company A to provide a mold drawing of part α, and Company A reluctantly provided it to Client B because Client B is a major client for Company A.
- After that, Company A no longer received orders for part α from Client B. Somehow Client B provided the drawing to Company C, who is competitor of Company A, and had Company C cheaply manufacture copies of part α, i.e. counterfeits.
- What measures should Company A have taken?

Confidential information of Company A: Mold drawing of the part “α”



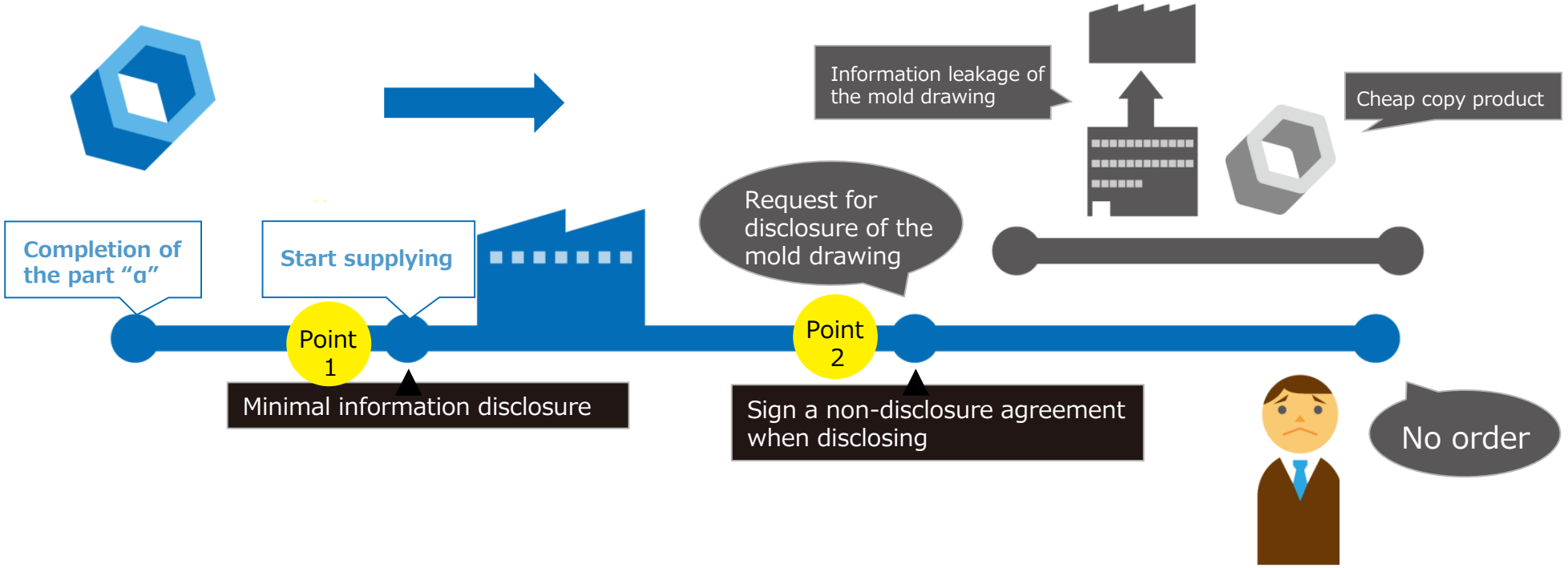
Case 1. Company A - a component supplier [Commentary]

Point 1 - Disclose the bare minimum of information necessary
(Restriction of access) [Item 3-4 (3) ① a of Chapter 3 in the Handbook]

- It is important to reject the disclosure of such information if the details of the deal with Client B do not actually necessitate such a disclosure.
- It is also effective to stipulate in advance in a contract or estimate that Company A will not disclose mold drawings.

Point 2 - Sign a non-disclosure agreement when disclosing information
(Raising awareness of confidential information) (Difficulty of removal) [Item 3-4 (3) ④ a, ② a of Chapter 3 in the Handbook]

- It is better to stipulate confidentiality, the prohibition of the use of confidential information for any purpose other than the stated purpose, the obligation to return or discard the mold drawing at the end of a contract and other such details in non-disclosure agreements regarding such mold drawings.



4. This actually happened!? Cases and measures

Case 2. Company D - a food company

[Measures targeting employees and resigning employees] An employee decided to quit, but…

- Information on recipe of soup is valuable source of corporate competitiveness in Company D, which manufactures instant noodles.
- News that a former employee of a company was arrested for misappropriation of trade secrets at new place of work appeared recently, but it could happen to anyone. Company D recently heard that a leader of the soup development team wanted to quit. His new place of work is Competitor E.
- What measures should Company D take to avoid losing this important recipe?

Company D confidential information: Soup recipe

Case 2. Company D - a food company [Commentary]

It is important to take measures to reduce risks of leakage associated with resigning/quitting employees.

Point 1

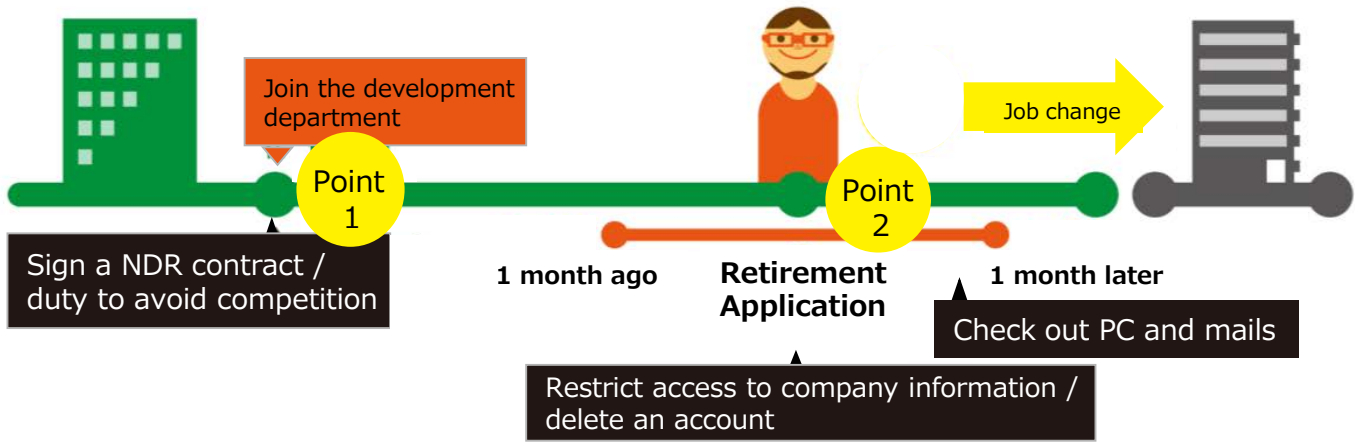
- Have employees sign a non-disclosure agreement not only in retirement, but also in entering and starting projects. For key persons, it is also conceivable to sign a non-competition obligation. (Raising awareness of confidential information) [Item 3-4 (2) ④a, b of Chapter 3 in the Handbook]

Point 2

- Quickly restrict access to company-internal information after the notice of resignation. Delete ID/account ASAP upon resignation. (Collect ID card and admission certificate) (Restriction of access) [Item 3-4 (2) ①a of Chapter 3 in the Handbook]
- Carefully check e-mails or PC logs for before and after receiving the notice of resignation (Ensuring visibility) [Item 3-4 (2) ③q, r of Chapter 3 in the Handbook]
- Investigate the current situation of the resigned employee and monitor the product information for the new place of work

Point 3

- Creating a good work environment and fair personnel evaluation system, thereby encouraging loyalty to the company can prevent malicious attitudes and prevent the loss of important resources. (Maintenance and enhancement of loyalty) [Item 3-4 (1) ⑤ of Chapter 3 in the Handbook]



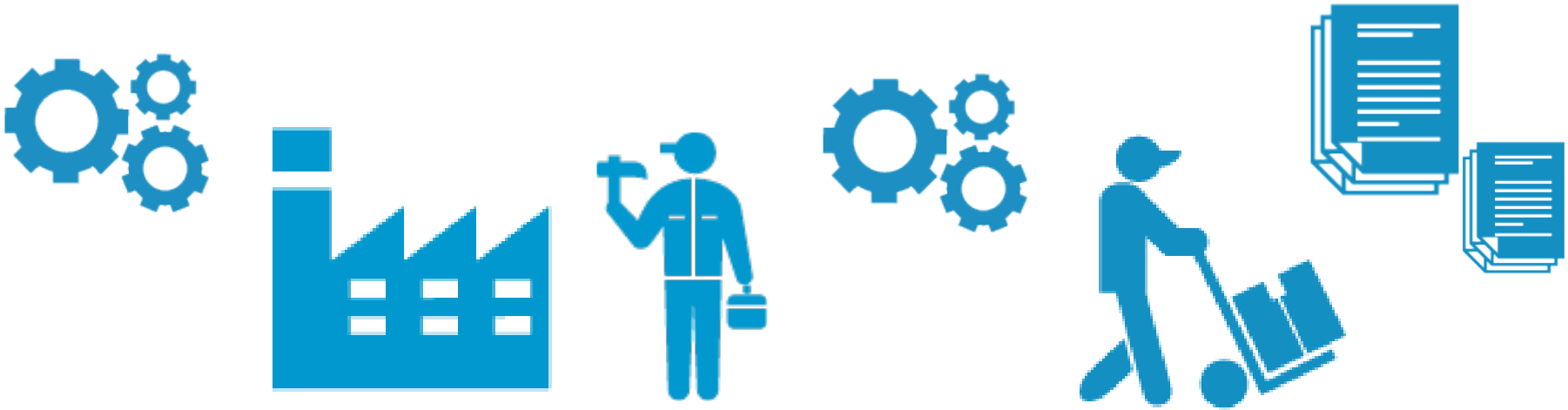
4. This actually happened!? Cases and measures

Case 3. Company J - a film manufacturer

[Measures against employees] Company J want to establish new manufacturing line…

- Company J is soon to establish a new manufacturing line of heat-resistant films.
- The manufacturing line, which improves the equipment and factory layout, will realize a highly efficient film manufacturing system compared to other companies. Therefore, Company J must take measures to prevent information leakage related to the manufacturing process and factory layout.
- What measures should Company J take?

Confidential information of Company J: Manufacturing process of heat-resistant films and factory layout



Case 3. Company J - a film manufacturer [Commentary]

It is important to restrict the number of people who can access the confidential information

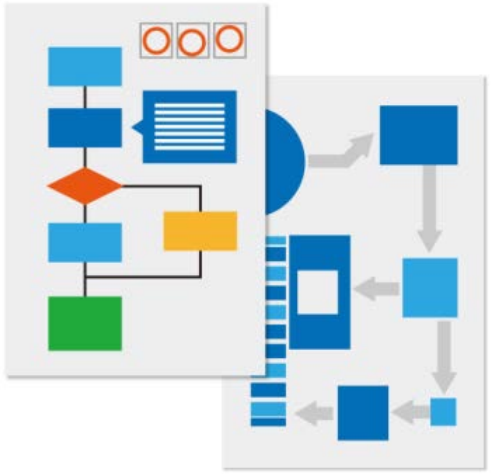
(Restriction of access) [Item 3-4 (1) ①a of Chapter 3 in the Handbook]

- Divide a series of operations between employees working on the line of the factory so that individual employees do not know or understand the information for the whole process.

It is important to take measures so employees accessing the information cannot remove it

(Difficulty of removal) [Item 3-4 (1) ②j of Chapter 3 in the Handbook]

- Restrict items that people can bring into the factory, such as cameras.
  (It is effective to obligate employees to wear work uniforms with no pockets and to ensure that employees only carry items in transparent bags when accessing sensitive areas.)



4. This actually happened!? Cases and measures

Case 4. Company K - a textile manufacturer

[Measures against external interference] Company K received suspicious e-mails, but…

- Company K buys materials, manufactures high-performance textiles and sell the textiles to customers.
- One day, employee L of the manufacturing department received an e-mail from someone pretending to be a customer. Employee L was suspicious of the e-mail and consulted the security department in Company K before opening the attached file. The e-mail turned out to be an Advanced Persistent Threat with a computer virus.
- Fortunately, employee L did not open the attached file at this time. If employees open the attached file by mistake in future, however, not only customer information and manufacturing know-how, but also information disclosed by suppliers will be in danger of leaking.
- What measures should Company K take to prevent damage by unauthorized access or Advanced Persistent Threats?

Confidential information of Company K: Manufacturing know-how of high-performance textiles, customer information, material information disclosed by suppliers

Case 4. Company K - a textile manufacturer [Commentary]

Point 1

Cut external connections to the degree possible

(Restriction of approach) [Item 3-4 (4) ①e of Chapter 3 in the Handbook]

- It is good to store as much confidential information as possible on equipment with no external connections.

Point 2

Take measures to keep damage from unauthorized access or Advanced Persistent Threats to a minimum

(Restriction of access) [Item 3-4 (4) ①f of Chapter 3 in the Handbook]

- It is important to install firewall/anti-virus software and update the software regularly in cases where confidential information is stored on PCs with external network connections.

(Difficulty of taking out)[Item 3-4 (4) ②c of Chapter 3 in the Handbook]

- It is also effective to encrypt electronic data of confidential information.

※Tips for identifying Advanced Persistent Threat are described in “Column 3, What is an Advanced Persistent Threat?” on page 89 in the Handbook.

4. This actually happened!? Cases and measures

Case 5. Company F - a food company

[Measures to avoid trouble] Made with in-house technologies, but…

- Company F that manufactures miso soup with lots of freeze-dried vegetable ingredients is developing Japanese dried fruits as new products.
- One day, Company F received a joint development offer from Company G that is a food processing manufacturer which owns freeze drying technologies. However, Company F declined the offer due to costs.
- After that, Company F developed new dried fruits β by utilizing its own technologies and started sales of products β. Suddenly, Company F received a warning letter asserting that technologies owned by Company G were used in the product β and the manufacture and sales are to be stopped.
- When Company F received the offer, however, Company F did not receive any information on concrete technologies owned by Company G and did not use confidential information of Company G in the new products.
- What can Company F do in order to substantiate the product β was developed by Company F's own technologies?

Case 5. Company F - a food company [Commentary]

Point 1 Avoid receiving confidential information owned by other companies to the degree possible
Point 2 Record documentation on development in order to substantiate internal technologies
[Item 5-1 of Chapter 5 in the Handbook]
<In case of technical information>

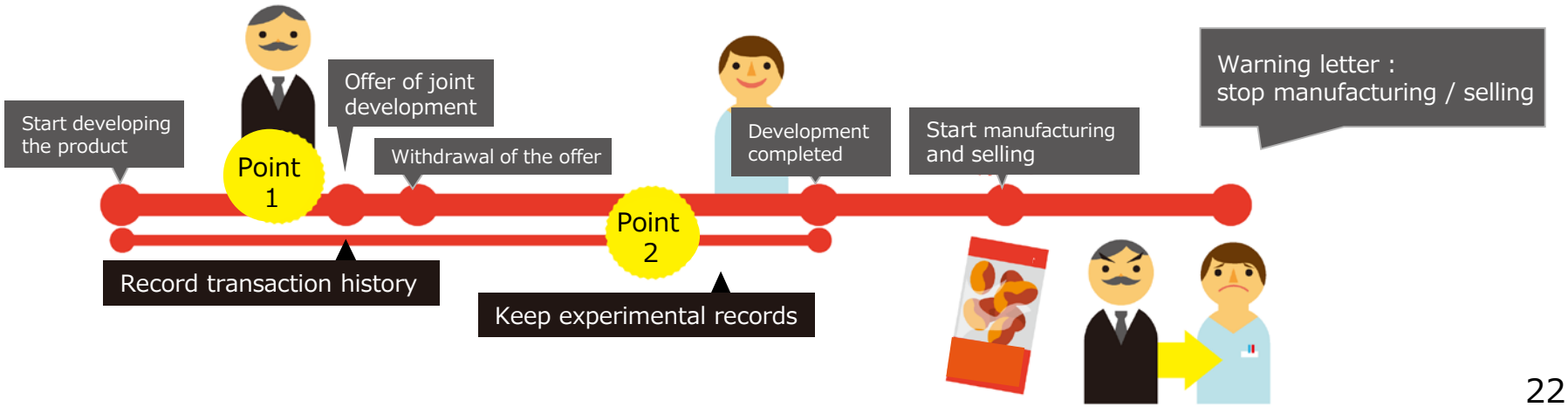
- Take notes that describe experimental process, method, etc. and save them until the technologies have been developed
- Utilize timestamps, etc. to certify dates
- Save other relevant documents (E-mails, Study materials, Minutes, etc.)

<In case of customer lists>

- Record history related to customers (Visit/Purchase history, membership applications, etc.)

<In case of transaction information>

- Record history of transactions (Original bills describing purchase and sales prices or amounts, etc.)

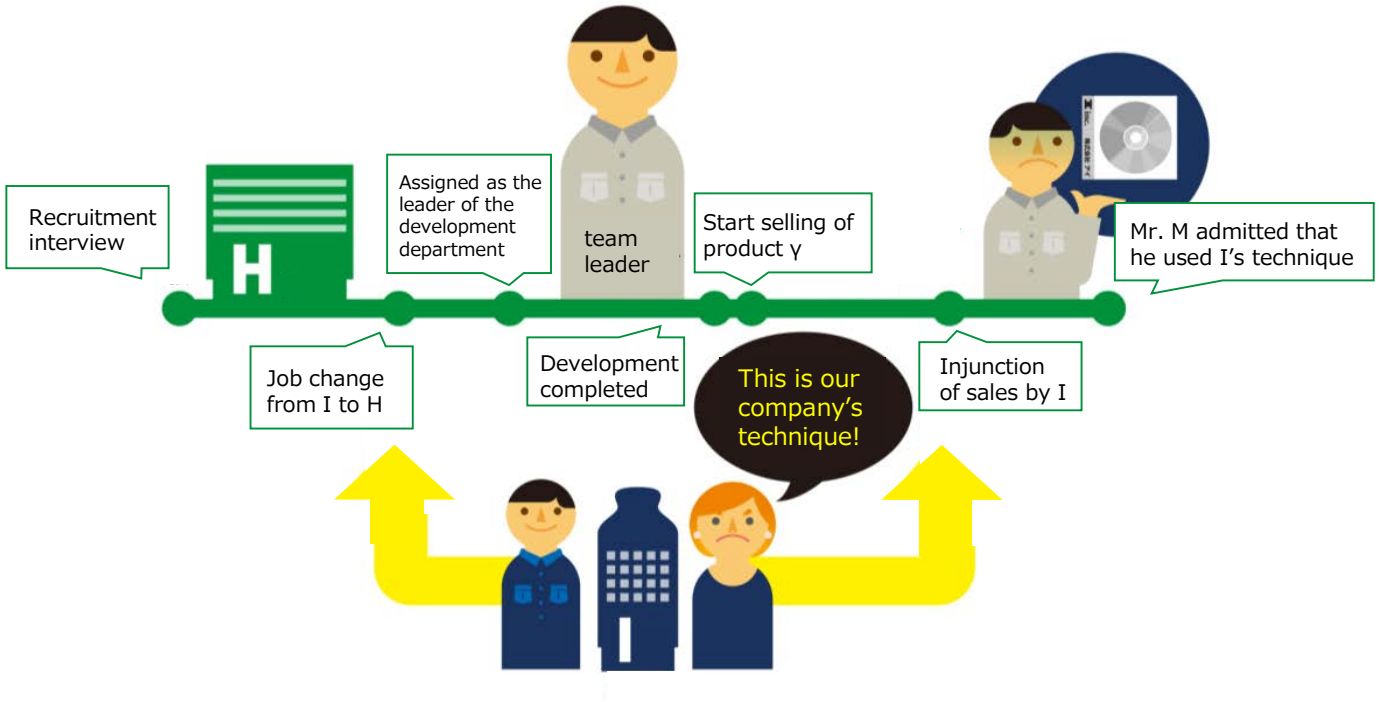


4. This actually happened!? Cases and measures

Case 6. Company H - a container manufacturer

[Measures against new employees] Company H developed new products with new employees from other companies, but…

- Company H decided to focus on the development of strong, light-weight food storage containers, and then employed Mr. M who has experience in container development from Competitor I.
- Mr. M, a leader in the development department, proceeded with development, and developed container γ that is the lightest and strongest container ever. Then Company H started sales of the products γ.
- A few months after launching the sales for products γ, however, Company H received a notice from Company I, which is Mr. M's previous workplace, indicating that product γ includes confidential information owned by Company I and that sales are to be stopped.
- Company H asked Mr. M about the information, Mr. M acknowledged that he developed the new product partially using technologies of Company I.
- What measures should Company H have taken when recruiting Mr. M?



Case 6. Company H - a container manufacturer [Commentary]

Point 1

Confirm obligations of new employees entering other companies

- It is important to check the details of new employees' obligations such as non-disclosure agreements, non-competition obligations, etc., through an interview. It is also effective to record and save the minutes, etc. of the interview.

Point 2

Check that the new employees do not bring in confidential information from other companies when recruiting

- It is important to warn new employees not to bring in confidential information from the previous workplace.
- It is also important to receive a written oath that they will not bring in such confidential information, including;
  - They did not take out any storage medium that contains confidential information of third parties.
  - They did not bring any confidential information owned by third parties into the new workplace.

Point 3

To manage roles and responsibilities of the new employees, etc. carefully after recruiting

- It is important to regularly check their roles and responsibilities
- It is also effective to prohibit the use or possession of media such as personal USB devices in the workplace.
- It is conceivable to have new employees pledge in writing not to appropriate knowledge regarding equipment and specification from their previous company (Company H) in fulfilling their roles and responsibilities at their new company (Company I).