

# **Latest revision of Unfair Competition Prevention Act**

**~Established provisions for shared data with limited access~**

**Intellectual Property Policy Office  
METI, JAPAN**

# Outline

1. Overview on Unfair Competition Prevention Act
2. Background of the revision
3. Overview on this revision of the act
4. Civil remedies against wrongful acquisition and use of “Protected Data”
  - a. View of environment improvement to utilize valuable data
  - b. Image of “Protected Data”
  - c. Act of unfair acquisition, use, disclosure of “Protected Data”

# 1. Overview on Unfair Competition Prevention Act

## Purpose of Act ( Article 1 )

(The bill was passed in May 2018)

## Types of Unfair Competition ( Article 2 )

Creating confusion with a well-known indication of goods, etc

Imitation of the configuration of a third party's product

Infringement of Trade Secrets

Providing a product which circumvents technological restriction measures

Misleading representation regarding the place of origin, quality, etc.

⋮

Wrongful acquisition, usage of Protected Data

Wrongful acquisition, usage of a domain name

⋮

## Remedies

Civil Remedies  
&  
Criminal Remedies

Civil Remedies

## Acts Prohibited by International Treaty (Article 16~18)

Prohibition of commercial use of foreign national flags, armorial bearings (Article 16) and a mark of an international organization (Article 17)

Prohibition of bribery of foreign public officials (Article 18)

Criminal Remedies

# (FYI) Details of Remedies

## Civil Remedies

- Right to seek an injunction (Article 3)
- Right to seek damages (Article 4)
- Presumption of amount of damages, etc. (Article 5 etc.)
- Order to submit documents to the courts (Article 7)
- Protection of trade secrets in civil court cases (Article 10 etc.)  
(protective order, restriction for inspection of the case record, in-camera proceedings )
- Measures to restore business reputation (Article 14)

## Criminal Remedies

The following punishments are prescribed against persons who commit certain acts of unfair competition:

### ○Penal Provisions (Article 21)

- offense of trade secret infringement: Imprisonment with work for not more than 10 years or a fine of not more than 20 million yen (30 million yen for the purpose of use outside Japan), or both
- any other offenses of infringements: Imprisonment with work for not more than 5 years or a fine of not more than 5 million yen, or both

### ○Corporate penalties (Article 22)

- part of offenses of trade secret infringements: a fine of not more than 500 million yen  
(1 billion yen for the purpose of use outside Japan).
- any other offenses of infringement: a fine of not more than 300 million yen.

### ○Punishments against an offense committed outside Japan (Article 21, paragraph(6),(7),(8))

(offense of trade secret infringement, violation of protective order, offense of bribery of a foreign public officer)

## 2. Background of the revision on “Protected Data”

- Data is becoming an increasingly valuable source of corporate competitiveness against the backdrop of the 4th Industrial Revolution with the progress of IoT, big data, artificial intelligence and information technology.
- We need an environment that rewards efforts of data creators, collectors, analyzers, and controllers.
- There have been calls for the introduction of legal measures against illegal conducts in order to reassure data providers.



### 3. Overview on this revision

Revision in 2018

#### (a) Civil remedies against wrongful acquisition and use of “Protected Data” [New]

— enforced on July 1st, 2019

- Defines “Protected Data”, which is protected by a management system (e.g. ID and password managing method) and provided to limited users.
- Positions wrongful acquisition, usage, etc. as acts of unfair competition.
- Provides civil remedies (claims for injunctions and damages) to victims.

#### (b) Enhancing regulation on acts of unfair competition that interfere with the technological restriction measures [Revised]

— enforced on November 29th, 2018

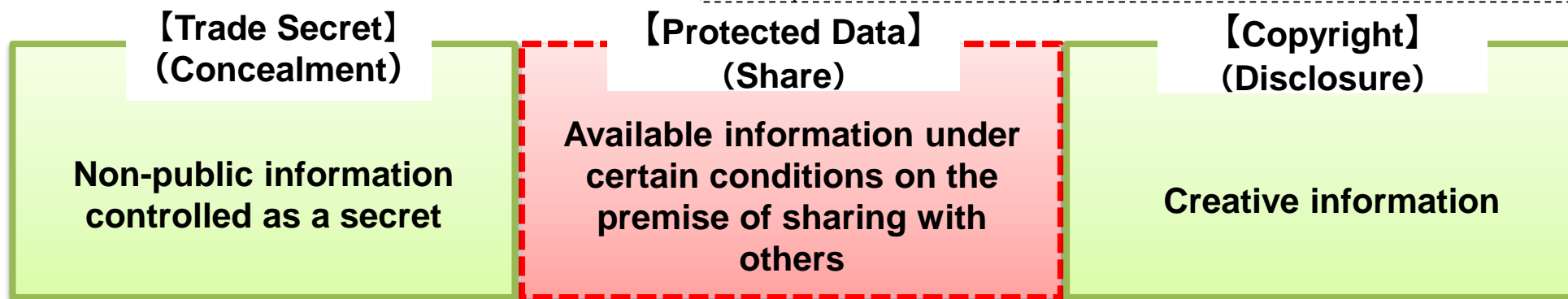
- For example, the revised Act newly covers the act of providing services of circumventing technological restriction measures to users.

## 4.a. View of environmental improvement to utilize valuable data

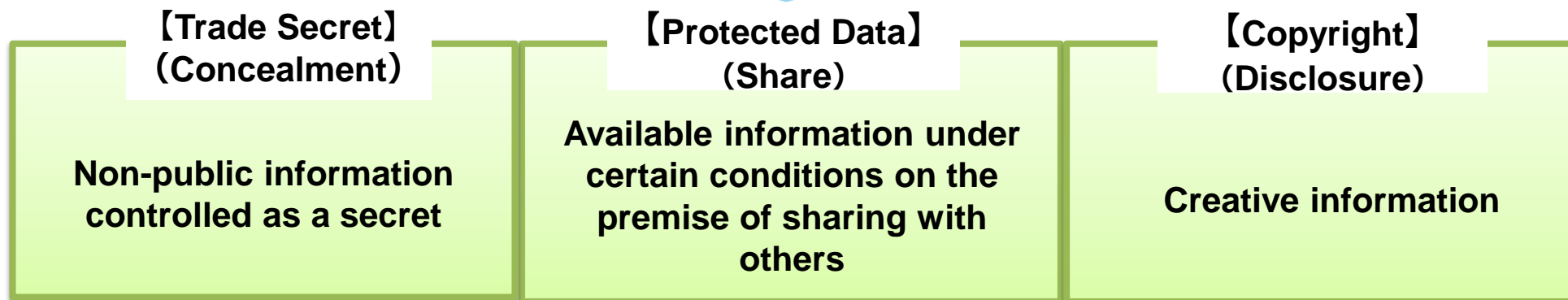
### ● Characteristics of valuable data

- Easy to duplicate.
- Circulation of wrongfully-acquired data may cause the damage rapidly and widely.
- Difficult to stop illegal circulation in cases where data does not fall under (1) the copyright law or (2) “Trade Secret”.

#### Before revision



#### After revision



# (FYI) Definition of “Protected Data”

- Article 2(7)

The term “Protected Data” means technical or business information accumulated and managed by electronic or magnetic means (**Electromagnetic management**) and accumulated considerably by electronic or magnetic means (**Significant accumulation**) as information distributed within a limited scope for business (**Limited provision**) (Exclusion from data managed as secret).

## Requirement

- Limited provision**
- Electromagnetic management (e.g. ID/password)**
- Significant accumulation**

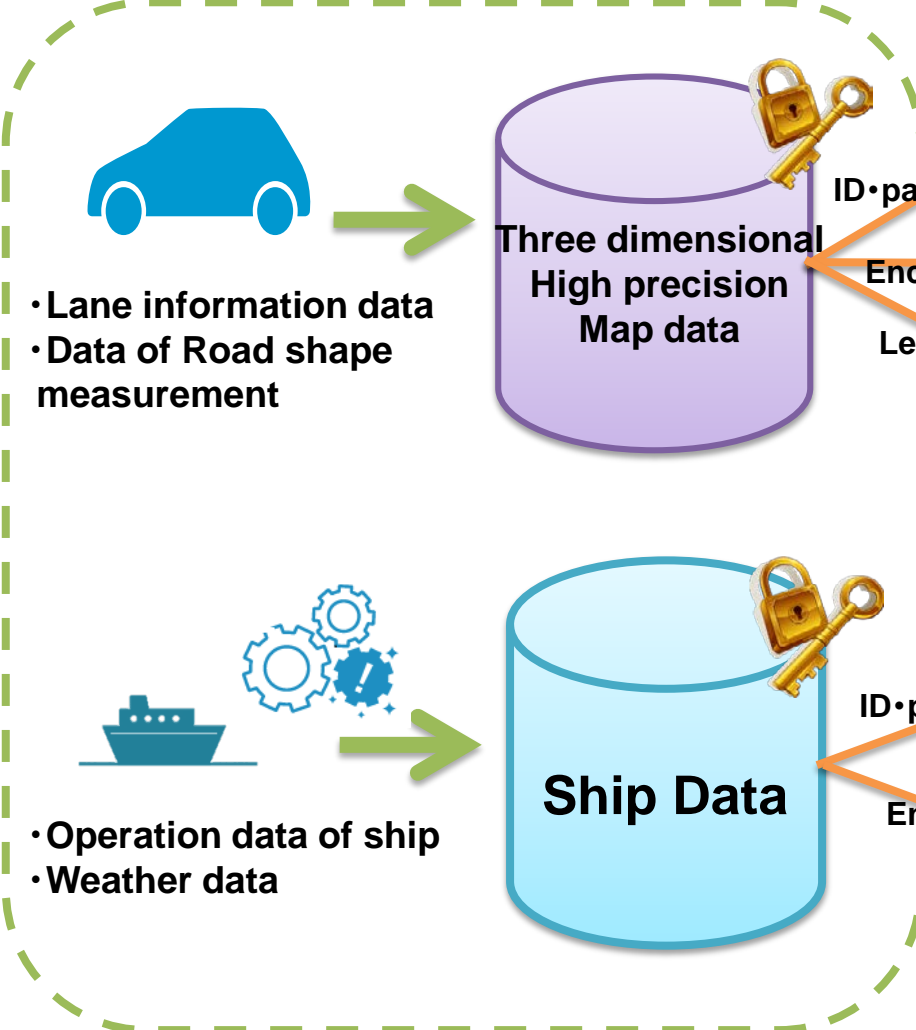
### <Examples of “Protected Data”>

- Map data provided for autonomous driving
- Sales data for each item collected by POS system
- Data summarizing technical information on materials such as chemical substances

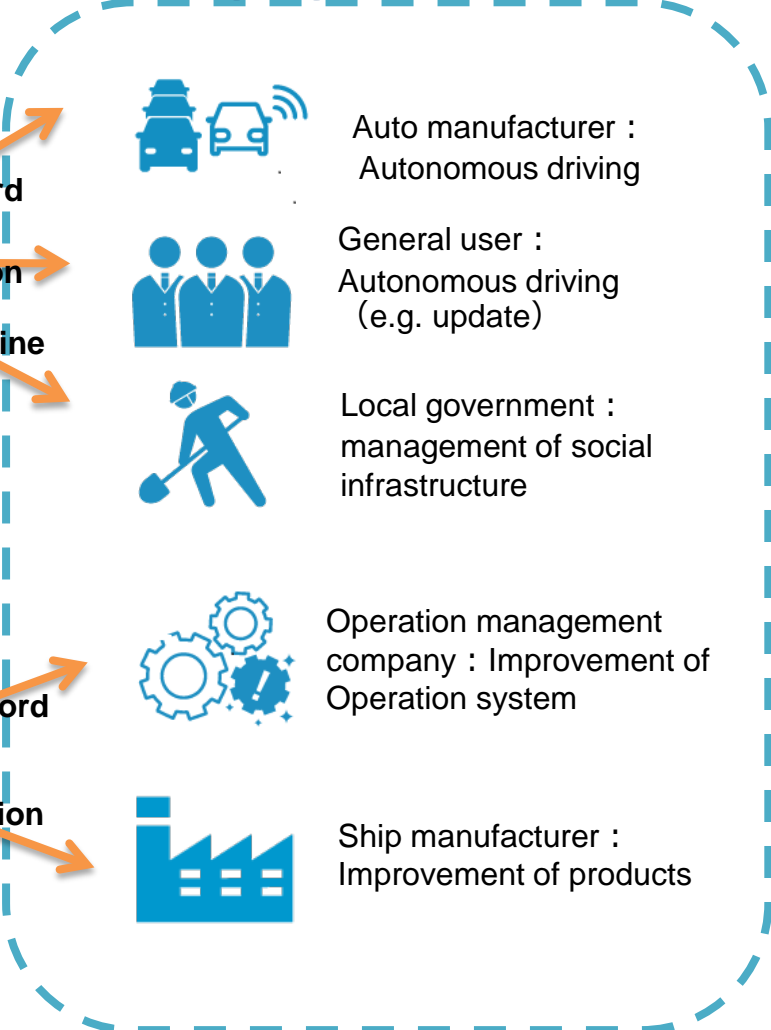
# 4.b. Image of “Protected Data”

- By providing and sharing “Protected Data” among companies, will lead to
  - Creation of new business
  - Value improvement of services and products

## Collecting · Analysis · Processing



## Encouraging data utilization

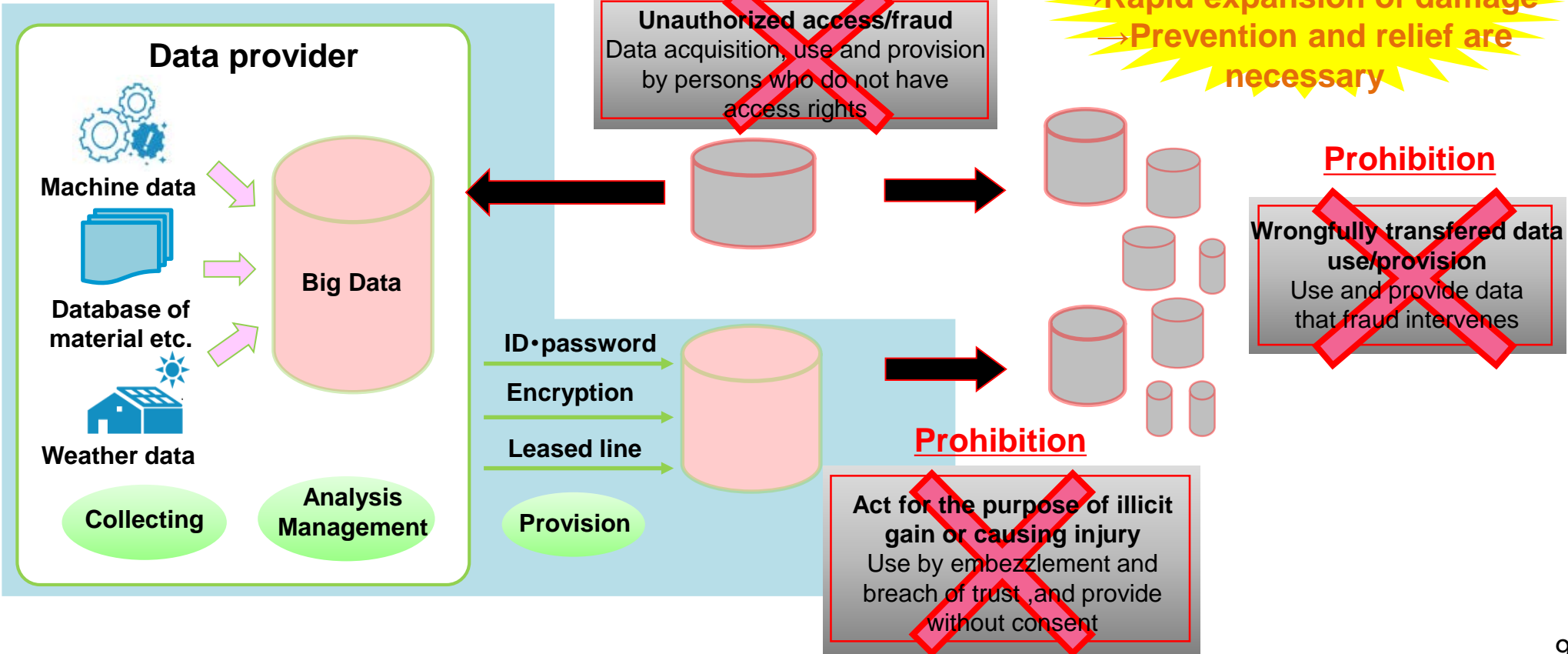


- Creation of new business
- Value improvement of services and products

# 4.c. Act of unlawful acquisition, use, disclosure of “Protected Data”

- Prohibited acts of unfair competition for “Protected Data”,
  - Unauthorized access/fraud
  - Wrongfully transferred data use/provision
  - Act for the purpose of illicit gain or causing injury, etc.

## Prohibited acts of unfair competition



# (FYI) Difference between “Trade Secrets” and “Protected Data”

## Trade Secrets

- ◆ Customer lists
- ◆ Production method

-

- i. Kept secret
- ii. Useful info
- iii. Not publicly known

Owner of trade secrets must attempt to keep information secret.



Examples



Exclusion from application



Requirements



Notes

## Protected Data

- ◆ Machine operation data
- ◆ Consumption trend data
- ◆ People flow data

- i. Excluding information that is kept secret
- ii. Excluding information that has been made available to the public

- i. Limited provision
- ii. Significant accumulation
- iii. Electromagnetic management

“Protected Data” can be utilized by many people under certain conditions.

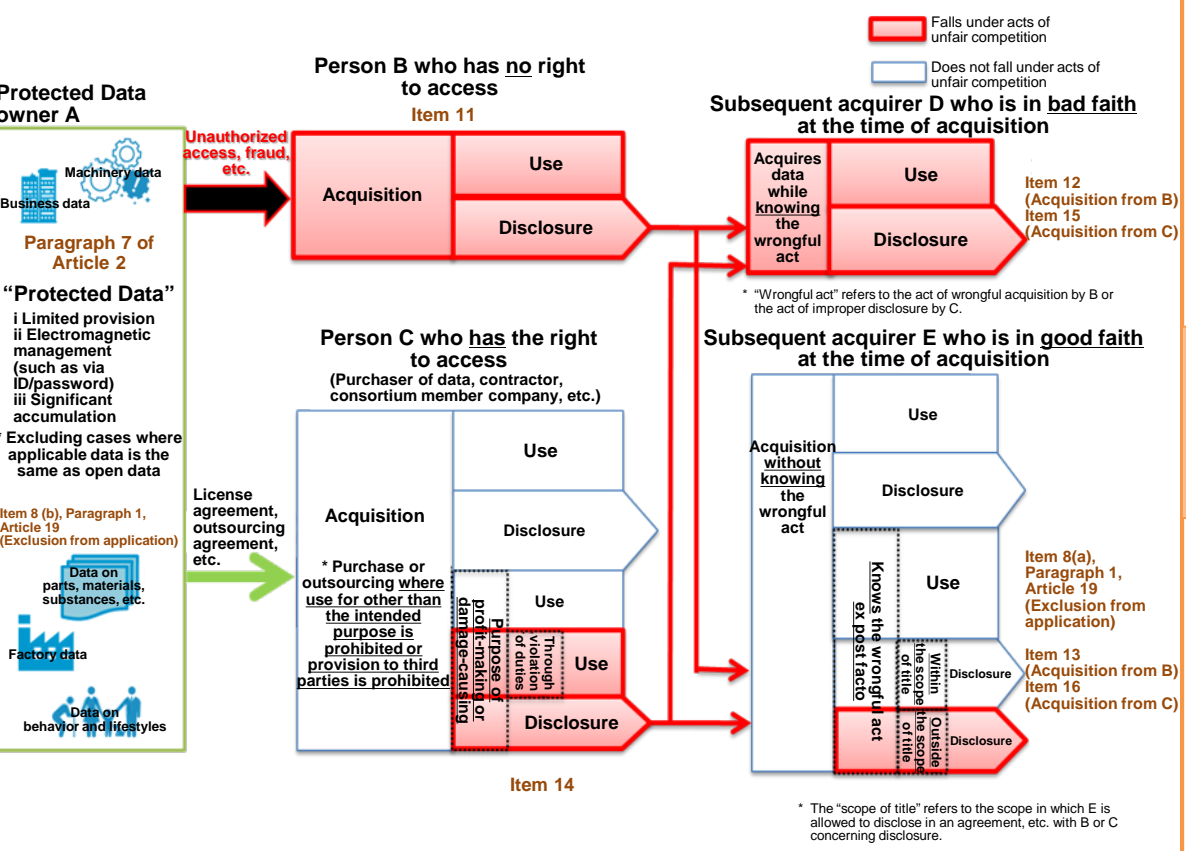
# **(FYI) Guidelines on Protected Data**

[https://www.meti.go.jp/english/policy/economy/chizai/chiteki/pdf/guidelines\\_on\\_protected\\_data.pdf](https://www.meti.go.jp/english/policy/economy/chizai/chiteki/pdf/guidelines_on_protected_data.pdf)

# (FYI) Overview of the Guidelines

- Taking into consideration opinions expressed in the “Interim Report: Study to Promote Data Utilization”, requirements for objects of protected data, the category of unauthorized acquisition, the category of significant violation of the principle of good faith, and the category of subsequent acquisition are discussed using specific examples.

## Categories of acts related to “Protected Data”



## Table of contents of the Guidelines on “Protected Data”

<b>Protected Data</b>
✓ About the definition of protected data
<b>Acts that fall under “unfair competition”</b>
✓ About “acquisition”, “use” and “disclosure”
<b>Category of unauthorized acquisition</b>
About “Person B who has no right to access”
<b>Category of significant violation of the principle of good faith</b>
✓ About “Person C who has the right to access”
<b>Category of subsequent acquisition</b>
✓ About subsequent acquirers D and E

# (FYI) Protected Data

## Article 2

7. The term “protected data” as used in this Act means technical or business information that is **accumulated in a reasonable amount by electronic or magnetic means** (meaning an electronic form, magnetic form, or any other form that is impossible to perceive through human senses alone; the same applies in the following paragraph) as information **provided to specific persons on a regular basis and that is managed** (excluding information that is kept secret).



3 requirements for Protected Data



### “Provided to specific persons on a regular basis” (**Limited provision**)

“On a regular basis” refers to cases where data owner provides data repeatedly and continuously (including cases where the intention of data owner to provide repeatedly and continuously is recognized even if data owner does not actually provide it). “Specific persons” refer to those who receive data under certain conditions.

**Example** “On a regular basis” : where data owner provides data repeatedly (including cases where data is provided to each person once)  
“Specific persons” : members allowed to access members-only databases

### “Accumulated in a reasonable amount by electronic or magnetic means” (**Significant Accumulation**)

In light of socially accepted conventions, data has value as a result of accumulation by electronic or magnetic means. “A reasonable amount” is determined depending on the nature of each data type, but the following and other factors are considered: value added to the data as a result of accumulation by electronic or magnetic means; possibility of utilization; transaction prices; and labor, time, costs, etc. used for collection and analysis. Note that the concept of significant accumulation applies to cases where labor, time and costs are used to collect or analyze a part of data, resulting in value being created for that part of data.

**Example** If a business operator that accumulates information on mobile phone locations nationwide extracts information for specific areas and sells it, data for those specific areas satisfies this requirement (if data is considered to have value from the commercial viewpoint as a result of the data being accumulated by electromagnetic means)

### “Managed by electronic or magnetic means” (**Electromagnetic management**)

The owner’s intention of managing data to provide the data only to specific persons is made clear to outside parties. More specifically, it is necessary to take measures such as implementation of technologies that restrict access, such as ID and password settings.

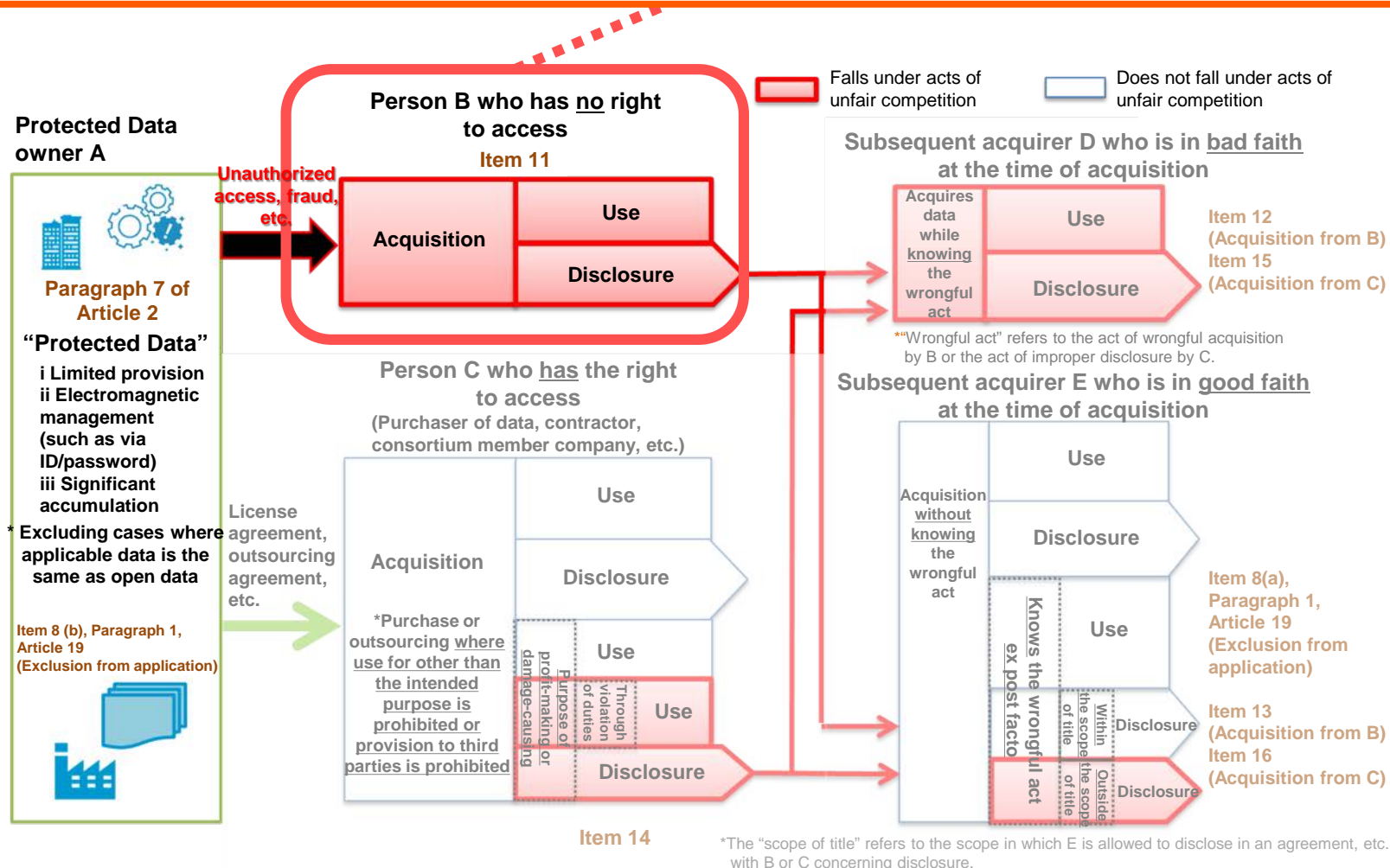
**Example** Access restriction by IDs, passwords, smart cards, specified terminals, tokens or biometric authentication.

\* Other than the above, in the “Guidelines on Protected Data”, an explanation is also provided about “technical or business information” and “excluding information that is kept secret”.  
\* Specific examples are also provided with regard to the scope of information that is “the same as open data” and that is excluded from application.

# (FYI) Acts that fall under “unfair competition” and the category of unauthorized acquisition

Article 2 The term “Unfair Competition” as used in this Act means any of the following:

(xi) the act of **acquiring** protected data by **theft, fraud, duress, or other wrongful means** (hereinafter referred to as an “act of wrongful acquisition of protected data”), or the act of **using** or **disclosing** protected data through an act of wrongful acquisition of protected data;



In relation to “unfair competition”, acts of “**acquisition**”, “**use**” and “**disclosure**” are set out and the Guidelines provide the following definitions in “III. Acts that fall under the category of unfair competition (general remarks)”.

### Acquisition

Refers to **placing data under one’s management**. This applies to cases where a person or a third party obtains data itself via media, etc. on which the data is recorded or cases where a person or a third party obtains data without media, etc. on which the data is recorded.

Example

Act of copying data stored on a server to one’s own PC

### Use

Refers to **the act of using data**. Note that the use, etc. of products (goods, etc. developed using the data) created by using the data acquired does not fall under the act of unfair competition unless such products are considered virtually the same as the data acquired.

Example

Act of creating a program by using data acquired

### Disclosure

Refers to **making data available by a third party**. It does not matter whether or not a third party actually accesses the data.

Example

Act of uploading data to a website that is accessible by a third party.

\*With regard to the “category of significant violation of the principle of good faith” and the “category of subsequent acquisition”, the terms “acquisition”, “use” and “disclosure” are defined in the same manner.

### Theft, fraud, duress or other wrongful means

As for “theft, fraud, duress or other wrongful means”, “theft”, “fraud” and “duress” are presented as examples of wrongful means. “Other wrongful means” are considered to not only refer to **acts subject to criminal punishment, such as a charge of theft and a charge of fraud**, but also to **the case of using a means that is against public policy such as being deemed illegal to the same extent as the above acts in light of socially accepted conventions**.

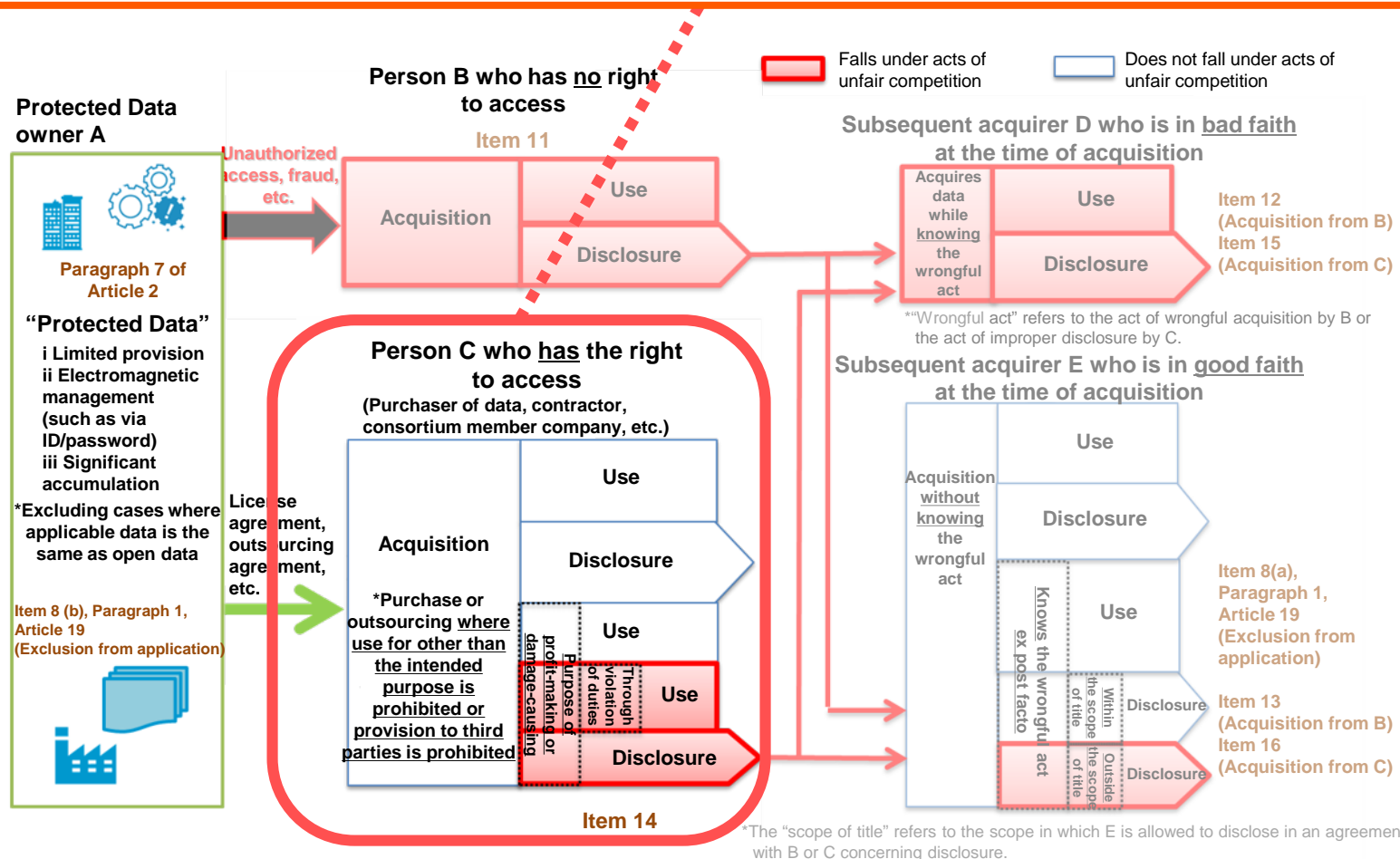
\*The Guidelines also present examples of acts that fall under “theft, fraud, duress or other wrongful means”.

Example) The act of having an access to a PC of another company via a network without permission, operating the PC and deactivating the password to acquire data.

# (FYI) Category of significant violation of the principle of good faith

Article 2 The term “Unfair Competition” as used in this Act means any of the following:

(xiv) the act of using (limited an act conducted in breach of the duties regarding the management of the protected data) or the act of disclosing protected data disclosed by the company that owns it (hereinafter referred to as the “protected data owner”) **for the purpose of wrongful gain or causing damage to the protected data owner;**



**Act of use that satisfies requirements (1) and (2) below**  
**Act of disclosure that satisfies the requirement (1) below**



**Falls under acts of unfair competition**

**(1) “for the purpose of wrongful gain or causing damage to the protected data owner”  
(purpose of profit-making or damage-causing)**

When determining whether requirements for the purpose of profit-making or damage-causing are satisfied, it is assumed that it is obvious for both parties concerned that the relevant act of use or disclosure is not permitted by the protected data owner, and that the legitimate acquirer is aware of such fact.

**[Requirements for the purpose of profit-making or damage-causing: satisfied]**

**When the items i through iii below are applicable**

- i. Cases where although it is obvious for parties concerned that the use (or disclosure) is not permitted and they are aware of such fact,
- ii. the party uses or discloses acquired data for the purpose of wrongful gain for itself or a third party or causing damage to the protected data owner;
- iii. except where there is a justifiable purpose for such act

**[Requirements for the purpose of profit-making or damage-causing: not satisfied]**

- ◆ When a contract does not clearly state the obligation of non-disclosure to a third party
- ◆ In the case of violation by negligence
- ◆ When conducted for the benefit of the protected data owner
- ◆ When there is a justifiable purpose: conducted in emergency, in accordance with laws and regulations, there are reasons based on public interests such as life saving)

**(2) Act “conducted in breach of the duties regarding the management of the protected data”**

**As for “the duties regarding the management of the protected data”, it refers to cases considered to include duties conducted for the protected data owner, rather than duties under a simple data agreement.** More specifically, this refers to cases where there is a relationship in which one party outsources services to, and places confidence in, the other party.

**[Duties related to management: satisfied]**

- ◆ When upon the request of the protected data owner, a person conducts analysis using protected data.

# (FYI) Category of subsequent acquisition

## [Category of subsequent acquisition in bad faith at the time of acquisition]

Article 2 The term “Unfair Competition” as used in this Act means any of the following:

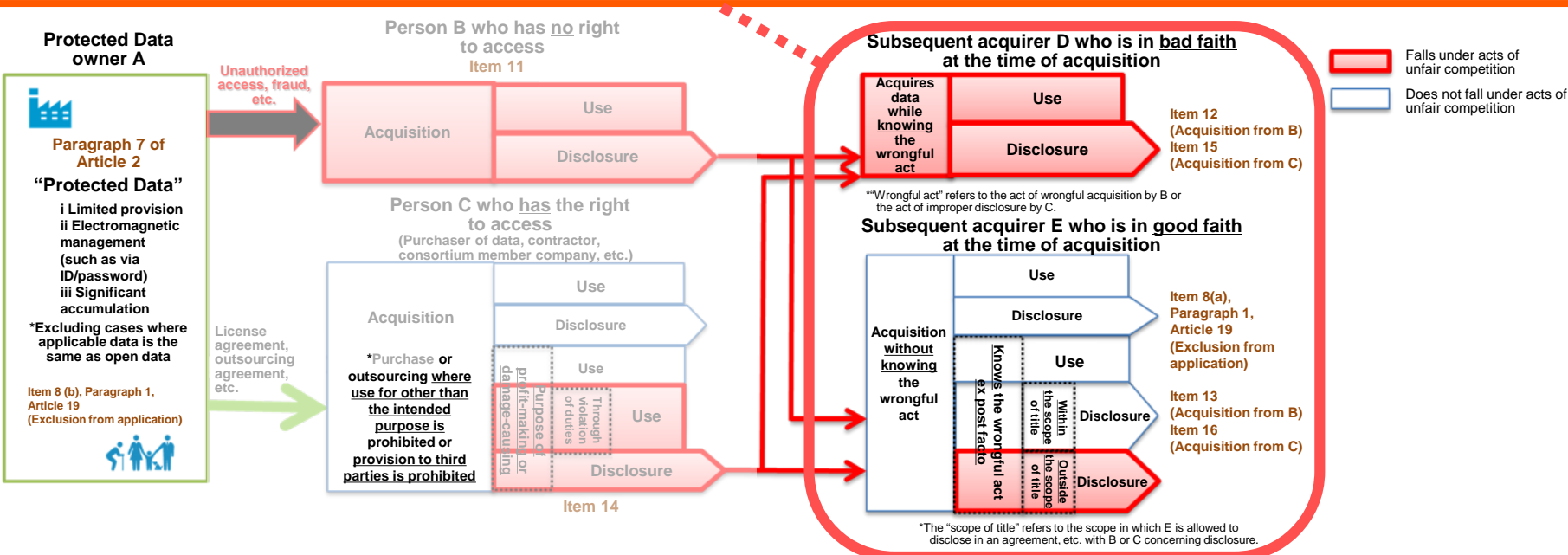
- (xii) the act of acquiring protected data **with the knowledge that there had been an intervening act of wrongful acquisition of protected data**, or the act of using or disclosing protected data acquired in such a way;
- (xv) the act of acquiring protected data **with the knowledge that the disclosure of the protected data is an act of improper disclosure of protected data** (meaning, in the case prescribed in the preceding item, the act of disclosing protected data for the purpose prescribed in the same item; the same applies hereinafter) **or that there has been an intervening act of improper disclosure of protected data with regard to the relevant protected data**, or the act of using or disclosing protected data acquired in such a way;

## [Category of subsequent acquisition in good faith at the time of acquisition]

Article 2 The term “Unfair Competition” as used in this Act means any of the following:

- (xiii) the act of disclosing acquired protected data after **having learned, subsequent to its acquisition, that there had been an intervening act of wrongful acquisition of protected data**;
- (xvi) the act of disclosing acquired protected data after **having learned, subsequent to its acquisition, that disclosing it was an act of improper disclosure of protected data or that there had been an intervening act of improper disclosure of protected data** with regard to the relevant protected data;

\*Item 8 (a) under Paragraph 1 of Article 19 sets out that with respect to the category of subsequent acquisition in good faith at the time of acquisition, the “act of disclosing protected data **within the scope of title acquired through the transaction**” shall be excluded from application.



## **“With the knowledge that there had been an intervening act of wrongful acquisition of protected data” (=“bad faith”)**

To argue that the subsequent acquirer is in “bad faith”, the following requirements (a) and (b) must be satisfied.

**(a) The subsequent acquirer is aware that the act of wrongful acquisition of protected data or the act of improper disclosure of protected data has been conducted.**

(Example)

- ◆ If the subsequent acquirer has requested the legitimate acquirer of data to unrightfully provide data in exchange for money or goods
- ◆ If the subsequent acquirer has received from the data owner a warning clearly evidencing that there has been a wrongful act



**(b) The subsequent acquirer is aware that data for which the act of wrongful acquisition of protected data or the act of improper disclosure of protected data is conducted is the same as data subject to the subsequent acquisition.**

(Example)

- ◆ If it has been confirmed as a result of analysis of a digital watermark, etc. for traceability that the data is identical
- ◆ If the subsequent acquirer has received from the data owner a warning clearly evidencing that the data is identical

\*Cases where it is not evident whether there has been an intervening act of wrongful acquisition cannot be considered cases involving “bad faith”.

\*It is clearly stated that the subsequent acquirer does not owe the duty of care or the duty of investigation such as the obligation of checking whether a wrongful act has been committed.

## **“Within the scope of title”**

This refers to “within the scope in which conditions (disclosure period, purpose and manner) set forth in a transaction (sale, licensing, etc.) where protected data is acquired are applicable”. In the case of an agreement whose contractual relationship is reasonably expected to continue although the term of the agreement has expired formally, such continued agreement is considered to be covered “within the scope of title”.

**Example** Cases where a person executes an agreement subject to automatic renewal, the agreement is renewed automatically after learning of a relevant wrongful act, and, after the renewal, s/he provides data (that has been acquired before learning of the relevant wrongful act) to a third party

## ◆Any questions?

E-MAIL: [ip\\_policy\\_office@meti.go.jp](mailto:ip_policy_office@meti.go.jp)

TEL: +81-3-3501-3752

Webpage:

<http://www.meti.go.jp/english/policy/economy/chizai/chiteki/index.html>