

Provisional Translation (英語仮訳)

Original: 総務省, 中小企業など担当者向けテレワークセキュリティの手引き (チェックリスト) (初版), 2020 available at: https://www.soumu.go.jp/main_content/000706649.pdf
[accessed 16 February 2021]

Note: In case of dispute over translation, Japanese text shall prevail.

(当文章は仮訳であり、正文は日本語とします)

Telework Security Guide for SMEs (Checklist) (1st Edition)



September 11, 2020 (ver.1.0)

Q&A on Telework Security and the corresponding pages of the book

Q1. What to do first? I want to access the checklist quickly.

A1. First, confirm your telework pattern in Part 1-2 **Determine Your Telework Pattern**.

Next, check your security measures with the checklist corresponding to your pattern in **Part 2-1 Security Measure Checklists for Each Pattern**.

Q2. I want to know a more specific explanation of each telework pattern.

A2. See **Part 1-3 Explanation of Telework Patterns** where features of each pattern are explained using tables and figures.

Q3. Why do we need the measures in the checklist? I need a reason that convinces the people of the company

A3. **Part 1-4 “Explanation of Possible Threats in a Telework Environment”** explains threats and influence on the business when the measures listed in the checklist are not taken. The measures are designed to reduce these threats and influence on the business.

Q4. What are specific product settings for implementation of the checklist?

A4. **Part 2-2 List of Setting Examples of the Security Measure Checklists** explains setting examples of popular telework products in order to satisfy the checklist requirement

Q5. I want to see the entire checklists rather than the checklist of each pattern.

A5. **Part 2-3 List of Security Measures for Telework Environment and Possible Threats** organizes and lists the contents of the checklists.

Part 1

1. Introduction

2. Determine your telework pattern.

p 9

3. Explanation of telework patterns

p 11

4. Explanation of Possible Threats in a Telework Environment

p 24

Part 2

1. Security Measure Checklist for Each Telework Pattern

P. 31

2. List of Setting Examples of the Security Measure Checklists

P. 64

3. List of Security Measures for Telework Environment and Possible Threats

P. 64

Contents

Part 1

1	Introduction	5
	(A) Purpose of the book	5
	(B) What is Telework?	5
	(C) Expected Readers of the Book	6
	(D) How to use this book	7
2	Determine your telework pattern	8
	(A) Steps for determination of telework pattern	9
3	Explanation of Telework Patterns	10
	(A) Outline of the telework patterns	11
	① Cases using terminals provided by the company for telework	11
	② Cases of using terminals owned by the employees as telework terminal	13
	(B) Detail of the telework patterns	14
	① Company terminals and VPN/remote desktop pattern	14
	② Company terminals not connected to the company pattern (cloud service type)	16
	③ Company terminals not connected to the company pattern (work-at-hand type)	17
	④ Terminal provided by the company and secure browser pattern	18
	⑤ Employee terminals and VPN/remote desktop pattern	19
	⑥ Employee terminals not connected to the company pattern (cloud service type)	21
	⑦ Terminal owned by the employee not connected to the company pattern (work-at-hand type)	22
	⑧ Terminal owned by the employee and secure browser pattern	23
4	Explanation of Possible Threats in a Telework Environment	24
	(A) Explanation of threats: malware infection	25
	① What is malware infection?	25
	② Examples of malware infection	26
	(B) Explanation of threats: Unauthorized access	28
	① What is unauthorized access?	28
	② Examples of unauthorized access	28
	(C) Explanation of threats: loss/theft of terminal	29
	① What does the loss/theft of terminals mean?	29
	② Examples of loss/theft of terminal	29
	(E) Information tapping	30
	① What does information tapping mean?	30
	② Examples of information tapping	30

Part 2

1	Security Measure Checklist for Each Pattern	31
	(A) Scope of Security Measures	31
	(B) Approach to priority level	32
	(C) Security Measure Checklist	33
	① Company terminals and VPN/remote desktop pattern	33
	② Company terminals not connected to the company pattern (cloud service type)	38

③	Company terminals not connected to the company pattern (work-at-hand type)	42
④	Employee terminals and secure browser pattern	46
⑤	Employee terminals and VPN/remote desktop pattern	50
⑥	Employee terminals not connected to the company pattern (cloud service type)	54
⑦	Employee terminals not connected to the company pattern (work-at-hand type)	58
⑧	Employee terminals and secure browser pattern	62
2	List of Setting Examples of the Security Measure Checklists	66
3	List of Security Measures for Telework Environment and Possible Threats	66
Reference		
1	Glossary	74
2	Reference information on Telework Security	76

The book was created under the 2020 "Survey and Study on Checklist Development Concerning Telework Security" project of the Ministry of Internal Affairs and Communications (entrusted to MRI Secure Technologies Ltd.)

Part 1

1 Introduction

(A) Purpose of the book

This book presents in a simple way security measures of high feasibility and priority, which people in charge at SME, etc. should implement based on the risks that SMEs should consider when introducing and using telework.

To this purpose, the security measures presented in this book are not necessarily exhaustive but basic and important (minimum required) measures. By setting implementation of the measures as the first goal, you can efficiently take security measures.

The Telework Securities Guidelines (Fourth Edition) that was published separately from this book organizes security approaches and measures for a wide range of enterprises, etc. regardless of size, while this book is designed for SMEs, etc. whose budget and internal security system may be insufficient. (See also (C) “Expected Readers of the Book” on the next page.)

(B) What is Telework?

Telework assumed in the book refers to diverse work arrangements and styles for effective utilization of time and space by taking advantage of information communication technologies (ICT.) In this book, the term is used as a collective term for the following three arrangements/styles:

- ① Working at home
- ② Mobile work
- ③ Working at a satellite office



Working at home



Mobile work



Working at a satellite office

With the progress of ICT, operation productivity can be maintained in many telework environments at a level which may not be equal to but is comparable with the standard office environment. Telework is said to have the following advantages:

- **Saving commuting time and eliminating the stress of commuting**
- **Balancing work and childrearing/family care/ medical treatment**
- **Securing Business Continuity Plan, BCP**

On the other hand, introduction of telework across the board to all job categories and employees may not produce the expected results. It is recommended not to set the introduction of telework itself as the goal but to introduce telework after determining the advantages you expect from the introduction.

On this premise, I hope you use this book to implement the minimum required security measures for introduction and use of telework.

(C) Expected Readers of the Book

We assume persons in charge of security and system management (including those with an equivalent role) at SME, etc. as the readers of this book. Specifically, the following conditions are assumed and the terms and explanations are added with these in mind.

Property	Expected readers of this book	Reference: Expected readers of the Telework Security Guidelines
Approach to security budget	It is difficult to raise outsourcing budget	Outsourcing budget can be raised as needed.
Security promotion system	No dedicated personnel	There is dedicated personnel or a dedicated department
Security literacy	They can determine the measures just based on abstract requests such as “appropriately” and “in accordance with the level,” which are left to the interpretation of the readers.	They can study, determine and implement measures in response to abstract requests such as “appropriately” and “in accordance with the level,” which are left to interpretation by the readers.
IT literacy	They have heard of VPN, filtering, antivirus and other basic IT terms and can imagine their uses.	They understand the mechanism of VPN, filtering, antivirus and other basic IT terms
	They can handle basic system settings through net search.	They can comfortably handle basic system settings

(D) How to use this book

The main part of this book consists of two parts as shown in the table below.

In Part 1, Readers of this guide can determine the telework pattern their organization will adopt. In Part 2, readers can use the checklist corresponding to the telework pattern chosen in Part 1.

Overall structure of the book

Structure		Outline
Part 1	1 Introduction	Explains the purpose of using this book, assumed telework and utilizing methods
	2 Determine Your Telework Pattern	With uses of telework in mind, this section presents steps for determining the telework pattern that is introduced or to be introduced.
	3 Explanation of Telework Patterns	Description of the details of the telework patterns
	4 Explanation of Possible Threats in a Telework Environment	Description of the outline of possible threats in a telework environment
Part 2	1 Security Measure Checklists for Each Pattern	Checklist to determine the security measures to be implemented for each telework pattern
	2 List of Examples of Settings of the Security Measure Checklists	List of products for which examples of settings are described for reference when taking measures in the checklist
	3 List of Security Measures for a Telework Environment and Possible Threats	Presents “content of measures,” “priority” and “possible threats” of security measures in a telework environment and “necessity of the measures for individual patterns”
Reference	Glossary	Explanation of key terms used in the book
	Reference information on telework security	References and web sites useful for implementation of the checklists

In Part 1, determine the applicable telework pattern based on your telework job content and the terminals used with reference to “2 Determine Your Telework Pattern.” Next, understand the details of your telework pattern and choose the checklist corresponding to the applicable pattern with reference to “3 Explanation of Telework Patterns.”

In Part 2, take the security measures corresponding to the applicable pattern with reference to “1 Security Measure Checklists for Each Pattern.” For reference for implementing the content of the checklists in a specific environment, we have prepared materials that explain the settings of some products. “2 List of Examples of Settings of the Security Measure Checklists” lists the products that are covered by the explanation above. Please use the list for reference as needed.

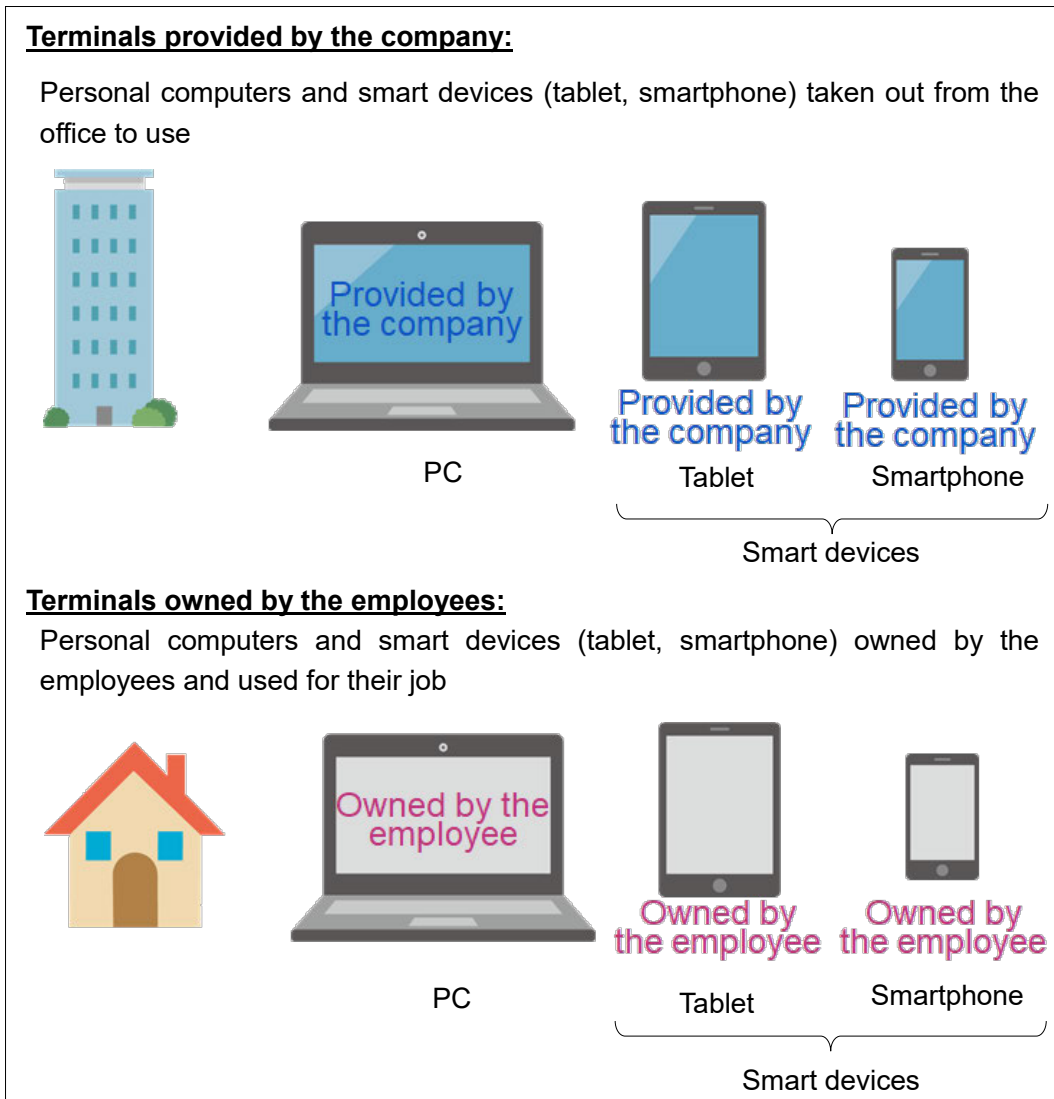
“4 Explanation of Possible Threats in a Telework Environment” of Part 1 is created as a material that can be used for promotion of better understanding of security measures when your organization or the management requests an explanation of the importance of and need for security measures, for example.

2 Determine your telework pattern

There are multiple telework patterns in accordance with the system and environment used. Specifically, the patterns can be classified based on the type of terminals used for telework, method of connection to the office network, and whether or not the data is stored in the telework terminals*, for example. Security measures to be considered vary depending on the pattern.

In order to determine the telework pattern that is introduced (scheduled for introduction) in your organization, select the telework pattern based on the telework operation content of your company, terminals used and other conditions. If you envisage use of multiple patterns in your organization, determine each applicable pattern.

Examples of telework terminals



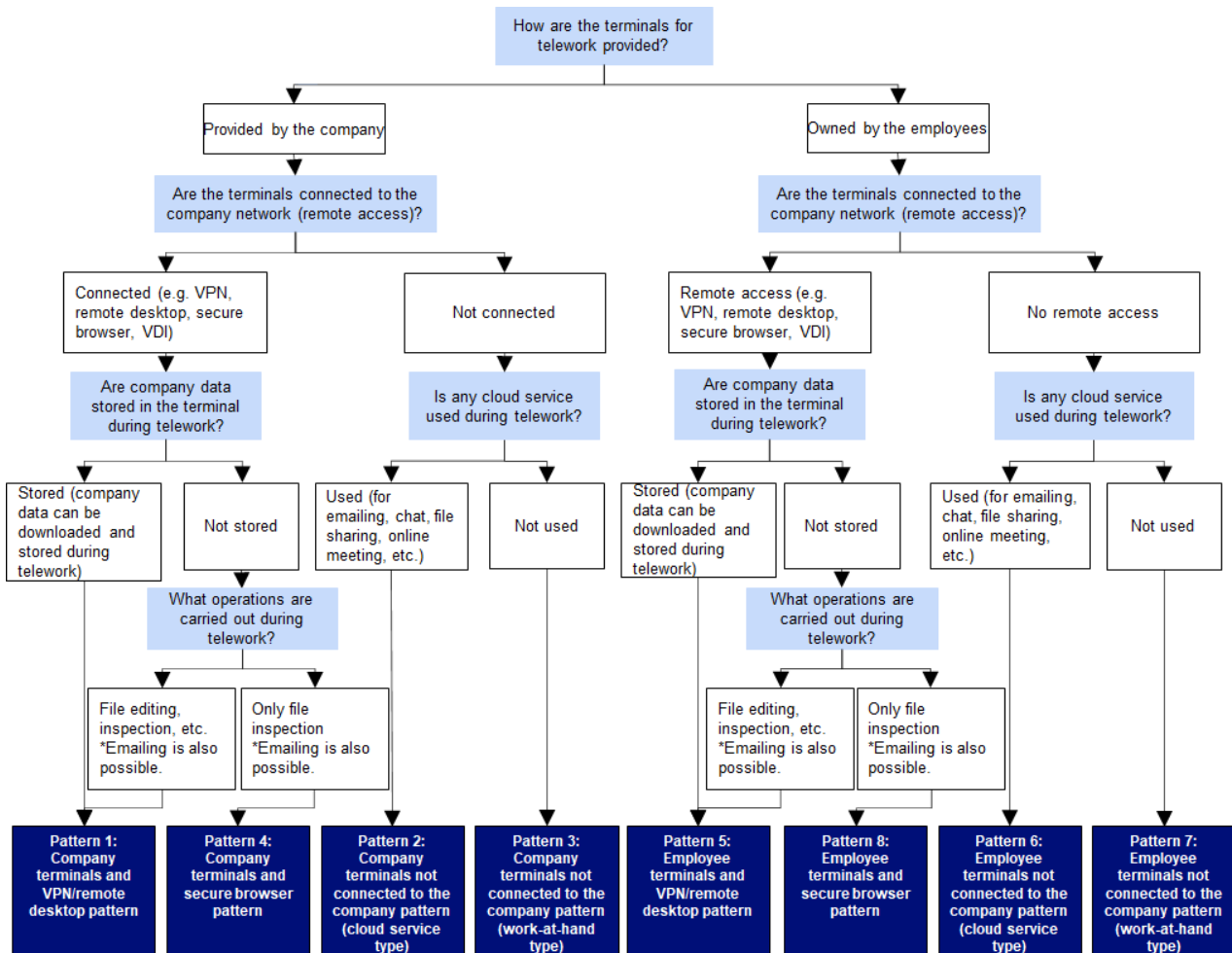
(A) Steps for determination of telework pattern

You can determine the applicable pattern by selecting the answer that is applicable to your environment for each question in the flowchart below.

See “3 Explanation of Telework Patterns” for detailed description of individual patterns.

Checklist of security measures for the applicable pattern is organized for each pattern in “1 Security Measure Checklists for Each Pattern.” If multiple patterns are applicable, check the checklists of all applicable patterns.

Flowchart to determine your telework pattern



* If you use multiple environments including personal computers and smart devices and the use form varies depending on the environment, determine the pattern for each environment using the flowchart above.

3 Explanation of Telework Patterns

Below is a specific explanation of the individual Telework patterns in the flowchart of the preceding page.

Please use the explanation also to check the appropriateness of the telework pattern that you have selected as “adopted in your organization or scheduled for adoption.”

The checklists are organized by pattern in **“Part 2-1 Security Measure Checklists for Each Pattern.”**

If multiple patterns are applicable, check the checklists of all applicable patterns.

Common terms in the explanation of the patterns are described in the table below for your reference.

Term	Description
VPN	An abbreviation for Virtual Private Network. The technology enables safe access to the internal network remotely from home, visiting destination and other remote locations as if it were communication within the network.
Remote desktop	Technology to transfer screens of the computers in the internal network to the computer at hand (telework terminal,) via the network, display the screens and remotely operate the computer in the internal network.
Secure browser	Dedicated software for viewing the information stored in the internal system or a cloud service which can prevent storage of the data in the terminal while viewing the information. Some products can limit screen shots, text copying and pasting and accessible pages.
Cloud service	Generic term for various services that enable use through networks including the Internet of software, data, etc. that were conventionally managed and used through personal computers/servers. This book assumes mailing, chat, online meeting, file sharing and other cloud services, which include use of mail services provided by ISPs.
Data storage in telework terminal	This refers to storing of data in the terminal used (taken out and used) in a telework environment rather than storing in an internal server or cloud service. If it is not clear where the data are stored, and the data is accessible without connection of the telework terminal to the network (internal network or the Internet,) you can assume that the data is stored in the telework terminal.

(A) Outline of the telework patterns

For outlining individual telework patterns, the patterns are divided into cases using “terminal provided by the company” and cases using “terminals owned by the employee” for telework

① Cases using terminals provided by the company for telework

Pattern	Connection to the office network	Use of cloud service	Data storage in telework terminal	Outline	Corresponding pages
Pattern 1: Company terminals and VPN/remote desktop pattern	VPN, remote desktop, etc.	Includes both “used” and “not used”	Stored *includes “not stored” for remote desktop connection	Pattern to do work through VPN connection from the telework terminal provided by the company to the office network; Or the pattern to do work through remote desktop connection from the telework terminal provided by the company to the office network. Both cases include working on the terminal at hand.	Explanation of the pattern p.14 - 15 Checklist p.33 -
Pattern 2: Company terminals not connected to the company pattern (cloud service type)	Not connected	Used	Includes both “stored” and “not stored”	Pattern to do work by accessing the application software provided by a cloud service on the internet from the telework terminal provided by the company, which includes doing work on a terminal at hand	Explanation of the pattern p.16 Checklist p.38 -
Pattern 3: Company terminals not connected to the company pattern (work-at-hand type)	Not connected	Not used	Stored	Pattern to take out the telework terminal provided by the company to a telework environment and to do work on a terminal at hand by viewing and editing only the files stored in advance on the terminal at hand	Explanation of the pattern p.17 Checklist p.42 -

<p>Pattern 4: Company terminals and secure browser pattern</p>	<p>Secure browser</p>	<p>Used</p>	<p>Not stored</p>	<p>Pattern to do work by accessing application software in the internal system or cloud service from the telework terminal provided by the company by using a special secure browser (that limits data storage in the terminal at hand, for example)</p>	<p>Explanation of the pattern p.18 Checklist p.46 -</p>
--	-----------------------	-------------	-------------------	--	---

② Cases of using terminals owned by the employees as telework terminal

Pattern	Connection to the office network	Use of cloud service	Data storage in telework terminal	Outline	Corresponding pages
Pattern 5: Employee terminals and VPN/remote desktop pattern	VPN, remote desktop, etc.	Includes both "used" and "not used"	Stored *includes "not stored" for remote desktop connection	Pattern to do work through VPN connection from the telework terminal owned by the employee to the office network, which includes doing work on a terminal at hand. Or the pattern to do work through remote desktop connection from the telework terminal owned by the employee to the office network. Both cases include working on the terminal at hand.	Explanation of the pattern p.19 - 20 Checklist p.50 -
Pattern 6: Employee terminals not connected to the company pattern (cloud service type)	Not connected	Used	Includes both "stored" and "not stored"	Pattern to do work by accessing the application software provided by a cloud service on the internet from the telework terminal owned by the employee, which includes doing work on a terminal at hand.	Explanation of the pattern p.21 Checklist p.55 -
Pattern 7: Employee terminals not connected to the company pattern (work-at-hand type)	Not connected	Not used	Stored	Pattern to take out the telework terminal owned by the employee to a telework environment and to do work on a terminal at hand by only viewing and editing the files stored in advance.	Explanation of the pattern p.22 Checklist p.59 -
Pattern 8: Employee terminals and secure browser pattern	Secure browser	Used	Not stored	Pattern to do work by accessing application software in an internal system or cloud service from the telework terminal owned by the employee by using a special secure browser (that limits data storage in the terminal at hand, for example)	Explanation of the pattern p.23 Checklist p.63 -

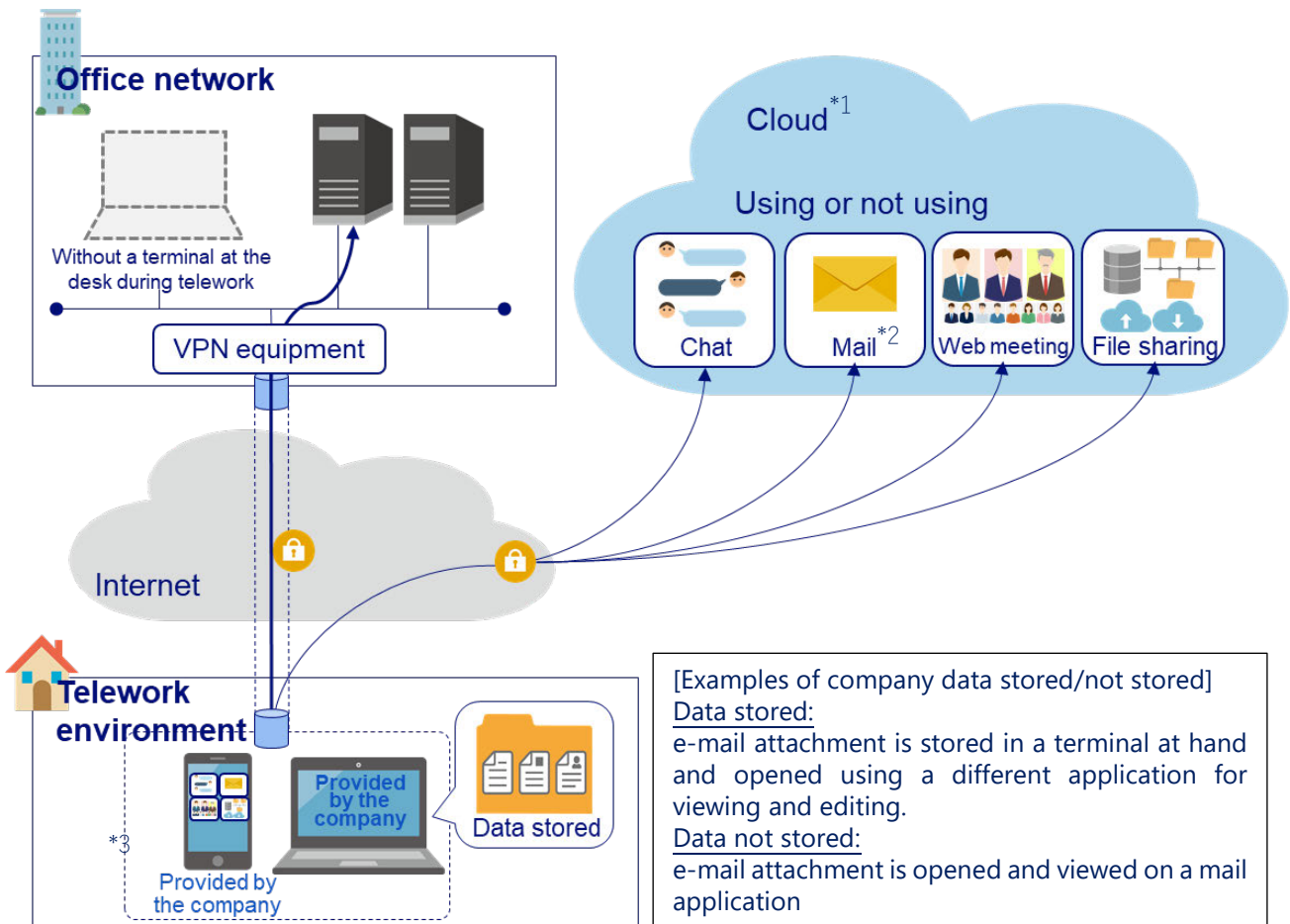
(B) Detail of the telework patterns

Each telework pattern is specifically explained with illustration.

① **Company terminals and VPN/remote desktop pattern**

The connection methods of the two patterns (1) and (2) below fall under this category.

- (1) Work is done through VPN connection from the telework terminal provided by the company to the office network. In this way, a business environment equal to that of the office can be established. The pattern includes simultaneous working on a telework terminal at hand.

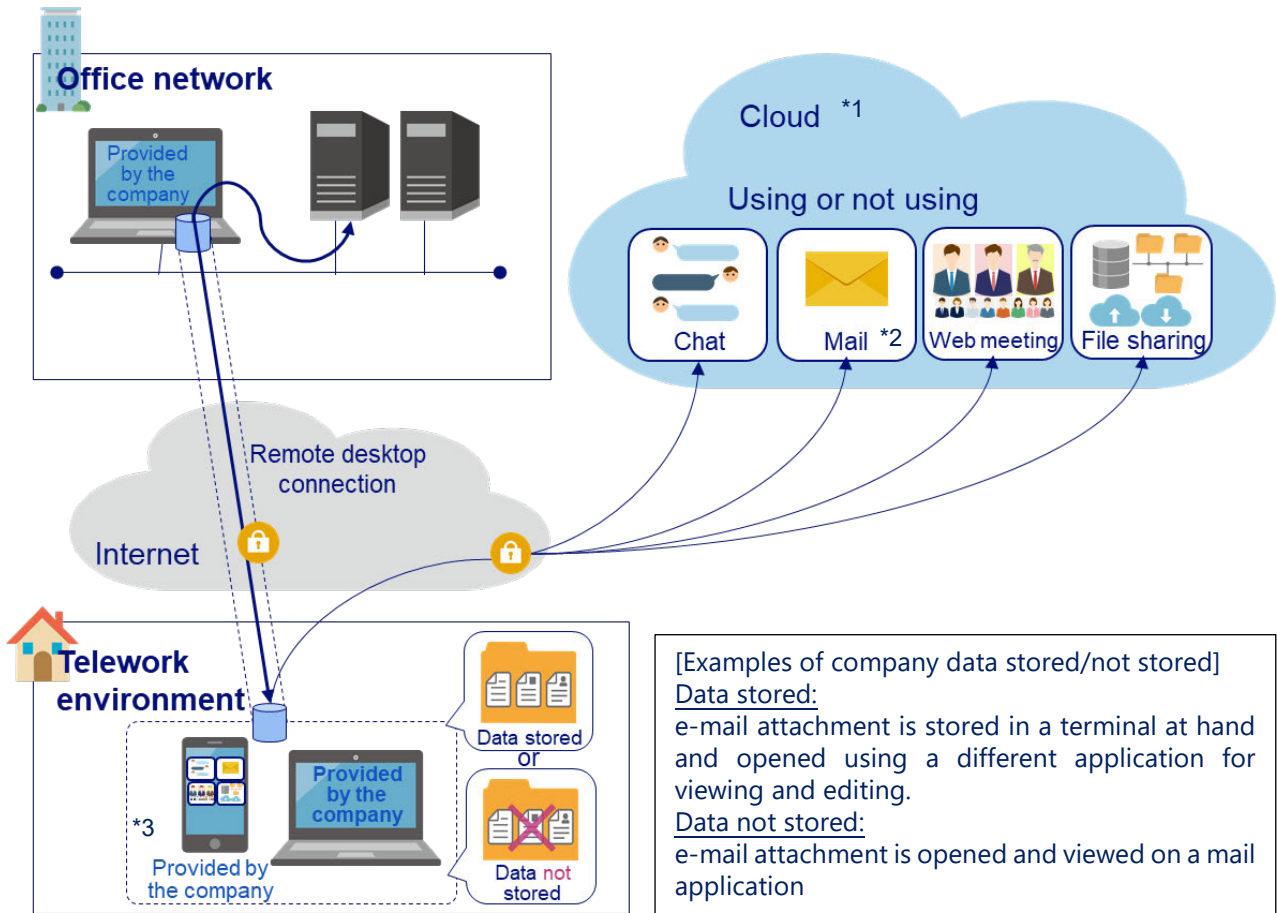


*1 "Using a cloud service" applies to using all or part of the service.

*2 Use of mail service provided by ISP also falls under use of cloud service.

*3 Using an application of a tablet terminal or smartphone for mailing also falls under "using a cloud service."

(2) Work is done through remote desktop connection from the telework terminal provided by the company to the terminal provided by the company in the office network. In this way, a business environment equal to that of the office can be established. The pattern includes simultaneous working on a telework terminal at hand.



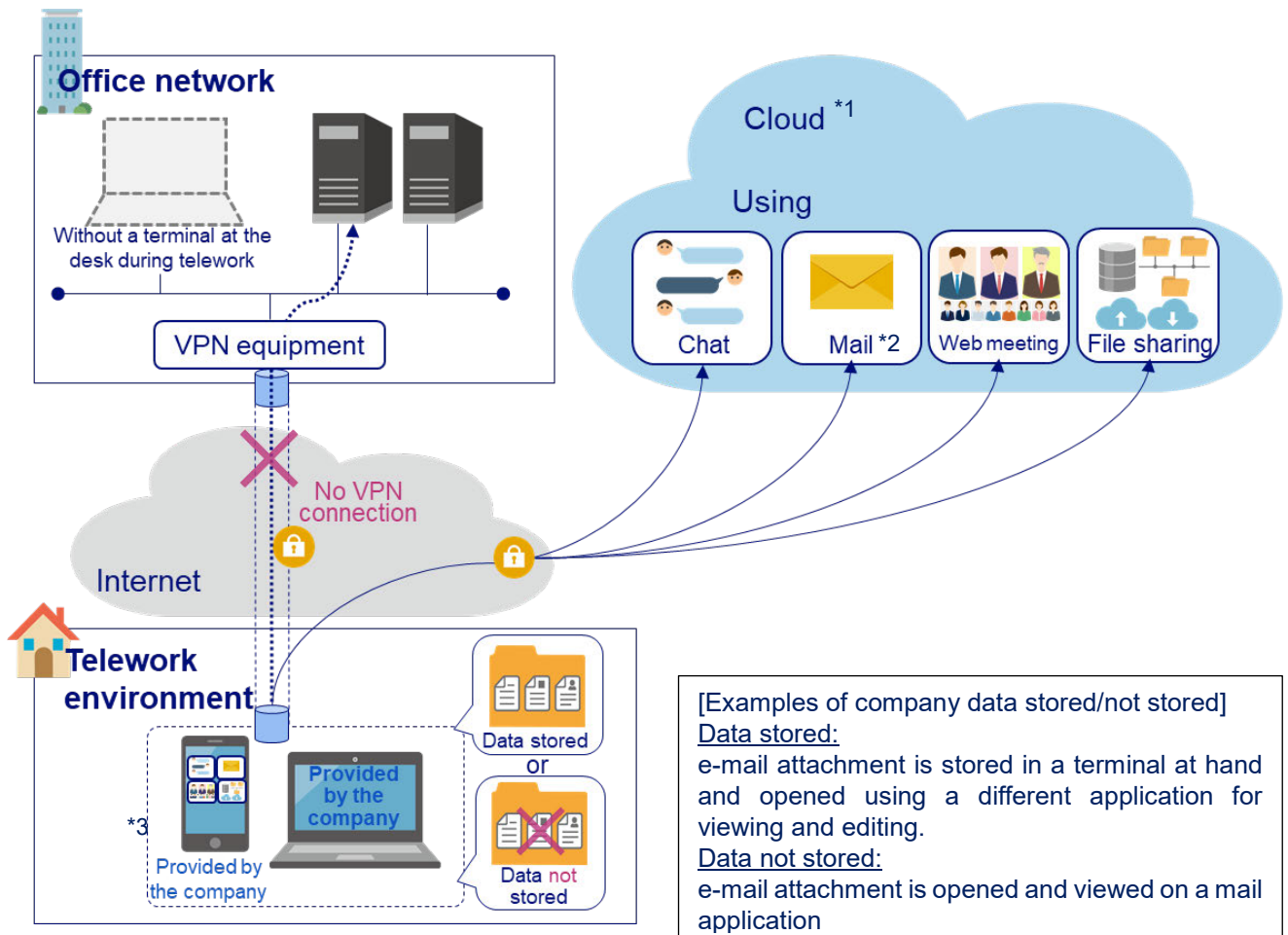
*1 "Using a cloud service" applies to using all or part of the service.

*2 Use of mail service provided by ISP also falls under use of cloud service.

*3 Using an application of a tablet terminal or smartphone for mailing also falls under "using a cloud service."

② **Company terminals not connected to the company pattern (cloud service type)**

Work is done by accessing application software provided by a cloud service on the Internet from the telework terminal provided by the company. Its feature is that the terminal is not connected to the office network. Use of a cloud service can establish a work environment equal to that of the office. The pattern includes simultaneous working on a telework terminal at hand.



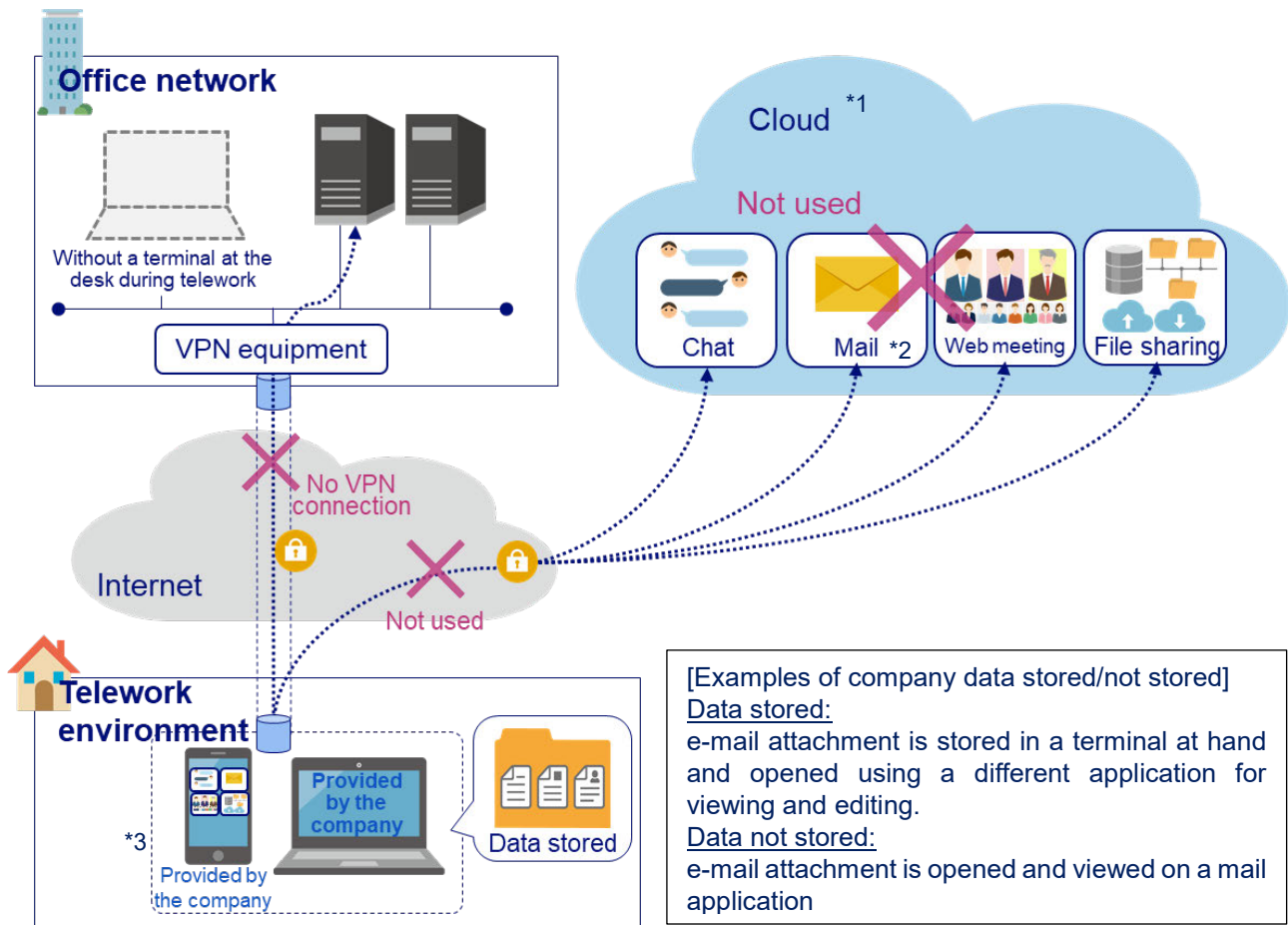
*1 "Using a cloud service" applies to using all or part of the service.

*2 Use of mail service provided by ISP also falls under use of cloud service.

*3 Using an application of a tablet terminal or smartphone for mailing also falls under "using a cloud service."

③ **Company terminals not connected to the company pattern (work-at-hand type)**

Work is done by taking out the telework terminal provided by the company to a telework environment and editing and viewing the data stored in the terminal in advance. Its feature is that the terminal is not connected to the office network and cloud service is not used. Only limited work is carried out.



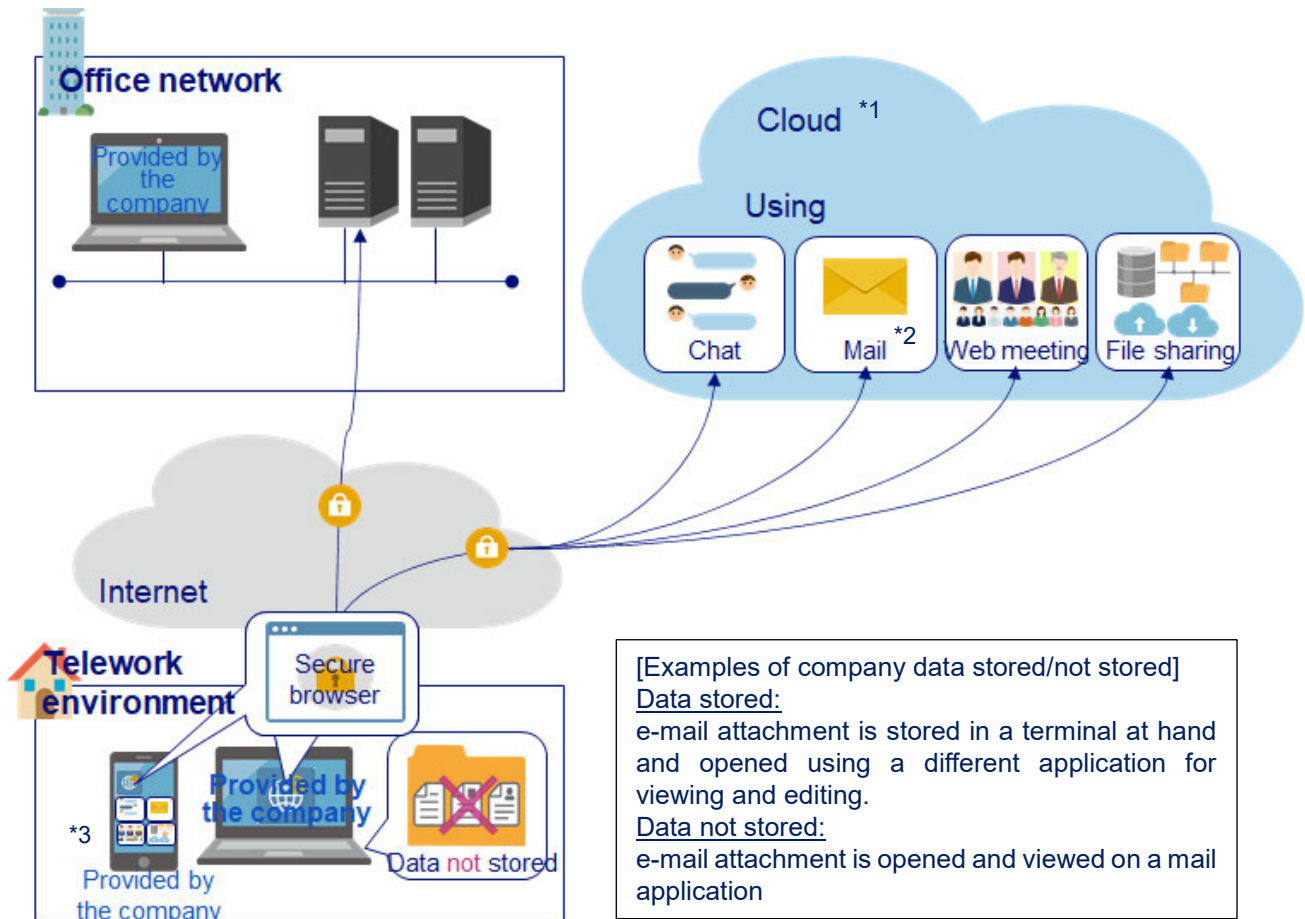
*1 "Using a cloud service" applies to using all or part of the service.

*2 Use of mail service provided by ISP also falls under use of cloud service.

*3 Using an application of a tablet terminal or smartphone for mailing also falls under "using a cloud service."

④ Terminal provided by the company and secure browser pattern

Work is done by accessing application software provided by an internal system or cloud service through a special internet browser (secure browser) from the telework terminal provided by the company. Its feature is that data is not stored in the terminal. Only limited work is carried out.



*1 "Using a cloud service" applies to using all or part of the service.

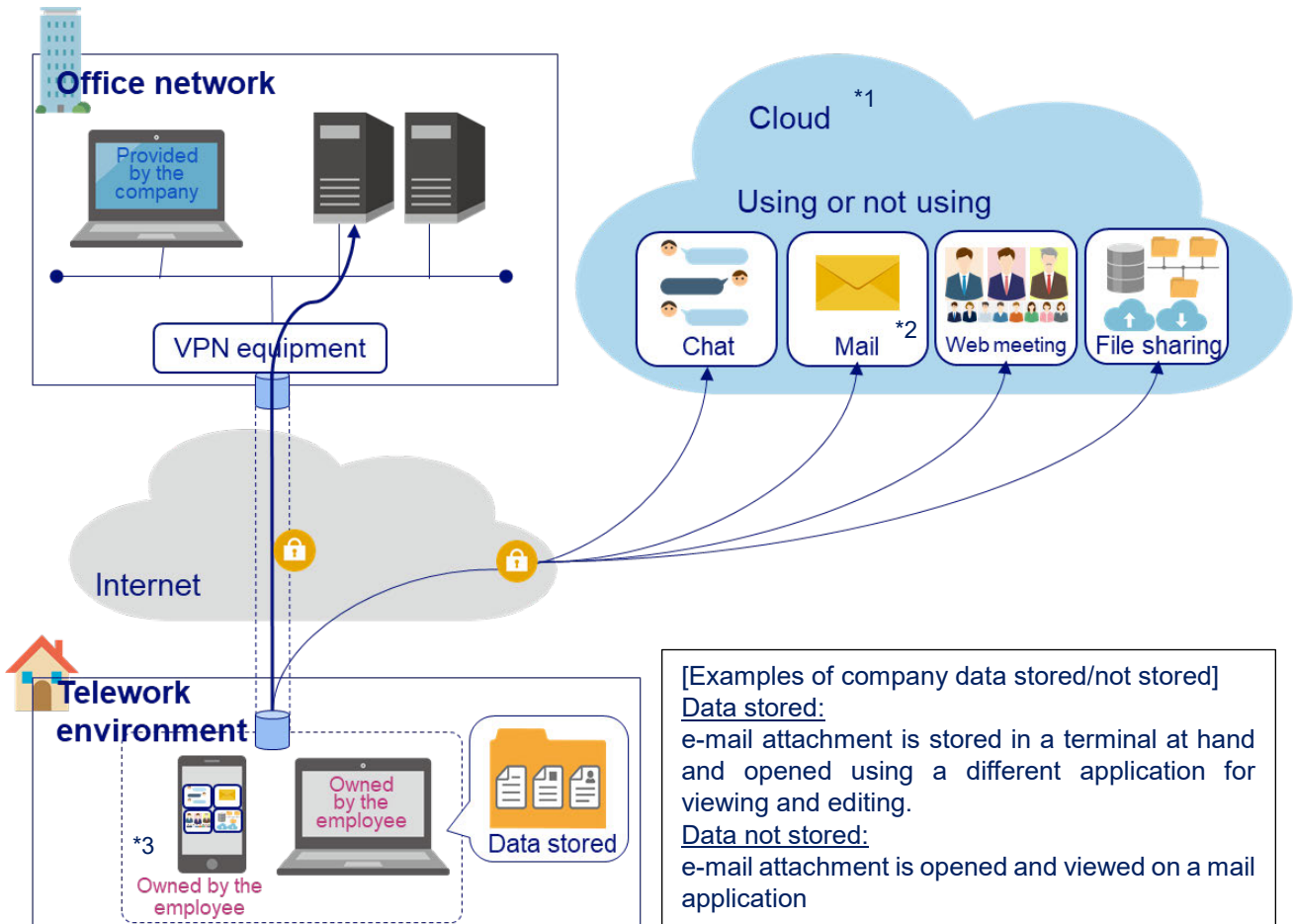
*2 Use of mail service provided by ISP also falls under use of cloud service.

*3 Using an application of a tablet terminal or smartphone for mailing also falls under "using a cloud service."

⑤ Employee terminals and VPN/remote desktop pattern

The connection methods of the two patterns (1) and (2) below fall under this category.

(1) Work is done through VPN connection of the telework terminal owned by the employee to the office network. In this way, a business environment equal to that of the office can be established. The pattern includes simultaneous working on a telework terminal at hand.

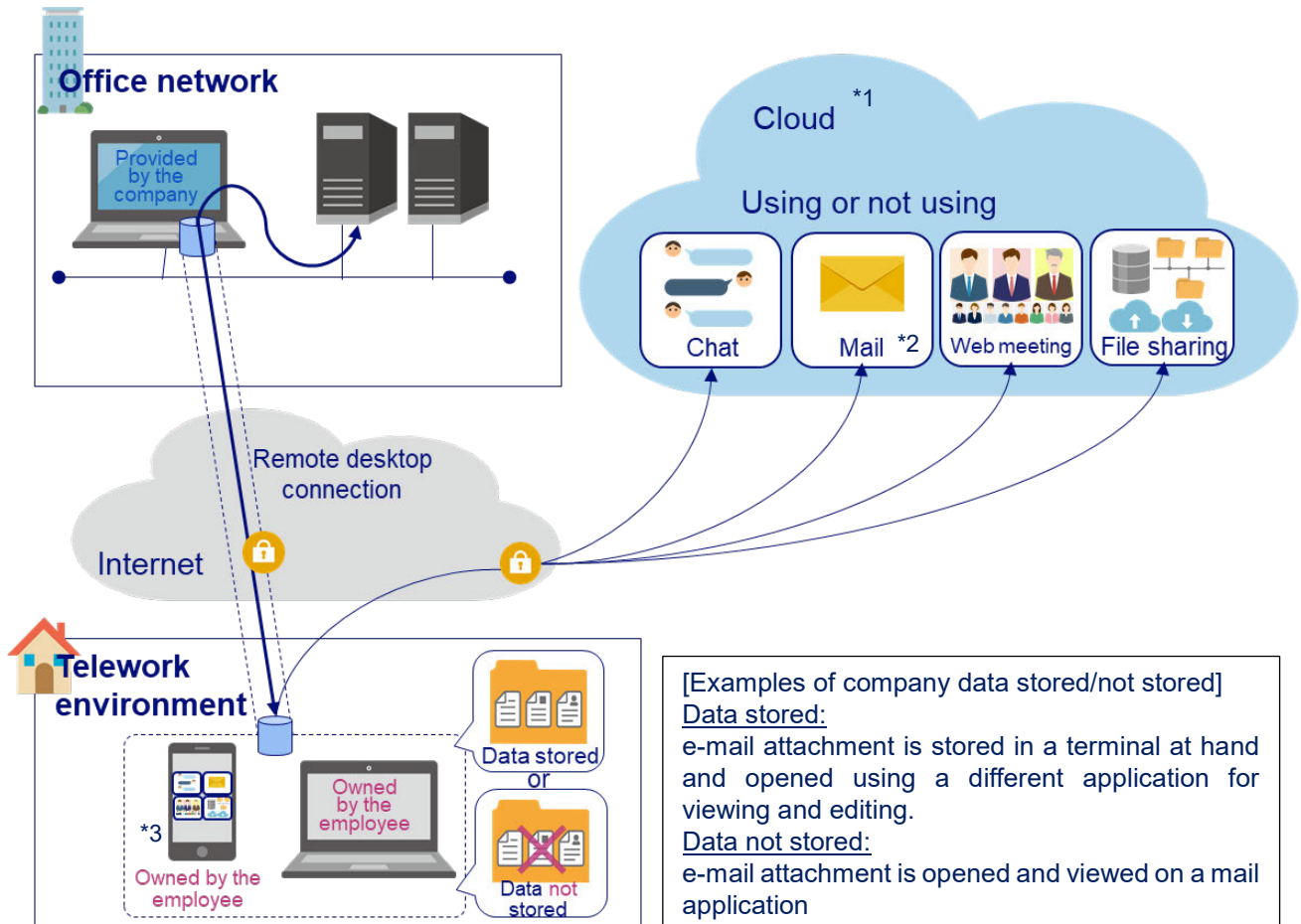


*1 "Using a cloud service" applies to using all or part of the service.

*2 Use of mail service provided by ISP also falls under use of cloud service.

*3 Using an application of a tablet terminal or smartphone for mailing also falls under "using a cloud service."

(2) Work is done through remote desktop connection from the telework terminal owned by the employee to the terminal provided by the company. In this way, a business environment equal to that of the office can be established. The pattern includes simultaneous working on a telework terminal at hand.



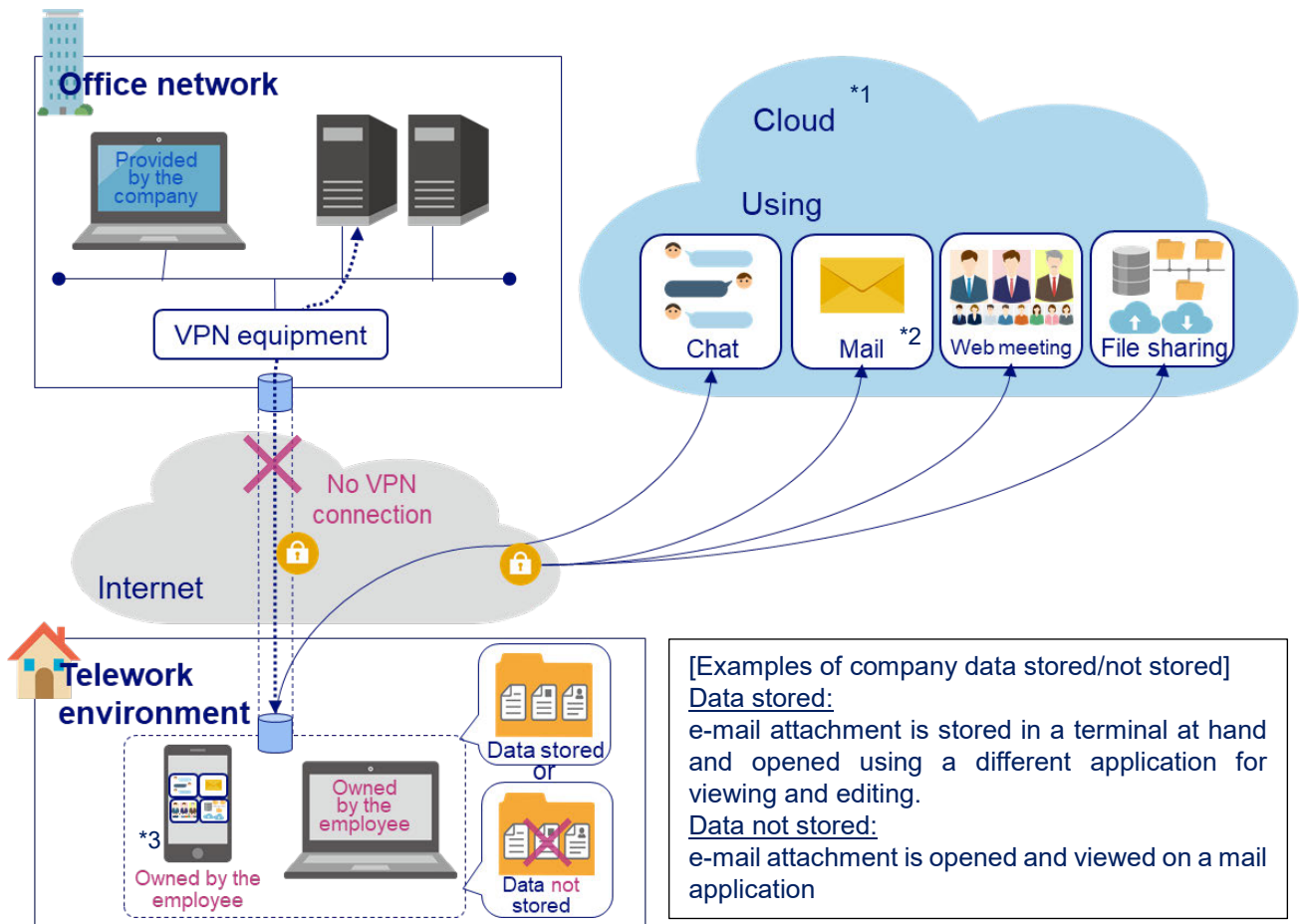
*1 "Using a cloud service" applies to using all or part of the service.

*2 Use of mail service provided by ISP also falls under use of cloud service.

*3 Using an application of a tablet terminal or smartphone for mailing also falls under "using a cloud service."

⑥ Employee terminals not connected to the company pattern (cloud service type)

Work is done by connecting the telework terminal owned by the employee to application software provided by a cloud service on the Internet. Its feature is that the terminal is not connected to the office network. Use of a cloud service can establish a work environment equal to that of the office. The pattern includes simultaneous working on a telework terminal at hand.



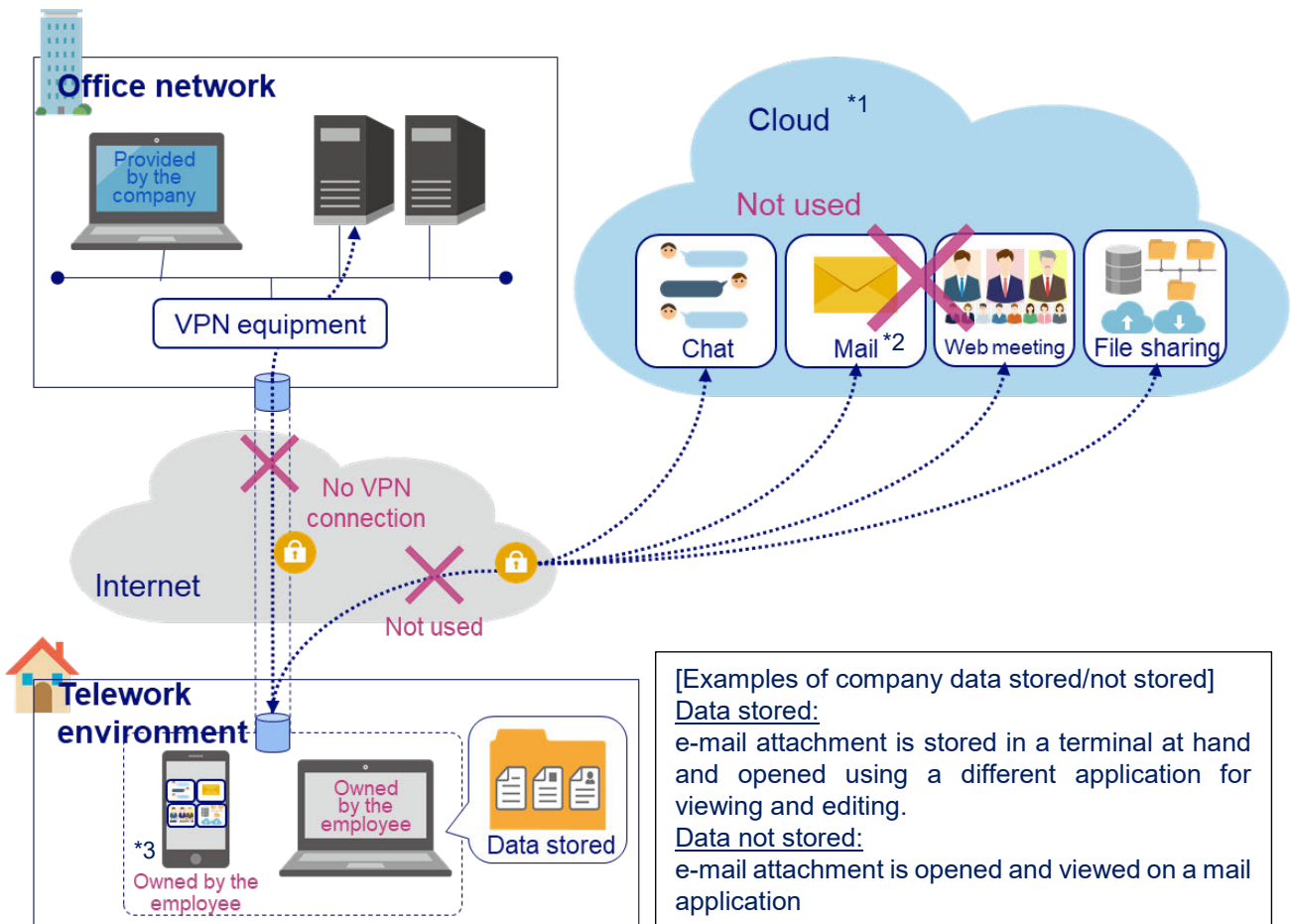
*1 "Using a cloud service" applies to using all or part of the service.

*2 Use of mail service provided by ISP also falls under use of cloud service.

*3 Using an application of a tablet terminal or smartphone for mailing also falls under "using a cloud service."

⑦ **Terminal owned by the employee not connected to the company pattern (work-at-hand type)**

Work is done by taking out the telework terminal owned by the employee to a telework environment and editing and viewing the data stored in the terminal in advance. Its feature is that the terminal is not connected to the office network and cloud service is not used. Only limited work is carried out.



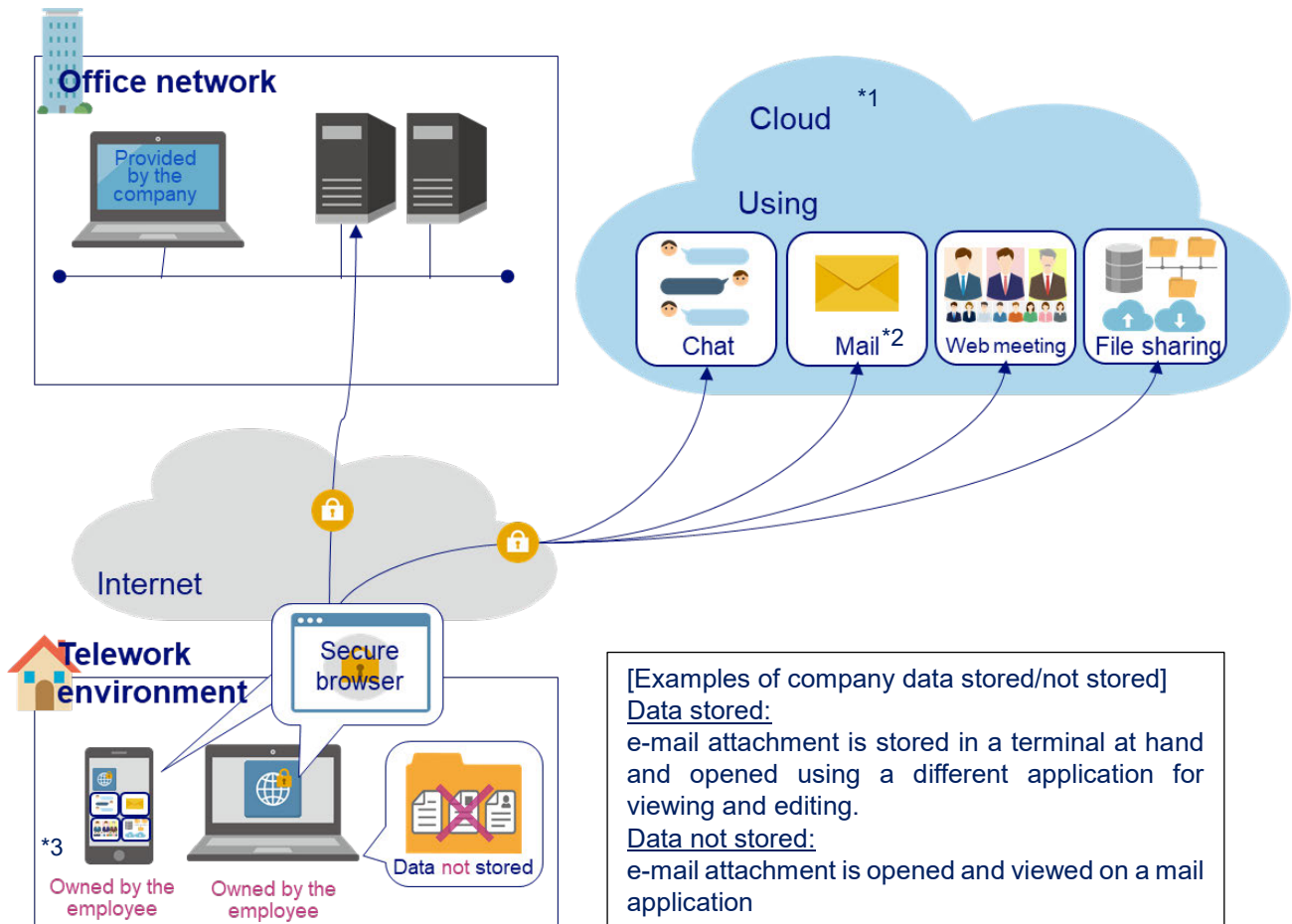
*1 "Using a cloud service" applies to using all or part of the service.

*2 Use of mail service provided by ISP also falls under use of cloud service.

*3 Using an application of a tablet terminal or smartphone for mailing also falls under "using a cloud service."

⑧ Terminal owned by the employee and secure browser pattern

Work is done by accessing application software provided by an internal system or a cloud service through a special internet browser (secure browser) from the telework terminal owned by the employee. Its feature is that data is not stored in the terminal. Only limited work is carried out.



*1 "Using a cloud service" applies to using all or part of the service.

*2 Use of mail service provided by ISP also falls under use of cloud service.

*3 Using an application of a tablet terminal or smartphone for mailing also falls under "using a cloud service."

4 Explanation of Possible Threats in a Telework Environment

For people of SMEs, etc. to deepen their understanding of possible threats in a telework environment, this section outlines each type of threat and provides brief explanations of the processes of exposure and their influence on business. The explanation can be used by people in charge of system to convince the importance and need of security measures in the organization when they promote the measures.

For individual threats, individual threat types and damages anticipated from them for typical attack methods and attack methods that are increasing and attracting attention are illustrated in three steps of cause, process and damage.

The step (cause, process or damage) where each measure in Part 2-1 Security Measure Checklists for Each Pattern is effective is shown in “Relevant checklist measure” in the illustration.

(A) Explanation of threats: malware infection

① What is malware infection?

Malware is the general term for malicious software and codes created for the purpose of unauthorized and harmful operations. What are generally called “computer viruses” are also a type of malware.

Ransomware, which is currently in the news, is a type of malware that locks the infected terminals or disables them by encrypting the data in the terminals.



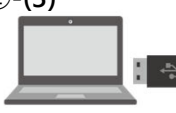




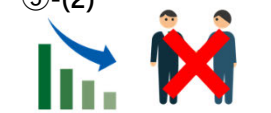
Malware infection refers to integration of malicious software or codes in the affected software.

Infection of typical malware can cause interference with the original operation of the equipment, suspension of business due to data destruction, information leak through transmission of data outside. In addition, you can become “an assailant” if your equipment is used for attacking others.

Infection with ransomware can lead to “suspension of business” due to encryption of data in the infected terminal and, through the terminal, files stored in the internal file servers, external hard disc and other external storage media. In this case, the attacker demands money in exchange for restoration. However, paying money is not recommended because restoration is not guaranteed for the payment and it would encourage further attack.









② Examples of malware infection

○ Typical malware

Examples of malware infection			Step No.	Number of checklist measure
Step 1 Cause*	①-(1)  Receiving and opening a mail with attached file	①-(2)  Viewing a malicious site and downloading software	①-(1)	2-1 2-2 5-1 5-2
	①-(3)  Connecting an USB memory		①-(2) ①-(3)	2-1 5-1 5-2
Step 2 Process	②  Malware infection	③  Connecting to an attacker server without permission	② ③ ④	2-1 2-3
		④  Stealing important information and transmitting outside		
Step 3 Damage	⑤-(1)  Leak of personal information with obligation for compensation	⑤-(2)  Ruining the trust of business partners and clients and losing their business due to malware infection	⑤-(1) ⑤-(2)	7-1 7-2 7-3

*Because attacks are increasingly diverse every day, malware infection can occur without opening an attached file, downloading software or other operations listed in the examples above.

○ Examples of ransomware

Examples of Ransomware			Step No.	Number of checklist measure	
Step 1 Cause	①-(1)  Receiving and opening a mail with attached file	①-(2)  Viewing a malicious site and downloading software	①-(3)  Connecting an USB memory	①-(1)	2-1 2-2 5-1 5-2
				①-(2) ①-(3)	2-1 5-1 5-2
Step 2 Process	②  Ransomware infection	③  Data in the terminal or connectable file server / external storage media are encrypted	④  Threatening and demanding money for restoration	② ③ ④	2-1 2-3
Step 3 Damage	⑤-(1)  The information is not restored with negative influence on the business	⑤-(2)  Ruining the trust of business partners and clients and losing their business due to malware infection		⑤-(1) ⑤-(2)	7-1 7-2 7-3

(B) Explanation of threats: Unauthorized access


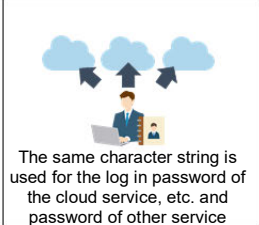
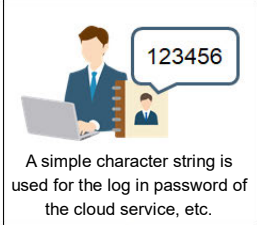

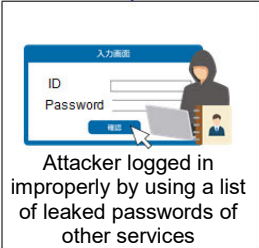

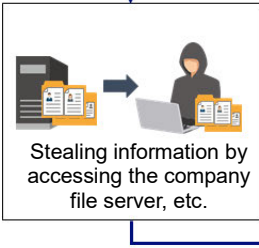



① What is unauthorized access?

Unauthorized access refers to the following acts:

- Invasion by a third party without access permission by abusing vulnerabilities of the computer OS, application software or hardware
- Receiving services that are provided to the users by using their ID and password without their permission

An authorized access can cause “information leak”, “compensation liability” associated to the leak, “loss of trust” of business partners and clients and “losing business.”

② Examples of unauthorized access

Examples of Unauthorized access			Step No.	Number of checklist measure		
Step 1 Cause	 <p>Failure to respond to publication of vulnerability of VPN equipment</p>	 <p>The same character string is used for the log in password of the cloud service, etc. and password of other service</p>	 <p>A simple character string is used for the log in password of the cloud service, etc.</p>	①-A	5-1、5-2 5-3、5-4	
				①-B	9-4	
				①-C	9-1、9-2 9-3、10-2	
Step 2 Process	 <p>Attacker abused the vulnerability and broke into the company system through the authentication process</p>	 <p>Attacker logged in improperly by using a list of leaked passwords of other services</p>	 <p>Unauthorized log in by guessing the password</p>	②-A	3-1 3-2 8-3 10-1 10-3	
	 <p>Stealing information by accessing the company file server, etc.</p>	 <p>Stealing client information or/and trade secret information by accessing the cloud service</p>	②-B ②-C			3-1 8-3 9-3 10- 10-3
	 <p>Leak of customer information incurred liability for compensation</p>		 <p>Exposure of unauthorized access ruined the trust and business of business partners and customers.</p>		⑤-(1) ⑤-(2)	7-1 7-2 7-3


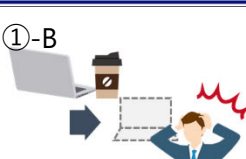
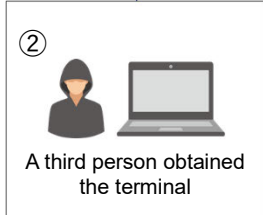
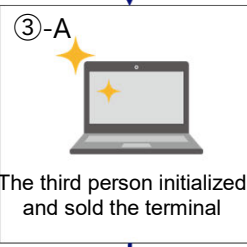
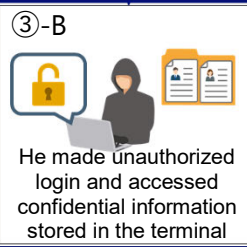

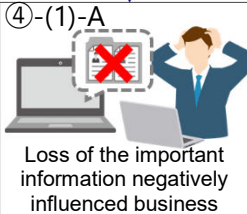
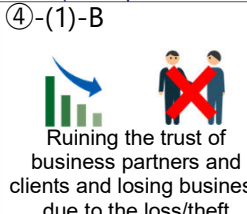
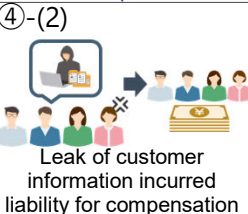
(C) Explanation of threats: loss/theft of terminal

① What does the loss/theft of terminals mean?

This refers to theft of physical devices including terminals by a third party or loss of such devices.

Theft or loss of a terminal can cause “information leak”, “compensation liability” associated to the leak, “loss of trust” of business partners and clients and “losing their business.”

② Examples of loss/theft of terminal

Examples of Information tapping		Step No.	Number of checklist measure
Step 1 Cause	<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid black; padding: 5px; width: 45%;"> <p>①-A </p> <p>Left and lost the terminal in the satellite office</p> </div> <div style="border: 1px solid black; padding: 5px; width: 45%;"> <p>①-B </p> <p>A terminal was stolen when the worker temporarily left it in the seat in a café, etc.</p> </div> </div>	<p>①-A</p> <p>①-B</p>	<p>8-1</p> <p>8-2</p>
Step 2 Process	<p>② </p> <p>A third person obtained the terminal</p>	<p>③-B</p> <p>③-C</p>	<p>8-3</p> <p>8-4</p>
	<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid black; padding: 5px; width: 30%;"> <p>③-A </p> <p>The third person initialized and sold the terminal</p> </div> <div style="border: 1px solid black; padding: 5px; width: 30%;"> <p>③-B </p> <p>He made unauthorized login and accessed confidential information stored in the terminal</p> </div> <div style="border: 1px solid black; padding: 5px; width: 30%;"> <p>③-C </p> <p>He removed the hard disk and accessed confidential information stored in it</p> </div> </div>		
Step 3 Damage	<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid black; padding: 5px; width: 30%;"> <p>④-(1)-A </p> <p>Loss of the important information negatively influenced business</p> </div> <div style="border: 1px solid black; padding: 5px; width: 30%;"> <p>④-(1)-B </p> <p>Ruining the trust of business partners and clients and losing business due to the loss/theft</p> </div> <div style="border: 1px solid black; padding: 5px; width: 30%;"> <p>④-(2) </p> <p>Leak of customer information incurred liability for compensation</p> </div> </div>	<p>④-(1)-A</p> <p>④-(1)-B</p> <p>④-(2)</p>	<p>7-1</p> <p>7-2</p> <p>7-3</p>


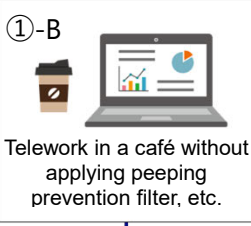

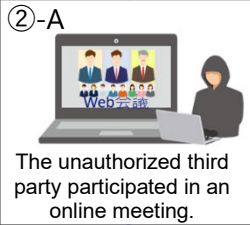
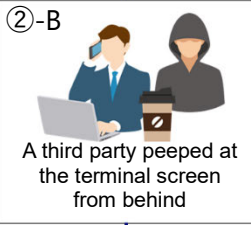

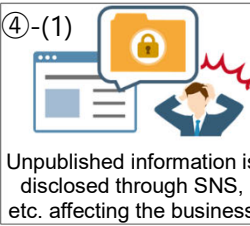

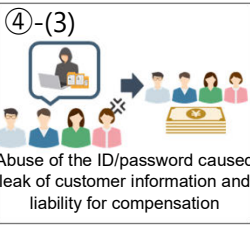
(E) Information tapping

① What does information tapping mean?

It refers to stealing glances at data exchanged on network or peeping at a terminal.

If information was tapped, it can cause “information leak”, “compensation liability” associated to the leak, “loss of trust” of business partners and clients and “losing their business.”

② Examples of information tapping

Examples of Information tapping			Step No.	Number of checklist measure	
Step 1 Cause	①-A  A third party improperly obtained the URL of an online meeting	①-B  Telework in a café without applying peeping prevention filter, etc.	①-C  The worker used a radio access point of a café.	①-A	3-4
				①-B	4-1
				①-C	6-1、6-2
Step 2 Process	②-A  The unauthorized third party participated in an online meeting.	②-B  A third party peeped at the terminal screen from behind	②-C  A third party wirelessly tapped communication	②-A	3-3、3-4 3-5、8-3 8-5
				②-B	4-1
				②-C	6-1 6-2 6-3
Step 3 Damage	④-(1)  Unpublished information is disclosed through SNS, etc. affecting the business	④-(2)  Ruining the trust of business partners and clients and losing their business	④-(3)  Abuse of the ID/password caused leak of customer information and liability for compensation	④-(1) ④-(2) ④-(3)	7-1 7-2 7-3

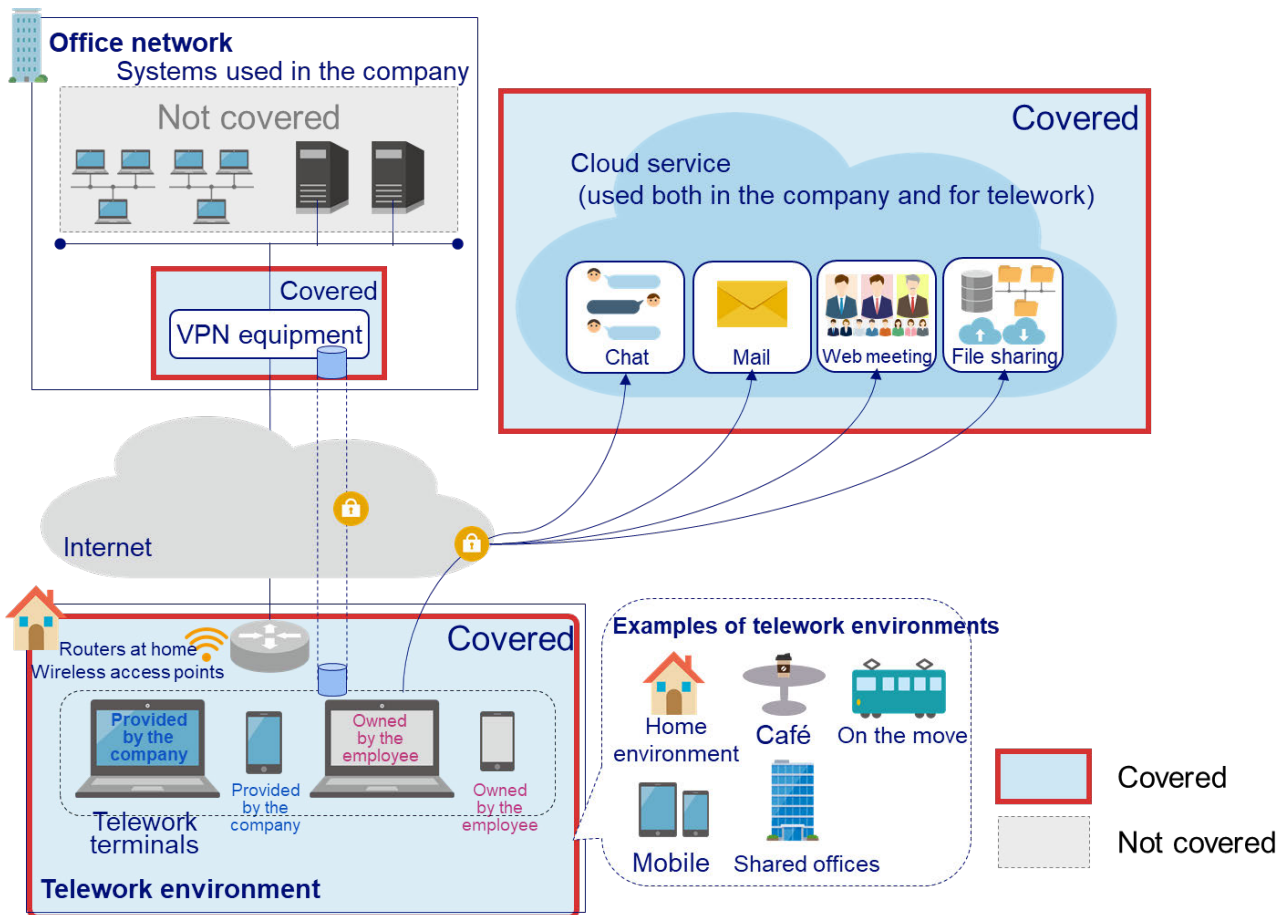
Part 2

1 Security Measure Checklist for Each Pattern

This section presents specific measures in the form of checklist for SMEs, etc. to check security measures to be implemented for each telework pattern when introducing and using telework. Priority level of each measure is defined for efficient promotion of security measures.

(A) Scope of Security Measures

The security measures of the checklists cover systems and equipment necessary for introduction and use of telework.



The figure of the preceding page covers:

- Telework environment
- Cloud service (environment used both in the company and for telework) and
- VPN equipment in the office network, which is used for access outside and inside of the company. Systems used in the company (office network), etc. regardless of introduction of telework are not considered in the checklists. It is recommended to consider security measures separately for them.

(B) Approach to priority level

Priority level of individual measures is defined as follows. It is recommended to begin and implement measures with higher priority.

Priority level : ◎

- Measures with a high level of security importance (highly effective when implemented) and a low degree of difficulty in implementation (requiring less knowledge and additional costs)

Priority level : ○

- Measures with a high level of security importance (highly effective when implemented) and not very difficult to implement (requiring knowledge of IT security but not difficult to install)
- Measures with a medium level of importance (certain effect is expected when implemented) and a low degree of difficulty in implementation (requiring less knowledge and fewer additional costs)

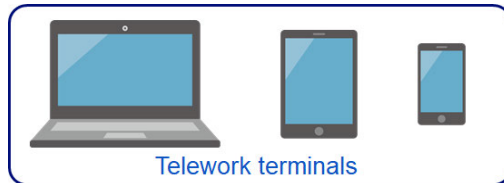
(C) Security Measure Checklist

① Company terminals and VPN/remote desktop pattern

“Telework terminals” among the terms used in the checklist are divided into the following three categories:

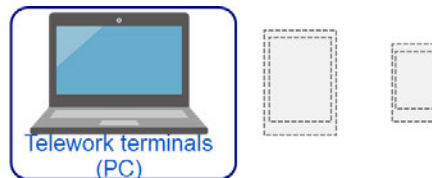
Telework terminal:

Applicable to personal computers and smart devices (tablet and Smartphone) used for telework.



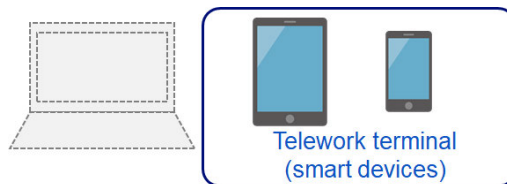
Telework terminal (PC):

Applicable to personal computers used for telework.



Telework terminal (smart devices):

Applicable to smart devices (tablet and Smartphone) used for telework.



◆ Measures to be taken beforehand

No.	Category	Description	Possible threats
1-1	Asset management	<input type="checkbox"/> Only the telework terminals permitted by the company are used for telework and all terminals used and their users are known.	Malware infection, Unauthorized access, Theft/loss
1-2	Asset management	<input type="checkbox"/> All systems used for telework and important information* handled in telework are known. * Trade secrets and other information necessary for the business and valuable for the organization, personal information of customers and employees and other information involving responsibility for management	Unauthorized access, Information tapping

* Regarding the measures of the category “asset management,” management of information assets is not a measure that directly addresses security issues but presupposed for implementation of other measures.

Items of Priority ◎

No.	Category	Description	Possible threats
2-1	Malware countermeasure	<input type="checkbox"/> Anti-virus software is installed on the telework terminals and real time scan is enabled in setting.* Setting of automatic update of the anti-virus software definition file is made or a rule is created to manually update to the latest version. * Installation is not needed if you use the anti-virus software that is standard-install in Windows products or in the case of iOS products, if you use only applications that are installed in a way whose safety has been confirmed (use of official application store, for example.)	Malware infection
3-1	Access control (logical)	<input type="checkbox"/> Access control through the system and password setting, etc. for important information itself ensures that only admitted people can use the important information.	Unauthorized access
4-1	Access control (physical)	<input type="checkbox"/> Peep prevention filter is applied on the telework terminals and a rule is made to lock the screen when leaving one's seat.	Information tapping
5-1	Vulnerability management	<input type="checkbox"/> OS versions or application software no longer supported by the manufacturer is not used for the telework terminals.	Unauthorized access
5-2	Vulnerability management	<input type="checkbox"/> The latest security update is applied to the OS and application software of the telework terminals.	Unauthorized access
5-4	Vulnerability management	<input type="checkbox"/> Products no longer supported by the manufacturer are not used and the latest security update is applied to the VPN equipment used for remote access by the telework terminals to the company, remote desktop application, etc. of the company terminal.	Unauthorized access
7-1	Incident response and management	<input type="checkbox"/> In preparation for information security incidents, policies to address actual and possible incidents (when a suspicious email is opened, for example) have been decided and a system of communication to relevant parties has been established.	Malware infection, Unauthorized access, Theft/loss, Information tapping
8-1	Data protection	<input type="checkbox"/> Positional information of lost telework terminals (smart devices) can be detected.	Theft/loss
9-1	Authentication	<input type="checkbox"/> "Long" and "complicated" passwords that are difficult to detect are set for the log-in account of the telework terminals and the account of each system used for telework. Setting is made to enforce a certain level of password strength wherever possible.	Unauthorized access
9-2	Authentication	<input type="checkbox"/> Passwords to log in the telework terminals and the initial password of the account of each system used in telework are changed.	Unauthorized access

◆ Items of Priority level: ○

No.	Category	Description	Possible threats
2-2	Malware countermeasure	<input type="checkbox"/> Awareness is promoted not to open a suspicious email, click the URL included in the mail or open its attached file. When the email product we use has a function to exclude suspicious emails, the function is enabled. (This measure is not included if cloud service (web mail) is not used.)	Malware infection,
2-3	Malware countermeasure	<input type="checkbox"/> Installation of applications to the telework terminals is limited to installation using methods whose safety can be confirmed (an official application store for example.)	Malware infection
3-2	Access control (logical)	<input type="checkbox"/> Access other than from ports and IP addresses that are necessary for accessing the internal system through the Internet is obstructed by firewalls, routers, etc. on the boundary between the internal network and the Internet.	Unauthorized access
3-3	Access control (logical)	<input type="checkbox"/> The organizer of an online meeting verifies the identity of the participants at the beginning of the meeting and when an additional participant joined midway. (Not included when cloud service (online meeting) is not used.)	Information tapping
3-4	Access control (logical)	<input type="checkbox"/> URL for access to an online meeting and passwords to participate in the meeting are not told to the members who don't need them. Password setting is enforced for all participants wherever possible. (Not included when cloud service (online meeting) is not used.)	Information tapping
3-5	Access control (logical)	<input type="checkbox"/> Organizer of an online meeting makes the meeting progress appropriately by dismissing inappropriate participants as needed, for example. (Not included when cloud service (online meeting) is not used.)	Information tapping
5-3	Vulnerability management	<input type="checkbox"/> Wi-Fi routers at home, mobile Wi-Fi, etc. that are no longer supported by the manufacturer are not used for telework and the latest firmware is used for them.	Unauthorized access
6-1	Encryption of communication	<input type="checkbox"/> When using cloud service (e.g. Web mail, chat, online meeting, cloud storage) for telework, HTTPS communication and correctness of the URL to connect are confirmed (not included when no cloud service is used.)	Information tapping
6-2	Encryption of communication	<input type="checkbox"/> When connecting to a cloud service or a service where an ID, password and other information is entered, it is confirmed before use that this is encrypted HTTPS communication.	Information tapping
6-3	Encryption of communication	<input type="checkbox"/> When using a Wi-Fi router or other equipment at home, WPA2 is used for Wi-Fi security and passwords that are difficult for a third party to guess are used.	Information tapping
7-2	Incident response and management	<input type="checkbox"/> Time synchronization setting is made between the telework terminals and the systems that the terminals access.	Malware infection, Unauthorized access, Theft/loss, Information tapping

No.	Category	Description	Possible threats
7-3	Incident response and management	<input type="checkbox"/> Access log is collected for access by the telework terminals to the internal system.	Malware infection, Unauthorized access, Theft/loss, Information tapping
8-2	Data protection	<input type="checkbox"/> When a telework terminal (smart device) is lost, MDM* or similar software is introduced to remotely erase data and force security settings including login authentication policy and hard disc encryption. * Abbreviation from Mobile Device Management that refers to unitary management and operation of smart devices including Smartphone and software that provides the function.	Theft/loss
8-3	Data protection	<input type="checkbox"/> Built-in storage medium including hard disc and flash memory* are encrypted in order to prevent information leak when a telework terminal is stolen or lost** (not included when company data is not stored in the terminals.) * refers to "nonvolatile semiconductor memory" that a kind of storage medium different from hard disk. This storage medium can hold data after turning off of power. ** This is not required for iOS products that are encrypted at the initial state.	Theft/loss
8-4	Data protection	<input type="checkbox"/> Important information is not stored in the telework terminals in principle. When it is necessary to store important information*, the file is encrypted (password setting, for example.) (not included when company data is not stored in the terminals.) * This refers to local file storage in the telework terminals. Storing in a file server, cloud storage or in the system of various cloud services is not included here.	Unauthorized access, Theft/loss
8-5	Data protection	<input type="checkbox"/> When implementing an online meeting, important information is not included in the title or agenda of the meeting, password setting and automatic deletion after designated time are implemented for video files of the meeting. Setting is made to force the rules above wherever possible. (Not included when cloud service (online meeting) is not used.)	Information tapping
9-3	Authentication	<input type="checkbox"/> The accounts of the telework terminals and each system used for telework are set to reject any password input after a predetermined number of input errors.	Unauthorized access
9-4	Authentication	<input type="checkbox"/> It is set to request multifactor authentication for access to individual systems used for telework.	Unauthorized access
10-1	Privilege management	<input type="checkbox"/> Administrator rights of the telework terminals and each system used for telework are given to the minimum number of people necessary for the business.	Unauthorized access

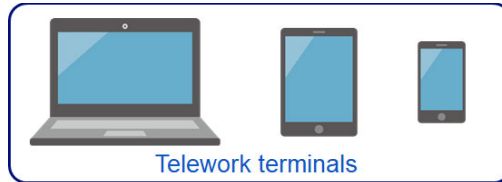
No.	Category	Description	Possible threats
10-2	Privilege management	<input type="checkbox"/> A strict password policy is applied to the passwords of administrator rights of the telework terminals and individual systems used for telework.	Unauthorized access
10-3	Privilege management	<input type="checkbox"/> Administrator rights of the telework terminals and each system used for telework are used only for operations where the rights are necessary.	Unauthorized access

② **Company terminals not connected to the company pattern (cloud service type)**

“Telework terminals” among the terms used in the checklist are divided into the following three categories:

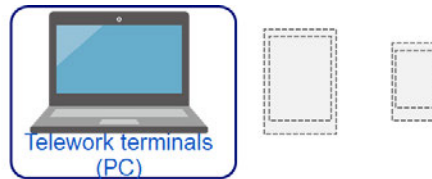
Telework terminal:

Applicable to personal computers and smart devices (tablet and Smartphone) used for telework



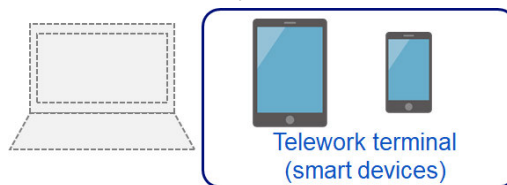
Telework terminal (PC):

Applicable to personal computers used for telework



Telework terminal (smart devices) :

Applicable to smart devices (tablet and Smartphone) used for telework



◆ Measures to be taken beforehand

No.	Category	Description	Possible threats
1-1	Asset management	<input type="checkbox"/> Only the telework terminals permitted by the company are used for telework and all terminals used and their users are known.	Malware infection, Unauthorized access, Theft/loss
1-2	Asset management	<input type="checkbox"/> All systems used for telework and important information* handled in telework are known. * Trade secrets and other information necessary for the business and valuable for the organization, personal information of customers and employees and other information involving responsibility for management	Unauthorized access, Information tapping

* Regarding the measures of the category “asset management,” management of information assets is not a measure that directly addresses security issues but presupposed for implementation of other measures.

Items of Priority ②

No.	Category	Description	Possible threats
2-1	Malware countermeasure	<input type="checkbox"/> Anti-virus software is installed on the telework terminals and real time scan is enabled in setting.*. Setting of automatic update of the anti-virus software definition file is made or a rule is created to manually update to the latest version. * Installation is not needed if you use the anti-virus software that is standard-install in Windows products or in the case of iOS products, if you use only applications that are installed in a way whose safety has been confirmed (use of official application store, for example.)	Malware infection
3-1	Access control (logical)	<input type="checkbox"/> Access control through the system and password setting, etc. for important information itself ensures that only admitted people can use the important information.	Unauthorized access
4-1	Access control (physical)	<input type="checkbox"/> Peep prevention filter is applied on the telework terminals and a rule is made to lock the screen when leaving one's seat.	Information tapping
5-1	Vulnerability management	<input type="checkbox"/> OS versions or application software no longer supported by the manufacturer is not used for the telework terminals.	Unauthorized access
5-2	Vulnerability management	<input type="checkbox"/> The latest security update is applied to the OS and application software of the telework terminals.	Unauthorized access
7-1	Incident response and management	<input type="checkbox"/> Products no longer supported by the manufacturer are not used and the latest security update is applied to the VPN equipment used for remote access by the telework terminals to the company, remote desktop application, etc. of the company terminal.	Malware infection, Unauthorized access, Theft/loss, Information tapping
8-1	Data protection	<input type="checkbox"/> Positional information of lost telework terminals (smart devices) can be detected.	Theft/loss
9-1	Authentication	<input type="checkbox"/> "Long" and "complicated" passwords that are difficult to detect are set for the log-in account of the telework terminals and the account of each system used for telework. Setting is made to enforce a certain level of password strength wherever possible.	Unauthorized access
9-2	Authentication	<input type="checkbox"/> Passwords to log in the telework terminals and the initial password of the account of each system used in telework are changed.	Unauthorized access

◆Items of Priority level: ○

No.	Category	Description	Possible threats
2-2	Malware countermeasure	<input type="checkbox"/> Awareness is promoted not to open a suspicious email, click the URL included in the mail or open its attached file. When the email product we use has a function to exclude suspicious emails, the function is enabled. (This measure is not included if cloud service (web mail) is not used.)	Malware infection
2-3	Malware countermeasure	<input type="checkbox"/> Installation of applications to the telework terminals is limited to installation using methods whose safety can be confirmed (an official application store for example.)	Malware infection
3-3	Access control (logical)	<input type="checkbox"/> Access other than from ports and IP addresses that are necessary for accessing the internal system through the Internet is obstructed by firewalls, routers, etc. on the boundary between the internal network and the Internet.	Information tapping
3-4	Access control (logical)	<input type="checkbox"/> The organizer of an online meeting verifies the identity of the participants at the beginning of the meeting and when an additional participant joined midway. (Not included when cloud service (online meeting) is not used.)	Information tapping
3-5	Access control (logical)	<input type="checkbox"/> URL for access to an online meeting and passwords to participate in the meeting are not told to the members who don't need them. Password setting is enforced for all participants wherever possible. (Not included when cloud service (online meeting) is not used.)	Information tapping
5-3	Vulnerability management	<input type="checkbox"/> Wi-Fi routers at home, mobile Wi-Fi, etc. that are no longer supported by the manufacturer are not used for telework and the latest firmware is used for them.	Unauthorized access
6-1	Encryption of communication	<input type="checkbox"/> When using cloud service (e.g. Web mail, chat, online meeting, cloud storage) for telework, HTTPS communication and correctness of the URL to connect are confirmed (not included when no cloud service is used.)	Information tapping
6-2	Encryption of communication	<input type="checkbox"/> When connecting to a cloud service or a service where an ID, password and other information is entered, it is confirmed before use that this is encrypted HTTPS communication.	Information tapping
6-3	Encryption of communication	<input type="checkbox"/> When using a Wi-Fi router or other equipment at home, WPA2 is used for Wi-Fi security and passwords that are difficult for a third party to guess are used.	Information tapping
7-2	Incident response and management	<input type="checkbox"/> Time synchronization setting is made between the telework terminals and the systems that the terminals access.	Malware infection, Unauthorized access, Theft/loss, Information tapping

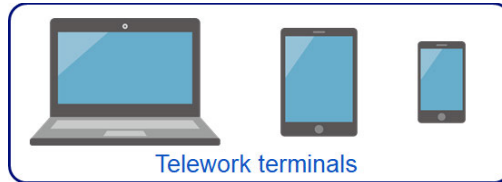
No.	Category	Description	Possible threats
8-2	Data protection	<input type="checkbox"/> When a telework terminal (smart device) is lost, MDM* or similar software is introduced to remotely erase data and force security settings including login authentication policy and hard disc encryption. * Abbreviation from Mobile Device Management that refers to unitary management and operation of smart devices including Smartphone and software that provides the function.	Theft/loss
8-3	Data protection	<input type="checkbox"/> Built-in storage medium including hard disc and flash memory* are encrypted in order to prevent information leak when a telework terminal is stolen or lost** (not included when company data is not stored in the terminals.) * refers to "nonvolatile semiconductor memory" that a kind of storage medium different from hard disk. This storage medium can hold data after turning off of power. ** This is not required for iOS products that are encrypted at the initial state.	Theft/loss
8-4	Data protection	<input type="checkbox"/> Important information is not stored in the telework terminals in principle. When it is necessary to store important information*, the file is encrypted (password setting, for example.) (not included when company data is not stored in the terminals.) * This refers to local file storage in the telework terminals. Storing in a file server, cloud storage or in the system of various cloud services is not included here.	Unauthorized access, Theft/loss
8-5	Data protection	<input type="checkbox"/> When implementing an online meeting, important information is not included in the title or agenda of the meeting, password setting and automatic deletion after designated time are implemented for video files of the meeting. Setting is made to force the rules above wherever possible. (Not included when cloud service (online meeting) is not used.)	Information tapping
9-3	Authentication	<input type="checkbox"/> The accounts of the telework terminals and each system used for telework are set to reject any password input after a predetermined number of input errors.	Unauthorized access
9-4	Authentication	<input type="checkbox"/> It is set to request multifactor authentication for access to individual systems used for telework.	Unauthorized access
10-1	Privilege management	<input type="checkbox"/> Administrator rights of the telework terminals and each system used for telework are given to the minimum number of people necessary for the business.	Unauthorized access
10-2	Privilege management	<input type="checkbox"/> A strict password policy is applied to the passwords of administrator rights of the telework terminals and individual systems used for telework.	Unauthorized access
10-3	Privilege management	<input type="checkbox"/> Administrator rights of the telework terminals and each system used for telework are used only for operations where the rights are necessary.	Unauthorized access

③ **Company terminals not connected to the company pattern (work-at-hand type)**

“Telework terminals” among the terms used in the checklist are divided into the following three categories:

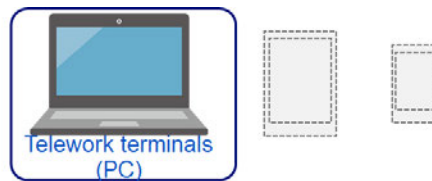
Telework terminal:

Applicable to personal computers and smart devices (tablet and Smartphone) used for telework



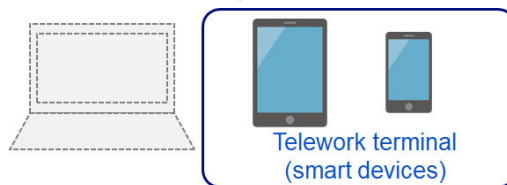
Telework terminal (PC):

Applicable to personal computers used for telework



Telework terminal (smart devices) :

Applicable to smart devices (tablet and Smartphone) used for telework



◆ Measures to be taken beforehand

No.	Category	Description	Possible threats
1-1	Asset management	<input type="checkbox"/> Only the telework terminals permitted by the company are used for telework and all terminals used and their users are known.	Malware infection, Unauthorized access, Theft/loss
1-2	Asset management	<input type="checkbox"/> All systems used for telework and important information* handled in telework are known. * Trade secrets and other information necessary for the business and valuable for the organization, personal information of customers and employees and other information involving responsibility for management	Unauthorized access, Information tapping

* Regarding the measures of the category “asset management,” management of information assets is not a measure that directly addresses security issues but presupposed for implementation of other measures.

Items of Priority ②

No.	Category	Description	Possible threats
2-1	Malware countermeasure	<input type="checkbox"/> Anti-virus software is installed on the telework terminals and real time scan is enabled in setting.* Setting of automatic update of the anti-virus software definition file is made or a rule is created to manually update to the latest version. * Installation is not needed if you use the anti-virus software that is standard-install in Windows products or in the case of iOS products, if you use only applications that are installed in a way whose safety has been confirmed (use of official application store, for example.)	Malware infection
3-1	Access control (logical)	<input type="checkbox"/> Access control through the system and password setting, etc. for important information itself ensures that only admitted people can use the important information.	Unauthorized access
4-1	Access control (physical)	<input type="checkbox"/> Peep prevention filter is applied on the telework terminals and a rule is made to lock the screen when leaving one's seat.	Information tapping
5-1	Vulnerability management	<input type="checkbox"/> OS versions or application software no longer supported by the manufacturer is not used for the telework terminals.	Unauthorized access
5-2	Vulnerability management	<input type="checkbox"/> The latest security update is applied to the OS and application software of the telework terminals.	Unauthorized access
7-1	Incident response and management	<input type="checkbox"/> In preparation for information security incidents, policies to address actual and possible incidents (when a suspicious email is opened, for example) have been decided and a system of communication to relevant parties has been established.	Malware infection, Unauthorized access, Theft/loss, Information tapping
8-1	Data protection	<input type="checkbox"/> Positional information of lost telework terminals (smart devices) can be detected.	Theft/loss
9-1	Authentication	<input type="checkbox"/> "Long" and "complicated" passwords that are difficult to detect are set for the log-in account of the telework terminals and the account of each system used for telework. Setting is made to enforce a certain level of password strength wherever possible.	Unauthorized access
9-2	Authentication	<input type="checkbox"/> Passwords to log in the telework terminals and the initial password of the account of each system used in telework are changed.	Unauthorized access

◆ Items of Priority level: ○

No.	Category	Description	Possible threats
2-3	Malware countermeasure	<input type="checkbox"/> Installation of applications to the telework terminals is limited to installation using methods whose safety can be confirmed (an official application store for example.)	Malware infection
5-3	Vulnerability management	<input type="checkbox"/> Wi-Fi routers at home, mobile Wi-Fi, etc. that are no longer supported by the manufacturer are not used for telework and the latest firmware is used for them.	Unauthorized access
6-2	Encryption of communication	<input type="checkbox"/> When connecting to a cloud service or a service where an ID, password and other information is entered, it is confirmed before use that this is encrypted HTTPS communication.	Information tapping
6-3	Encryption of communication	<input type="checkbox"/> When using a Wi-Fi router or other equipment at home, WPA2 is used for Wi-Fi security and passwords that are difficult for a third party to guess are used.	Information tapping
7-2	Incident response and management	<input type="checkbox"/> Time synchronization setting is made between the telework terminals and the systems that the terminals access.	Malware infection, Unauthorized access, Theft/loss, Information tapping
8-2	Data protection	<input type="checkbox"/> When a telework terminal (smart device) is lost, MDM* or similar software is introduced to remotely erase data and force security settings including login authentication policy and hard disc encryption. * Abbreviation from Mobile Device Management that refers to unitary management and operation of smart devices including Smartphone and software that provides the function.	Theft/loss
8-3	Data protection	<input type="checkbox"/> Built-in storage medium including hard disc and flash memory* are encrypted in order to prevent information leak when a telework terminal is stolen or lost** (not included when company data is not stored in the terminals.) * refers to "nonvolatile semiconductor memory" that a kind of storage medium different from hard disk. This storage medium can hold data after turning off of power. ** This is not required for iOS products that are encrypted at the initial state.	Theft/loss
8-4	Data protection	<input type="checkbox"/> Important information is not stored in the telework terminals in principle. When it is necessary to store important information*, the file is encrypted (password setting, for example.) (not included when company data is not stored in the terminals.) * This refers to local file storage in the telework terminals. Storing in a file server, cloud storage or in the system of various cloud services is not included here.	Unauthorized access, Theft/loss
9-3	Authentication	<input type="checkbox"/> The accounts of the telework terminals and each system used for telework are set to reject any password input after a predetermined number of input errors.	Unauthorized access

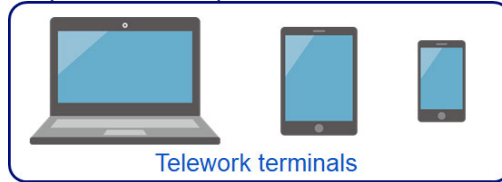
No.	Category	Description	Possible threats
9-4	Authentication	<input type="checkbox"/> It is set to request multifactor authentication for access to individual systems used for telework.	Unauthorized access
10-1	Privilege management	<input type="checkbox"/> Administrator rights of the terminals and each system used for telework are given to the minimum number of people necessary for the business.	Unauthorized access
10-2	Privilege management	<input type="checkbox"/> A strict password policy is applied to the passwords of administrator rights of the terminals and individual systems used for telework	Unauthorized access
10-3	Privilege management	<input type="checkbox"/> Administrator rights of the terminals and each system used for telework are used only for operations where the rights are necessary.	Unauthorized access

④ Employee terminals and secure browser pattern

“Telework terminals” among the terms used in the checklist are divided into the following three categories:

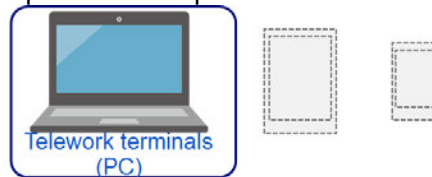
Telework terminal:

Applicable to personal computers and smart devices (tablet and Smartphone) used for telework



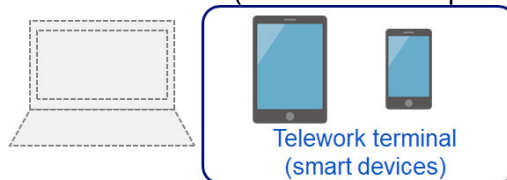
Telework terminal (PC):

Applicable to personal computers used for telework



Telework terminal (smart devices) :

Applicable to smart devices (tablet and Smartphone) used for telework



◆ Measures to be taken beforehand

No.	Category	Description	Possible threats
1-1	Asset management	<input type="checkbox"/> Only the telework terminals permitted by the company are used for telework and all terminals used and their users are known.	Malware infection, Unauthorized access, Theft/loss
1-2	Asset management	<input type="checkbox"/> All systems used for telework and important information* handled in telework are known. * Trade secrets and other information necessary for the business and valuable for the organization, personal information of customers and employees and other information involving responsibility for management	Unauthorized access, Information tapping

* Regarding the measures of the category “asset management,” management of information assets is not a measure that directly addresses security issues but presupposed for implementation of other measures.

Items of Priority ◎

No.	Category	Description	Possible threats
2-1	Malware countermeasure	<input type="checkbox"/> Anti-virus software is installed on the telework terminals and real time scan is enabled in setting.*. Setting of automatic update of the anti-virus software definition file is made or a rule is created to manually update to the latest version. * Installation is not needed if you use the anti-virus software that is standard-install in Windows products or in the case of iOS products, if you use only applications that are installed in a way whose safety has been confirmed (use of official application store, for example.)	Malware infection
3-1	Access control (logical)	<input type="checkbox"/> Access control through the system and password setting, etc. for important information itself ensures that only admitted people can use the important information.	Unauthorized access
4-1	Access control (physical)	<input type="checkbox"/> Peep prevention filter is applied on the telework terminals and a rule is made to lock the screen when leaving one's seat.	Information tapping
5-1	Vulnerability management	<input type="checkbox"/> OS versions or application software no longer supported by the manufacturer is not used for the telework terminals.	Unauthorized access
5-2	Vulnerability management	<input type="checkbox"/> The latest security update is applied to the OS and application software of the telework terminals.	Unauthorized access
7-1	Incident response and management	<input type="checkbox"/> In preparation for information security incidents, policies to address actual and possible incidents (when a suspicious email is opened, for example) have been decided and a system of communication to relevant parties has been established.	Malware infection, Unauthorized access, Theft/loss, Information tapping
8-1	Data protection	<input type="checkbox"/> Positional information of lost telework terminals (smart devices) can be detected.	Theft/loss
9-1	Authentication	<input type="checkbox"/> "Long" and "complicated" passwords that are difficult to detect are set for the log-in account of the telework terminals and the account of each system used for telework. Setting is made to enforce a certain level of password strength wherever possible.	Unauthorized access
9-2	Authentication	<input type="checkbox"/> Passwords to log in the telework terminals and the initial password of the account of each system used in telework are changed.	Unauthorized access

◆ Items of Priority level: ○

No.	Category	Description	Possible threats
2-2	Malware countermeasure	<input type="checkbox"/> Awareness is promoted not to open a suspicious email, click the URL included in the mail or open its attached file. When the email product we use has a function to exclude suspicious emails, the function is enabled. (This measure is not included if cloud service (web mail) is not used.)	Malware infection
2-3	Malware countermeasure	<input type="checkbox"/> Installation of applications to the telework terminals is limited to installation using methods whose safety can be confirmed (an official application store for example.)	Malware infection
3-2	Access control (logical)	<input type="checkbox"/> Access other than from ports and IP addresses that are necessary for accessing the internal system through the Internet is obstructed by firewalls, routers, etc. on the boundary between the internal network and the Internet.	Unauthorized access
3-3	Access control (logical)	<input type="checkbox"/> The organizer of an online meeting verifies the identity of the participants at the beginning of the meeting and when an additional participant joined midway. (Not included when cloud service (online meeting) is not used.)	Information tapping
3-4	Access control (logical)	<input type="checkbox"/> URL for access to an online meeting and passwords to participate in the meeting are not told to the members who don't need them. Password setting is enforced for all participants wherever possible. (Not included when cloud service (online meeting) is not used.)	Information tapping
3-5	Access control (logical)	<input type="checkbox"/> Organizer of an online meeting makes the meeting progress appropriately by dismissing inappropriate participants as needed, for example. (Not included when cloud service (online meeting) is not used.)	Information tapping
5-3	Vulnerability management	<input type="checkbox"/> Wi-Fi routers at home, mobile Wi-Fi, etc. that are no longer supported by the manufacturer are not used for telework and the latest firmware is used for them.	Unauthorized access
6-1	Encryption of communication	<input type="checkbox"/> When using cloud service (e.g. Web mail, chat, online meeting, cloud storage) for telework, HTTPS communication and correctness of the URL to connect are confirmed (not included when no cloud service is used.)	Information tapping
6-2	Encryption of communication	<input type="checkbox"/> When connecting to a cloud service or a service where an ID, password and other information is entered, it is confirmed before use that this is encrypted HTTPS communication.	Information tapping
6-3	Encryption of communication	<input type="checkbox"/> When using a Wi-Fi router or other equipment at home, WPA2 is used for Wi-Fi security and passwords that are difficult for a third party to guess are used.	Information tapping
7-2	Incident response and management	<input type="checkbox"/> Time synchronization setting is made between the telework terminals and the systems that the terminals access.	Malware infection, Unauthorized access, Theft/loss, Information tapping

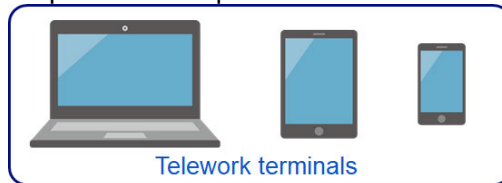
No.	Category	Description	Possible threats
7-3	Incident response and management	<input type="checkbox"/> Access log is collected for access by the telework terminals to the internal system.	Malware infection, Unauthorized access, Theft/loss, Information tapping
8-2	Data protection	<input type="checkbox"/> When a telework terminal (smart device) is lost, MDM* or similar software is introduced to remotely erase data and force security settings including login authentication policy and hard disc encryption. *Abbreviation from Mobile Device Management that refers to unitary management and operation of smart devices including Smartphone and software that provides the function.	Theft/loss
8-5	Data protection	<input type="checkbox"/> When implementing an online meeting, important information is not included in the title or agenda of the meeting, password setting and automatic deletion after designated time are implemented for video files of the meeting. Setting is made to force the rules above wherever possible. (Not included when cloud service (online meeting) is not used.)	Information tapping
9-3	Authentication	<input type="checkbox"/> The accounts of the telework terminals and each system used for telework are set to reject any password input after a predetermined number of input errors.	Unauthorized access
9-4	Authentication	<input type="checkbox"/> It is set to request multifactor authentication for access to individual systems used for telework.	Unauthorized access
10-1	Privilege management	<input type="checkbox"/> Administrator rights of the telework terminals and each system used for telework are given to the minimum number of people necessary for the business.	Unauthorized access
10-2	Privilege management	<input type="checkbox"/> A strict password policy is applied to the passwords of administrator rights of the telework terminals and individual systems used for telework.	Unauthorized access
10-3	Privilege management	<input type="checkbox"/> Administrator rights of the telework terminals and each system used for telework are used only for operations where the rights are necessary.	Unauthorized access

⑤ Employee terminals and VPN/remote desktop pattern

“Telework terminals” among the terms used in the checklist are divided into the following three categories:

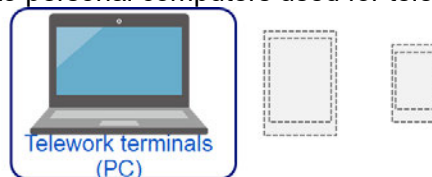
Telework terminal:

Applicable to personal computers and smart devices (tablet and Smartphone) used for telework



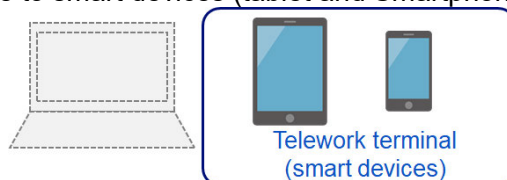
Telework terminal (PC):

Applicable to personal computers used for telework



Telework terminal (smart devices) :

Applicable to smart devices (tablet and Smartphone) used for telework



◆ Measures to be taken beforehand

No.	Category	Description	Possible threats
1-1	Asset management	<input type="checkbox"/> Only the telework terminals permitted by the company are used for telework and all terminals used and their users are known.	Malware infection, Unauthorized access, Theft/loss
1-2	Asset management	<input type="checkbox"/> All systems used for telework and important information* handled in telework are known. * Trade secrets and other information necessary for the business and valuable for the organization, personal information of customers and employees and other information involving responsibility for management	Unauthorized access, Information tapping

* Regarding the measures of the category “asset management,” management of information assets is not a measure that directly addresses security issues but presupposed for implementation of other measures.

Items of Priority ◎

No.	Category	Description	Possible threats
2-1	Malware countermeasure	<input type="checkbox"/> Anti-virus software is installed on the telework terminals and real time scan is enabled in setting.* Setting of automatic update of the anti-virus software definition file is made or a rule is created to manually update to the latest version. * Installation is not needed if you use the anti-virus software that is standard-install in Windows products or in the case of iOS products, if you use only applications that are installed in a way whose safety has been confirmed (use of official application store, for example.)	Malware infection
3-1	Access control (logical)	<input type="checkbox"/> Access control through the system and password setting, etc. for important information itself ensures that only admitted people can use the important information.	Unauthorized access
4-1	Access control (physical)	<input type="checkbox"/> Peep prevention filter is applied on the telework terminals and a rule is made to lock the screen when leaving one's seat.	Information tapping
5-1	Vulnerability management	<input type="checkbox"/> OS versions or application software no longer supported by the manufacturer is not used for the telework terminals.	Unauthorized access
5-2	Vulnerability management	<input type="checkbox"/> The latest security update is applied to the OS and application software of the telework terminals.	Unauthorized access
5-4	Vulnerability management	<input type="checkbox"/> Products no longer supported by the manufacturer are not used and the latest security update is applied to the VPN equipment used for remote access by the telework terminals to the company, remote desktop application, etc. of the company terminal.	Unauthorized access
7-1	Incident response and management	<input type="checkbox"/> In preparation for information security incidents, policies to address actual and possible incidents (when a suspicious email is opened, for example) have been decided and a system of communication to relevant parties has been established.	Malware infection, Unauthorized access, Theft/loss, Information tapping
8-1	Data protection	<input type="checkbox"/> Positional information of lost telework terminals (smart devices) can be detected.	Theft/loss
9-1	Authentication	<input type="checkbox"/> "Long" and "complicated" passwords that are difficult to detect are set for the log-in account of the telework terminals and the account of each system used for telework. Setting is made to enforce a certain level of password strength wherever possible.	Unauthorized access
9-2	Authentication	<input type="checkbox"/> Passwords to log in the telework terminals and the initial password of the account of each system used in telework are changed.	Unauthorized access

◆ Items of Priority level: ○

No.	Category	Description	Possible threats
2-2	Malware countermeasure	<input type="checkbox"/> Awareness is promoted not to open a suspicious email, click the URL included in the mail or open its attached file. When the email product we use has a function to exclude suspicious emails, the function is enabled. (This measure is not included if cloud service (web mail) is not used.)	Malware infection
2-3	Malware countermeasure	<input type="checkbox"/> Installation of applications to the telework terminals is limited to installation using methods whose safety can be confirmed (an official application store for example.)	Malware infection
3-2	Access control (logical)	<input type="checkbox"/> Access other than from ports and IP addresses that are necessary for accessing the internal system through the Internet is obstructed by firewalls, routers, etc. on the boundary between the internal network and the Internet.	Unauthorized access
3-3	Access control (logical)	<input type="checkbox"/> The organizer of an online meeting verifies the identity of the participants at the beginning of the meeting and when an additional participant joined midway. (Not included when cloud service (online meeting) is not used.)	Information tapping
3-4	Access control (logical)	<input type="checkbox"/> URL for access to an online meeting and passwords to participate in the meeting are not told to the members who don't need them. Password setting is enforced for all participants wherever possible. (Not included when cloud service (online meeting) is not used.)	Information tapping
3-5	Access control (logical)	<input type="checkbox"/> Organizer of an online meeting makes the meeting progress appropriately by dismissing inappropriate participants as needed, for example. (Not included when cloud service (online meeting) is not used.)	Information tapping
5-3	Vulnerability management	<input type="checkbox"/> Wi-Fi routers at home, mobile Wi-Fi, etc. that are no longer supported by the manufacturer are not used for telework and the latest firmware is used for them.	Unauthorized access
6-1	Encryption of communication	<input type="checkbox"/> When using cloud service (e.g. Web mail, chat, online meeting, cloud storage) for telework, HTTPS communication and correctness of the URL to connect are confirmed (not included when no cloud service is used.)	Information tapping
6-2	Encryption of communication	<input type="checkbox"/> When connecting to a cloud service or a service where an ID, password and other information is entered, it is confirmed before use that this is encrypted HTTPS communication.	Information tapping
6-3	Encryption of communication	<input type="checkbox"/> When using a Wi-Fi router or other equipment at home, WPA2 is used for Wi-Fi security and passwords that are difficult for a third party to guess are used.	Information tapping
7-2	Incident response and management	<input type="checkbox"/> Time synchronization setting is made between the telework terminals and the systems that the terminals access.	Malware infection, Unauthorized access, Theft/loss, Information tapping

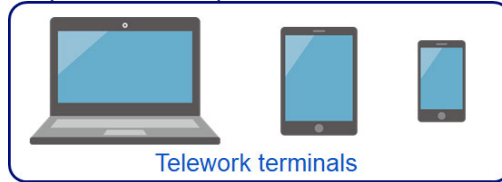
No.	Category	Description	Possible threats
7-3	Incident response and management	<input type="checkbox"/> Access log is collected for access by the telework terminals to the internal system.	Malware infection, Unauthorized access, Theft/loss, Information tapping
8-2	Data protection	<input type="checkbox"/> When a telework terminal (smart device) is lost, MDM* or similar software is introduced to remotely erase data and force security settings including login authentication policy and hard disc encryption. * Abbreviation from Mobile Device Management that refers to unitary management and operation of smart devices including Smartphone and software that provides the function.	Theft/loss
8-3	Data protection	<input type="checkbox"/> Built-in storage medium including hard disc and flash memory* are encrypted in order to prevent information leak when a telework terminal is stolen or lost** (not included when company data is not stored in the terminals.) * refers to "nonvolatile semiconductor memory" that a kind of storage medium different from hard disk. This storage medium can hold data after turning off of power. ** This is not required for iOS products that are encrypted at the initial state.	Theft/loss
8-4	Data protection	<input type="checkbox"/> Important information is not stored in the telework terminals in principle. When it is necessary to store important information*, the file is encrypted (password setting, for example.) (not included when company data is not stored in the terminals.) * This refers to local file storage in the telework terminals. Storing in a file server, cloud storage or in the system of various cloud services is not included here.	Unauthorized access, Theft/loss
8-5	Data protection	<input type="checkbox"/> When implementing an online meeting, important information is not included in the title or agenda of the meeting, password setting and automatic deletion after designated time are implemented for video files of the meeting. Setting is made to force the rules above wherever possible. (Not included when cloud service (online meeting) is not used.)	Information tapping
9-4	Authentication	<input type="checkbox"/> It is set to request multifactor authentication for access to individual systems used for telework.	Unauthorized access
10-1	Privilege management	<input type="checkbox"/> Administrator rights of the telework terminals and each system used for telework are given to the minimum number of people necessary for the business.	Unauthorized access
10-2	Privilege management	<input type="checkbox"/> A strict password policy is applied to the passwords of administrator rights of the telework terminals and individual systems used for telework.	Unauthorized access

⑥ Employee terminals not connected to the company pattern (cloud service type)

“Telework terminals” among the terms used in the checklist are divided into the following three categories:

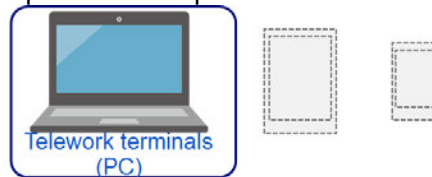
Telework terminal:

Applicable to personal computers and smart devices (tablet and Smartphone) used for telework



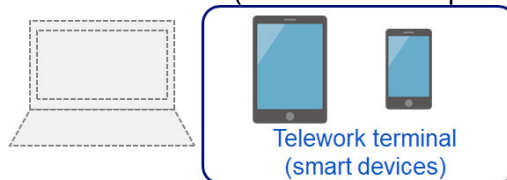
Telework terminal (PC):

Applicable to personal computers used for telework



Telework terminal (smart devices) :

Applicable to smart devices (tablet and Smartphone) used for telework



◆ Measures to be taken beforehand

No.	Category	Description	Possible threats
1-1	Asset management	<input type="checkbox"/> Only the telework terminals permitted by the company are used for telework and all terminals used and their users are known.	Malware infection, Unauthorized access, Theft/loss
1-2	Asset management	<input type="checkbox"/> All systems used for telework and important information* handled in telework are known. * Trade secrets and other information necessary for the business and valuable for the organization, personal information of customers and employees and other information involving responsibility for management	Unauthorized access, Information tapping

* Regarding the measures of the category “asset management,” management of information assets is not a measure that directly addresses security issues but presupposed for implementation of other measures.

Items of Priority ②

No.	Category	Description	Possible threats
2-1	Malware countermeasure	<input type="checkbox"/> Anti-virus software is installed on the telework terminals and real time scan is enabled in setting.* Setting of automatic update of the anti-virus software definition file is made or a rule is created to manually update to the latest version. * Installation is not needed if you use the anti-virus software that is standard-install in Windows products or in the case of iOS products, if you use only applications that are installed in a way whose safety has been confirmed (use of official application store, for example.)	Malware infection
3-1	Access control (logical)	<input type="checkbox"/> Access control through the system and password setting, etc. for important information itself ensures that only admitted people can use the important information.	Unauthorized access
4-1	Access control (physical)	<input type="checkbox"/> Peep prevention filter is applied on the telework terminals and a rule is made to lock the screen when leaving one's seat.	Information tapping
5-1	Vulnerability management	<input type="checkbox"/> OS versions or application software no longer supported by the manufacturer is not used for the telework terminals.	Unauthorized access
5-2	Vulnerability management	<input type="checkbox"/> The latest security update is applied to the OS and application software of the telework terminals.	Unauthorized access
7-1	Incident response and management	<input type="checkbox"/> In preparation for information security incidents, policies to address actual and possible incidents (when a suspicious email is opened, for example) have been decided and a system of communication to relevant parties has been established.	Malware infection, Unauthorized access, Theft/loss, Information tapping
8-1	Data protection	<input type="checkbox"/> In preparation for information security incidents, policies to address actual and possible incidents (when a suspicious email is opened, for example) have been decided and a system of communication to relevant parties has been established.	Theft/loss
9-1	Authentication	<input type="checkbox"/> Positional information of lost telework terminals (smart devices) can be detected.	Unauthorized access
9-2	Authentication	<input type="checkbox"/> "Long" and "complicated" passwords that are difficult to detect are set for the log-in account of the telework terminals and the account of each system used for telework. Setting is made to enforce a certain level of password strength wherever possible.	Unauthorized access

◆ Items of Priority level: ○

No.	Category	Description	Possible threats
2-2	Malware countermeasure	<input type="checkbox"/> Awareness is promoted not to open a suspicious email, click the URL included in the mail or open its attached file. When the email product we use has a function to exclude suspicious emails, the function is enabled. (This measure is not included if cloud service (web mail) is not used.)	Malware infection
2-3	Malware countermeasure	<input type="checkbox"/> Installation of applications to the telework terminals is limited to installation using methods whose safety can be confirmed (an official application store for example.)	Malware infection
3-3	Access control (logical)	<input type="checkbox"/> The organizer of an online meeting verifies the identity of the participants at the beginning of the meeting and when an additional participant joined midway. (Not included when cloud service (online meeting) is not used.)	Information tapping
3-4	Access control (logical)	<input type="checkbox"/> URL for access to an online meeting and passwords to participate in the meeting are not told to the members who don't need them. Password setting is enforced for all participants wherever possible. (Not included when cloud service (online meeting) is not used.)	Information tapping
3-5	Access control (logical)	<input type="checkbox"/> Organizer of an online meeting makes the meeting progress appropriately by dismissing inappropriate participants as needed, for example. (Not included when cloud service (online meeting) is not used.)	Information tapping
5-3	Vulnerability management	<input type="checkbox"/> Wi-Fi routers at home, mobile Wi-Fi, etc. that are no longer supported by the manufacturer are not used for telework and the latest firmware is used for them.	Unauthorized access
6-1	Encryption of communication	<input type="checkbox"/> When using cloud service (e.g. Web mail, chat, online meeting, cloud storage) for telework, HTTPS communication and correctness of the URL to connect are confirmed (not included when no cloud service is used.)	Information tapping
6-2	Encryption of communication	<input type="checkbox"/> When connecting to a cloud service or a service where an ID, password and other information is entered, it is confirmed before use that this is encrypted HTTPS communication.	Information tapping
6-3	Encryption of communication	<input type="checkbox"/> When using a Wi-Fi router or other equipment at home, WPA2 is used for Wi-Fi security and passwords that are difficult for a third party to guess are used.	Information tapping
7-2	Incident response and management	<input type="checkbox"/> Time synchronization setting is made between the telework terminals and the systems that the terminals access.	Malware infection, Unauthorized access, Theft/loss, Information tapping

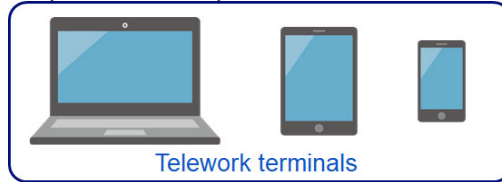
No.	Category	Description	Possible threats
8-2	Data protection	<input type="checkbox"/> When a telework terminal (smart device) is lost, MDM* or similar software is introduced to remotely erase data and force security settings including login authentication policy and hard disc encryption. * Abbreviation from Mobile Device Management that refers to unitary management and operation of smart devices including Smartphone and software that provides the function.	Theft/loss
8-3	Data protection	<input type="checkbox"/> Built-in storage medium including hard disc and flash memory* are encrypted in order to prevent information leak when a telework terminal is stolen or lost** (not included when company data is not stored in the terminals.) * refers to "nonvolatile semiconductor memory" that a kind of storage medium different from hard disk. This storage medium can hold data after turning off of power. ** This is not required for iOS products that are encrypted at the initial state.	Theft/loss
8-4	Data protection	<input type="checkbox"/> Important information is not stored in the telework terminals in principle. When it is necessary to store important information*, the file is encrypted (password setting, for example.) (not included when company data is not stored in the terminals.) * This refers to local file storage in the telework terminals. Storing in a file server, cloud storage or in the system of various cloud services is not included here.	Unauthorized access, Theft/loss
8-5	Data protection	<input type="checkbox"/> When implementing an online meeting, important information is not included in the title or agenda of the meeting, password setting and automatic deletion after designated time are implemented for video files of the meeting. Setting is made to force the rules above wherever possible. (Not included when cloud service (online meeting) is not used.)	Information tapping
9-4	Authentication	<input type="checkbox"/> It is set to request multifactor authentication for access to individual systems used for telework.	Unauthorized access
10-1	Privilege management	<input type="checkbox"/> Administrator rights of the telework terminals and each system used for telework are given to the minimum number of people necessary for the business.	Unauthorized access
10-2	Privilege management	<input type="checkbox"/> A strict password policy is applied to the passwords of administrator rights of the telework terminals and individual systems used for telework.	Unauthorized access

⑦ Employee terminals not connected to the company pattern (work-at-hand type)

“Telework terminals” among the terms used in the checklist are divided into the following three categories:

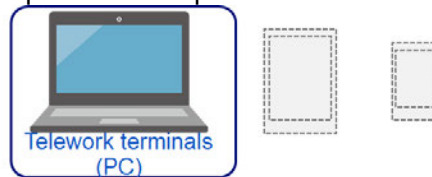
Telework terminal:

Applicable to personal computers and smart devices (tablet and Smartphone) used for telework



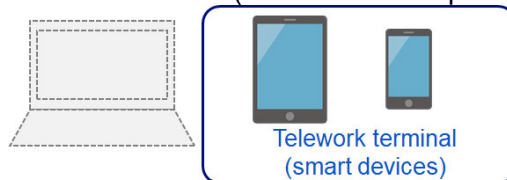
Telework terminal (PC):

Applicable to personal computers used for telework



Telework terminal (smart devices) :

Applicable to smart devices (tablet and Smartphone) used for telework



◆ Measures to be taken beforehand

No.	Category	Description	Possible threats
1-1	Asset management	<input type="checkbox"/> Only the telework terminals permitted by the company are used for telework and all terminals used and their users are known.	Malware infection, Unauthorized access, Theft/loss
1-2	Asset management	<input type="checkbox"/> All systems used for telework and important information* handled in telework are known. * Trade secrets and other information necessary for the business and valuable for the organization, personal information of customers and employees and other information involving responsibility for management	Unauthorized access, Information tapping

* Regarding the measures of the category “asset management,” management of information assets is not a measure that directly addresses security issues but presupposed for implementation of other measures.

Items of Priority ◎

No.	Category	Description	Possible threats
2-1	Malware countermeasure	<input type="checkbox"/> Anti-virus software is installed on the telework terminals and real time scan is enabled in setting.* Setting of automatic update of the anti-virus software definition file is made or a rule is created to manually update to the latest version. * Installation is not needed if you use the anti-virus software that is standard-install in Windows products or in the case of iOS products, if you use only applications that are installed in a way whose safety has been confirmed (use of official application store, for example.)	Malware infection
3-1	Access control (logical)	<input type="checkbox"/> Access control through the system and password setting, etc. for important information itself ensures that only admitted people can use the important information.	Unauthorized access
4-1	Access control (physical)	<input type="checkbox"/> Peep prevention filter is applied on the telework terminals and a rule is made to lock the screen when leaving one's seat.	Information tapping
5-1	Vulnerability management	<input type="checkbox"/> OS versions or application software no longer supported by the manufacturer is not used for the telework terminals.	Unauthorized access
5-2	Vulnerability management	<input type="checkbox"/> The latest security update is applied to the OS and application software of the telework terminals.	Unauthorized access
7-1	Incident response and management	<input type="checkbox"/> In preparation for information security incidents, policies to address actual and possible incidents (when a suspicious email is opened, for example) have been decided and a system of communication to relevant parties has been established.	Malware infection, Unauthorized access, Theft/loss, Information tapping
8-1	Data protection	<input type="checkbox"/> Positional information of lost telework terminals (smart devices) can be detected.	Theft/loss
9-1	Authentication	<input type="checkbox"/> "Long" and "complicated" passwords that are difficult to detect are set for the log-in account of the telework terminals and the account of each system used for telework. Setting is made to enforce a certain level of password strength wherever possible.	Unauthorized access
9-2	Authentication	<input type="checkbox"/> Passwords to log in the telework terminals and the initial password of the account of each system used in telework are changed.	Unauthorized access

◆ Items of Priority level: ○

No.	Category	Description	Possible threats
2-3	Malware countermeasure	<input type="checkbox"/> Installation of applications to the telework terminals is limited to installation using methods whose safety can be confirmed (an official application store for example.)	Malware infection
5-3	Vulnerability management	<input type="checkbox"/> Wi-Fi routers at home, mobile Wi-Fi, etc. that are no longer supported by the manufacturer are not used for telework and the latest firmware is used for them.	Unauthorized access
6-2	Encryption of communication	<input type="checkbox"/> When connecting to a cloud service or a service where an ID, password and other information is entered, it is confirmed before use that this is encrypted HTTPS communication.	Information tapping
6-3	Encryption of communication	<input type="checkbox"/> When using a Wi-Fi router or other equipment at home, WPA2 is used for Wi-Fi security and passwords that are difficult for a third party to guess are used.	Information tapping
7-2	Incident response and management	<input type="checkbox"/> Time synchronization setting is made between the telework terminals and the systems that the terminals access.	Malware infection, Unauthorized access, Theft/loss, Information tapping
8-3	Data protection	<input type="checkbox"/> Built-in storage medium including hard disc and flash memory* are encrypted in order to prevent information leak when a telework terminal is stolen or lost** (not included when company data is not stored in the terminals.) * refers to "nonvolatile semiconductor memory" that a kind of storage medium different from hard disk. This storage medium can hold data after turning off of power. ** This is not required for iOS products that are encrypted at the initial state.	Theft/loss
8-4	Data protection	<input type="checkbox"/> Important information is not stored in the telework terminals in principle. When it is necessary to store important information*, the file is encrypted (password setting, for example.) (not included when company data is not stored in the terminals.) * This refers to local file storage in the telework terminals. Storing in a file server, cloud storage or in the system of various cloud services is not included here.	Unauthorized access, Theft/loss
8-5	Data protection	<input type="checkbox"/> When implementing an online meeting, important information is not included in the title or agenda of the meeting, password setting and automatic deletion after designated time are implemented for video files of the meeting. Setting is made to force the rules above wherever possible. (Not included when cloud service (online meeting) is not used.)	Information tapping
9-4	Authentication	<input type="checkbox"/> It is set to request multifactor authentication for access to individual systems used for telework.	Unauthorized access

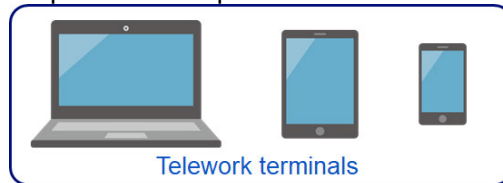
No.	Category	Description	Possible threats
10-1	Privilege management	<input type="checkbox"/> Administrator rights of the telework terminals and each system used for telework are given to the minimum number of people necessary for the business.	Unauthorized access
10-2	Privilege management	<input type="checkbox"/> A strict password policy is applied to the passwords of administrator rights of the telework terminals and individual systems used for telework.	Unauthorized access

⑧ Employee terminals and secure browser pattern

“Telework terminals” among the terms used in the checklist are divided into the following three categories:

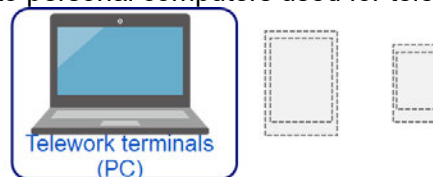
Telework terminal:

Applicable to personal computers and smart devices (tablet and Smartphone) used for telework



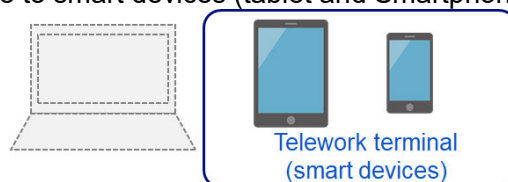
Telework terminal (PC):

Applicable to personal computers used for telework



Telework terminal (smart devices) :

Applicable to smart devices (tablet and Smartphone) used for telework



◆ Measures to be taken beforehand

No.	Category	Description	Possible threats
1-1	Asset management	<input type="checkbox"/> Only the telework terminals permitted by the company are used for telework and all terminals used and their users are known.	Malware infection, Unauthorized access, Theft/loss
1-2	Asset management	<input type="checkbox"/> All systems used for telework and important information* handled in telework are known. * Trade secrets and other information necessary for the business and valuable for the organization, personal information of customers and employees and other information involving responsibility for management	Unauthorized access, Information tapping

* Regarding the measures of the category “asset management,” management of information assets is not a measure that directly addresses security issues but presupposed for implementation of other measures.

Items of Priority ◎

No.	Category	Description	Possible threats
2-1	Malware countermeasure	<input type="checkbox"/> Anti-virus software is installed on the telework terminals and real time scan is enabled in setting.* Setting of automatic update of the anti-virus software definition file is made or a rule is created to manually update to the latest version. * Installation is not needed if you use the anti-virus software that is standard-install in Windows products or in the case of iOS products, if you use only applications that are installed in a way whose safety has been confirmed (use of official application store, for example.)	Malware infection
3-1	Access control (logical)	<input type="checkbox"/> Access control through the system and password setting, etc. for important information itself ensures that only admitted people can use the important information.	Unauthorized access
4-1	Access control (physical)	<input type="checkbox"/> Peep prevention filter is applied on the telework terminals and a rule is made to lock the screen when leaving one's seat.	Information tapping
5-1	Vulnerability management	<input type="checkbox"/> OS versions or application software no longer supported by the manufacturer is not used for the telework terminals.	Unauthorized access
5-2	Vulnerability management	<input type="checkbox"/> The latest security update is applied to the OS and application software of the telework terminals.	Unauthorized access
7-1	Incident response and management	<input type="checkbox"/> In preparation for information security incidents, policies to address actual and possible incidents (when a suspicious email is opened, for example) have been decided and a system of communication to relevant parties has been established.	Malware infection, Unauthorized access, Theft/loss, Information tapping
8-1	Data protection	<input type="checkbox"/> Positional information of lost telework terminals (smart devices) can be detected.	Theft/loss
9-1	Authentication	<input type="checkbox"/> "Long" and "complicated" passwords that are difficult to detect are set for the log-in account of the telework terminals and the account of each system used for telework. Setting is made to enforce a certain level of password strength wherever possible.	Unauthorized access
9-2	Authentication	<input type="checkbox"/> Passwords to log in the telework terminals and the initial password of the account of each system used in telework are changed.	Unauthorized access

◆ Items of Priority level: ○

No.	Category	Description	Possible threats
2-2	Malware countermeasure	<input type="checkbox"/> Awareness is promoted not to open a suspicious email, click the URL included in the mail or open its attached file. When the email product we use has a function to exclude suspicious emails, the function is enabled. (This measure is not included if cloud service (web mail) is not used.)	Malware infection
2-3	Malware countermeasure	<input type="checkbox"/> Installation of applications to the telework terminals is limited to installation using methods whose safety can be confirmed (an official application store for example.)	Malware infection
3-2	Access control (logical)	<input type="checkbox"/> Access other than from ports and IP addresses that are necessary for accessing the internal system through the Internet is obstructed by firewalls, routers, etc. on the boundary between the internal network and the Internet.	Unauthorized access
3-3	Access control (logical)	<input type="checkbox"/> The organizer of an online meeting verifies the identity of the participants at the beginning of the meeting and when an additional participant joined midway. (Not included when cloud service (online meeting) is not used.)	Information tapping
3-4	Access control (logical)	<input type="checkbox"/> URL for access to an online meeting and passwords to participate in the meeting are not told to the members who don't need them. Password setting is enforced for all participants wherever possible. (Not included when cloud service (online meeting) is not used.)	Information tapping
3-5	Access control (logical)	<input type="checkbox"/> Organizer of an online meeting makes the meeting progress appropriately by dismissing inappropriate participants as needed, for example. (Not included when cloud service (online meeting) is not used.)	Information tapping
5-3	Vulnerability management	<input type="checkbox"/> Wi-Fi routers at home, mobile Wi-Fi, etc. that are no longer supported by the manufacturer are not used for telework and the latest firmware is used for them.	Unauthorized access
6-1	Encryption of communication	<input type="checkbox"/> When using cloud service (e.g. Web mail, chat, online meeting, cloud storage) for telework, HTTPS communication and correctness of the URL to connect are confirmed (not included when no cloud service is used.)	Information tapping
6-2	Encryption of communication	<input type="checkbox"/> When connecting to a cloud service or a service where an ID, password and other information is entered, it is confirmed before use that this is encrypted HTTPS communication.	Information tapping
6-3	Encryption of communication	<input type="checkbox"/> When using a Wi-Fi router or other equipment at home, WPA2 is used for Wi-Fi security and passwords that are difficult for a third party to guess are used.	Information tapping
7-2	Incident response and management	<input type="checkbox"/> Time synchronization setting is made between the telework terminals and the systems that the terminals access.	Malware infection, Unauthorized access, Theft/loss, Information tapping

No.	Category	Description	Possible threats
7-3	Incident response and management	<input type="checkbox"/> Access log is collected for access by the telework terminals to the internal system.	Malware infection, Unauthorized access, Theft/loss, Information tapping
8-2	Data protection	<input type="checkbox"/> When a telework terminal (smart device) is lost, MDM* or similar software is introduced to remotely erase data and force security settings including login authentication policy and hard disc encryption. * Abbreviation from Mobile Device Management that refers to unitary management and operation of smart devices including Smartphone and software that provides the function.	Theft/loss
8-5	Data protection	<input type="checkbox"/> When implementing an online meeting, important information is not included in the title or agenda of the meeting, password setting and automatic deletion after designated time are implemented for video files of the meeting. Setting is made to force the rules above wherever possible. (Not included when cloud service (online meeting) is not used.)	Information tapping
9-4	Authentication	<input type="checkbox"/> It is set to request multifactor authentication for access to individual systems used for telework.	Unauthorized access
10-1	Privilege management	<input type="checkbox"/> Administrator rights of the telework terminals and each system used for telework are given to the minimum number of people necessary for the business.	Unauthorized access
10-2	Privilege management	<input type="checkbox"/> A strict password policy is applied to the passwords of administrator rights of the telework terminals and individual systems used for telework.	Unauthorized access

2 List of Setting Examples of the Security Measure Checklists

For reference when implementing the individual measures included in the checklists, we have prepared “Setting explanation materials” that include examples of settings and uses of specific products that are often used for telework, together with their explanation.

Examples of telework tool settings (Setting explanation materials)

No.	Document name	Product kind	Product name
1	Setting explanation material (Cisco WebEx Meeting)	Online meeting system	Cisco WebEx Meeting
2	Setting explanation material (Microsoft Teams)	Online meeting system	Microsoft Teams
3	Setting explanation material (Zoom)	Online meeting system	Zoom

The materials in the table above are published at the following URL:

https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

Setting explanation materials for other products that are often used for telework will be developed in series.

These setting explanation materials do not recommend use or avoidance of any specific products.

3 List of Security Measures for Telework Environment and Possible Threats

The pages that follow presents “Measures,” “Priority,” “Possible threats” and “Need for the measure for each pattern.” Details of the possible threats addressed by each measure are explained. Please use them as reference as needed.

No.	Category	Measure	Possible threats (Outline)	Possible threats (Detail)	Priority level	Remarks	Pattern 1	Pattern 2	Pattern 3	Pattern 4	Pattern 5	Pattern 6	Pattern 7	Pattern 8
1-1	Asset management	Only the telework terminals permitted by the company are used for telework and all the terminals used and their users are known.	Malware infection, Unauthorized access, Theft/loss	If any devices used for telework and their users are not known, it will increase the risk that there are terminals for which security measures are not taken. If the serial number and other device-specific information are not known, it could make understanding of the situation difficult when the terminal is stolen or lost.	—		✓	✓	✓	✓	✓	✓	✓	✓
1-2	Asset management	All systems used for telework and important information* ¹ handled in telework are known. * ¹ Trade secrets and other information necessary for the business and valuable for the organization, personal information of customers and employees and other information involving responsibility for management	Unauthorized access, Information tapping	If any operation carried out in telework, or any system used or important information handled is not known, it will increase the concern that some of the security measures for the systems used and handling of important information will not be taken.	—		✓	✓	✓	✓	✓	✓	✓	✓
2-1	Malware countermeasure	Anti-virus software is installed on the telework terminals and real time scan is enabled in their setting* ² . Setting of automatic update of the anti-virus software definition file is made or a rule is created to manually update to the latest version. * ² Installation is not needed if you use the anti-virus software (Windows Defender) that is standard-install in Windows products or in the case of iOS products, you use only applications that are installed in a way whose safety has been confirmed (official application store, for example.)	Malware infection	Risk of malware infection of the terminals used for telework will increase because some malware that can be removed by the latest virus definition file may not be removed.	◎		✓	✓	✓	✓	✓	✓	✓	✓
2-2	Malware countermeasure	Awareness is promoted not to open a suspicious email, click an URL included in the mail or open its attached file. When the email product we use has a function to exclude suspicious emails, the function is enabled. (The measure is not included if cloud service (web mail) is not used.	Malware infection	If you access an URL included in a suspicious email, you will be directed to a malicious site, which increases the risk of malware infection or leak of authentication information for access to important information. Opening of a suspicious attached file will increase the risk of malware infection.	○	Not included if cloud service (web mail) is not used	✓	✓	×	✓	✓	✓	×	✓

2-3	Malware countermeasure	Installation of applications to the telework terminals is limited to installation using methods whose safety can be confirmed (an official application store for example.)	Malware infection	Installing applications from a site other than official application stores will increase the risk of malware infection by installing malware imitating the genuine applications.	○		✓	✓	✓	✓	✓	✓	✓	✓	✓
3-1	Access control (logical)	Access control through the system and password setting, etc. for important information itself ensure that only admitted people can use the important information.	Unauthorized access	If access to important information is not limited to people who need the information for business by controlling access by systems/tools that store important information or by setting passwords for the information, for example, the risk of leak of important information increases through unauthorized use of the account of a person who does not need the access permission or through inaction (e.g. operation error) of a user.	◎		✓	✓	✓	✓	✓	✓	✓	✓	✓
3-2	Access control (logical)	Access that is not from ports and IP addresses that are necessary for accessing the internal system through the Internet is obstructed by firewalls, routers, etc. on the boundary between the internal network and the Internet.	Unauthorized access	If access that is not from ports or IP addresses that are necessary for accessing the internal system through the Internet is not obstructed by firewalls, routers, etc. on the boundary between the internal network and the Internet, the risk of unauthorized access will increase through malicious attack (attack exploiting the vulnerability, impersonation of accounts) using the unnecessarily authorized ports.	○	Not included when the system is not connected to the internal NW.	✓	×	×	✓	✓	×	×	✓	
3-3	Access control (logical)	The organizer of an online meeting verifies the identity of the participants at the beginning of the meeting and when an additional participant joined midway (Not included when cloud service (online meeting) is not used.)	Information tapping	If identity verifications are not made at the beginning of the meeting and when an additional participant joined midway, the risk of information leak through the meeting will increase due to failure to detect unauthorized participation of inappropriate users. Because an online meeting is not a face-to-face meeting, it is necessary to confirm that the participants are persons whose name is displayed on the system through video image, voice or/and other methods.	○	Not included when cloud service (online meeting) is not used.	✓	✓	×	✓	✓	✓	×	✓	
3-4	Access control (logical)	URL for access to an online meeting and the password to participate in the meeting are not told to the members who don't need them. Password setting is forced for all participants wherever possible. Password setting is enforced for all participants wherever possible. (Not included when cloud service (online meeting) is not used.)	Information tapping	Telling the URL for access to an online meeting and the password to participate in the meeting to members who don't need them will increase the risk of information leak through the meeting due to unauthorized attendance of an inappropriate user. If password setting is not (cannot be) forced, users may not set password or set an easily guessable password, which will increase the risk of unauthorized participation in the meeting. For prevention of unauthorized participation in a meeting, concealing the URL and password can be substituted by thorough identity verification at the beginning of the meeting.	○	Not included when cloud service (online meeting) is not used.	✓	✓	×	✓	✓	✓	×	✓	

3-5	Access control (logical)	Organizer of an online meeting makes the meeting progress appropriately by dismissing inappropriate participants as needed, for example. (Not included when cloud service (online meeting) is not used.)	Information tapping	Because you cannot physically dismiss improper participants from an online meeting, if the organizer cannot force participants to leave the meeting, the risk will increase that you cannot perform appropriate activities.	○	Not included when cloud service (online meeting) is not used.	✓	✓	×	✓	✓	✓	×	✓
4-1	Access control (physical)	Peep prevention filter is applied on telework terminals and it is made into a rule to lock the screen when leaving one's seat.	Information tapping	There is a concern that it is relatively easy for inappropriate persons including family members to physically peek into the telework terminal (shoulder hacking) in a telework environment compared with an office environment. For this reason, failure to apply a peep prevention filter or lock the screen when leaving one's seat will increase the risk of information leak and unauthorized use through the telework terminal.	◎		✓	✓	✓	✓	✓	✓	✓	✓
5-1	Vulnerability management	OS versions or application software no longer supported by the manufacturer are not used for the telework terminals.	Unauthorized access	If OS versions or application software no longer supported by the manufacturer are used, security of the product will not be updated, which will increase the risk of unauthorized access, etc. through an attack to the product's vulnerability.	◎		✓	✓	✓	✓	✓	✓	✓	✓
5-2	Vulnerability management	The latest security update is applied to the OS and the application software of the telework terminals.	Unauthorized access	If the latest security update is not applied to the OS and the application software of the telework terminals, it will increase the risk of unauthorized access, etc. through an attack to the product's vulnerability.	◎		✓	✓	✓	✓	✓	✓	✓	✓
5-3	Vulnerability management	Wi-Fi router at home or mobile Wi-Fi no longer supported by manufacturer is not used for telework and the latest firmware is applied.	Unauthorized access	If old or no-longer-supported firmware is used for Wi-Fi router or other products that are installed at home and used for telework, it will increase the risk of unauthorized access, etc. through an attack to the product's vulnerability.	○		✓	✓	✓	✓	✓	✓	✓	✓
5-4	Vulnerability management	Products no longer supported by the manufacturer are not used and the latest security update is applied to the VPN equipment used for remote access by the telework terminals to the company, remote desktop application, etc. of the company terminal.	Unauthorized access	VPN equipment installed in the company for implementation of telework permits communication from the Internet because of its purpose. For this reason, if a product no longer supported by the manufacturer or a product with old firmware is used, it will increase the risk of unauthorized access, etc. by an attack to the firmware's vulnerability through the Internet.	◎		✓	×	×	×	✓	×	×	×
6-1	Encryption of communication	When using cloud service (e.g. Web mail, chat, online meeting, cloud storage) for telework, HTTPS communication and correctness of the URL to connect are confirmed. (not included when no cloud service is used.)	Information tapping	When teleworkers access a cloud service via the Internet, it is presumed that wiretapping due to use of a wireless LAN, etc. is more likely compared with access from an office environment. Use of an online meeting system that regularly uses unencrypted communication will increase the risk of information leak through wiretapping by a malicious third person.	○	Not included when cloud service is not used.	✓	✓	×	✓	✓	✓	×	✓

6-2	Encryption of communication	When connecting to a cloud service or a service where information such as an ID and password is entered, it is confirmed before use that this is encrypted HTTPS communication.	Information tapping	Public wireless LAN used by teleworkers poses security concerns including fragile apparatus and encryption strength. For this reason, use of unencrypted communication will increase the risk of information leak through wiretapping by a malicious third person.	○		✓	✓	✓	✓	✓	✓	✓	✓
6-3	Encryption of communication	When using a Wi-Fi router or other equipment at home, WPA2 is used for Wi-Fi security and passwords that are difficult for a third party to guess are used.	Information tapping	If teleworkers use a security method with weak encryption strength (other than WPA2) or easy-to-guess password, this will increase the risk of information leak through wiretapping by a malicious third person.	○		✓	✓	✓	✓	✓	✓	✓	✓
7-1	Incident response and management	In preparation for information security incidents, policies to address actual and possible incidents (when a suspicious email is opened, for example) have been decided and a system of communication to relevant parties has been established.	Malware infection, Unauthorized access, Theft/loss, Information tapping	If policies to address information security incidents or a system of communication to relevant parties is not established, it will increase the risk of increasing damage of security incidents in general because you will not be able to detect occurrence of a security incident or prevent spread of damage at an early stage.	◎		✓	✓	✓	✓	✓	✓	✓	✓
7-2	Incident response and management	Time synchronization setting is made between the telework terminals and the systems accessed by them.	Malware infection, Unauthorized access, Theft/loss, Information tapping	If the time of the telework terminals and the systems accessed by them are not in sync, it will make it difficult to narrow down and identify the cause and damages of information security incidents by using various system logs. As a result, you will not be able to take appropriate measures to prevent the spread of damage of incidents and increase the risk of increasing damages of security incidents in general.	○		✓	✓	✓	✓	✓	✓	✓	✓
7-3	Incident response and management	Access log is collected for access by the telework terminals to the internal system.	Malware infection, Unauthorized access, Theft/loss, Information tapping	Failure to collect access log of access by the telework terminals to the internal system will make it difficult to narrow down and identify the cause and damages of information security incidents. As a result, you will not be able to take appropriate measures to prevent the spread of damage of incidents and increase the risk of increasing damages of security incidents in general.	○	Not included when the system is not connected to the internal NW.	✓	×	×	✓	✓	×	×	✓
8-1	Data protection	Positional information of lost telework terminals (smart devices) can be detected.	Theft/loss	A telework environment poses a concern of a higher possibility of a third party physically obtaining a lost telework terminal compared with an office environment. If application software to detect position information of telework terminals is not introduced, resulting difficulty of early discovery of the terminal will increase the risk of information leak including unauthorized data access by a third person who has obtained the lost terminal.	◎	Only for Smartphone	×	×	×	✓	×	×	×	✓

8-2	Data protection	<p>When a telework terminal (smart device) is lost, MDM*³ or similar software is introduced to remotely erase data and force security settings including login authentication policy and encryption of the hard disc.</p> <p>*3 Abbreviation from Mobile Device Management that refers to unitary management and operation of smart devices including Smartphone or software that provides the function</p>	Theft/loss	<p>A telework environment poses a concern of a higher possibility of a third party physically obtaining a lost telework terminal compared with an office environment. If the function of remote data deletion, authentication policy for login, hard disc encryption, etc. are not required, it will increase the risk of information leak including unauthorized data access by a malicious third party who obtained the lost device.</p>	○	Only for Smartphone	x	x	x	✓	x	x	x	✓
8-3	Data protection	<p>Built-in storage medium in hard disc, flash memory*⁴, etc. is encrypted in order to prevent information leak when a telework terminal is stolen or lost*⁵. (not included when company data is not stored in the terminals.)</p> <p>*4 refers to “nonvolatile semiconductor memory” that is a kind of storage medium different from a hard disk. This storage medium can hold data after turning off of power.</p> <p>*5 This is not required for iOS products that are encrypted at the initial state.</p>	Theft/loss	<p>A telework environment, compared with working in an office, etc., poses a concern of higher risk that a malicious third party physically obtains a telework terminal through loss or theft. If the hard disc is not encrypted, the risk of leak of the stored information will increase because a third party can access its data without account authentication by connecting it to a device that can read the hard disk.</p>	○	Not included when company data is not stored in the terminals.	✓	✓	✓	x	✓	✓	✓	x
8-4	Data protection	<p>Important information is not stored in the telework terminals in principle. When it is necessary to store important information*⁶, the file is encrypted (e.g. password setting.) (not included when company data is not stored in the terminals.)</p> <p>*6 This applies to local file storage in the telework terminals. Storing in a file server, cloud storage and in the system of various cloud services is not included here.</p>	Unauthorized access, Theft/loss	<p>A telework environment, compared with working in an office, etc., poses a concern of higher risk that a malicious third party physically obtains a telework terminal through loss or theft. If important information stored in a telework terminal is not encrypted (including password setting,) it will increase the risk of information leak through access to the important information when the hard disk is stolen or malware is used.</p>	○	Not included when company data is not stored in the terminals.	✓	✓	✓	x	✓	✓	✓	x

8-5	Data protection	When implementing an online meeting, important information is not included in the title or agenda of the meeting, and password setting and automatic deletion after the designated time are implemented for video files of the meeting. Setting is made to force the rules above wherever possible. (Not included when cloud service (online meeting) is not used.)	Information tapping	Failure to establish appropriate rules for online meetings poses a concern of sharing information that is not necessary to share. Specifically, the risk of information leak will increase through inclusion of important information in the published information of the meeting itself (e.g. the title of the meeting,) sharing of desktop screen information, video screen, sound, etc. which are not intended for sharing during the meeting due to inaction, or viewing of a video file of the meeting by an inappropriate third person, for example. If compliance with the rules above cannot be forced by the system itself, the risk of information leak will increase due to users' failure to observe the rules.	○	Not included when cloud service (online meeting) is not used.	✓	✓	×	✓	✓	✓	×	✓
9-1	Authentication	"Long" and "complicated" passwords that are difficult to detect are set for the log-in account of the telework terminals and the account of each system used for telework. It is set to force a certain level of password strength wherever possible.	Unauthorized access	If the passwords of the login account of the terminal used by employees or the accounts of the system used for telework are easy to detect, malicious third parties will be able to detect the password easily, which will increase the risk of unauthorized access through impersonation.	◎		✓	✓	✓	✓	✓	✓	✓	✓
9-2	Authentication	Passwords to log into the telework terminals and the initial password of the account of each system used for telework are changed.	Unauthorized access	If the initial passwords of the login account of the terminal used by employees or the accounts of the system used for telework are not changed, malicious third parties will be able to detect the password easily, which will increase the risk of unauthorized access through impersonation.	◎		✓	✓	✓	✓	✓	✓	✓	✓
9-3	Authentication	The account of the telework terminals and the account of each system used for telework are set to reject any password input after a predetermined number of input errors.	Unauthorized access	If the account of the telework terminals and the account of each system used for telework are not set to reject any password input after a predetermined number of input errors, it will facilitate trials by malicious third parties and increase the risk of unauthorized access through impersonation.	○	Terminals owned by employee are excluded because it is assumed that they are used also for non-business purposes.	✓	✓	✓	✓	×	×	×	×
9-4	Authentication	It is set to request multifactor authentication for access to individual systems used for telework.	Unauthorized access	If multifactor authentication is not set for access to individual systems used for telework and authentication is made only with an ID and password, it will increase the risk of unauthorized access through impersonation when the password is obtained by a malicious third person.	○		✓	✓	✓	✓	✓	✓	✓	✓
10-1	Privilege management	Administrator rights of the telework terminals and each system used for telework are given to the minimum number of people as necessary for the business.	Unauthorized access	If the administrator rights of the terminals and systems used for telework are given to people who don't need the rights in the course of business, it will increase the likelihood of access to important information by malicious third parties and increase the risk of leak of important information and information leak due to inaction of the user.	○		✓	✓	✓	✓	✓	✓	✓	✓

10-2	Privilege management	A strict password policy is applied to the passwords of administrator rights of the telework terminals and individual systems used for telework	Unauthorized access	If a strict password policy is not applied to the passwords of administrator rights of the terminals and individual systems used for telework, users may set easy-to-detect passwords and malicious third parties will be able to detect the passwords easily, which will increase the risk of unauthorized access through impersonation.	○		✓	✓	✓	✓	✓	✓	✓	✓	✓
10-3	Privilege management	The administrator rights of the telework terminals and each system used for telework are used only for operations where the rights are needed.	Unauthorized access	Use of administrator rights for operations that do not need the rights will make it difficult to detect possible unauthorized access based on the information on the use of the rights, and increase the risk of information leak due to the user's inaction.	○	Terminals owned by employee are excluded because it is assumed that they are used also for non-business purposes.	✓	✓	✓	✓	x	x	x	x	

Reference

1 Glossary

Term	Description
OS (Operating System)	Software needed to run the basic operations of a computer or smart device, such memory and hard drive management and keyboard and other I/O functions.
USB memory	Portable storage medium that is used by connecting to a USB connector
VPN	An abbreviation for Virtual Private Network. The technology enables safe access to the internal network remotely from home, visiting destination and other remote locations as if it were communication within the network.
WPA2	One of the wireless LAN security methods, which is currently dominant. WPA and WEP are other methods with weaker security. It is recommended to use WPA2.
Account	Permission to log into a network or internal system (such as a user ID).
Access log	A record of activity on servers or routers. Access logs record information on access sources and access destinations and are used for analyzing past operations and identifying causes of security incidents.
Virus	A type of malware. Unlike a worm, viruses do not replicate themselves in order to spread. Instead, they modify files saved on the infected computer or smartphone to save a copy of themselves. The virus spreads with the file propagating through networks and storage devices.
Cloud service	Generic term for various services that enable use through networks including the Internet of software, data, etc. that were conventionally managed and used through personal computers/servers. This book assumes mailing, chat, online meeting, file sharing and other cloud services, which include use of mail services provided by ISPs.
Satellite office	A facility in an office format located separately from the primary workplace. Some satellite offices are set up for the exclusive use of one company, while others are shared by multiple companies.
Serial number	Identification information provided for a personal computer and other products. A serial number is assigned not to the type of PC but to individual terminals.
Smart device	General term for iPhone, Smartphone with Android OS, iPad and other tablets.
Vulnerability	An information security flaw in an ICT device, system, or usage environment. Vulnerability refers to unintentional flaws built into equipment or systems during the design, development, or installation process as well as flaws created by incorrect settings, negligence, or other actions in the use of a system.
Secure browser	Dedicated software for viewing the information stored in the internal system or a cloud service which can prevent storage of the data in the terminal while viewing the information. Some products can limit screen shots, text copying and pasting and accessible pages.

Security update	Refers to replacement of a software part with a security defect by a new part with a safety measure, or correction program used for replacement.
Security method	Connection method of a wireless router, which is called "encryption protocol," "encryption" or "security" depending on the equipment including a wireless router
Definition file	Also called "signature" or "pattern file", it refers to files describing features of viruses. Such files are used for detection of virus.
Telework terminal	Refers to personal computer, Smartphone and other equipment that is brought out to an environment other than an office in order to do telework.
Data storage in telework terminal	This refers to storing of data in the terminal used (taken out and used) in a telework environment rather than storing in an internal server or cloud service. If it is not clear where the data are stored, and the data is accessible without connection of the telework terminal to the network (internal network or the Internet,) you can assume that the data is stored in the telework terminal.
Peep prevention filter	Filter applied to a screen in order to make the content difficult to read for a third person who peeks at the screen.
Encryption of hard disk	Function of encryption to prevent viewing by connecting a physically stolen hard disc to another terminal. BitLocker that is a default function of Windows10 falls under this function.
Firewall	Software that can block communication flowing through the network.
Firmware	Software that is installed in close coordination with the hardware of electronic equipment such as a computer or router as an integral component.
Remote desktop	Technology to transfer screens of the computers in the internal network to the computer at hand (telework terminal,) via the network, display the screens and remotely operate the computer in the internal network.
Router	A device that controls the communication channels between devices connected to a network.

2 Reference information on Telework Security

Below are literature and websites that may serve as a useful reference for understanding this book. The standards and guidelines will be revised. Please see the latest version as needed.

○**Telework Security Guidelines (Fourth Edition) [Ministry of Internal Affairs and Communications]**

https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

The guideline presents approaches to and examples of security measures for introduction of telework, in order to address security concerns over implementation of telework so that companies, etc. can safely introduce and use telework.

○**Information Security Handbook for Network Beginners [National Center of Incident Readiness and Strategy for Cybersecurity]**

<https://www.nisc.go.jp/security-site/handbook/>

General points of attention for using the Internet are compiled in a handbook.

○**Cybersecurity Management Guidelines Ver2.0 [METI / Information Technology Promotion Agency]**

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

The material is compiled for enterprise managers to promote cybersecurity measures under management leadership.

○**Information Security Measure Guidelines for SMEs (Information-technology Promotion Agency, Japan)**

<https://www.ipa.go.jp/security/keihatsu/sme/guideline/>

The guidelines present specific steps for SME managers and persons in charge to understand the need for information security measures and safely manage information.

○**Work-Style Reforms Beginning with Telework: Telework Adoption and Operation Guidebook (Ministry of Health, Labour and Welfare)**

<https://telework.mhlw.go.jp/wp/wp-content/uploads/2019/12/H28hatarakikatakaikaku.pdf>

The guidebook compiles telework introduction and operation mainly from the viewpoint of labor and personnel management.

○**For People Implementing Telework [National Center of Incident Readiness and Strategy for Cybersecurity]**

<https://www.nisc.go.jp/security-site/telework/>

○**Important Points for Security when Implementing Telework [National Center of Incident Readiness and Strategy for Cybersecurity]**

<https://www.nisc.go.jp/active/general/pdf/telework20200414.pdf>

○**Important Points for Security in Continuing Efforts for Telework [National Center of Incident Readiness and Strategy for Cybersecurity]**

<https://www.nisc.go.jp/active/general/pdf/telework20200611.pdf>

○**Security Precautions for Telework [Information Technology Promotion Agency]**

<https://www.ipa.go.jp/security/announce/telework.html>

Related organizations put forward important points for telework security.