Provisional Translation (英語仮訳)
Original: 総務省，テレワークセキュリティガイドライン 第４版，2018 available at:
https://www.soumu.go.jp/main_content/000545372.pdf [accessed 3 August 2020]

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 Guidelines
Fourth Edition

Ministry of Internal Affairs and Communications

April 2018

Complete Table of Contents

These guidelines divide information security measures, depending on their importance, into the following two types in descriptions from Page 26 on.

Basic Security Measures (in orange boxes)
These are fundamental security measures that everyone involved in telework should implement.

Recommended Security Measures
These are security measures that can be postponed when first adopting security measures but that should be implemented to ensure secure telework environments.

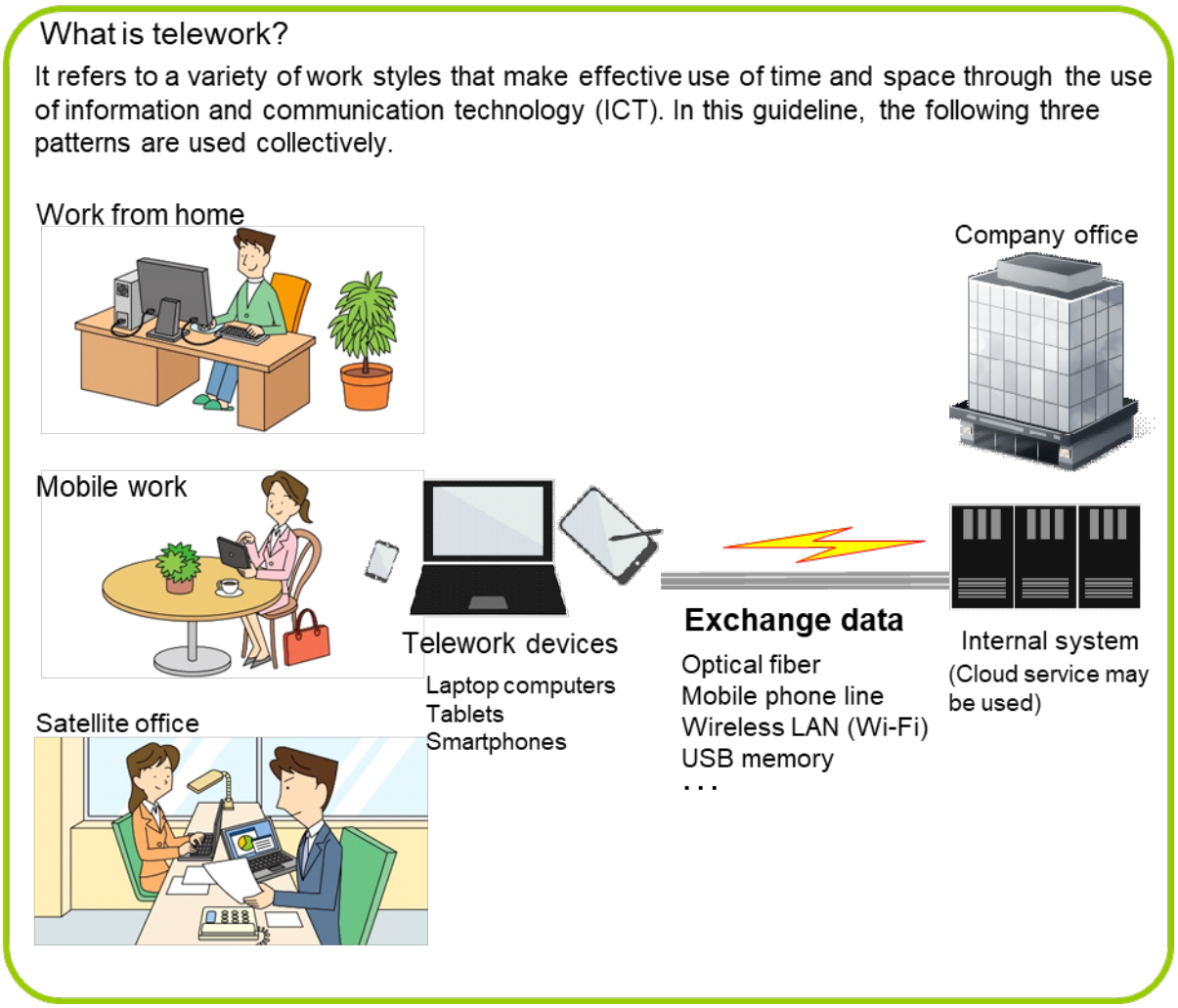
Table of Contents by Purpose

List of References for Teleworkers

List of Case Studies of Telework Security Incidents and Solutions

Introduction

Telework adoption has been expanding in recent years in many areas of society (see the illustration below). Telework lets enterprises set up employment and work arrangements that make more effective use of time and location. The benefits of telework for enterprises are not limited to enhanced competitiveness. These arrangements help generate new business, promote work-style reforms, and bolster business continuity. They also contribute to flexible and balanced work-styles that accommodate the lifestyles of a diverse range of individuals. Telework is recognized for the positive effects it has on a host of objectives — such as measures to address declining birthrates and an aging population, economic reform, job creation, regional revitalization, and disaster-mitigation and environmental measures. Further proliferation of telework is expected to realize a society in which more creative skills can be unleashed with more efficiency.



ICT application is essential to efficient telework. ICT permits work to be carried out at homes or outside locations almost as efficiently as in offices, with near instantaneous delivery of files created at telework locations to offices via the Internet and through videoconferencing between teleworkers. In the past, work done outside the office was considered either inconvenient, because the necessary materials were not at hand, or risky, due to concerns of information being leaked outside the organization. These problems are no longer a hindrance to telework, thanks to faster Internet speeds and the application of encryption and other information security technologies. This is substantiated by the fact that companies in Japan and around the world allow employees to work from home and use other forms of telework. Adopting telework after taking solid information security measures is expected to boost corporate value and make corporate social responsibility (CSR), a key management strategy, more visible.

These guidelines have been established as a reference for companies considering telework adoption to evaluate information security measures. Performing work outside of an office environment presents various risks depending on the work arrangements, but for each of those risks there are security measures as well. Through these guidelines, you can learn the basic approaches to selecting security measures to maintain security continually. The security measures described in these guidelines are also useful references for independent proprietors and self-employed people not attached to a company who telework. If you are self-employed or an independent proprietor, please refer to the sections for managers and for system administrators.

To be a handy reference for as many enterprises as possible, these guidelines describe information security measures based on the approaches most often used by enterprises in Japan. The descriptions have been made easy to understand for companies that have not used the Internet for work before, so all enterprises can easily determine the best security measures for them. Specifically, the guidelines have been organized with a general overview of the key points of information security measures for telework, followed by an introduction to approaches for specific security measures.

The descriptions in these guidelines provide examples of model security measures, presuming risks found in standard telework arrangements. Therefore, not all the information security measures illustrated here apply to all forms of telework. Depending on how your organization implements telework, some measures may be

unnecessary, while you may need additional measures. Refer to *Approaches to Security Measures Adapted to Different Telework Patterns* on Page 11 and work out the security measures that best fit your company or organization.

1. Approaches to Telework Information Security Measures

A. Implementing Measures that Strike a Balance between Rules, People, and Technology

How does telework differ from work performed in an office in terms of information security? Two obvious differences are the need for employees to use the Internet to exchange information with each other and that work takes place in locations accessible by non-employees.

Information assets of a company refers to the collection of paper documents, electronic data, information systems, and other information managed by the company. Information assets are usually managed in offices where non-employees cannot see them. In the case of telework, however, information is passed over the Internet and easily transported devices such as laptop computers are often used. As a result, information assets in telework are more susceptible to various threats — such as virus or worm infections, the loss or theft of telework devices or storage devices, and the interception of communications — than in offices, where measures are in place to safeguard information assets from attacks via the Internet. When *vulnerabilities* (information security deficiencies; refer to the *Glossary*) to such threats exist in telework devices, their settings, or in how they are used, telework can lead to real security incidents, such as data breaches or losses. Figure 1 provides several typical threats and vulnerabilities found in telework.

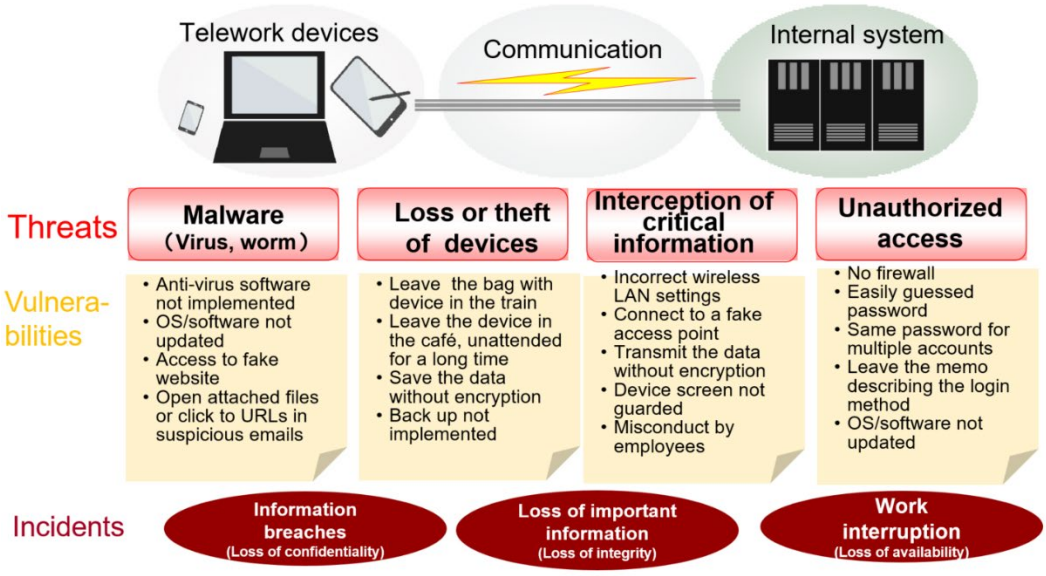


Figure 1 — Telework threats and vulnerabilities

To implement information security measures efficiently, it is important for companies to take a stepwise approach. First, information assets to be protected are identified and the types of threats, vulnerabilities, and risks are determined and recognized. Next, information assets are divided into levels according to their relative importance and systematic measures are put in place for each asset level. One particular characteristic of information security measures is that the weakest link determines the overall security level. This characteristic can be understood from the illustration below of filling buckets with water. The overall security level cannot be improved no matter how much you enhance other measures if even a single security hole exists somewhere. The key takeaway from this is to implement strategies to protect information assets that balance three critical components — *rules*, *people*, and *technology* — and ensure the overall security level is not compromised in any way (see Figure 2).

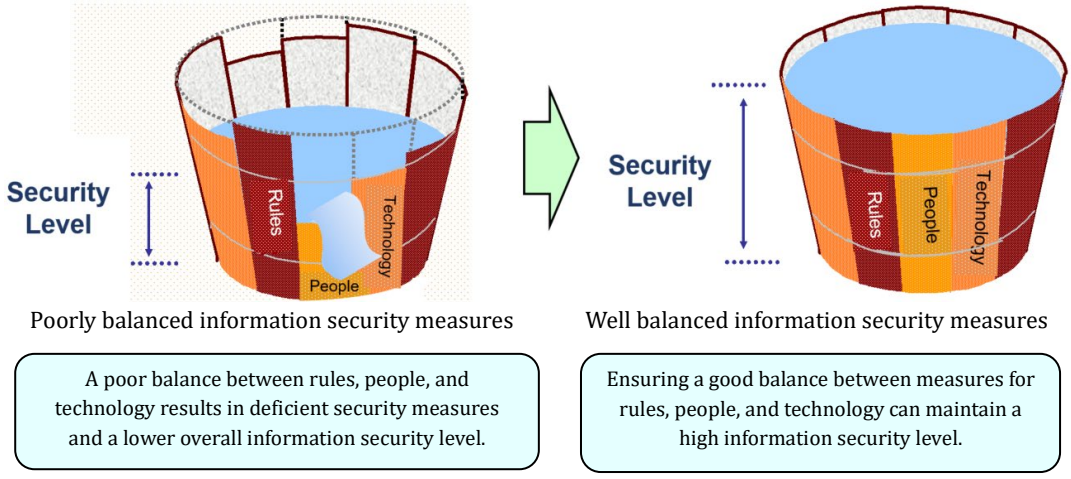


Figure 2 — Balanced approach to information security measures

Initiatives Assisting Information Security Measures by SMEs

SMEs considering establishing information security measures in tandem with adopting telework often find it difficult to work out on their own what kind of problems exist at the present time and what measures should they take in the future. The example initiatives listed below are useful in overcoming these concerns.

1. Security Action (Information-technology Promotion Agency, Japan (IPA))

   SMEs that make self-declarations that they have taken the following initiatives based on the IPA's *Information Security Measure Guidelines for SMEs* can promote their company by publishing Security Action logos on their website and in other materials.

   Implement the Five Articles of Information Security … One star ★

   Establish and publish a security policy based on the Company Diagnosis Sheet … Two stars

★★

2. What you need to know: Information Security Self-Check Questionnaire (Japan Network Security Association (JNSA))

This questionnaire provides employees with a way to check how well they understand important telework security matters, such as knowledge about email, using the Internet, knowledge about computer viruses, and password management.

Other assistance initiatives include the IT Coordinator System and the Registered Information Security Specialist System. These systems register people who have a certain degree of specialist knowledge in these fields. See the *Reference Links* section (Page 71) at the end of these guidelines for more details on these systems, including the two initiatives above.

Definitions of Rules, People, and Technology in the Telework Information Security Context

Rules

As employees proceed with work operations, judging in an ad hoc manner whether the work operations are secure from an information security standpoint and taking measures as needed is not entirely efficient. Moreover, employees who are not security specialists cannot necessarily make correct judgements. A better approach is to establish work rules that spell out how to perform work operations that ensure security. When rules are in place, employees need to be only concerned about obeying the rules to carry out their work securely.

In the case of telework, work is performed in environments different from offices. Consequently, new rules must be set to ensure the security of telework. This requires organizations to pay attention to what kind of rules should be established and adhered to.

People

Of the three critical factors in information security measures — rules, people, and technology, measures connected to people are the hardest to implement. Established rules will be of no benefit unless teleworkers and system administrators actually follow the rules. This is particularly true of teleworkers who carry out work operations in locations hard to monitor from offices. Consequently, companies and organizations must take into consideration the difficulty in verifying whether teleworkers are following rules. This is why it is

important, in order to entrench rules, to get teleworkers and related employees to understand the rationale of rules on their own terms through training and self-development and to have them realize that abiding by rules is advantageous for them. Furthermore, if teleworkers acquire necessary information security knowledge, they will be less susceptible to harm from phishing, targeted attacks, and other threats.

Technology

Technical security measures cover areas that cannot be addressed with rules and personnel measures. Technical security measures automatically carry out certification, detection, control, and defense measures against all kinds of threats. Given the diversity of teleworking environments, appropriate technical measures must be devised to ensure information security in each type of environment.

B. Approaches to Security Measures Adapted to Different Telework Patterns

There are several conceivable telework patterns, which vary depending on the nature of the work operations performed by telework, budget considerations, and other factors. The table below classifies telework into six patterns according to several factors, such as: Is electronic data stored on the telework device? What is the relationship with devices used in offices? Are cloud services used?

Table 1 — Six telework patterns

	Pattern 1	Pattern 2	Pattern 3	Pattern 4	Pattern 5	Pattern 6
	Remote desktop pattern	Virtual desktop pattern	Cloud app pattern	Secure browser pattern	App wrapping pattern	Company computer take-home pattern
Description	Remotely control a device located in an office	Remotely control a virtual device set up for telework	Use cloud apps from inside and outside the company	A special browser is used to limit the saving of data on the device	App wrapping provides functions that block saving data on the telework device	The employee takes an office device home and uses it as a telework device
Is electronic data stored on the telework device?	No	No	Either is possible	No	No	Yes
Does the telework device use the same environment as office devices?	Yes	Dedicated telework environment	Same in terms of the cloud apps	Same in terms of the apps used via the browser	Dedicated telework environment	Yes
Are cloud services used?	No	No	Yes	Yes	Either is possible	Either is possible
Is the use of personal devices for telework permitted (BYOD)?	Possible under certain conditions	Possible under certain conditions	Possible under certain conditions	Possible under certain conditions	Possible under certain conditions	n/a
Is a high-speed Internet connection required?	Yes	Yes	Preferred	Preferred	Preferred	No
Remarks	–	–	–	–	–	Taking paper documents off premises is also classified

						under this pattern

The following sections detail each pattern and its security measure characteristics. Note that telework in patterns 1 through 4 is carried out without saving electronic data on the telework device. This method of telework is sometimes referred to as the *thin client* method.

Pattern 1 — Remote desktop pattern

In this pattern, teleworkers, from the telework device, remotely control and view a desktop environment on a computer or other device located in an office. This pattern's main advantage is that teleworkers can carry out operations in the telework environment in the same way they had previously in the office, since the exact same environment can be used. Another advantage is that work results are saved on the office side and no electronic data are left on the device used in the telework environment. This permits the use of personal devices as telework devices. One drawback of this pattern is the need to pay attention to poor operability and productivity if sufficient speeds cannot be maintained over the Internet connection between the telework device and the office.

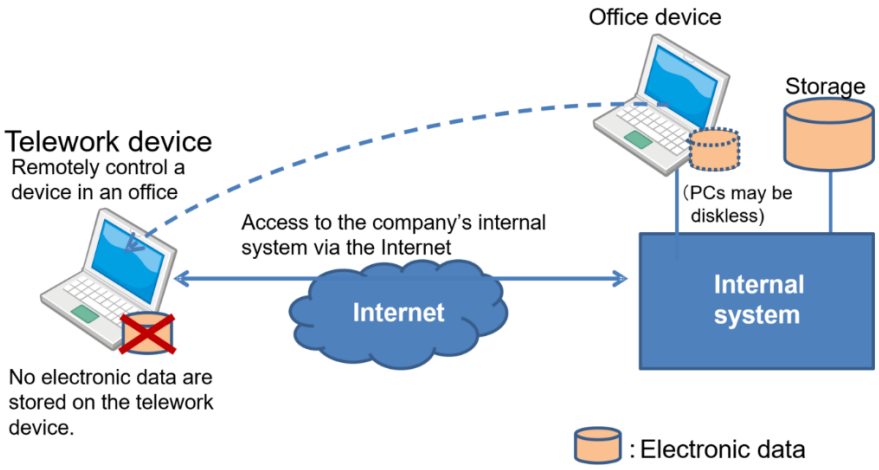


Figure 3 — Remote desktop pattern

Pattern 2 — Virtual desktop pattern

In this pattern, the teleworker logs in remotely from the telework device and uses virtual desktop infrastructure (VDI) provided on an office server. As with Pattern 1, no electronic data are left on the telework device, but there is no need to prepare a physical device in the office. Further advantages are that the system administrator can centrally manage virtual desktop environments and that uniform security

measures can be rolled out. The reliance of the telework device's operability on the speed of the Internet connection between the device and the office is identical to Pattern 1.

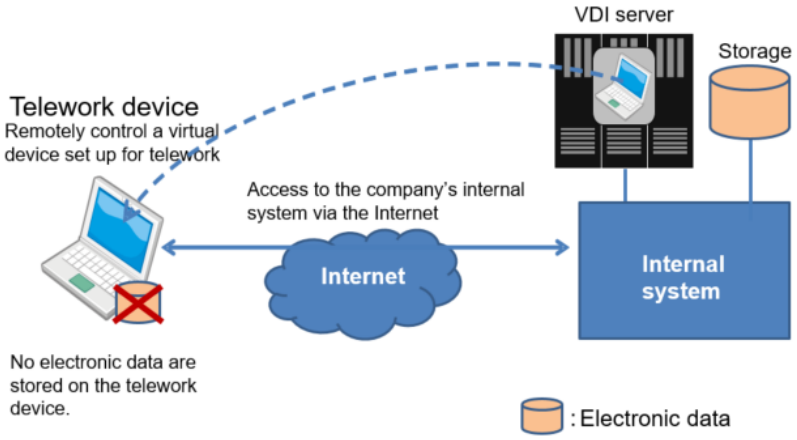


Figure 4 — Virtual desktop pattern

Pattern 3 — Cloud app pattern

In this pattern, work is carried out by accessing apps provided on a cloud server from any Internet-connected environment, whether it be in an office or in a telework location. Data created with apps can be selectively stored either on the cloud or in the local environment, which can cause management issues should a teleworker store work-related data on the telework device. However, compared to patterns 1 and 2, Internet speeds between the telework device and the cloud server have a limited impact on work operability.

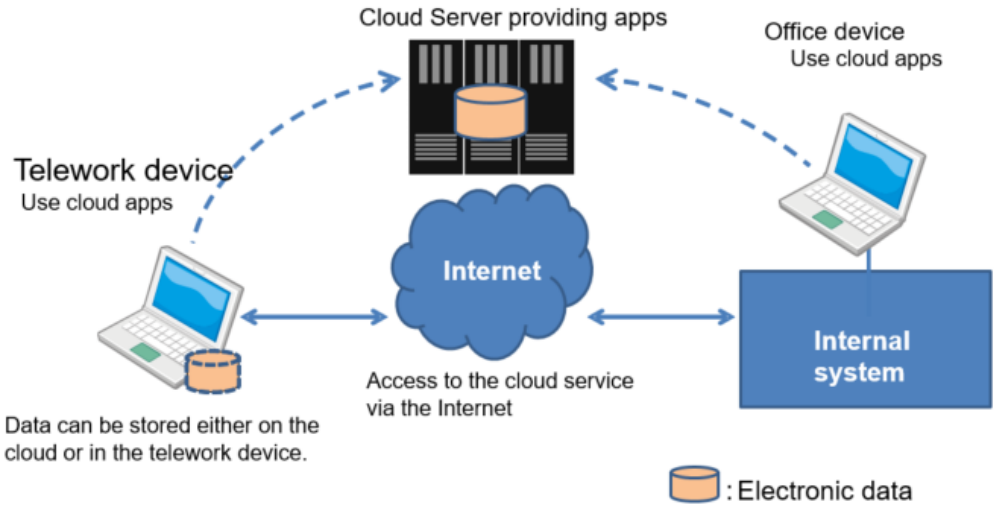


Figure 5 — Cloud app pattern

Pattern 4 — Secure browser pattern

This pattern improves upon the security of Pattern 3 (cloud app pattern). By using a special Internet browser, it is possible to place limits on file downloading, printing, and other functions to ensure electronic data used in work operations is not stored on a telework device. Although this pattern does improve security, the applications accessible from the telework device are limited to those available via the special Internet browser. The impact of Internet speeds is the same as with Pattern 3.

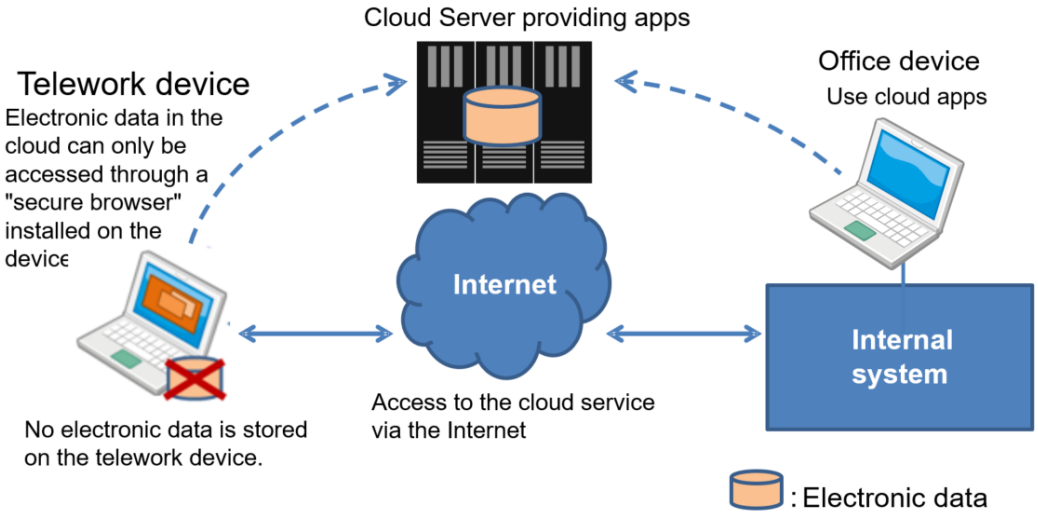


Figure 6 — Secure browser pattern

Pattern 5 — App wrapping pattern

This pattern involves setting up a *container* on the telework device, which is a virtual environment independent from the local environment. Work applications for telework run within the container. Applications (such as document creation apps or Internet browsers) running in the container cannot be accessed from the local environment. The applications, therefore, can be used without leaving electronic data on the telework device. Another advantage of this pattern is that it is not very susceptible to Internet speeds, as the operating system and applications running in the container are installed on the local computer.

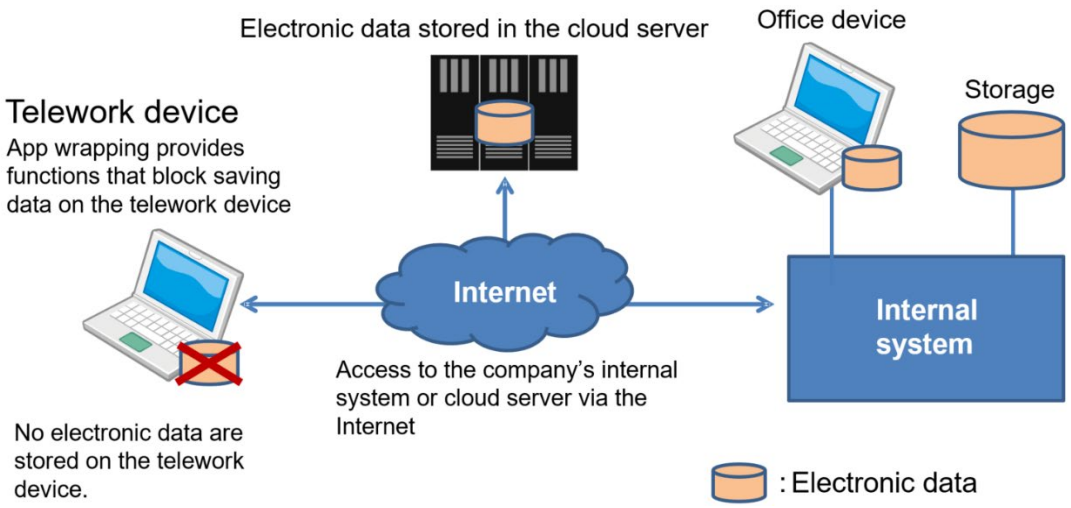


Figure 7 — App wrapping pattern

Pattern 6 — Company computer take-home pattern

In this pattern, the teleworker takes a device used in an office to the telework location and performs work operations. This pattern assumes the device accesses the office, when necessary, via a VPN connection as a security measure against data breaches along the Internet path. The speed of the Internet connection between the telework environment and the office does not affect operability or productivity. Thus, stable work operations can be done in unstable communication environments, such as on public transportation. A disadvantage of this pattern is that the device must be carried from the office each time telework will be done at home. Moreover, because telework cannot be done unless the device has been taken home, this pattern is not suited for situations where emergency telework is required due to weather conditions, for example. And because this pattern assumes electronic data will be stored on the telework device, it requires the most stringent device information security measures of the six patterns.

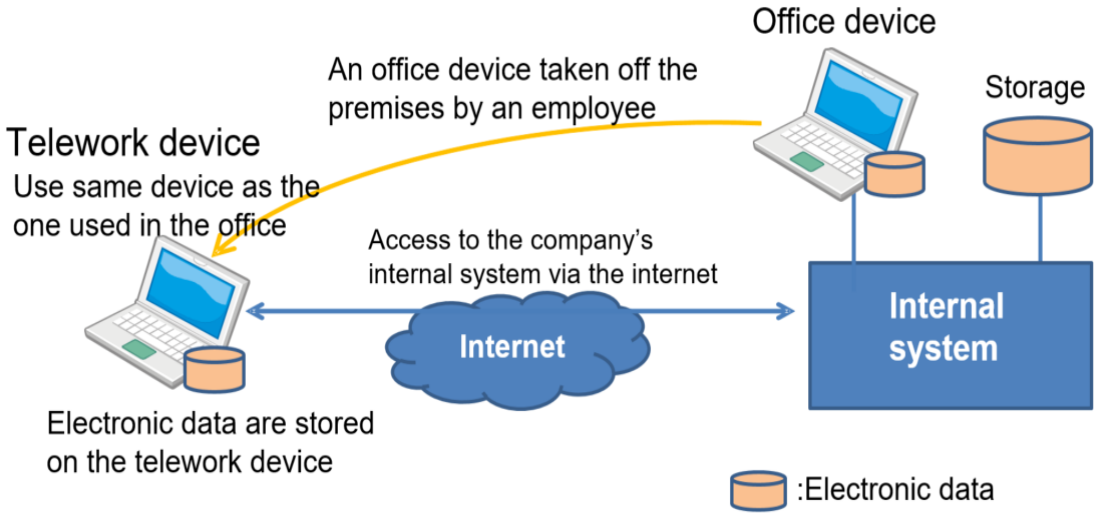


Figure 8 —Company computer take-home pattern

The differences among the telework patterns outlined above mainly affect technical security measures. The following sections on security measures indicate which of the patterns are applicable. Please use these as references in accordance with the telework patterns in effect at your organization. When no indication is given, the section applies to all patterns.

Examining the best telework patterns for your company

Telework, as we saw above, can be divided into six main patterns. The security measures that should be implemented also vary depending on whether the use of personal devices is allowed. Telework implementation costs can be kept down by allowing the use of personal devices. On the other hand, due to concerns of insufficient device security management and control, managers must carefully weigh security risks against implementation costs when considering the telework patterns right for their company.

Four of the telework patterns described above are compatible with the use of personal devices: namely, Pattern 1 — Remote desktop pattern, Pattern 2 — Virtual desktop pattern, Pattern 4 — Secure browser pattern, and Pattern 5 — App wrapping pattern. In each of these patterns, no electronic data are stored on the telework device, thus making the devices less likely to cause a security incident even if the devices' security were to be managed poorly. Conversely, electronic data are stored on the personal device in Pattern 3 — Cloud app pattern. Consequently, negligent security measures on a personal device can lead directly to a security incident.

There is a tendency to believe using personal devices will keep implementation costs low. In reality, however, allowing the use of personal devices incurs higher costs for additional information security measures (both at telework implementation and while telework is employed). And once the potential for losses from security incidents due to lower information security levels is factored in, personal devices do not necessary bring the expected cost reductions. It may well be that lending devices from the company is more economical in the long run.

Using cloud services

Cloud computing services, also known as cloud services, are drawing attention today as a means of using large-scale high-speed computing resources at low prices. Cloud services allow users to access via networks just the resources they need from the resources on offer from the cloud service operator, such as networked information systems or storage. There are many variants of cloud services tailored to user needs, such as providing networked resources as rental servers, as remote disks, or as applications. Cloud services, which take advantage of their economies of scale, are generally cheaper than an organization setting up its own server and operating equivalent services. An advantage for SMEs, in addition to the cost savings, is not having to deploy someone in the office to manage the server. This is why many companies are abandoning in-office servers and migrating to cloud services.

Migrating to cloud services has advantages for telework too. To allow telework locations to access servers located in offices, companies are forced to open a type of "hole" in their firewall positioned at their connection point to the Internet. This hole permits outside entities to access internal resources, but it must be configured with due caution as the hole may be used in an attack. Migrating from office servers to cloud servers eliminates the need to open a hole in the firewall, simplifying the management of firewalls and other security equipment. Consequently, a benefit of using cloud services is minimizing the risks to office networks due to telework adoption. If telework Pattern 4 — Secure browser pattern — described on Page 16, is adopted, another benefit is that electronic data used in telework can only be saved on the cloud service, which simplifies data protection.

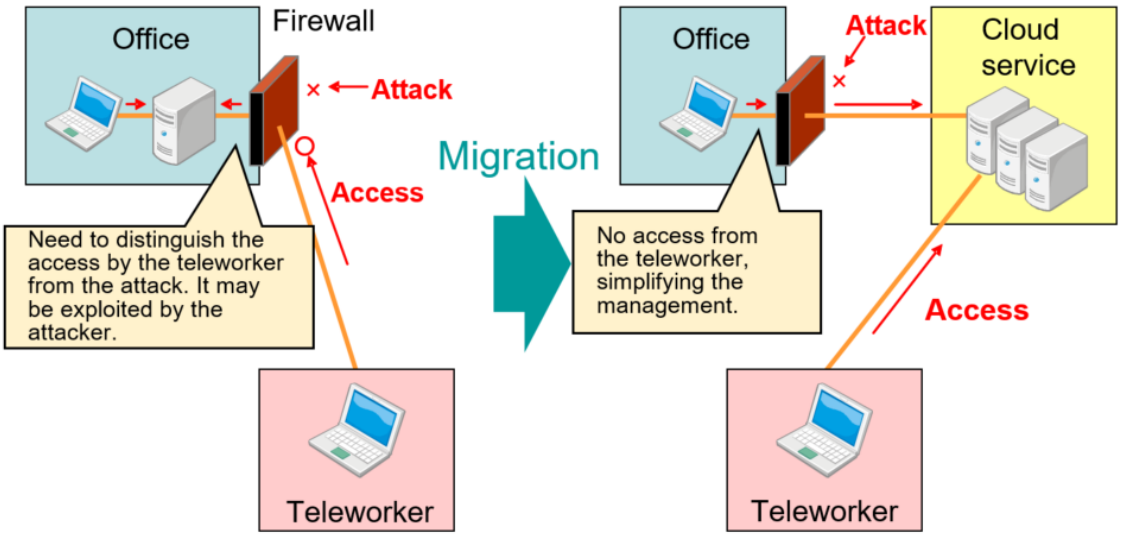


Figure 9 — Migrating to cloud services

The drawback from a security perspective is cloud services are designed to be broadly accessible from the Internet — leaving aside *private clouds* that cannot be accessed directly from the outside. This makes them prone to external attacks, a point that must be weighed in any decision about cloud services. Along with hard-to-guess passwords, encryption keys, and other security measures used with cloud services, strict management protocols should be put in place to avoid external data breaches. Where possible, user authentication security measures should be tightened, deploying, for example, multi-factor authentication or combining authentication with digital certificates. Many aspects of information security measures for cloud services are the responsibility of the cloud service user. Many cloud service data breaches and other security incidents have been caused by mistaken settings by the user that nullified or compromised access controls over information that should have been secret.

Another recent trend is individuals setting up free cloud service accounts (such as online email, groupware, or social media) for telework use. Some of these free services in practice do provide sufficient functionality and security, so there is no need to unilaterally ban all such services for business use. Nevertheless, they should be used with the following points in mind.

- Using a personal account for cloud services runs the risk of unintentionally syncing work-related information on a computer used for personal use or sharing work-related information to unrelated third parties. These risks must be fully understood in advance.

- Stringent password management controls, like those mentioned above, are necessary even for personal accounts to prevent hijacking or spoofing by malicious third parties.
- In order to provide the services for free, cloud service operators display ads matching the written content or sell statistical analyses of cloud service usage as marketing data. Consider the use of paid services if you wish to avoid such situations.
- The use of cloud services provided by a cloud service operator involves entrusting data to the operator. Therefore, attention must be paid to the trustworthiness of the cloud service operator.

Managers should consider the use of cloud services for telework after accounting for their information security merits and demerits given above.

C. The Positions of Managers, System Administrators, and Teleworkers

When implementing telework, managers, system administrators, and teleworkers must be conscious of how they should protect telework security from their respective positions.

Managers

Section A above touched on the importance of rule-making. It is the job of managers to create rules and to promote active rule-making. Given that today ICT is widely used in work operations, managers must be aware that information security incidents arising through work operations, including telework, have direct consequences on their business. Therefore, they must set as rules the necessary security measures to prevent such incidents. Furthermore, managers must recognize they are responsible for implementing all aspects of telework security preservation seen from the broader perspective. As a practical example, managers, after establishing the information security measures to be taken, must ensure the necessary staffing and budgets to implement and operate the measures. See the *Cybersecurity Management Guidelines* (included in the *Reference Links* section on Page 71) issued by the Ministry of Economy, Trade and Industry for specific considerations managers should take into account.

System Administrators

Internal systems contain all kinds of electronic data that should be safeguarded from the standpoint of the company. Enabling outside access to internal company systems, such as that to allow access from telework devices, increases the likelihood of unauthorized intrusions or accesses to internal systems. Furthermore, adequate measures must be taken to address other threats, such as the misuse of internal systems to spread viruses. System administrators, who manage entire systems, need to recognize they should be implementing security measures based on these and other threats.

Teleworkers

Workers who perform telework must be aware of many security aspects. For example, when a suspicious email arrives, it is easy in an office setting for a worker to ask someone nearby: “Do you think this email is strange?” Such quick confirmations can be much more difficult in a telework setting. Furthermore, as the teleworker is the system administrator for the telework device, security management operations are more complex than with an in-office device.

Teleworkers, therefore, should be aware of the importance of managing security on their own and manage the applicable security measures.

2. Considerations for Telework Security Measures

The following tables list important considerations for information security measures in regard to telework. The descriptions of each consideration start from Page 26. It should be noted that there are many possible information security measures, depending on the type and extent of envisioned risks. In practice, an organization must select from, add to, and adapt the security measures listed below, in view of the particular risks it faces, when creating actual measures.

The tables below can also serve as a self-assessment check list to determine to what extent your organization has implemented security measures. Any organization-specific rules that have been set can be added to this list.

A. Telework Security Measures for Managers

General framework of measures for information security preservation

1	Managers establish information security policies that take telework into account, audit the policies regularly, and make revisions as needed.	Page 26
2	Managers sort information handled within the organization into security levels based on the information's importance and then establish handling rules for information security levels that can be used with telework and information security levels that cannot.	Page 29
3	Managers provide regular training and awareness-raising activities for teleworkers to ensure they understand the importance of information security measures and can apply those measures in their work operations.	Page 33
4	Managers create a contact system to ensure the organization can respond promptly to information security incidents and hold training exercises to ensure incident response capabilities.	Page 35
5	Managers demonstrate adequate understanding of information security measures related to telework and allocate sufficient budgets for the necessary personnel and resources to carry out information security measures.	Page 36

B. Telework Security Measures for System Administrators

General framework of measures for information security preservation

1	System administrators are aware of their important position in managing entire systems. They set out technical measures to maintain the security of telework in line with information security policies and regularly audit the implementation status of the measures.	Page 26
2	System administrators set access controls on electronic data, set whether encryption is necessary, set whether printing is permitted, and make other settings according to the information security level.	Page 29

	the rules and guidelines specific usage considerations for telework.	
18	System administrators set out usage rules on file sharing services and other public cloud services and prohibit types of usage where there is concern of data breaches.	Page 66

C. Telework Security Measures for Teleworkers

General framework of measures for information security preservation

1	Teleworkers are aware that they are responsible for the management of the information assets they use during telework, carry out work operations in line with technical, physical, and personnel security measure standards that are specified in information security policies, and perform regular self-assessments of the state of their implementation of security measures.	Page 26
2	Teleworkers handle information used in telework following rules set for each pre-established information security level.	Page 29
3	Teleworkers work to improve their understanding of information security by actively participating in regular training and awareness-raising activities on information security.	Page 33
4	Teleworkers verify the contact system so they can contact the specified person in charge immediately in response to information security incidents and participate in training exercises to ensure incident response capabilities.	Page 35

Measures against malicious software

5	Teleworkers do not access external websites unless the operating system and browser (including extensions) on their telework device have been updated to the latest version to prevent malware infections.	Page 37
6	Before installing an application, teleworkers apply for permission from their system administrator and only install applications for which permission has been given.	Page 39
	Teleworkers give due consideration to security before selecting applications to install on devices used for telework (when using personal devices for telework).	
7	Before starting work operations, teleworkers verify that anti-virus software has been installed on the telework device and that the latest definition file is being applied.	Page 41
8	Before starting work operations, teleworkers verify that the telework device's operating system and software have been updated to the latest version.	Page 44
9	Teleworkers use devices for telework on which information security measures specified in rules have been applied and do not perform unauthorized modifications, such as jailbreaking or rooting, to smartphones, tablets, or other devices.	Page 45
10	Teleworkers are aware that a failure or delay in reporting a malware infection that occurred during telework may lead to greater damage to the organization and exercise due caution when opening email attachments or clicking on links in email messages.	Page 47

Measures against the loss or theft of devices

3. Explanations of Telework Security Measures

A. General Framework of Measures for Information Security Preservation

Managers 1	Managers establish information security policies that take telework into account, audit the policies regularly, and make revisions as needed.
System Administrators 1	System administrators are aware of their important position in managing entire systems. They set out technical measures to maintain the security of telework in line with information security policies and regularly audit the implementation status of the measures.
Teleworkers 1	Teleworkers are aware that they are responsible for the management of the information assets they use during telework, carry out work operations in line with technical, physical, and personnel security measure standards that are specified in information security policies, and perform regular self-assessments of the state of their implementation of security measures.

Managers — Basic Security Measures

- The most fundamental rule when deploying information security measures is the organization's information security policy. An information security policy is a document that consolidates the organization's principles and action guidelines on information security. By creating an information security policy, an organization can ensure consistent information security levels throughout the organization.
- An information security policy consists of three levels as shown in Figure 10 on the next page. The first level is the *basic policy* that forms the foundation for all information security. The second level is the *security measure standards*, which establish what information security measures should be implemented and what information should be protected based on the basic policy. The third level is the *implementation details*, which spell out concrete procedures for executing the measures defined in the security measure standards. The specifics of these three levels vary according to the enterprise's corporate philosophy, management strategies, business size, the information assets to be protected, and its industry and line of business. Therefore, an information security policy must be devised that matches the business activities of your organization.
- The basic policy, as its name suggests, states very general concepts and does not need to be modified to account for telework. The security measure standards and the implementation details, however, need to account for telework. For example, when the department that manages the operation of devices used for telework is separate from the departments to which teleworkers belong, the information security policy must define in advance which

department is responsible should a security incident occur during telework.

Figure 10 — Structure of an information security policy

Managers — Recommended security measures

It is not enough to just define an information security policy. It is vital that managers keep rules up to date following the four steps of the PDCA cycle and strive to continually raise the level of information security measures (see Figure 11).

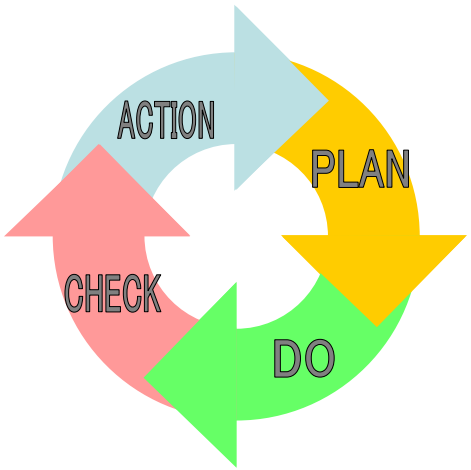


Figure 11 — PDCA cycle for information security

Trivial mistakes by company employees or internal misconduct can turn into enormous losses for the company. Because telework can be done in many kinds of environments, two effective measures are to set rules to prevent external leaks of confidential information (such as checks on whether encryption and other measures are being followed to the letter when electronic data are taken off

premises or requiring permission to take electronic data off premises) and, as a deterrent effect, to set provisions in work regulations or other company rules that spell out penalties for violating these rules.

System administrators — Recommended security measures

System administrators occupy an important position in managing entire systems. Therefore, they must set out technical measures to promote telework security in line with the information security policy and regularly audit the implementation status of the measures.

They also provide necessary information when managers are establishing rules.

Teleworkers — Recommended security measures

Offices normally have someone in charge of managing information security. During telework, however, the teleworker is the person in charge of managing information security in the telework location. Especially when information assets are taken off premises for telework, the teleworker is responsible for managing the information assets the entire time they are off premises. As long as the teleworker carries out work operations adhering to the specified rules (such as encryption of critical information or the use of secure information channels), the teleworker does not bear responsibility should a security incident occur during work and information is lost or exposed to outside parties. However, if the teleworker does not obey rules or is guilty of gross negligence, the teleworker must take responsibility for the incident. As telework is done out of the supervisor's direct oversight, teleworkers must understand that working without obeying rules can result in serious consequences for them.

Managers 2	Managers sort information handled within the organization into security levels based on the information's importance and then establish handling rules for information security levels that can be used with telework and information security levels that cannot.
System Administrators 2	System administrators set access controls on electronic data, set whether encryption is necessary, set whether printing is permitted, and make other settings according to the information security level.
Teleworkers 2	Teleworkers handle information used in telework following rules set for each pre-established information security level.

Managers and System Administrators — Basic Security Measures

- Managers and system administrators usually classify internal information assets into three security levels — such as *confidential information*, *operational information*, and *public information* — and establish methods of handling information assets not classified as public information.
  - † Confidential information refers to personal information (including that of company employees), private information entrusted by customers, sensitive information, trade secrets, and information connected to company management.
  - † Operational information refers to information not defined as confidential information and is not intended to be released to the public (such as internal meeting materials, attendance management ledgers, training materials).
  - † Telework involving taking information assets off premises runs a higher risk of the information, either electronic data or paper documents, being exposed to outside parties. Consequently, rules could be put in place so that, for example, only operational information or public information is permitted to be taken off premises.
- Managers and system administrators indicate the security level of information assets so information asset users can readily distinguish the security level.
  - † Electronic data: Differentiate by folder, append [Confidential] to the file name, etc.
  - † Paper documents: Mark [Confidential] in the page margins, mark the security level on the spine of file folders, etc.

Managers and system administrators — Recommended security measures

When information assets are managed using internal file servers for example, managers and system administrators can set access restrictions on folders containing electronic data so users or devices that do not need to view or edit the confidential information cannot access the confidential information. Access controls on information assets can be implemented regardless of which of the telework patterns explained in Chapter 1 is selected. Nevertheless, as described

above, taking confidential information off premises entails serious risks.

In cases where confidential information has to be handled during telework, implementing access controls based on the importance of the information assets and the user's security clearance — in addition to adopting either the remote desktop pattern or the virtual desktop pattern — can both protect confidential information and permit its use in telework.

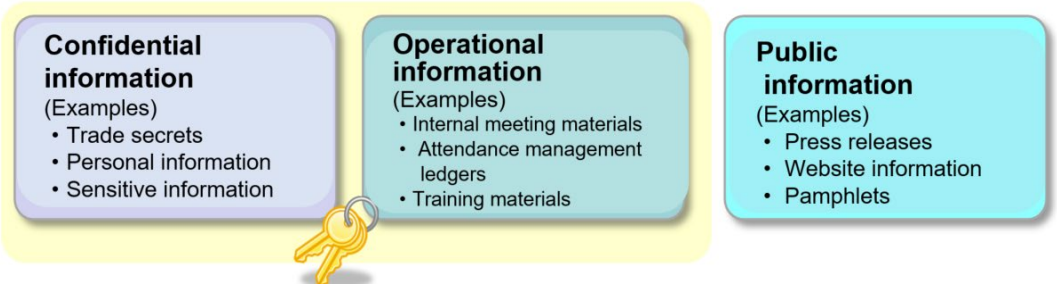


Figure 12 — Dividing information assets into security levels

Case Study No. 1 of Telework Security Incidents and Solutions

- Security incident related to sorting information into security levels -

Telework Security Incident

A company set up its internal systems so that outside parties could access all files on the internal systems in the same way as inside the company. An employee doing telework out of the office left his computer open with a work screen displaying confidential information belonging to a client. The confidential information was read by a third party who posted the information anonymously on an online forum. As a result, the client declared it was ceasing its business with the company.

Possible Solutions

To address this type of security incident, measures must be taken that recognize the respective problem areas with rules, people, and technology, as pointed out on Page 9. Telework performed in mobile environments often means work is done in an environment with many unrelated people nearby. Consequently, it is necessary to account for the risk of data breaches resulting from people reading device screens, a possibility that is difficult to imagine in offices where outsiders are not allowed entry.

As for specific measures, first for rules, system administrators should sort information into security levels based on policies set by managers and define handling methods for each level. Next, a possible technical measure would be to set up systems to block external access to critical information. However, this measure cannot be applied to information that has to be accessed from telework devices. Therefore, the solution requires personnel measures — i.e., striving to prevent incidents by raising the awareness of teleworkers — such as informing teleworkers about the dangers of leaving screens open when handling critical information.

Taking Paper Documents Off Premises

Going paperless is recommended for telework because information needed for work operations can be managed as electronic data, which allows such security measures as encryption. Nevertheless, many companies have not converted all their information to digital, and it is a reality that information on paper has to be taken off premises in some cases.

According to the Japan Network Security Association's *Survey Report of Information Security Incidents* (June 14, 2017), paper media accounted for nearly half, 47.0 percent, of all data breaches. When taking paper materials off premises is permitted, rules must be established that recognize the risks of data breaches due to the loss or theft of paper documents. Possible concrete measures include stipulating limits on the types of materials that can be taken off premises, stipulating how to discard paper documents, and mandating entries in document management ledgers when taking materials off premises.

Caution is also needed when using paper documents for telework or meetings in coworking

spaces. The environment in coworking spaces is similar to that of an office, compared to a café or other establishment, which can foster a false sense of security. As a result, paper documents are often left unattended in coworking spaces.

Managers 3	Managers provide regular training and awareness-raising activities for teleworkers to ensure they understand the importance of information security measures and can apply those measures in their work operations.
System Administrators 3	System administrators provide regular training and awareness-raising activities for teleworkers to ensure teleworkers are aware of information security.
Teleworkers 3	Teleworkers work to improve their understanding of information security by actively participating in regular training and awareness-raising activities on information security.

Managers and System Administrators — Basic Security Measures

- Training and awareness-raising activities are essential to ensure teleworkers have a solid understanding of information security. Information security training and awareness-raising activities are not one-off activities. It is important that they form daily routines and are provided regularly (see Figure 13).
- An effective way to keep teleworkers continually aware of information security is to fashion clear messages, such as those in Figure 14 on the next page, and publish them on the company's intranet or put up posters with the messages in conspicuous areas. Another idea is to print and distribute small cards with contact information in the event of a security emergency at a telework location. This allows teleworkers to carry the information with them at all times.
- It is not easy for system administrators to confirm whether teleworkers are abiding by established rules at their telework locations. Therefore, managers should include, in work regulations or other rules, provisions on the duty to protect confidentiality during telework and on penalties for violations. They should also strive to get teleworkers to understand the benefits of complying with rules.

Teleworkers — Basic Security Measures

- It is important for teleworkers to work habitually to improve their understanding of information security by actively participating in regular training and awareness-raising activities on information security.

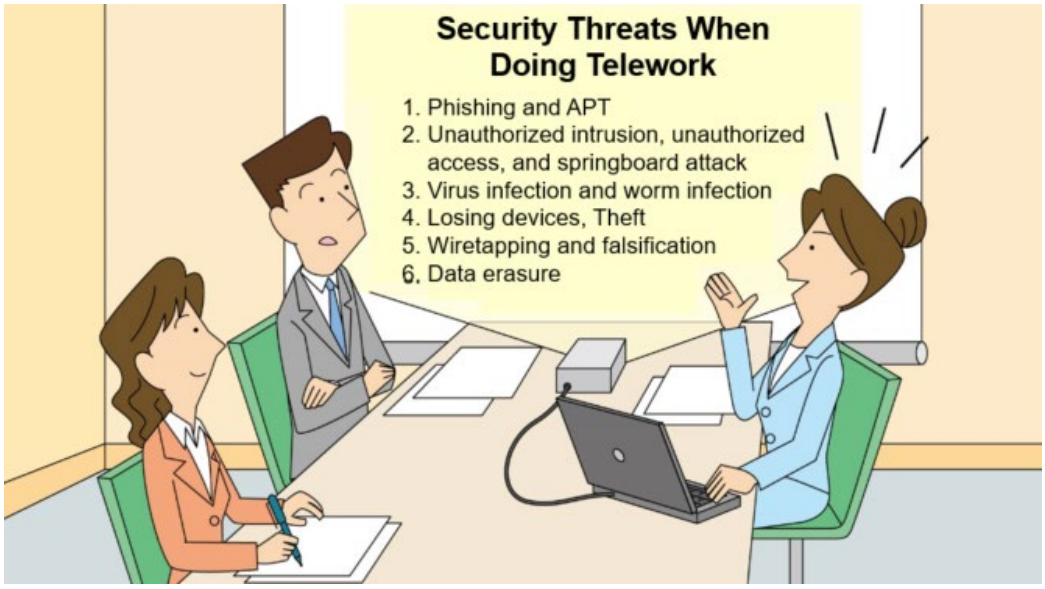


Figure 13 — Information security training

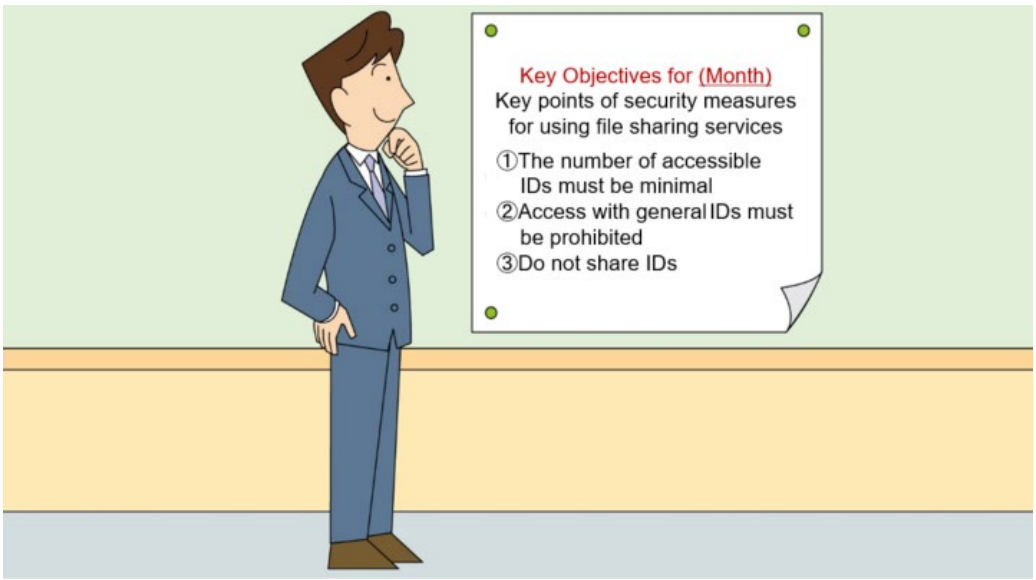


Figure 14 — Raise awareness on intranets and with posters

Managers and system administrators — Recommended security measures

In addition to the security measures described above, means are needed for teleworkers to verify easily whether they are performing telework appropriately or not. Self-assessments can be used as a tool for such verifications. Self-assessments should be performed regularly, roughly once a year, as they are equivalent to an internal audit. Managers and system administrators should communicate in advance to teleworkers that the company will assist them with improving any non-compliant areas. Offering support will discourage teleworkers from giving false answers on self-assessments.

Managers **4**	Managers create a contact system to ensure the organization can respond promptly to information security incidents and hold training exercises to ensure incident response capabilities.
System Administrators **4**	System administrators verify the contact system to ensure the organization can respond promptly to information security incidents and hold training exercises to ensure incident response capabilities.
Teleworkers **4**	Teleworkers verify the contact system so they can contact the specified person in charge immediately in response to information security incidents and participate in training exercises to ensure incident response capabilities.

Managers, System Administrators, and Teleworkers — Basic Security Measures

- It is vital to set up a contact system to ensure the organization can quickly enact response measures in the event of an information security incident and to verify regularly that the contact system works as expected. The impact of information security incidents can be minimized by early detection and early responses.
- Furthermore, analyzing the causes of information security incidents and striving to prevent their reoccurrence is effective in reducing information security incidents across the organization.

Managers, system administrators, and teleworkers — Recommended security measures

There is no way of knowing whether an emergency contact system will function properly in the event of a real emergency just by establishing the system in advance. It is important to run exercises (drills) and actually use the emergency contact system as often as possible (for example, once a year) by setting up various scenarios, such as a new strain of malware that has spread throughout the Internet and paralyzed Internet communications.

Managers 5	Managers demonstrate adequate understanding of information security measures related to telework and allocate sufficient budgets for the necessary personnel and resources to carry out information security measures.

Managers — Basic Security Measures

- Telework is a new form of work. In order to roll out telework securely and reasonably in workplaces without telework experience, appropriate investments are needed in information security measures for telework environments, just as outlays are needed to implement crime prevention measures in office environments. Such investments include more than just the purchase of equipment and devices needed for communications and information security measures. They also include securing human resources to operate and manage the equipment and devices.
- Investing large sums in telework information security measures is not enough on its own. Instead, what is important is first defining how to implement telework at your company and what information assets need to be protected, selecting security methods that suit your telework implementation, and then making the necessary investments in those security methods.

B. Measures against Malware

System administrators 5	System administrators set up filters and other measures to ensure teleworkers do not access dangerous sites.
Teleworkers 5	Teleworkers do not access external websites unless the operating system and browser (including extensions) on their telework device have been updated to the latest version to prevent malware infections.

Teleworkers — Basic Security Measures

- Telework often involves the use of the Internet. Therefore, it is important to make specific provisions for viruses, worms, and other threats that often infect devices and networks via the Internet. Some effective measures are to minimize accesses to non-company websites during telework and to ensure the operating system, web browser, and related applications such as Flash Player and Acrobat Reader have been updated before accessing external sites.

System administrators — Recommended security measures

One effective measure system administrators can take is setting up filters and other mechanisms to ensure teleworkers do not access dangerous sites from the outset.

Case Study No. 2 of Telework Security Incidents and Solutions

- Security incident related to a malware infection -

Telework Security Incident

An employee took a laptop computer normally used at the company off premises and used it for telework. In order to gather information necessary for work, the employee browsed an overseas website (an information aggregator site), after which the computer was infected with ransomware through the site and the screen was locked. Work had to be stopped during the recovery process, resulting in delivery delays.

Possible Solutions

Simply browsing some websites will result in the website attempting to install malware or malicious software on your computer. If some dialog or notice appears on your screen before installation, be sure to thoroughly read what is being installed. In addition, taking multiple security measures such as those listed below will help construct a safe and secure telework environment.

Security measures for teleworkers

- Install anti-virus software on computers and other telework devices
- Keep the operating system and applications up to date
- Install filtering software that blocks accesses to dangerous or illegal sites

Security measures for system administrators

- Install anti-virus software for servers

System Administrators 6	System administrators require teleworkers to apply for permission prior to installing an application on a telework device and give permission after verifying the application poses no information security problems.
Teleworkers 6	Before installing an application, teleworkers apply for permission from their system administrator and only install applications for which permission has been given.
	Teleworkers give due consideration to security before selecting applications to install on devices used for telework (when using personal devices for telework).

System administrators — Recommended security measures

System administrators should require teleworkers to apply for permission prior to installing an application on a telework device and give permission to use the application after verifying the application poses no information security problems. Caution teleworkers to not install applications at their own discretion.

Teleworkers — Recommended security measures

Teleworkers should not download or install applications on a device used as a telework device except for applications provided for work use. If an application must be installed for some reason, teleworkers should apply for permission from their system administrator and only install applications for which permission has been given.

Case Study No. 3 of Telework Security Incidents and Solutions

- Security incident related to anti-virus software -

Telework Security Incident

An employee installed an application (a video download tool made overseas) not permitted for use at the company. The application also installed malware and unfamiliar overseas ads began appearing on the device's screen. Since the ads covered the screen, the employee's work efficiency declined. The employee wanted to uninstall the malware but couldn't.

Possible Solutions

- Prohibit the installation of new applications on devices used for telework. Set devices so that only preinstalled applications can be used.
- Alternatively, create and share a list within the company of applications already deemed secure. Teleworkers are allowed to install applications on the list.

In either case above, after the system administrator has established rules, the rules must be publicized throughout the company. It is pointless to create a list of secure applications if teleworkers don't know where to find it.

Furthermore, system administrators should devise ways to determine what applications teleworkers have installed on devices. For example, system administrators should examine installing ICT asset management software on devices used for telework.

System Administrators 7	System administrators install anti-virus software on telework devices lent out by the organization and configure the software to apply the latest definition files.
Teleworkers 7	Before starting work operations, teleworkers verify that anti-virus software has been installed on the telework device and that the latest definition file is being applied.

System Administrators — Basic Security Measures

- In many instances it is difficult for each member of an organization to apply computer and other information security measures (such as updating virus definition files and applying updates). It is effective, therefore, to select products that can be configured to automatically apply definition files and updates so that uniform security measures can be rolled out in line with the organization's information security manager or system administrator's instructions. Any oversight in the implementation of security measures becomes a vulnerability for the entire organization. Another possibility is to announce critical updates to teleworkers.

Teleworkers — Basic Security Measures

- Telework often involves the use of the Internet. Therefore, it is important to make specific provisions for viruses, worms, and other threats that often infect devices and networks via the Internet. Teleworkers must check that the level of security measures on their telework device is the same as at the office every time before starting work operations. These checks include confirming that the anti-virus software has not expired and that the software is updated with latest pattern file (virus check list).
- Daily updates are ideal, but updates must be performed at least once a week.

Case Study No. 4 of Telework Security Incidents and Solutions

- Security incident related to application use -

Telework Security Incident

An employee performed telework after forgetting to update the pattern file for the security software installed on the telework device. The employee noticed that the device had suddenly been infected by malware.

Possible Solutions

Teleworkers must strictly abide by the following security measures at all times.

- Start telework only after confirming whether new definition files for the security software have been distributed (is the latest definition file applied?).
- Set up the software to update definition files automatically.

News media, the Information-technology Promotion Agency (IPA), and other organizations publish information when malware or malicious software capable of causing major damage are prevalent. Teleworkers should strive to keep themselves informed about the latest security-related news.

Next-Generation Anti-Virus Software

Standard anti-virus software is unable to detect most of the recent malware used for targeted attacks. This is because in targeted attacks, unlike conventional attacks where broadly spreading the malware is a goal, the attackers launch attacks at a small number of targets using new types of malware designed on purpose to evade anti-virus software. Consequently, anti-virus software vendors cannot prepare pattern files to detect the malware.

Various companies have released next-generation anti-virus software to deal with this type of malware. Next-generation anti-virus software programs do not save the characteristics of known malware in pattern files and detect malware by how close suspicious programs match these patterns. Instead they monitor all applications running on the computer or other device, identify applications behaving similarly to malware, and then either display a warning or forcibly stop the operations of the malware. Installing such next-generation anti-virus software programs on devices used for relatively high-risk operations, such as when it is necessary to confirm files attached to emails sent from abroad, is a possible way to implement multi-layered security measures.

System Administrators 8	System administrators update the operating system and software on telework devices lent out by the organization and ensure they are up to date.
Teleworkers 8	Before starting work operations, teleworkers verify that the telework device's operating system and software have been updated to the latest version.

System Administrators — Basic Security Measures

- System administrators must perform updates not only for operating systems but also for primary applications and middleware. If updates are not performed, vulnerabilities will be left open, increasing the likelihood of successful external attacks.

Teleworkers — Basic Security Measures

- Teleworkers should confirm on their own that the operating system and software have been updated to the latest version in the same way as with anti-virus software.

Case Study No. 5 of Telework Security Incidents and Solutions

- Security incident related to software updates -

Telework Security Incident

A dedicated computer had been used for telework only a couple of times a year. An employee booted up the computer and noticed the operating system and installed applications had not been updated. But because work was urgent, the employee used the computer for telework as is and searched the Internet in the process of creating materials for a survey. At the time, the employee did not notice any abnormalities, but the next time the computer was started up, fake security software ads — "Your computer is infected with multiple viruses. You must buy our product to remove them immediately." — kept popping up continuously, which drastically reduced the employee's work efficiency.

Possible Solutions

Teleworkers must bear in mind that starting up a computer used only occasionally will have vulnerabilities right after launching. Therefore, teleworkers must first perform updates of the operating system and applications before starting on work operations. Because such updates may take a long time, regularly updating computers is a possible strategy to ensure efficient work operations. It is also worth considering the virtual desktop pattern, as it allows the use of a desktop device that does not need this update process.

System Administrators 9	When personal devices are permitted for telework, system administrators approve personal devices after verifying the devices have the required information security measures in place.
Teleworkers 9	Teleworkers use devices for telework on which information security measures specified in rules have been applied and do not perform unauthorized modifications, such as jailbreaking or rooting, to smartphones, tablets, or other devices.

System administrators — Recommended security measures

When teleworkers use their own devices for telework (bring your own device, or BYOD), system administrators should remind teleworkers to confirm that the device has the required information security measures in place prior to permitting them to use their own devices.

Teleworkers — Recommended security measures

Using a personal device for telework runs the risk that the device will cause a company-wide security breach if the device is not properly managed. An improperly managed device is susceptible to malicious software infections or being used as an entry point to gain unauthorized access. Recently, smartphones and tablets, along with computers, are increasingly used for telework. Teleworkers, however, must make sure not to use devices with unauthorized modifications (for example, jailbreaking or rooting a smartphone) as telework devices for work operations. Even after obtaining permission to use a personal device for telework, be sure to always abide by the established rules on the use of personal devices.

Using a device lent by the company for telework for purposes other than the originally defined work operations is not only inappropriate, since a company asset is being used for a non-company purpose; it can also lead to a malicious software infection or other security risk. In addition to being conscious of how you use the device, it is vital that you do not let anyone else use the device when working in environments where large numbers of unknown people come and go.

System Administrators 10	System administrators save backups of critical electronic data in locations isolated from internal systems to guard against ransomware infections.

System administrators — Recommended security measures

Ransomware is a special type of malware that does not steal data from a device. Instead, it encrypts data accessible from the infected computer or device making it impossible to use the data. Only the attacker knows the decryption key for the encrypted data. Users who cannot make use of their data suffer losses when they pay the sum demanded by the attacker to obtain the decryption key. It is not recommended to pay money to attackers, as there are cases where data was not decrypted even after paying the sum demanded.

Case Study No. 6 of Telework Security Incidents and Solutions

- Security incident related to ransomware -

Telework Security Incident

A company's internal systems were infected by ransomware via a telework device used by an employee. The ransomware made it impossible to access critical information, and the attacker demanded a large sum of money to remove the ransomware. The company was forced to pay the amount demanded by the attacker in order to regain access to the critical information, but the attacker did not send the key to decrypt the data.

Possible Solutions

System administrators can prevent losses from ransomware by making backup copies of critical company information and storing the backups in locations inaccessible from networks or in locations where data cannot be overwritten. The following examples are possible anti-ransomware measures.

- Store backup copies on USB flash drives or removable hard drives or SSDs, remove the storage devices from their associated devices, and safeguard them in a locked location
- Store backup copies on media that cannot be overwritten, such as DVD-R disks, and safeguard the media
- Store backup copies on a partition of a server configured so that no users of any computers susceptible to infections have permission to overwrite or delete data in the partition

System Administrators 11	System administrators configure mailing systems to classify suspicious email, such as email masquerading as business communications from financial institutions or distributors, as spam.
Teleworkers 10	Teleworkers are aware that a failure or delay in reporting a malware infection that occurred during telework may lead to greater damage to the organization and exercise due caution when opening email attachments or clicking on links in email messages.

Teleworkers — Basic Security Measures

- Threats that must be watched out for during telework include targeted targets by malware and phishing attacks. These threats exist when working in an office environment as well, but in an office setting, it is easy to ask a nearby coworker to double-check whether an email is suspicious or not. With telework, on the other hand, it is not easy to double-check suspicious emails with others and email is used frequently for work conversations and exchanges, raising the odds that teleworkers will accidently open a phishing email. The biggest danger in telework are emails that appear to be sent from the email address of an acquaintance. Teleworkers should aim to isolate any emails that seem suspicious without opening them. The same holds for clicking on links on untrustworthy websites.

System administrators — Recommended security measures

System administrators should strive to prevent risks as much as possible by configuring mailing systems to flag suspicious email as spam so teleworkers do not open them by accident. Recently, however, emails used for targeted attacks are designed very cleverly and many appear to be from a legitimate sender. Therefore, system administrators must understand that complete protection is virtually impossible.

Teleworkers — Recommended security measures

If your device is infected with malware during telework or you suspect it has been infected, be sure to immediately report the infection to your department supervisor or system administrator. Failing to report or delaying a report may lead to the malware infecting the entire company via the telework device and causing significant damage. There is a tendency to not want to report infections because reporting will have consequences for you, such as not being able to proceed with your work for a while. Nevertheless, you should decide to report infections, after considering the potential for an unreported infection to paralyze the entire company and cause extensive losses to everyone at the company.

Use of Internal Social Media

Telework generally relies on frequent use of email as a communication tool. Furthermore, there is no one close at hand who can double-check suspicious emails. Consequently, telework is seen as being more susceptible to phishing, spoofing, and other harm.

To avoid such harm, an increasing number of companies are using internal social media and other communication tools other than email for inter-employee communications. Internal social media is expected to both boost security and make work operations more efficient, through more active communications and easier file sharing.

Case Study No. 7 of Telework Security Incidents and Solutions

- Security incident related to a suspicious email -

Telework Security Incident

During telework, an employee received an email with the subject line "Re: Credit Card Charges" delivered to her work email address. The email was from the employee's credit card company, but since the employee had not made any recent purchases with the card, she wanted to check whether an incorrect charge had been made. The employee clicked on the link in the email message and entered the card number and expiry date as instructed. Shortly thereafter the credit card was used fraudulently. In retrospect, the employee realized she should have noticed the email was suspicious because she hadn't informed her credit card company of her work email address.

Possible Solutions

Suspicious emails can be flagged as spam and stored in a separate location from your regular inbox or deleted automatically. There are three ways to deal with suspicious email.

Security measures for teleworkers

- Use anti-spam functions in mailing applications

Security measures for system administrators

- Install security tools on telework devices that can both detect malware and ascertain all kinds of threats, such as abnormal behavior
- Weed out email matching certain criteria (such as written in a language other than Japanese or has an executable file attached) at your worksite mail server, for example
- Use anti-spam functions offered by your Internet service provider

C. Measures against Loss or Theft of Devices

Teleworkers 11	Before taking information assets outside the office, teleworkers store the originals in a secure location.
Applies to Telework Pattern 6 (Company computer take-home pattern)	

Teleworkers — Recommended security measures

From the standpoint of data breaches, risk levels are the same for original documents and duplicates. Nevertheless, preparing duplicates as backups is a final means of defense against electronic data tampering or destruction caused, for example, by a virus. Such backups should be saved on storage devices that can be removed from computers or other devices, such as external hard drives, SSDs, or USB flash drives. If the original copy has been saved, it is possible to restore altered or lost electronic data.

The use of duplicates is also a measure against accidental deletion of electronic data by employees or computer malfunctions or losses, in addition to virus infections. Making backups is an essential security measure especially for devices on which data for work documents are used and for devices used to develop programs, create websites, or carry out similar operations.

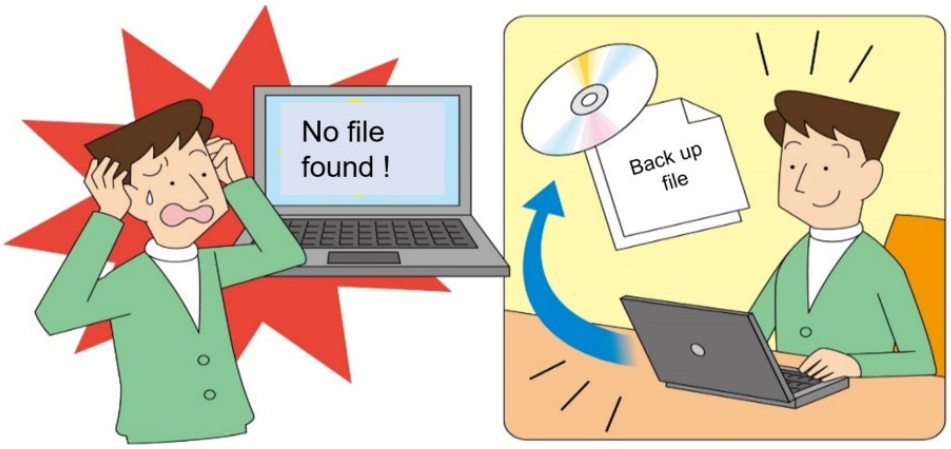


Figure 15 — Importance of backing up electronic data

System Administrators 12	System administrators establish a registry or other tracking method to manage the location, user, and other particulars of telework devices lent out by the organization.
Teleworkers 12	Teleworkers devise working arrangements to avoid the necessity of extra management for electronic data requiring confidentiality protection. In unavoidable circumstances, teleworkers always encrypt and store electronic data requiring confidentiality protection and take precautions against the theft of devices or storage media (such as USB flash drives) containing electronic data.

System administrators — Recommended security measures

System administrators must appropriately manage the lending out of telework devices by the company so no one other than the employee with prior permission uses the telework device. A registry or other tracking method should be established in order to know where each telework device is and its status. Including a column for noting the status of patch applications and other security measures on the telework device is useful, as system administrators can check whether a device is ready to be lent out immediately. Similarly, having a registry or other tracking method is effective even when personal devices are used for telework.

Care must be taken when disposing or transferring devices, USB flash drives, or other storage media that have been used for telework. Placing data in the recycle bin and emptying the recycle bin does not completely delete the data. Extra measures are needed to ensure data cannot be recovered, such as using specialized deletion software or physically destroying hard drives.

Teleworkers — Recommended security measures

Telework devices are assumed to be used in various locations. In some of these locations, it may be easy for malicious third parties to come close to telework devices. Teleworkers need to be aware of these risks, and approaches should be devised so that telework can be performed without handling confidential electronic data. In cases where confidential electronic data have to be managed on a telework device, prevent unauthorized use of the telework device by others by, for example, encrypting electronic data on the telework device. Encryption can also prevent data breaches through data theft or the loss or theft of telework devices or storage media. There are two ways of encrypting stored data: encrypting the entire drive or USB flash drive or encrypting individual files. Select the method according to how the data are used and the confidentiality level of the information. Using both types of encryption is an idea to protect highly sensitive information.

Teleworkers must take security measures when doing telework in a coffee shop, on public transportation, or in a waiting area where the environment is shared with third parties, in order that the telework device is not used by anyone else. These security measures include setting a password or using fingerprint or facial recognition for user authentication or setting an auto screen lock (the screen locks after a set time when the computer is idle). When leaving your seat on a train or in a public waiting area, you should carry the device with you. When this is not practical, you can take such measures as securely locking the screen and installing an anti-theft cable.

Teleworkers must be aware of the cautions given above in the section for system administrators when disposing or transferring personal devices, USB flash drives, or other storage media that have been used for telework. If you cannot reliably delete data on your own, consider asking your system administrator to do it for you.

Case Study No. 8 of Telework Security Incidents and Solutions

- Security incident related to the loss of a device -

Telework Security Incident

An employee travelling by train forgot his bag that contained a telework device. The device stored a client list, which included past transactions, on the local disk. Realizing he had forgotten his bag, the employee contacted the train company the next day, but there had been no reports of lost property. Several months later, a client lodged a complaint that it had "received a sales call to a phone number only known by your company". This resulted in all sales representatives making efforts to apologize to the client.

Possible Solutions

The most appropriate security measure for devices that are frequently taken off premises and are more likely to be stolen or lost is for the system administrator to prepare specific devices without any information stored internally and have teleworkers use these devices. This is suitable for the remote desktop, the virtual desktop, and the cloud app telework patterns. In cases where not having information on the device is inconvenient, such as being unable to use a smartphone or other device in a location out of range of radio signals, the system administrator can encrypt work information on the internal hard drive or SSD and ensure the decryption key (password to unlock files) is not stored on the device.

Teleworkers should normally enable remote wipe (a function that can remotely delete data on a device) on smartphones or other devices with this capability. It must be remembered, however, that remote wipe will not work when a device is deliberately stolen in order to steal data and the device is turned on in a location out of range of radio signals.

D. Measures against Interception of Critical Information

Teleworkers 13	Teleworkers always encrypt electronic data requiring confidentiality protection prior to sending the data.

Teleworkers — Basic Security Measures

- Malicious third parties can intercept communications over the Internet. Caution must be exercised especially when using public Wi-Fi.*
- When exchanging electronic data, whether it is confidential or not, back and forth with your office, for security reasons, use a communication channel like a VPN that allows communications to be encrypted. Note also that emails sent via the Internet are not encrypted unless expressly specified that they are encrypted.

*See the MIC's *Simple Manual for Wi-Fi Users* for details.

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/wi-fi.html

Case Study No. 9 of Telework Security Incidents and Solutions

- Security incident related to the use of public Wi-Fi -

Telework Security Incident

A teleworker sent and received emails using public Wi-Fi. It was discovered later that a rival company had found out about confidential information contained in a file attached to one of the emails.

Possible Solutions

As described on the next page, communications over public Wi-Fi, hotel Internet connections, and other networks without password protection are at risk of being intercepted by other users on the network at the same time. Even when a network is password protected but the password is given out to many people, attackers can still intercept communications by spoofing the access point with a fake spoofing access point. When it is necessary for teleworkers to send or receive confidential information in such environments, it is appropriate to encrypt files containing confidential information in advance, use mailing applications with encryption functions, or use services like a VPN that encrypt the communications channel. Note that sending the password for decryption in a separate email is not a secure measure. A better scheme is needed, such as providing the password over the phone or by a short message.

System Administrators 13	System administrators ensure appropriate measures are taken to protect telework devices against Wi-Fi vulnerabilities.
Teleworkers 14	Teleworkers understand the risks associated with Wi-Fi use and use Wi-Fi for telework only within the extent where appropriate measures commensurate with the proper security level can be taken.

Teleworkers — Basic Security Measures

- The following two points must be kept in mind when using Wi-Fi at home.
  - † Enable WPA2 encryption of your communication channel on your Wi-Fi router and set a password that others cannot easily guess.
  - † Ensure you update your telework device and take measures so no known Wi-Fi vulnerabilities are present.
- When using a Wi-Fi access point accessible by the general public while out of the office, in addition to taking the security vulnerability measures above, use the access point with a method that satisfies one or more of the following conditions.
  - † Use the access point via an VPN.
  - † Limit your use to websites with addresses starting with “https:”.
  - † Only use trustworthy applications (computer, smartphone, tablet).
  - † Limit your use to activities that will not cause a problem even if security is breached (such as looking up maps or routes).

Teleworkers — Recommended security measures

It should be obvious that information communicated over unencrypted Wi-Fi access points is liable to be intercepted. Even when communications are encrypted, there is still a risk of security breaches through access point spoofing of access points where the password is widely known (including Internet access provided by hotels and coworking spaces). Therefore, you should not consider an access point secure because it is encrypted. You should instead implement multi-layered security measures, such as using a VPN (see Figure 16).

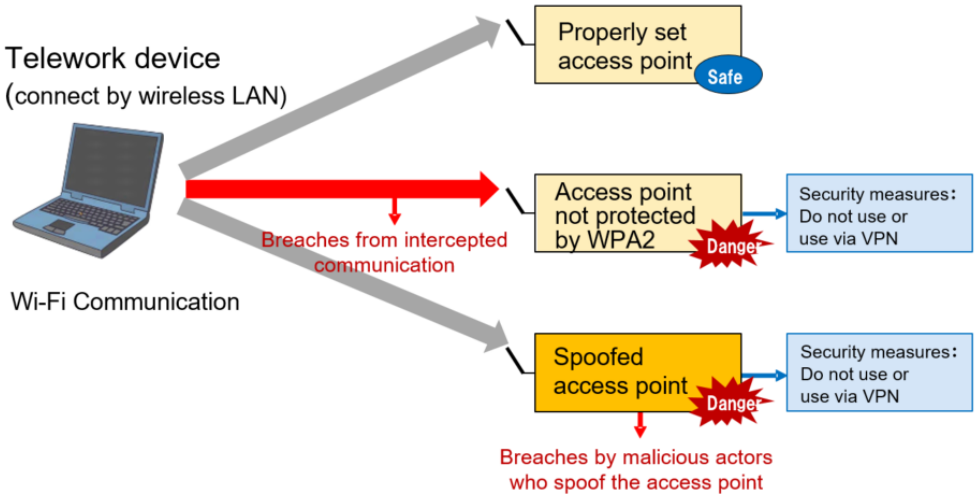


Figure 16 — Risks associated with Wi-Fi use

Teleworkers 15	When working in a shared environment with third parties, teleworkers strive to prevent others from viewing their device screen by, for example, installing a privacy filter over the screen or choosing a discreet work location.

Teleworkers — Recommended security measures

Teleworkers must pay attention to the threat of third parties viewing and stealing work information displayed on a screen while performing telework in an environment shared with third parties, such as a café, a coworking space, on public transportation, or a waiting area. One measure is installing a privacy filter on the telework device screen to prevent shoulder surfing by people in adjacent seats. It is also more secure when it is possible to choose a seat where your back is against a wall. Unfortunately, these schemes cannot fully keep your device's screen out the line of sight of other people. Therefore, teleworkers should avoid viewing or editing information they do not want to expose to the gaze of third parties in shared environments. In cases where teleworkers know in advance they cannot avoid working with sensitive information in shared environments, a possible measure is to remove proper nouns and other sensitive data from materials in order to limit damage should the information be stolen or intercepted.

Case Study No. 10 of Telework Security Incidents and Solutions

- Security incident related to shoulder surfing -

Telework Security Incident

A teleworker worked on presentation materials about a new unannounced product while traveling for work on a bullet train. Soon after, an unknown person posted information from the materials on social media with the comment: “Leaked information on Company X’s new product”.

Possible Solutions

Teleworkers should install a privacy filter on their devices when carrying out telework in an environment in the line of sight of others in order to make shoulder surfing more difficult. Nevertheless, people in adjacent seats may still be able to read through privacy filters when you are editing presentation slides or other documents with large text sizes. Consequently, teleworkers should endeavor not to look at or create such materials while in an environment where others can see their device screen.

E. Measures against Unauthorized Accesses

System Administrators 14	System administrators set out clear technical standards for user authentication for external access to internal organization systems and manage and operate the standards correctly.
Teleworkers 16	Teleworkers properly manage their user authentication credentials (passwords, IC cards, etc.) required for external access to internal organization systems.
These measures apply to telework Pattern 1 — remote desktop pattern, Pattern 2 — virtual desktop pattern, Pattern 5 — app wrapping pattern, and Pattern 6 — company computer take-home pattern	

System Administrators — Basic Security Measures

- Channels to access internal organization systems from telework locations may become channels for malicious third parties to illegally infiltrate internal systems. Therefore, system administrators must set out clear technical standards for user authentication of teleworkers to access to internal organization systems and manage and operate the standards correctly. These standards may include the use of multi-factor authentication methods or combining authentication with digital certificates.
- The remote desktop and virtual desktop telework patterns allow teleworkers at remote locations to view only screen images of data (graphical data) and not the actual electronic data. A benefit, therefore, of these patterns is that even if the telework device were stolen, no data breaches or other damage would occur since no actual electronic data are stored on the device. However, should the account and password to connect to internal systems be stolen along with the device, a malicious third party would be able to spoof the teleworker, access internal systems, and perform all kinds of operations. Consequently, system administrators must deploy appropriate protection measures, such as ensuring passwords and other authentication credentials are not saved on telework devices.

Teleworkers — Recommended security measures

Teleworkers must correctly manage their user authentication credentials (passwords, IC cards, etc.) used for external access to internal organization systems. If such credentials were divulged, it would expose all kinds of critical information to danger, such as third parties spoofing the teleworker and accessing critical information.

System Administrators 15	System administrators define acceptable access methods when teleworkers access internal organization systems via the Internet. Furthermore, system administrators install firewalls, routers, and other security equipment at the boundary between internal systems and the Internet to monitor accesses and to block unnecessary accesses.
Teleworkers 17	Teleworkers use only the access methods specified by the system administrator when accessing internal organization systems via the Internet.

System Administrators — Basic Security Measures

- Malicious third parties probe for vulnerabilities in information systems via telework devices and illegally infiltrate internal organization systems or masquerade as account holders and illegally access internal systems. System administrators, therefore, must take measures to prevent both unauthorized intrusions and unauthorized accesses. Unauthorized intrusions can be prevented by installing firewalls or other security equipment either between the Internet and internal systems or at boundaries with information assets to be protected within the organization. Unauthorized accesses can be prevented and access to information assets controlled by implementing stringent authentication measures to confirm individuals' identity and by beefing up authentication functions using, for example, access passwords or one-time passwords.

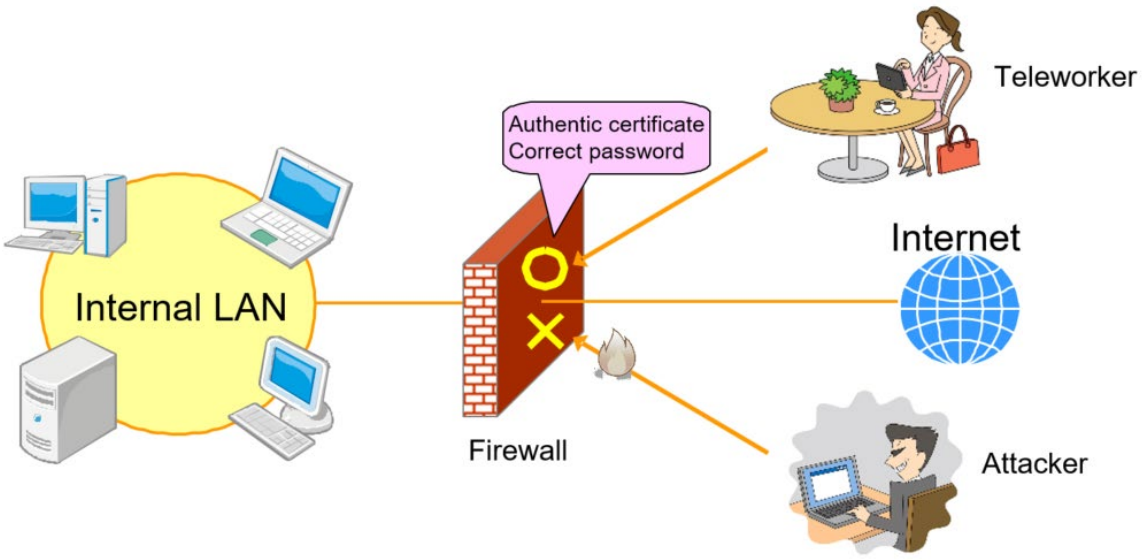


Figure 17 — Location of a firewall

System Administrators — Recommended security measures

If internal organization systems become infected by viruses or worms, they could

potentially infect large numbers of telework devices and consequently have large consequences for the entire organization. Although stopping the spread of viruses or worms is both technically and operationally challenging, system administrators need to implement security measures that aim for early detection / early response and detection and control.

Immediate detection and control of data breaches caused by unauthorized intrusions or unauthorized accesses is difficult. Collecting access logs, however, of the usage status of internal systems can aid in investigating and tracking data breaches caused by unauthorized intrusions or unauthorized accesses.

Teleworkers — Recommended security measures

Telework is founded on sending and receiving electronic data over the Internet. This activity exposes electronic data to the possibility of being intercepted, stolen, or tampered with. Therefore, teleworkers must ensure they use communication channels with high security levels, such as encrypted communications. From this perspective, teleworkers need to adhere to the means of communication specified by their system administrator.

The proper use of Wi-Fi has become increasingly important recently, as more smartphones use Wi-Fi. See the manual below* for specific information security measures for Wi-Fi.

*MIC's *Simple Manual for Wi-Fi Users* available at
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/wi-fi.html

Another danger is telework devices being turned into bots that attackers then use to connect to internal organization systems and cause harm to third parties. Teleworkers, therefore, must always keep their telework devices in a secure state by applying proper security measures to protect devices from becoming attack targets.

Case Study No. 11 of Telework Security Incidents and Solutions

- Security incident related to bots -

Telework Security Incident

A system administrator installed a firewall at the boundary between the company's internal systems and the Internet and limited access to internal systems from the Internet to only telework devices used by employees. Unfortunately, a single telework device was infected by malware. An attacker took over the device and used it as a bot to infiltrate the internal systems and make off with customer information.

Possible Solutions

The security measures teleworkers apply to their telework devices are critical in protecting telework devices from being turned into bots. Over and above installing anti-virus software and keeping it up to date, measures are required to prevent infiltration from the outside, such as enabling firewall functions on devices.

System administrators should analyze logs of internal system accesses from telework devices so they can surmise from irregular access patterns the possibility that a device has been turned into an attack bot.

System Administrators 16	System administrators set up measures that prevent the use of weak passwords for accessing internal organization systems.
Teleworkers 18	Teleworkers avoid using their telework password for other sites and strive to use a difficult-to-guess password longer than the prescribed length.

System Administrators — Basic Security Measures

- The need to pay attention to password management is not limited to telework. Telework, however, exposes lots of critical information to the danger of being breached because telework involves environments that anyone can access via the Internet. Should a password be exposed in such an environment, third parties can successfully spoof the teleworker and access critical information. This is why the management of passwords used for telework requires special attention. System administrators should endeavor to ensure teleworkers do not use the same password used for other applications, such as online shopping or online banking, and use difficult-to-guess passwords.

System Administrators — Recommended security measures

System administrators should prohibit passwords for accessing internal organization systems that meet any of the conditions listed below.

- Passwords that are the same as passwords used for other systems or for private use
- Short passwords (generally meaning passwords shorter than eight characters)
- Simple passwords (such as “11111111”, “ABCDEFGH”, or “password”)
- Passwords that use the same character string as the user ID or are the user ID plus one additional character
- A single word or combination of words found in the dictionary (such as “telework”)

System administrators should make use of commonly available system functions that prevent users from setting short or simple passwords.

Teleworkers — Recommended security measures

It is difficult to remember passwords when different passwords are used for each

site. It is acceptable, therefore, to write down passwords that cannot be remembered. But teleworkers must strive not to carry around password notes in the same bag or case as their telework device. If carrying password notes together with the telework device is unavoidable, teleworkers should not write the exact passwords down but instead devise rules known only to them (such as removing numbers or changing the order of characters in the password) so that other people cannot log in by entering the characters as written down.

There is no need to change passwords frequently, but teleworkers should change passwords as soon as possible if the password notes are seen by an untrusted person or after logging into internal systems from a shared device.

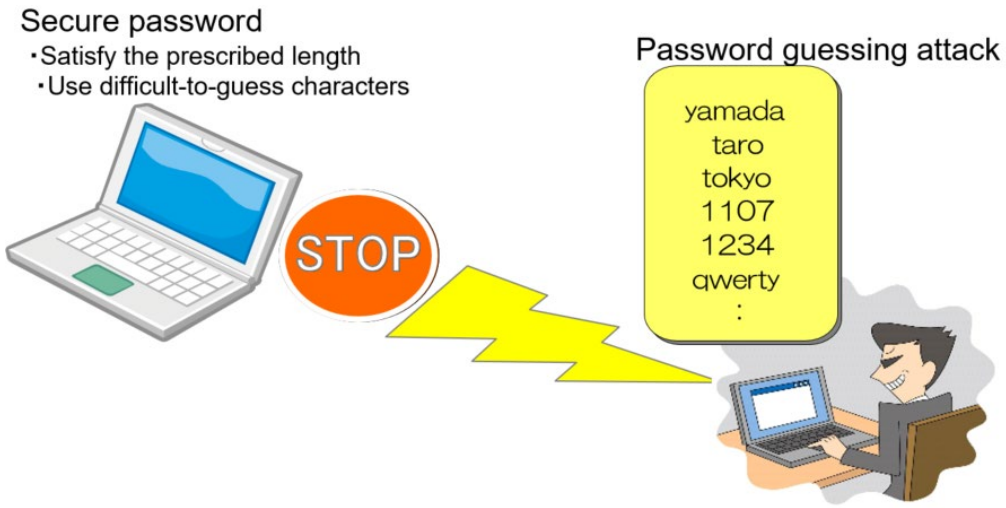


Figure 18 — Management of account passwords

A Way to Manage Passwords

You shouldn't use the same password for different services, but password management becomes increasingly complicated as you set different passwords for more and more services.

One way of simplifying password management is to create a master password string that only you know and then append a set of characters or numbers to the master password string to form passwords for each service. To guard against forgetting a password, you may store just the appended portions either in an electronic file or as written notes. This way, even if your password notes are stolen, the risk of unauthorized accesses is low because the master password string is concealed. Methods such as these can simplify secure password management.

Example:

Master password string: telesec1794

Password for service A: telesec1794Se1

Password for service B: telesec1794k4O

Password for service C: telesec17942R3

Case Study No. 12 of Telework Security Incidents and Solutions

- Security incident related to password management -

Telework Security Incident

An employee set a combination of the company's abbreviation and her birthdate as a password for a file server. Evidence was later discovered that someone had guessed the password and successfully logged in illegally. The file server stored personal information on customers. The company had to apologize to all customers whose personal information may have been exposed.

An employee used his password for an online shop he used privately for telework as well. The online shop's passwords were hacked and the stolen password was used to illegally access the employee's work account as well.

Possible Solutions

Teleworkers must create passwords for telework that meet the following conditions to prevent such unauthorized accesses. A specific method for generating passwords is given in the sidebar on the previous page.

- Select a character string that others cannot easily guess or deduce
- Select a character string that is different from any password used for other services or applications
- Select a character string that is not a word or combination of words in the dictionary

Is It Safe to Let Your Browser Remember IDs and Passwords?

Many Internet browsers have a function that remembers website IDs and passwords for you. This type of function is convenient because it alleviates the need to enter IDs and passwords. But you must be aware of the security risks of using such a function.

When a browser remembers IDs and passwords, they are saved on the device's hard disk. Consequently, if the device is infected with malware for example, it is possible that the IDs and passwords the browser has stored on the hard disk will be stolen. Therefore, it is recommended that you enter IDs and passwords for important services yourself and not let the browser remember them for you.

F. Measures for the Use of External Services

System Administrators 17	System administrators set out usage rules and guidelines for employees regarding social media, including messaging applications, and include in the rules and guidelines specific usage considerations for telework.
Teleworkers 19	When using social media, including messaging applications, for telework, teleworkers follow the social media usage rules and guidelines set by the organization.

System Administrators — Basic Security Measures

- Facebook, Twitter, Instagram, and other social media services are particularly convenient for teleworkers because information can be shared easily over the Internet from anywhere. But because of their convenience, social media exchanges of work-related information are susceptible to being breached or hacked.
- Social media services allow users to set limits on who can see information, such as "friends only". But if you have friended many people, information can make its way to people who should not receive it.
- Therefore, system administrators should set social media usage rules and guidelines containing the following stipulations in advance and make teleworkers aware of the rules.
  - † Do not handle work-related information subject to confidentiality obligations on social media.
  - † Do not make posts that violate laws or ethics and do not make non-factual posts.
  - † Make clear distinctions between public and private conversations and take care that your posts are not mistaken as being statements from the company.

System Administrators and Teleworkers — Recommended security measures

- Social media messaging apps, such as Line or Facebook Messenger, are designed to send messages only to specified parties; therefore, there is less need, compared with social media, to restrict the content of messages as described in the basic security measures above. Security incidents can still occur however, if messages are sent to the wrong party. Particular attention must be paid when sending messages from a personal device at home used for telework, because work addresses and private acquaintances can be easily confused.
- When using social media on a telework device, operations performed on the device, such as online shopping, may be accidentally communicated to

acquaintances. To avoid such side-effects, the secure approach is to not log into social media accounts from the telework device.

Case Study No. 13 of Telework Security Incidents and Solutions

- Security incident related to social media use -

Telework Security Incident

A teleworker received an email from work requesting the teleworker to share information. The teleworker meant to answer by posting the information to work group X on social media but accidentally posted the information to an active public group related to the teleworker's personal interests. Furthermore, the teleworker did not notice the mistake and left the post up. The teleworker deleted the post a few hours later after being alerted to its existence, but the teleworker got stuck going around and apologizing to everyone connected with the posted information and couldn't work for three days.

Possible Solutions

Using a single social media account both for work communications and private messages is the cause of such data breach incidents. The following are potential security measures to avoid this risk.

Security measures for teleworkers

- Pay meticulous attention to who can see the post before posting on social media

Security measures for system administrators

- Prohibit the use of social media for work purposes
- Establish guidelines on using social media for work and ensure teleworkers comply with the guidelines
- Regularly monitor social media posts to check whether they are related to the company

System Administrators 18	System administrators set out usage rules on file sharing services and other public cloud services and prohibit types of usage where there is concern of data breaches.
Teleworkers 20	Teleworkers only use file sharing services or other public cloud services for telework within the extent permitted by organization rules.

System Administrators — Basic Security Measures

- When a teleworker is exchanging data with a client, it is often easier to use file-sharing services or file-transfer services on the Internet rather than transferring data via the work-provided VPN. These type of data transfers that the teleworker's supervisor or system administrator don't know about can lead to data breaches or other security incidents because of inadequate encryption or other security measures.
- Therefore, system administrators should establish rules or guidelines with the following stipulations on teleworkers' use of file-sharing services and make teleworkers aware of the rules or guidelines.
  - † Teleworkers may only use pre-specified file-sharing services.
  - † Encrypt files before uploading.
  - † Promptly delete files from the file-sharing service once the receiver has downloaded the files.

Teleworkers — Recommended security measures

- Saving data used for work on a public cloud is convenient because the data can be accessed from anywhere. Caution must be exercised however, because public cloud services are designed to be directly connected to the Internet, making them easy targets for attacks. It is possible to limit data access to only users with access privileges by using passwords or digital certificates. Nevertheless, data may still be exposed to danger in the following instances.
  - † When vulnerabilities are found in the systems used by the public cloud.
  - † When one of the users with access privileges to the data on the public cloud has passwords or other authentication credentials stolen.
- Another possibility is to use a secure cloud solution or similar service when regularly sharing data over the Internet is absolutely necessary. Such public cloud services provide added value in the form of enhanced security functions.

Case Study No. 14 of Telework Security Incidents and Solutions

- Security incident related to public cloud use -

Telework Security Incident

A teleworker saved work files related to a project on a public cloud service and shared them with related people including outside contractors. Unfortunately, the teleworker made a mistake with the security settings and didn't apply access controls, meaning anyone could access the work files. As a result, the company lost its first-mover advantage to a rival company and eventually the project was cancelled.

Possible Solutions

Wrong settings on cloud services often lead to data breaches and other incidents. Both system administrators and teleworkers must pay attention to the following considerations in order to share files securely using cloud services.

- Prior to using a service to save critical information, confirm that access is denied to IDs without access permission.
- Set limits on the source IP addresses or domains that can access the files.
- Use cloud services from operators that prioritize security, such as promptly patching vulnerabilities.
- Strictly manage IDs, passwords, digital certificates, and other credentials used to access the cloud service.
- Use multi-layered security measures, such as encrypting files before transferring them to the cloud.

Glossary

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.
Access point	A special device that relays communications between devices and the Internet that communicates with devices wirelessly and to the Internet through a wired connection.
Account	Permission to log into a network or internal system (such as a user ID).
Bot	A computer that is hijacked by a third party without the user's knowledge and used as a relay point for unauthorized access attempts or sending out spam.
Definition file	A file containing the characteristics of viruses, worms, and other forms of malware. Definition files are used to detect viruses, worms, and other forms of malware.
Firewall	Equipment designed to protect servers and other equipment connected to internal networks from unauthorized access via the Internet.
Information security policy	Information security policies can refer to a basic policy on information security, to a basic policy and security measure standards, or to a basic policy, security measure standards, and implementation details. These guidelines use information security policy to refer the general concept that encompasses all three of these components.
Malware	A generic term for malicious software, including viruses, worms, and Trojan horses. Malware infects computers, smartphones, and other devices without the owner's knowledge and performs unwanted activities, such as interfering with the device's normal operations, destroying data, or sending data to outside parties.
Middleware	Software that performs intermediate processing between the operating system and other applications.
One-time password	An authentication method that enables the generation of a password that can be used only one time.
Operating system (OS)	Software needed to run the basic operations of a computer or other device, such memory and hard drive management and keyboard and other I/O functions.
Patch	A program to improve and enhance existing software that is specifically written to repair parts of existing

	software.
Personal firewall	Software installed on a computer that provides functions to block unauthorized access and other connections to the computer.
Phishing	An attack method that masquerades as an email or website from an actual legitimate address that urges the receiver to enter credit card numbers or other confidential information or tries to infect the device with a virus.
Ransomware	Malware that encrypts data accessible from an infected computer. Attackers make profits by demanding money from the user of the computer in turn for decrypting the data.
Router	A device that controls the communication channels between devices connected to a network.
Safe domain	A domain where critical information assets that must be protected can be placed in a normal state free from harm or damage. A safe domain must ensure the three main factors of information security — confidentiality, integrity, and availability. Such domains must be examined from both physical security measures, such as seismic-protection equipment and entry and exit controls, and logical information security measures, such as access controls and user authentication.
Satellite office	A facility in an office format located separately from the primarily workplace. Some satellite offices are set up for the exclusive use of one company, while others are shared by multiple companies.
Solid state drive (SSD)	A storage device using semiconductor memory designed to be used as a disk drive in the same way as a hard drive.
Targeted attack	Unlike viruses or worms that attack any target, an attack limited to a specific organization or user that often uses email masquerading as coming from a known sender.
Telework center	A facility in an office format provided as a workplace for teleworkers. Also called a satellite office.
Thin client	A function on the device side that involves installing a special application on the computer, smartphone, or tablet that connects to a peripheral device (usually in a form similar to a USB flash drive). This service enables the device user to connect remotely to internal systems and view and edit electronic data on the internal systems without creating a copy of the data on the device.
Trojan horse	A type of malware. Masquerading as useful software to be installed on computers, smartphones, or other

	devices, a Trojan horse has, as part of the software, functions that act with malicious intent and cause harm to the owner of the device.
Update	Refers to the electronic data, and the process of applying the data, that replace defective portions of existing software with code that apply security measures or that add code to enhance the functions of existing software.
USB flash drives	A portable storage device that is used by connecting it to a USB connector.
Virtual desktop infrastructure (VDI)	An environment in which multiple virtual computers are set up on a server in a way that lets users of the server access the virtual computers that have the same usability as if an individual computer were set up for them. VDI is one way of implementing thin clients.
Virtual private network (VPN)	A method of building a protected virtual dedicated communication line using authentication technology, encryption, and other technologies over a public network like the Internet.
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.
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.
Worm	A type of malware. Worms run on computers, smartphones, and other devices and have functions to send copies of themselves to other devices on networks in order to spread the infection.

Reference Links

- **Work-Style Reforms Beginning with Telework: Telework Adoption and Operation Guidebook** (Ministry of Health, Labour and Welfare)
  http://work-holiday.mhlw.go.jp/material/pdf/category7/01_01.pdf
  Based on knowledge and expertise gained through a three-year pilot project run by the Ministry of Health, Labour and Welfare and the Ministry of Internal Affairs and Communications, the guidebook describes the benefits of telework, approaches to labor management and how to use labor management tools when adopting telework, how to select ICT systems and tools from the point of security, and procedures for using ICT systems and tools.

- **Cybersecurity Management Guidelines** (Ministry of Economy, Trade and Industry)
  http://www.meti.go.jp/policy/netsecurity/mng_guide.html
  The guidelines put together three principles that managers must be aware of from the viewpoint of protecting enterprises from cyberattacks and ten priorities that managers should point out to leaders (such as CISOs) responsible for implementing information security measures.

- **Information Security Measure Guidelines for SMEs** (Information-technology Promotion Agency, Japan)
  https://www.ipa.go.jp/security/keihatsu/sme/guideline/
  The guidelines describe information security measure approaches and implementation methods with the goal of protecting critical information belonging to SMEs from such threats as data breaches, tampering, and losses. The main text consists of two parts along with seven appendices, including a five-minute information security self-assessment sheet.

- **Security Action** (Information-technology Promotion Agency, Japan)
  https://www.ipa.go.jp/security/security-action/index.html
  SMEs that make self-declarations that they have undertaken the information security measures given in the appendices of the *Information Security Measure Guidelines for SMEs*, given above, are permitted to display the Security Action logo on their business cards, envelopes, company brochures, websites, and elsewhere. Using the Security Action logo allows a company to promote its security initiatives to other parties.

- **Information Security Self-Check Questionnaire** (Japan Network Security Association)
  http://slb.jnsa.org/eslb/
  The questionnaire provides a way for companies to ascertain how well their employees understand information security. The questionnaire covers a broad range of knowledge useful for telework, such as knowledge about email, how to use the Internet, knowledge about viruses, and password management. The basic functions of the questionnaire are free to use. There is also a paid version with enhanced functions.

- **Business and IT Consultation Center** (IT Coordinators Association)
  https://www.itc.or.jp/management/diagnosis/
  To help solve business issues faced by SMEs, this center introduces SMEs to qualified IT coordinators with expert knowledge and long experience in assisting SMEs.

- **Registered Information Security Specialist System** (Information-technology

Promotion Agency, Japan)
https://www.ipa.go.jp/siensi/index.html
The Registered Information Security Specialist System began in 2017 for people with specialized knowledge and skills in the area of cybersecurity. You can find the fields of expertise, contact information, and other particulars about Registered Information Security Specialists on the website given above.