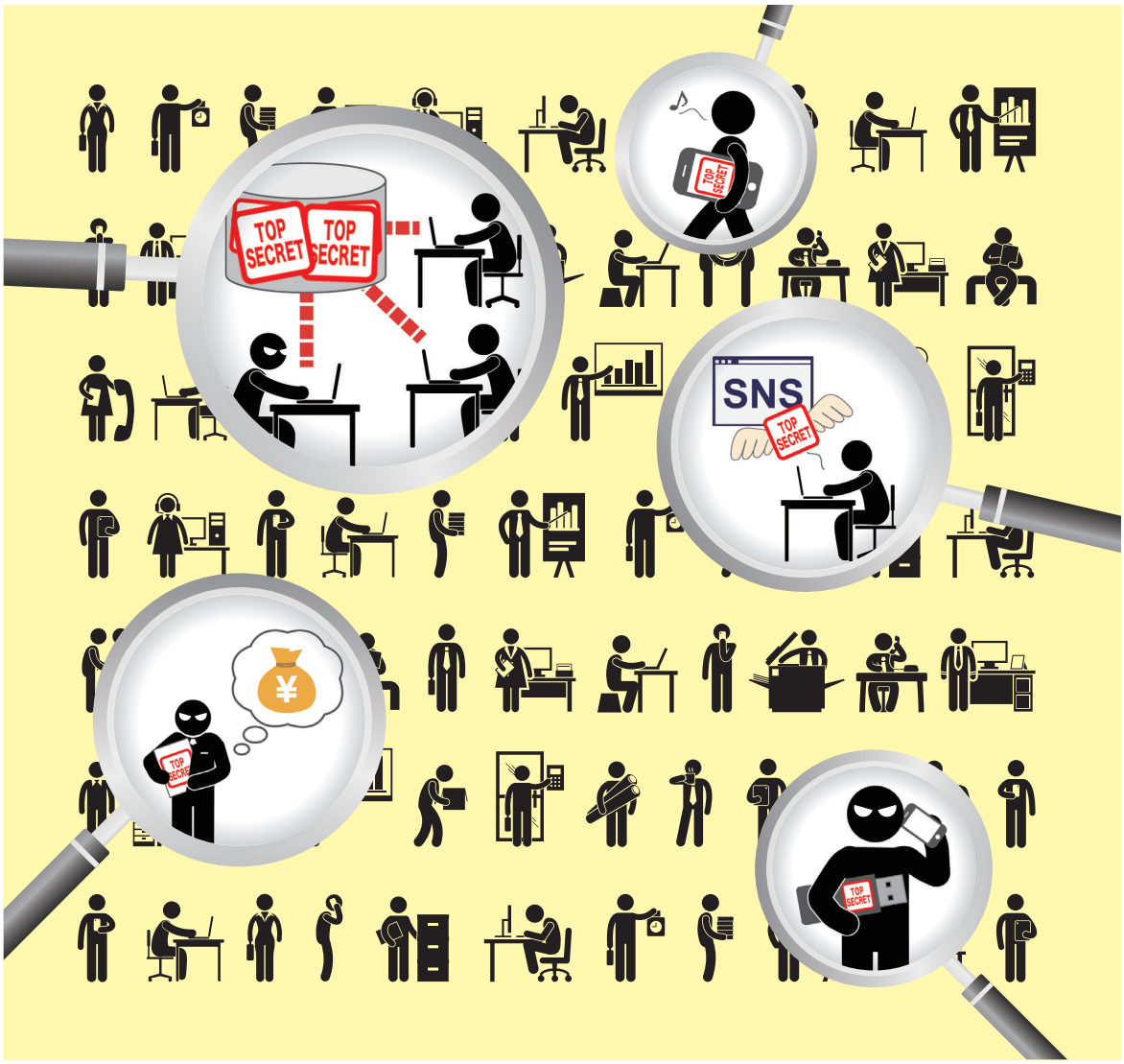
IPA

Guidelines for the Prevention of Internal Improprieties in Organizations



Information-technology Promotion Agency, Japan

Table of Contents

1. Background

Recently, information security incidents involving internal improprieties that threaten the very business of companies or other organizations have drawn attention. Typical examples include cases of employees or officers improperly selling customer data, resulting in large-scale leakages of personal information, and cases of employees improperly removing product information from a company when retiring resulting in the leakage of technical information. In addition to these there are cases involving employees who, acting without malice, take information home from the company without authorization in order to work at home, and then unintentionally leak the information from a home PC. Such information security incidents involving internal improprieties occur without fail every year which is being widely reported.

According to surveys by Japan Network Security Association (JNSA) which is a specified nonprofit corporation[1], one feature of incidents involving internal improprieties is that from 2005 to 2010 the number of incidents occurring due to internal crime or acts of internal impropriety made up only 1% of all the incidents involving leakage of personal data, but about 25% (a quarter) of all personal information leakages were the result of internal impropriety. As such, with the damage per incident greater than that from external attack, each occurrence inflicts a major impact on a business. Moreover, according to surveys by the Ministry of Economy, Trade and Industry[2], the vectors for leakage in companies experiencing leakage of trade secrets were reported as "leakage caused by departing (full-time) employees (50.3%)," "leakage caused by mistakes by active employees, etc. (26.9%)," and "leakage caused by current employees for motives of financial gain, etc. (10.9%)." As seen by this, leakages of trade information with value in maintaining competitiveness are almost entirely due to inside parties. For this reason, internal improprieties are viewed as one of the threats that organizations face, and must be addressed wholeheartedly by the top manager and management teams as a key management issue.

Incidents concerning internal improprieties tend to be handled within the organization for reasons including concerns over negative publicity or lack of coordination among parties concerned, and rarely become known outside the organization. As such, it is likely that in addition to those incidents that are disclosed in the media or in courts, there are also many incidents that are not brought to courts or which remain undisclosed cases of internal rules infractions. As sharing of information about internal improprieties among organizations is thus difficult, the status of such incidents in society is not well known, and it is difficult to consider the causes of and effective countermeasures for internal improprieties beyond the boundaries of the organization. As such consideration is not performed beyond the boundaries of the organization, at present each organization enacts countermeasures based on its own experiences. Moreover, interview surveys[3] by the Information-technology Promotion Agency, Japan (hereafter "IPA") have revealed companies in which incidents have occurred for the reason that such risks were underestimated and no measure was enacted. Underestimation by companies like this is due to the lack of sharing of information about internal improprieties and awareness of such threats. In fact, believing that "internal improprieties won't happen in our company" or "our employees wouldn't commit improper actions," these companies have underestimated their risks. As such, when

[1] "Survey Results on Information Security Incidents – Personal Information Leaks," JNSA

[2] "Questionnaire Survey Concerning the State of Management of Trade Secrets," Survey Results (Definitive Version), Ministry of Economy, Trade and Industry
URL: http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/121211HP.pdf

[3] Report on Survey of Incidents Due to Improper Activity by Organization Insiders
URL：http://www.ipa.go.jp/security/fy23/reports/insider/index.html

countermeasures are considered and decided strictly within organizations, those organizations may fail to realize the need for countermeasures in the first place.

In the absence of internal impropriety countermeasures, the organization may fail to prevent incidents. Furthermore, incidents may go unnoticed until the damage spreads to the parties involved, while the inability to resolve incidents due to uncertainty over their causes can prove a hindrance to follow-up measures. Moreover, even if the perpetrators of the improper actions can be identified, there may be cases in which duty of care has been lax, rendering disciplinary action invalid or making prosecution difficult.

In order to help organizations prevent internal improprieties, IPA created "Guidelines for the Prevention of Internal Improprieties in Organizations" (hereafter "these Guidelines") and made it available to the public. The content of these Guidelines enables the preparation of effective internal impropriety countermeasures in companies (especially small- and medium-sized businesses) that have not yet thought about, or have not known how to address, internal impropriety countermeasures.

Upon revision of September 2014 (ver. 2.0)

In the first half of 2014, security incidents caused by internal improprieties have been successively reported: the incidents includes ex-employees leaked out technologies overseas, employees illegally stole information; and eventually, an employee in a contract company that provides services for a company involving educational business leaked out extremely large amount of customer information. Effective countermeasures achieved through analyzing these incidents have been incorporated in this guideline.

Three key points of revision for ver.2.0 are as follows.

・Strengthening top managers leaderships

・Strengthening supervision of entrusted information systems management and operation

・Addressing advancing information communication technology

In accordance with the above strengthening of measures, we revised the internal improprieties check sheet and added internal improprieties case studies to the list, and created items lists for this guideline’s countermeasures related to personal information protection.

About March 2015 revision (ver. 3.0)

To make this guideline easy to use and more widely adopted, we incorporated requests from organizations using this guideline and addressed the latest standards and policies for information security.

Three key points of revision for ver.3.0 are as follows.

・Responding to requests from organizations using this guideline

・Conforming to revised ISMS standards (JIS Q 27001:2014) and fully revised Trade Secret Management Guidelines

・Additions of basic policies and countermeasures classification that serve as references for using this guideline

2. Overview

The chief aim of these Guidelines is the prevention of internal improprieties in organizations. Taking into account the actual occurrence of internal improprieties, these Guidelines also address early detection and prevention of the spread of damage following occurrences.

The targets for protection from internal improprieties are the information systems and information managed by organizations, for information recording media other than paper. However, the action of printing out information from information systems onto paper is also covered by these Guidelines.

2-1. Basic policies to prevent internal improprieties

This guideline applies ideas of “Situational Crime Prevention”[4] to internal improprieties prevention, and is based on the following five basic policies[5].

- Make crimes difficult (make harder to attempt)：

  Strength countermeasures to make criminal activities difficult to conduct.
- Raise risks to be caught (detected if committed)：

  Strength management and surveillance to raise risks to be caught.
- Reduce rewards from crimes (not worth doing)：

  Hide or remove targets, or make it unprofitable to prevent crimes.
- Reduce seduction of crimes (not to motivate)：

  Deter crimes by dampening enthusiasm to commit crimes.
- Not allow justification of crimes (not allow to excuse)：

  Get rid of reasonings for criminals’ self-justification of their activities.

2-2. Composition of and Ways to Use these Guidelines

These Guidelines are composed as described below, with a broad division into two parts: "Section 1: Background" and "Section 2: Overview" as the first half, and "Section 3: Definition of Terms, and Related Laws" and "Section 4: Model Management to prevent Internal Improprieties" as the second half.

[4] An urban crime prevention theory which criminologists Cornish and Clarke proposed in 2003. It classifies crime prevention countermeasures that should be conducted in five and further groups into twenty-five crime prevention techniques. It is a crime prevention measure that aims at defining appropriate “environment” controllable from outside by implementing supervisors, etc. to reduce criminal chances/motives, and includes direct and indirect countermeasures for deterring and preventing crimes.

[5] Each basic policy is further groped into five. See Appendix VI for summarized corresponding countermeasure case studies and related countermeasure items in this guideline.

Table 1 Composition and Assumed Readership of these Guidelines

Composition of these Guidelines	Assumed Readership	
	Top manager	Persons implementing countermeasures
Section 1: Background	○	○
Section 2: Overview	○	○
Section 3: Definition of Terms, and Related Laws	○	○
Section 4: Model Management to Prevent Internal Improprieties	○*1	○
Appendix I: Internal Impropriety Case Studies	-	(2)
Appendix II: Internal Impropriety Check Sheet	-	(1)(4)
Appendix III: Q&A	-	○
Appendix IV: Relationship with Other Guidelines, etc.	-	(3)
Appendix V: Examples of Basic Policies	○	○
Appendix VI: Five Basic Policies and twenty-five classifications of Internal Improprieties	○	○
Appendix VII: Countermeasures Classifications	-	(5)(6)

*1: See "4-1. Basic Policies"

See Figure 1 regarding (1)-(6).

Section 1 and Section 2 show the positioning and the way of using these Guidelines, and is content aimed at all readers.

These sections assume persons implementing countermeasures and the top manager (or management team)[6] to be readers, and discuss the importance of preventing internal improprieties, as well as an overview and the usage of these Guidelines. As for threats posed by internal improprieties, see "Appendix I: Internal Impropriety Case Studies", and you will better understand the importance of countermeasures.

Section 4 offers content for the formulation of specific countermeasures by persons implementing countermeasures, who are charged with countermeasures by the top manager (or management team). However, the top manager will also need to look over "Section 4, 4-1. Basic Policies" in order to understand his or her role in the organization. Persons charged with countermeasures should first assess the status of their organization's internal impropriety countermeasures by using the check sheet in Appendix II. To address items for which countermeasures are insufficient according to the results of the check sheet, consider specific countermeasures with reference to "4. Model Management to prevent Internal Improprieties" and "Appendix III: Q&A." Figure 1 shows how to use these Guidelines depending on what to consider.

[6] Top manager differs by company scale, management policies, and company form; in these Guidelines, the term indicates the main director of the company.

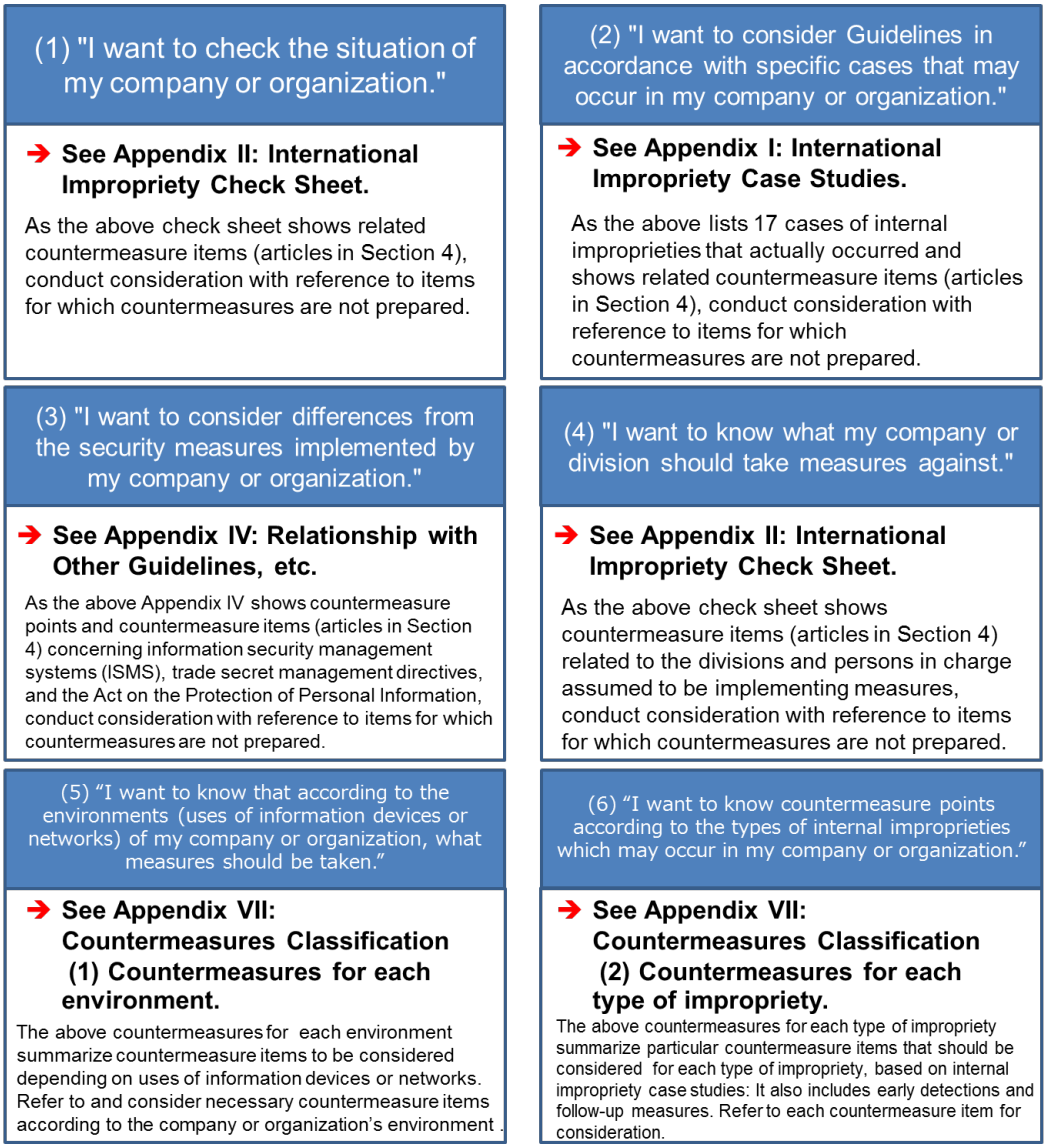


Figure 1 How to use these Guidelines depending on what to consider

2-3. The Importance of Constructing Systems for Internal Impropriety Countermeasures

In order to make use of these Guidelines to effectively and efficiently prevent internal improprieties, the top manager must bear responsibility inside and outside the organization for internal impropriety countermeasures, and must be actively involved in promoting these. The involvement of top managers plays an important role in improving awareness concerning internal impropriety countermeasures in the organization, and in disseminating implementation measures.

In addition, organization-wide action is vital in the formulation and dissemination of specific implementation measures. As the content of internal impropriety prevention countermeasures extends to the work of multiple parties (or divisions) concerned, there must be cooperation with these parties concerned in the formulation of implementation measures. Given that the organization will formulate implementation measures concerning the protection of information assets, it can be assumed that persons/divisions in charge of information

systems, office work, and personnel will be involved. As an example, when changes are made to work processes that handle information system, the information systems division or the division in charge carries out the task, while the division or persons in charge of personnel provide education on the changes. In addition, check by the legal affairs division as to legal matters might also be necessary. In this way, in dissemination, education, etc. concerning implementation measures, organizations must communicate directions organization-wide so as to avoid oversight of countermeasures, and must create systems enabling the summarization of implementation status and assessment by the top manager.

2-4. Systems for Internal Impropriety Countermeasures

As mentioned in Section 2-2, systems for internal impropriety countermeasures involve various divisions within an organization, and the roles of "CEO" and "Supervising Manager" who supervise and mediate those divisions become important.

Internal impropriety countermeasures are closely related to the internal controls required by the Companies Act[7] and the Financial Instruments and Exchange Act[8] in terms of risk management and there are some overlaps between them in terms of systems. Hence, by using a framework of existing internal controls, organizations can effectively and efficiently construct internal impropriety countermeasures.

The below explains how to construct internal impropriety countermeasures based on an internal control framework.

Explanations are given from the viewpoint of the roles of "CEO", "Supervising Manager" and "Divisions/persons in charge". See Figure 2 that shows examples of systems for internal impropriety countermeasures.

2-4-1. CEO

In internal impropriety countermeasures, as in internal controls, organizations must establish the role of the CEO. Budgetary and personnel authority is necessary for internal impropriety countermeasures, as is the one who takes responsibility for implementing that authority. In these Guidelines, that role is given to the CEO. The CEO formulates basic policies for internal impropriety countermeasures, and determines these by resolution of the Board of Directors. In addition, the CEO understands the management of the company, and appoints a Supervising Manager whose role is to implement and promote specific measures.

2-4-2. Supervising Manager

Organizations shall establish a role for specifically promoting internal impropriety countermeasures. In these Guidelines, that role is given to the Supervising Manager. The Supervising Manager bears the role of mediating between business divisions and the top manager while also implementing and checking specific countermeasures for the whole organization. This mediator role is also given to an internal control committee, and so on in internal control. So, when an internal control committee, and so on exist within an organization, it may be advisable for a member of these to concurrently serve as the Supervising Manager to reduce the workload of constructing systems.

---

[7] Under the Companies Act, important rules concerning the construction of internal control systems and basic policies of systems, etc. are matters for deliberation by the Board of Directors (Companies Act, Article 348, item 3.iv; Article 362, item 4.vi; Article 416, item 1.i.e). Note that in these Guidelines, when no Board of Directors exists in a company, the explanation applies to matters decided by Director(s).

[8] The U.S. Sarbanes-Oxley Act of 2002, or SOX Act, and the Japanese J-SOX Act similarly call for construction of internal controls.

2-4-3. Appointment of the Supervising Manager

It is not necessary for all companies or organizations to establish an internal control committee and so on for the purpose of internal impropriety countermeasures. In the case of small-scale companies, systems relating to internal control are often insufficient, with no internal control committee and so on in place. Even in such a case, it is possible to prepare systems for internal impropriety countermeasures by newly appointing a Supervising Manager responsible for internal impropriety countermeasures.

Depending upon the scale and form of the company, the CISO[9], CPO[10] or the top manager (CEO) may double as Supervising Manager. As an example, when the scale of a company is relatively small, the top manager has more of an organization-wide view than is possible in a large-scale company. As a result, the top manager can enact fast and effective countermeasures by directly undertaking internal impropriety countermeasures. In such a case, it may be possible for the top manager to concurrently serve as CEO and Supervising Manager, as well as to construct and prepare the systems. For details, see Q&A1:P66 and Appendix V: Examples of Basic Policies.

2-4-4. Systems for Participation and Cooperation by Related Divisions and Persons in Charge

The internal impropriety countermeasure initiatives addressed in these Guidelines are, within internal control, particularly concerned with overall internal control pertaining to IT. However, this does not mean that only information systems divisions with expert IT knowledge should participate. Internal impropriety countermeasures call for comprehensive countermeasures that involve multiple divisions – for example, preparation of workplace environments by the general affairs division, education and preparation of various internal rules by the personnel division. As such, active participation and cooperation by diverse divisions and persons in charge are necessary. Moreover, when the scale of these divisions is large, the responsible managers of the divisions noted below are also required to participate.

[9] CISO, or Chief Information Security Officer, is appointed by management as the highest person responsible for information security, and bears responsibility for the overall information security of the company or organization. This document explains such a role in terms of the CISO.

[10] CPO (Chief Privacy Officer) is a personal information protection manager appointed by management and bears responsibility and privileges for safe management of personal data in the company or organization. This document explains such a role in terms of CPO.

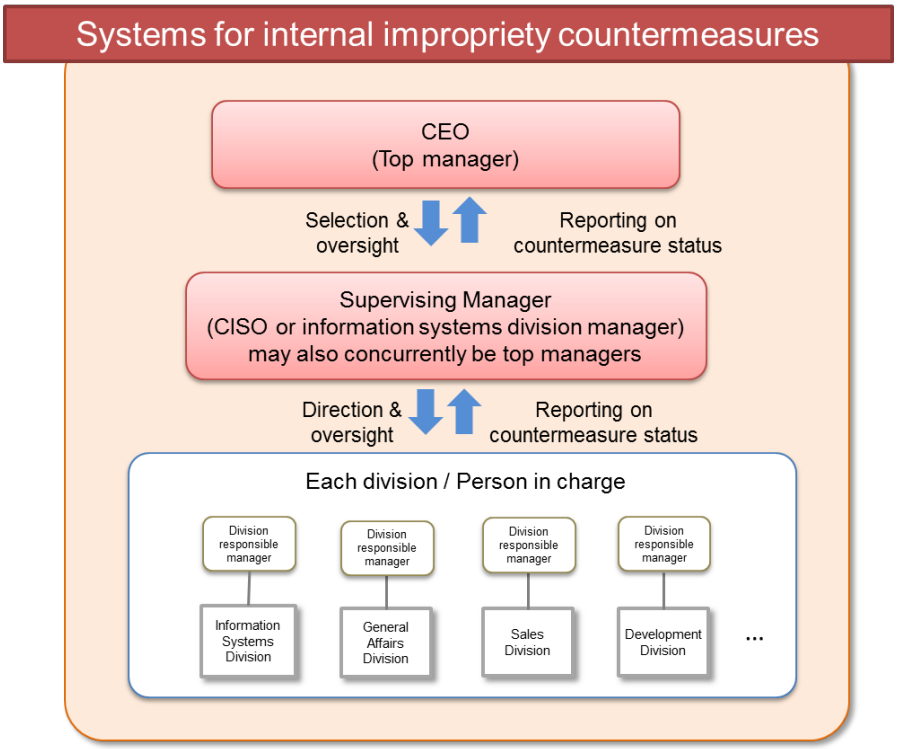


Figure 2: Systems for Internal Impropriety Countermeasures

- CEO: The top manager who bears highest responsibility for decision-making concerning internal impropriety countermeasures, in accordance with laws and regulations such as the Companies Act, and in accordance with deliberation by the Board of Directors.
- Supervising Manager: The manager supervising the systems for internal impropriety countermeasures, appointed by the top manager in accordance with laws and regulations such as the Companies Act. The Supervising Manager creates, manages, and implements specific countermeasures across the organization based on the top manager's basic policies, and checks and reviews the status of countermeasures.
- Responsible manager of division (for large size division): A person appointed by each division as the person responsible for the division. Under the direction of the Supervising Manager, responsible managers of divisions implement countermeasures in their divisions, and check and review the status of countermeasures.

3. Definition of Terms, and Related Laws

The definition of terms used in these Guidelines and an overview of related laws is described below.

3-1. Terms

(1) Organization

A corporation such as a company or a local government, or any other such body.

(2) Insiders

Any persons corresponding to officers, employees including contract employees, temporary workers etc. (hereafter "officers and employees"), or ex-officers or ex-employees who fulfill either of the following:

- Persons having privileges to access the organization's information systems or information (e.g., networks, systems, or data), either directly or over a network
- Persons engaged in work that may allow physical access (excepting janitorial staff, security staff, etc.)

(3) Internal improprieties

Internal improprieties include not only illegal activities but also improper activities such as violations of internal rules concerning information security, which cannot be regarded as violations of laws. Acts of internal impropriety shall include the theft, removal from premises, leakage, deletion, sabotage, etc. of important information or information assets (information systems, etc.). Actions by which insiders retired from organizations leak information that was gained while working in the organizations shall also be handled as internal improprieties.

(4) Important information

Information used by organizations having following features.

Information against which internal improprieties are conducted may affect business. A company or organization properly decides whether the information is important or not. Degree of importance is assigned to the important information based on rating, and its handling is decided by the categorized importance (See (3) Information rating categories).

(5) Contracting services

To make a service contract (quasi-delegation contract, or contract agreement) to entrust a part of services to contractors. Contract employees and temporary workers defined in Worker Dispatch Law are not included in this guideline.

(6) Contractor

Organizations to which services are entrusted.

(7) ”advisable”, “preferable”

Sentences with “must”, “required” indicate countermeasures considered to be necessary. Countermeasures expressed in “advisable”, “preferable” mean countermeasures desirable to be strengthening, with exceptions of sentences having “For example” at the beginning, for which importance is not specified.

(8) Information devices

Mobile devices with communication functions including PCs, servers, laptop PCs and smart devices.

3-2. Related Laws

An overview of laws related to these Guidelines is provided below. In order to comprehensively consider and take measures with respect to the related laws, etc. listed here, organizations must conduct said considerations together with persons in charge of the legal affairs division, as well as the personnel and general affairs divisions.

(1) Act on the Protection of Personal Information

This Act stipulates the obligations (safety management mechanisms, obligations to monitor employees and contractors, etc.) with which businesses that handle personal information must comply, in order to protect the rights and interests of individuals from the leakage or improper use of personal information. When a business violates this stipulation regarding obligations and handles personal information inappropriately, the competent minister having jurisdiction over the business may take measures including issuing suggestions and directions to the business. Failure to follow the directions may subject the business to penalties.

■ When important information must be protected as personal information

When organizations have the objective of protecting managed personal information from internal improprieties, they must comply with the rules for obligations concerning safety management mechanisms required by the Act on the Protection of Personal Information. For details, refer to the Personal Information Protection Guidelines for economic and industrial sectors (Article 2 of the Act; Articles 20-22; etc.).

See “Appendix IV: Relationship with Other Guidelines, etc. (3)” for relations with this Guideline.

(2) Unfair Competition Prevention Act

The Unfair Competition Prevention Act sets forth rules concerning the protection of trade secrets. With respect to the improper use or disclosure of trade secrets, it recognizes civil injunctions and applies criminal penalties in the case of highly illegal infringing conduct. However, in order to be recognized as a trade secret, information must be managed as confidential, and must be useful and not publicly known.

As these Guidelines show methods for handling important information, including trade secrets, they contain information beneficial for the protection of trade secrets. On the other hand, not all measures in this Guideline are required for management procedures seeking protections as trade secrets.

■ When important information must be protected as trade secrets

> When aiming at protecting expertise and other trade secrets from internal improprieties, refer to information including the "Trade Secret Management Guidelines" shown in the website of the Ministry of Economy, Trade and Industry.

See “Appendix IV: Relationship with Other Guidelines, etc. (2)” for relations with this Guideline.

(3) Labor Contract Act

This Act involves cases in which an employee commits internal improprieties such as leakage of information during the term of employment and, by violating the labor contract, is subject to dismissal, disciplinary action, claims for damages, etc. However, the efficacy of dismissal or other specific disciplinary action is to be determined based on the determination framework under labor laws. Moreover, in the event of damages to the company due to internal improprieties by an employee, said employee shall be subject to claims for damages based on default or improper activity under the labor contract.

(4) Act for Securing the Proper Operation of Worker Dispatching Undertakings and Improved Working Conditions for Dispatched Workers

Although employees bear confidentiality obligations as part of their obligations under labor contracts, there is no labor contract between dispatched workers and the companies that temporarily hire them. As the hiring companies cannot directly place confidentiality obligations upon the dispatched workers, in order to have temporary workers maintain confidentiality, the companies must take into account the Act for Securing the Proper Operation of Worker Dispatching Undertakings and Improved Working Conditions for Dispatched Workers.

(5) Others

In addition to the above, legislation concerning improper activity by insiders includes the Penal Code (e.g., larceny, embezzlement, breach of trust, etc.), the Civil Code (contractual liability, tort liability, etc.), labor jurisprudence (violation of confidentiality obligations, non-competition obligations, etc.), and the Whistleblower Protection Act.

4. Model Management for preventing Internal Impropriety

This Section comprehensively presents countermeasures required from the following 10 standpoints in order to implement specific internal impropriety countermeasures within organizations.

4-1. Basic Policies
4-2. Asset Management
4-3. Physical Management
4-4. Technological and Operational Management
4-5. Securing Evidence
4-6. Human Management
4-7. Compliance
4-8. Workplace Environment
4-9. Follow-up Measures
4-10. Organizational Management

Based on these 10 standpoints, 30 countermeasures are presented. However, as these are shown for hypothetical multiple internal improprieties, enacting all of the countermeasures may involve more countermeasures than is necessary when only a specific internal impropriety is targeted.

Following this, the flow of considerations based on the 30 countermeasure items is explained. In considering countermeasures, organizations must consider whether risks (i.e., impacts on business) can be allowed. As an example, if a given risk is allowed, it may not be necessary to enact all of the countermeasure items related to that risk. However, taking into account follow-up legal proceedings after an incident of internal improprieties, it would not be advisable to allow the risks under "4-2. Asset Management," "4-8. Human Management," and "4-7. Compliance." These items are necessary in order to show that fault lies not with the organization but with the perpetrators of the internal improprieties.

As shown in Figure 3, the countermeasures for the 30 items are composed of the following 3 points:

- "Countermeasure principles": Necessary countermeasures are shown in a box. These are also check sheet [11] items. Be sure to gain an overview of countermeasures.
- "What risks are there?": Shows the risks when the countermeasures shown in "Countermeasure principles" are not taken. Be sure to grasp the necessity of those countermeasures.
- "Countermeasure points": Provides ideas for drafting specific measures against the risks.

[11] These Guidelines summarize "countermeasure principles" and present them in Appendix Ⅱ as a check sheet used for checking the status of internal impropriety countermeasures. The check sheet is also available on the following website.
URL: http://www.ipa.go.jp/security/fy24/reports/insider/

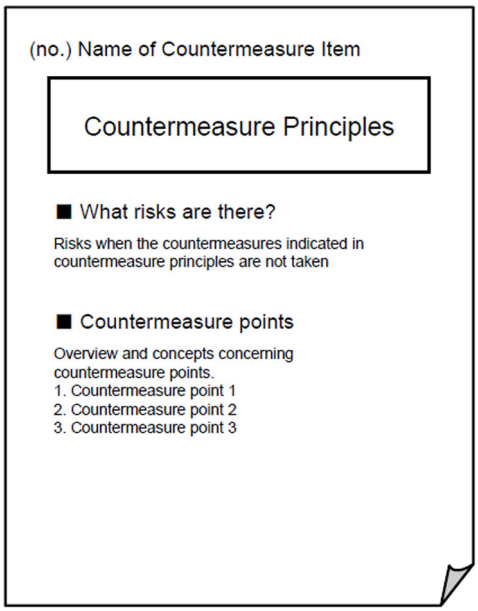


Figure 3　Structural overview of countermeasures

Per the following, consider specific countermeasures while reading the text from "Countermeasure principles" to "Countermeasure points." As some items may involve multiple parties (or divisions) concerned, these parties must participate. For the parties (or divisions) concerned for each item, see "Appendix II: Internal Impropriety Check Sheet".

(1) Read "Countermeasure principles" to gain an overview of countermeasures.
(2) Read "What risks are there?" to understand the risks when the countermeasures shown in "Countermeasure principles" are not taken. Consider the effects on business when the information security incidents occur. If the effects on business are negligible and risks are judged as allowable, it may not be necessary to conduct countermeasures.
(3) Read "Countermeasure points," and, taking costs, resources, etc. into account, draft specific implementation measures based on the effects on business of (2). "Appendix III: Q&A" and "Appendix IV: Relationship with Other Guidelines, etc." are attached as a supplement. Draft specific implementation measures with reference to these Appendices.

It is advisable to periodically review the specific implementation measures drafted in (3), as the allowable risks in (2) may change along with societal background and scale of the company. Moreover, as these Guidelines are expected to undergo revision in step with developments in the social background and in IT, it would be effective to time the above reviews to revisions to these Guidelines.

4-1. Basic Policies (Responsibilities of the Top Manager and Governance)

In preventing internal improprieties in the organization, the involvement of the top manager in promoting effective countermeasures throughout the organization is of extreme importance. Formulation of basic policies and construction of systematic management systems through the leadership of the top manager are also necessary. The top manager must view internal impropriety countermeasures as a management issue. In that event, it is important to undertake considerations as a component of risk management, from the standpoint of the confidentiality[12], integrity[13], and availability[14] of information assets.

With the top manager taking the lead, it is possible to thoroughly promote awareness of and initiatives toward internal impropriety countermeasures within the organization, by constructing and operating systems and mechanisms for internal impropriety countermeasures. In the end, an organization doing so will be able to strengthen protection of personal information and internal control, as well as respond to legal requests toward the company.

[12] I.e., enabling the use of information only by persons approved to access the information (e.g., not leaking information).

[13] I.e., ensuring that information and information processing methods are accurate, and that no changes are made by persons without privileges (e.g., ensuring that information is not falsified).

[14] I.e., enabling access to information and information systems whenever necessary, for users authorized to access the information (e.g., ensuring that system failure does not occur, making information and information systems unusable).

(1) Clarification of the Responsibilities of the Top Manager

1. Top managers are responsible for developing internal impropriety countermeasures, and must formulate “basic policies” to show fundamental directions within and outside the organization, and must disseminate the policies to the officers and employees.

2. Top managers must make decisions and provide instructions for securing resources necessary to implement countermeasures based on “basic policies”.

■ What risks are there?

Top managers must have strong sense of responsibility to conduct internal improprieties countermeasures, and according to their management strategies or policies, understand impact on their organizations caused by the improprieties; otherwise, organizations’ “basic policies” for the improprieties will be hard to be built.

Also, top managers must take leaderships to develop "basic policies", or else management responsibilities inside and outside the companies will be unclear, resulting in difficulties in building effective management structures. "Basic policies" must be developed to communicate top manager’s decisions to prevent internal improprieties. Otherwise, their intentions will not be conveyed to the officers and employees; consequently, taking specific measures or educating officers and employees about countermeasures for internal improprieties will be difficult.

If the top managers don’t make decisions to provide instructions for securing resources necessary to conduct countermeasures based on “basic policies”, this will also result in difficulties in developing effective management structures.

■ Countermeasure points

Considering management strategy or policies, the top manager must understand negative impact on the organizational operation caused by internal improprieties, and must formulate the basic policies that form the general framework for internal impropriety countermeasures to set the direction for internal impropriety countermeasures [15]. To make the countermeasures more effective, the top manager makes decisions and provide instructions necessary for securing resources, and periodically reviews basic policies and organizational resource allocation while monitoring [16] and evaluating the implementation status of countermeasures.

For these, the top manager him/herself understands the below countermeasures to take internal responsibility and external accountability.

1. According to management strategy or policy, the top manager understands impact on the organizational operation caused by internal improprieties [17].
2. With reference to these Guidelines, the top manager formulates basic policies *Q&A1:P66
3. The top manger makes decisions necessary for securing human resources and budget to conduct planned “basic policies”, and provide instructions.

---

[15] Corporate groups consisting of several companies such as holding companies usually have close operational relationship involving important information. These groups must plan internal improprieties countermeasures through the groups consensus based on their corporate governance design. In this case, cooperation and responsibility structures between group companies must be documented and clarified.

[16] Continuously assessing situations through periodic reporting

[17] As utilizing information has become increasingly important for various aspects of organizational operation, organizations must study effects caused by internal improprieties considering possible suspension of operational activities or downfall of social trust.

4. The top manager checks internal impropriety countermeasures for the formulated basic policies, and disseminates the countermeasures to officers and employees through education, etc.
5. Based on the results of monitoring and evaluation, the top manager periodically reviews the basic policies and organizational resource allocation.
6. The top manager discriminates between important information and other information.[*Q&A2:P67] Furthermore, it is advisable for the top manager to divide important information into several categories, taking into account their degree of importance to the business.[*Q&A3:P67]
7. The top manager regularly reviews the division and categorization of important information, as these may change along with societal background, changes in the business, etc.

(2) Appointment of the Supervising Manager and Construction of Cross-Organization Systems

1. The top manager appoints the Supervising Manager and approves management systems and implementation measures, showing the organization as a whole that these are top manager-led initiatives.

2. Following the basic principles, the Supervising Manager must construct cross-organizational management systems. Moreover, the Supervising Manager must formulate implementation measures.

However, if the organization is one in which the top manager has a view of the entire organization and implements internal impropriety countermeasures on his or her own, it may not be necessary to construct management systems.

■ What risks are there?

If the top manager does not appoint a Supervising Manager or give approval to the countermeasures to be implemented, it will be difficult to allocate the necessary budget and personnel, which in turn makes the construction of effective management systems difficult.

As the important information targeted by internal improprieties exists in diverse divisions in the organization, if cross-organizational management systems are not constructed, the organization may be unable to enact effective and efficient countermeasures or information management, or to establish them thoroughly. That latter failure heightens the risk of internal improprieties occurring.

■ Countermeasure points

The top manager takes the lead in constructing and operating systems for establishing internal impropriety countermeasures in the organization. Specifically, the organization is to establish and operate the following countermeasures.

1. A person with understanding of information security and management[*Q&A1:P66] is to be appointed as Supervising Manager in order to achieve efficient and effective internal impropriety countermeasures that take the business into account.
2. The Supervising Manager reifies and documents cross-organizational management systems and the roles of the related divisions and thoroughly establishes those roles. Responsible divisions, taking the lead with the Supervising Manager, construct organization-wide implementation measures and implementation systems for internal impropriety countermeasures. (e.g. Depending on business size and other aspects, setting up special divisions or committees related to handling of important information[*Q&A4:P67].) See Figure 4 for an overview of the important information and roles for the hypothetical related organizations.
3. In constructing cross-organizational management systems, the Supervising Manager appoints responsible managers or persons in charge for each division, who then serve as management and operational staff.
4. To build systems to fully implement internal improprieties countermeasures in the organization, the supervising manager clearly specifies abilities needed for division managers and persons in charge. If their abilities are found insufficient, organizations take actions to improve the abilities, or consider introducing specialists from outside the organization. The supervising manager supports managers and persons in charge so that they can achieve necessary knowledge and know-how according to their roles.

5. When developing management systems for prevention of internal improprieties and other systems involving privacy protection, compliance control and risk management in the organization, the top manager takes lead to define each role and cooperation systems within the organization.
6. Partnership structures must be developed with contractors included if necessary, when the contractors involve operations related to handling of important information (See (16) Confirmations of Contractors Services (including when using services provided by third parties).Generally, as for outsourcing services involving handling of important information, it may increase business efficiency by entrusting services to specialist groups while it may increase risks for implementing internal improprieties countermeasures[18]. Hence, operations involving handling of information must be addressed weighing efficiencies and risks: Think which is appropriate, handling the tasks within the organization or outsourcing them.

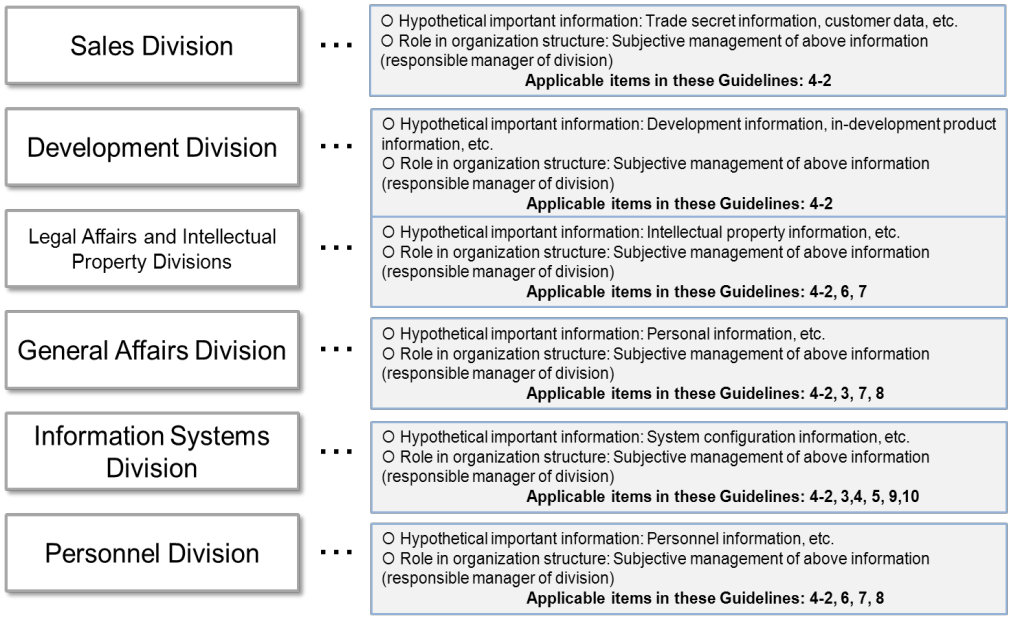


Figure 4 Overview of important information and roles for hypothetical related organizations

[18] Examples for increasing risks include being an indirect supervisor when implementing internal improprieties countermeasures, and basic policy differences in own organization and contractors.

4-2. Asset Management (Designation as Confidential, Designation of Access Privileges, Access Administration, etc.)

See Figure 5 for an overview of the flow for information asset listing or other handling and considerations.

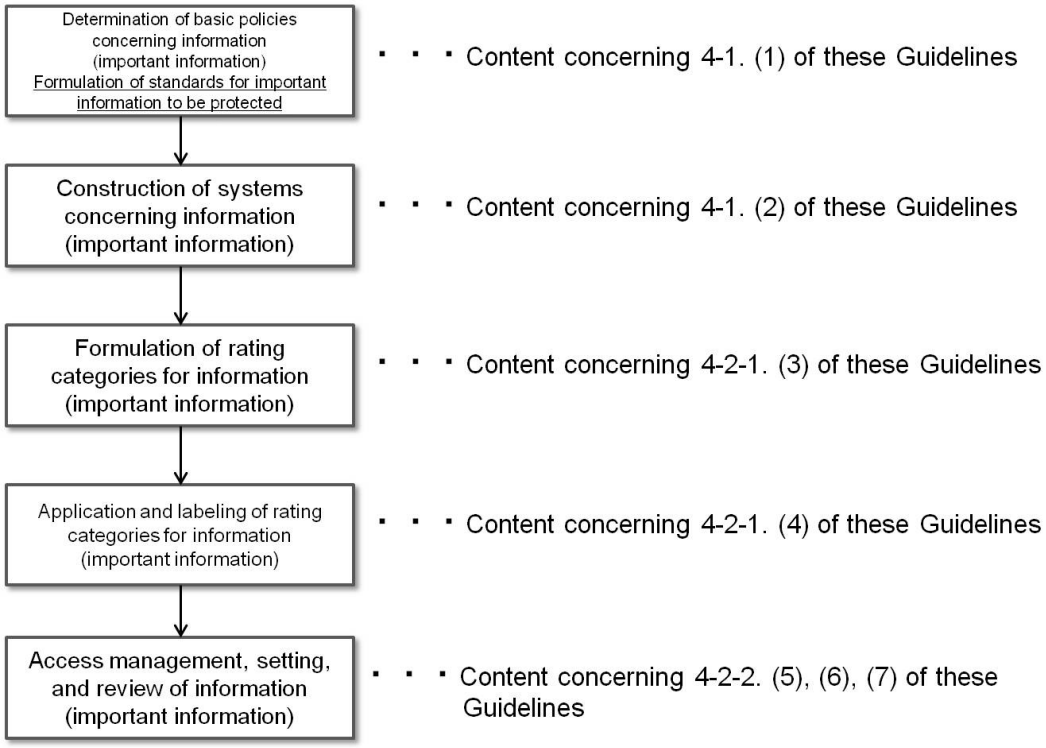


Figure 5　Flow diagram for information (important information) handling and considerations

4-2-1. Designation as Confidential

(3) Information rating categories

Organizations or the division in charge must assess important information, assign it rating categories according to degree of importance, and based on those categories, set the scope (e.g., position, job category, etc.) of insiders able to handle the information.

■ What risks are there?

If important information such as customer lists or technical knowledge is not separated from other information, officers and employees will not know which information is important information that must be protected, and may leak information without knowing that it is important. Moreover, if important information is not assigned rating categories and managed appropriately according to category, countermeasures may prove insufficient or too costly.

Organizations or the division in charge that do not perform this management may be unable to pursue the liability of employees committing improprieties. Moreover, doubt may be cast onto the management responsibility of the company or organization.

■ Countermeasure points

Organizations or the division in charge must establish the following in order to assess and appropriately manage important information.

1. Organizations or the division in charge are to establish handling for important information. When three or more degrees of importance have been assigned in the rating categorization, organizations or the division in charge are to establish handling for each degree of importance. Organizations or the division in charge are to periodically review the handling established for important information.
2. Organizations or the division in charge are to establish administrators for important information. As an example, organizations can set responsible manager of divisions, or persons in charge selected from responsible managers of divisions, as administrators. Large organizations are to establish an administrator for each division.

(4) The application and labeling of rating categories

1. In order to restrict the scope of handling important information, creators of important information must select one of the ratings categories established in (3), and must have the selection confirmed by the administrator for important information.

2. Furthermore, some sort of indicator, such as a confidentiality mark, must be set on digital documents or digital data containing important information, to let insiders identify important information.

■ What risks are there?

If organizations do not set ranking categories for important information, the scope of handling for the information will not be set, and even officers and employees having no need to handle such information will have access to it, and the possibility of leakage will increase as the important information becomes known to more officers and employees. As the number of officers and employees knowing of the important information increases, the environment for detecting internal improprieties will worsen, the likelihood of occurrence will grow, and the perpetrators of internal improprieties will become difficult to identify after occurrence.

If organizations do not set an administrator for important information (e.g., the responsible manager of the division, etc.), appropriate management of important information will not be thoroughly established, and important information may leak due to information assets in PCs, etc. being lost or taken from the premises without authorization.

Moreover, if labels are not shown[19] based on degree of importance, officers and employees may take information from the premises or leak it without knowing it is important information.

■ Countermeasure points

Organizations are to restrict the scope of handling important information, and are to set and operate the items below to make handling of the important information understood.

1. The scope of handling of important information is to be restricted to officers and employees with work-related need. In order to reduce the danger of improper use of important information, organizations are to set the scope of handling based on position, duties, role, scope of responsibility, form of employment, and so on.
2. Creators of important information must select one of the ratings categories established in (3), and must have the selection confirmed by the administrator for important information. In the same way, important information already created and stored must be assigned ranking categories.
3. A confidentiality mark (such as graphic data or a stamp, or a watermark with text, indicating confidentiality) making rating categories known to officers and employees must be attached to digital documents containing important information. For digital documents containing important information, along with the above confidentiality mark, it is advisable to designate and display a period of validity for the important information. The period of validity is to be reviewed periodically. When the period of validity has expired, the information is to be subjected to the established handling such as disposal.
4. When deleting important information from the storage media of their PCs or other information devices, officers and employees must select an erasing method based on the degree of importance of that information and then perform deletion[20].

[19] Some tools allow such specification through file properties.

4-2-2. Designation of access rights

(5) User access management in information systems

1. To enable access to important information by only those users specified by the scope of handling (e.g., position, job category, etc.) set in (4), information systems division must operate information systems with procedures established for registration, change, deletion, and other settings concerning user IDs and access rights.

2. User IDs and access rights that have become unnecessary due to transfer or retirement must be deleted promptly[21].

■ What risks are there?

If information systems division do not set user IDs and access rights appropriately in information systems, officers and employees not intended to have access rights to important information may be granted access, and important information may be used improperly. Conversely, officers and employees needing to access important information to perform their work may not be granted access.

If information systems division do not delete user IDs that have become unnecessary due to transfer or retirement, these may be improperly used by current- and ex- officers and employees to access important information.

Information systems division that does not perform this management may be unable to pursue the liability of current- and ex- officers and employees committing improprieties. Moreover, doubt may be cast onto the management responsibility of the company or organization.

■ Countermeasure points

Information systems division is to take the countermeasures below in order to correctly set user IDs and access rights in information systems.

1. Information systems division is to establish and operate procedures such as approval procedures for the registration, change, and deletion of user IDs and access rights, and notification of completion of settings.
2. Information systems division is to set access rights to important information for user IDs in information systems, based on the scope of handling established in (4). If access rights based on the scope of handling established in (4) are not set, this is to be remedied by review of (4) or functional changes to the information system.
3. Number of users to whom access rights for important information should be authorized to be minimal. Privileges to be authorized to users having access rights also to be minimal, with restricted period, depending on necessity. Measures in the agreement specified in (16) are needed especially when authorizing privileges to contract workers[22].

---

[20] When officers and employees are away from work involving extremely important information, the information should be completely deleted from the storage media of their PCs or other information devices. Complete deletion covers levels from OS-level formatting to random data overwriting.

[21] In cases such as access records are deleted upon deletion of user IDs, it is necessary to lock user IDs to disable access and save access logs.

[22] For example, when systems are changed due to contract workers resignation or relocation, these changes must be reported to contracting organizations to prevent account removal failures.

4. Operation to be in conjunction with personnel procedures, etc. concerning personnel relocation, in order to prevent oversights in procedures for registration, change, and deletion of user IDs and access rights[23].
5. Information systems division is to periodically review requirements for access rights, to confirm that user IDs and access rights are being granted appropriately. As an example, it is advisable to perform reviews, etc. at the same time as personnel relocations. Especially when specific users hold too many access rights, confirm the appropriateness and remove unnecessary access rights.
6. For information systems storing important information, it is advisable to control the systems based on time, traffic and other access conditions. For example, time based control enables organizations to restrict accesses to important information during the night, while traffic based control enables to alert supervisors when important information is downloaded in bulk[24].

[23] Access control systems corresponding to “Roll-based access control ” assigning access rights to jobs (rolls) rather than individuals can be implemented.

[24] When monitoring through notifications, it is necessary to check the contents of notification and act appropriately. Reference values must be kept secret from officers and employees so that the countermeasures are not bypassed.[25] When only one person in the organization is in charge of the system administrator, the organization (or the division in charge) cannot avoid such risks through privilege distribution. In such a case, the organization can mitigate those risks by having personnel other than the system administrator check the history of information system management operations.

(6) Rights management for system administrators

When there are multiple system administrators, organizations or the division in charge must assign an appropriate scope of rights for each system administrator ID, and must enable system administrators to monitor each other.

■ What risks are there?

If organizations do not assign an appropriate scope of rights for each system administrator ID, improper registration or deletion of user IDs can occur, and business may be obstructed by improper deletion or improper use of important information caused by improper registration. Furthermore, when the assignment of scope of rights is not appropriate, as when rights are overly concentrated in a single administrator, there may be obstructions to business continuity, such as destruction of information systems or deletion of important information[25].

■ Countermeasure points

To prevent internal improprieties by system administrators, organizations or the division in charge are to assign an appropriate scope of rights for each system administrator ID, and are to confirm that these are operated properly, as follows.

1. When determining system administrators, organizations or the division in charge are to appoint persons with appropriateness to the position, including high consciousness of rules. It is advisable that multiple administrators be appointed, enabling mutual monitoring.[26]
2. Rights should be distributed so as to not be concentrated in a single system administrator.
3. In order to enable mutual monitoring by system administrators, organizations or the division in charge are to create and keep task reports recording the content and time of tasks. Moreover, it is advisable that the content of task reports be confirmed by other system administrators.
4. System administrators do not use their special privileges when performing operations requiring no such privileges.

[25] When only one person in the organization is in charge of the system administrator, the organization (or the division in charge) cannot avoid such risks through privilege distribution. In such a case, the organization can mitigate those risks by having personnel other than the system administrator check the history of information system management operations.

[26] When multiple system administrators are put in place, not only can persons performing the work of information system configuration check the content of their work, but other system administrators can check whether the configuration work is implemented properly, allowing administrators to monitor each other. Work other than monitoring involving the presence of several persons can also be considered. Such work may use distribution and division of keys, etc.

(7) Identification and authentication of users in information systems

To identify users (insiders using information systems) and system administrators (insiders managing information systems) of information systems, organizations must perform authentication using individual passwords, IC cards, etc. for individual users and system administrators, without using shared IDs, shared passwords, shared IC cards, etc.

■ What risks are there?

When organizations use shared IDs, passwords, IC cards, etc. in information systems, in the event of internal improprieties the organizations become unable to identify which users accessed important information, making identification of the perpetrators of internal improprieties difficult. Moreover, when the identification of perpetrators of internal improprieties is difficult, an environment is created in which it is psychologically easy to take important information from the premises.

Organizations that do not perform this management may be unable to pursue the liability of the perpetrators of internal improprieties. Moreover, doubt may be cast onto the management responsibility of the company or organization.

■ Countermeasure points

In order to appropriately perform identification and authentication of users in information systems, organizations must prepare and operate rules for managing user IDs and system administrator IDs, as follows.

1. To identify users and system administrators, organizations are to assign a user ID or system administrator ID to each user or system administrator. In addition, user IDs and system administrator IDs are to be authenticated using passwords, etc.
2. In order to prevent improper use of a user's user ID by another user, organizations should establish administrative items[*Q&A4:P67] concerning passwords and should have users follow these. Examples include not setting simple text strings as passwords, and periodically changing passwords.
3. Organizations are to prohibit the lending of IDs, passwords, IC cards, etc. to other users.

4-3. Physical Management

(8) Physical protection and entry/exit management

Organizations must establish boundaries that physically protect locations where important information is stored, handled, etc. from entry other than by authorized persons, by protecting important information and information systems with walls and entry/exit management measures.

■ What risks are there?

When unauthorized persons have physical access to equipment storing important information, or to PCs or other information devices that handle important information, those information devices may be destroyed and obstacles to work created, or the devices may be stolen and information leaked. Alternately, leakage or deletion of important information may occur through manipulation of these information devices.

Particularly, storage devices and media for important information are required to be protected in server rooms, etc. where strict entering and exiting management is enforced, for once they are destroyed, operations may not be able to continue.

■ Countermeasure points

As an example, organizations must clarify areas for storage or handling of important information per Figure 6, and must physically protect these to restrict the insiders, or the delivery persons and other outsiders, who are able to enter these areas.

1. Organizations are to establish physical areas calling for strengthened security, and are to prepare security rules that should be followed *Q&A5:P67 in accordance with the importance of the information assets managed in each area. For example, IC card or biometric authentication is to be performed upon entry into the server room.
2. Organizations are to determine the areas which can be entered and exited by insiders (i.e., officers and employees) and outsiders (e.g., delivery persons) and are to manage their entry/exit, so as to prevent important information from being improperly taken from their premises. As an example, organizations may restrict entry/exit to the shipping entrance for delivery personnel, the reception room for clients, and the entranceway and work floors for officers and employees. Access to server rooms are to be restricted to system administrators and other qualified personnel, and to require prior permission from the administrative staff (including the responsible manager).
3. In entry/exit management, it is necessary that organizations create records of entry and exit in order to prevent internal improprieties and to track perpetrators after occurrences. Moreover, taking "records to identify individuals" (such as facial photographs) of those entering or leaving the room is highly effective in deterring internal improprieties. In this case, the "records of entry and exit" and "records to identify individuals" are to be audited regularly or at random.
4. For physical areas allowing access to important information, organizations must also take into account unauthorized entry during unmanned hours. As an example, it is advisable to install automatic security systems and surveillance cameras. It is also advisable that records of security system operators performing the unlocking of buildings (time of initial entry) and locking (time of final exit) include "records to identify individuals" such as their facial photographs.
5. Organizations must also consider preparing environments for disconnecting equipment containing important information from networks as required.

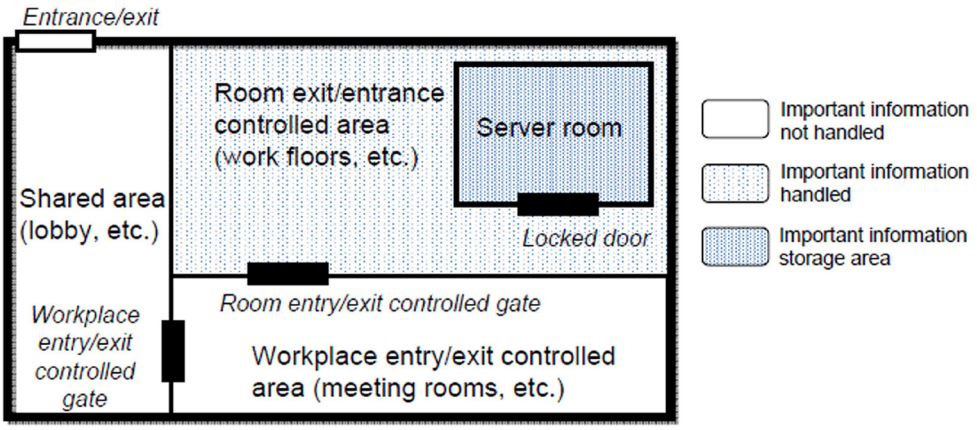


Figure 6　Example of areas to be physically protected

(9) Asset management and physical protection of information devices and storage media

1. Organizations or the division in charge must manage and protect PCs, other information devices, and portable external storage media[27] to prevent theft, improper removal from the premises, etc.

2. In addition, when disposing of unneeded information devices or storage media, organizations or the division in charge must confirm that important information has been completely deleted.

■ What risks are there?

When organizations or the division in charge do not manage information devices and storage media, an environment is created that facilitates theft or improper removal of items from the premises, and theft or improper removal may go unnoticed. Moreover, if organizations or the division in charge do not physically protect information devices, they might be stolen and important information leaked.

In addition, if devices or storage media on which important information is stored or has not been completely deleted are disposed of, this important information may be leaked.

■ Countermeasure points

Organizations or the division in charge must stipulate measures required for information devices and storage media that handle important information that should be protected, and manage and protect information devices and storage media in the way that they are protected from theft, improper removal from the premises, or careless disposal.

1. In order to facilitate the detection of the loss or improper removal of information devices organizations or the division in charge are to manage the installation locations and users of the devices via ledgers, etc., and are to periodically conduct inventory (i.e., checking of assets).
2. It is advisable that information devices be affixed to desks, etc. using security cables, etc. to prevent theft or improper removal from the premises. Moreover, mobile devices (laptop PCs, smart devices, etc.) and portable storage media (USB storage, etc.) are to be stored locked in shelves, desks, etc.
3. Information devices such as important information storage servers and access management servers are to be installed in a place such as a server room with strict entry/exit management, to prevent physical access by persons other than administrators.
4. When disposing of information devices and storage media, organizations or the division in charge are to completely delete important information from HDDs, USB storage, and other storage media so that restoration is not possible. Moreover, it is advisable that CD-Rs, DVD-Rs, HDDs, and other storage media are required to be physically destroyed using a crusher[28], etc.

[27] USB storage, portable HDD, etc.

[28] Crushers are equipped in devices such as shredders.

(10) Management of portable information devices and storage media

When mobile devices (laptop PCs, smart devices, etc.) and portable storage media (USB storage, CD-Rs, etc.) are taken from a physically protected location per (8), organizations or the division in charge must manage the approval and recording of the removal[29].

■ What risks are there?

If organizations or the division in charge do not have approval system in place for the removal of mobile devices and storage media from the premises, important information may be taken without authorization and may be leaked. Moreover, if organizations or the division in charge do not keep records of removal from the premises, investigation of any internal improprieties may be difficult.

■ Countermeasure points

In the management of removal of mobile devices and storage media from the premises, organizations or the division in charge must establish and operate the following items.

1. When removing mobile devices and storage media from the premises, the approval of division managers, etc. must be obtained.
2. When removing mobile devices and storage media from the premises, the information assets taken, the date and the person in charge, etc. must be recorded and managed.

[29] See (14) regarding the protection of important information stored in portable information devices and USB storage in the case those devices and storage are taken from a physically protected location per (8).

(11) Restrictions on bringing in and using personal information devices and storage media for work

Information systems division must properly restrict employees' bringing in and using personal mobile devices (laptop PCs, smart devices, etc.) and portable storage media (USB storage, etc.).

■ What risks are there?

When personal information devices and storage media are used for work, management of these by the organization becomes difficult. Information belonging to individuals and information belonging to organizations become handled together, increasing the risk of important information being leaked due to virus infection, erroneous operations, etc. Moreover, investigation of any internal improprieties may be difficult if owners of personal information devices and storage media do not comply with investigations of the personal items.

When personal information devices and storage media are brought into work floors or other areas that handle important information, important information may be stored on the personal information devices or storage media and taken from the premises. Moreover, in the case of information devices with cameras, important information may be photographed and taken from the premises. Information devices with communication functions may transmit important information to outside.

■ Countermeasure points

When restricting bringing in and using personal information devices and storage media for work, information systems division must take into account the degree of importance of important information and the installation location, etc. of information systems. Specifically, information systems division is to establish and operate the following.

1. Information systems division is to consider whether to allow the use of personal information devices and storage media for work.
2. Information systems division allowing this develops rules including the scope of work for which usage is allowed, as well as compliance items. If the scope of work for which usage is allowed is broad, information systems division should note that the important information handled will increase and management will become difficult. Moreover, it is advisable for information systems division to gain written consent on compliance items regarding use for work.
3. If personally owned information devices are required to access an organization's networks, only the devices with security measures specified in (12) should be allowed. In this case, it is preferable that the access be restricted only to authorized work systems and work services.
4. When information with a high degree of importance is handled on personal information devices, it is advisable that software, etc. allowing management of the important information on the personal information devices be installed as required, allowing organizations to manage the important information.
5. Personally owned laptop PCs, tablets, smart devices and other portable information devices must be strictly restricted to be brought or used in server rooms with servers storing important information and/or managing user access, and in other workspaces handling important information depending on the importance of the important information.
6. In areas where bringing in information devices is prohibited, it is advisable to provide warnings of this via posters, etc.

7. Information systems division is to restrict employees' bringing in personally-owned USB storage and other portable storage media. Only portable storage media provided by the company is to be used.
8. It is preferable to implement software[30] that restrict use of mobile devices including smart devices and other external recording media such as portable USB storages to address information leakage through personally owned information devices or recording media.

[30] Examples of hardware protection measures include uses of terminals without USB slots or with disabled USB slots.

4-4. Technological and Operational Management

(12) Safety management for network usage

To prevent the leakage of important information from users' PCs and other information devices in the use of organizations' networks, organizations must prepare safe network environments by restricting the use of file sharing software, social network services (SNS), external online storage, etc.

■ What risks are there?

If file-sharing software is installed on information devices, important information on the devices may be unintentionally leaked to the outside. Executing external files obtained by file sharing software may result in malware infection and even spread infection to other information devices in the organization.

Moreover, if organizations allow the use of SNS, the use of external online storage, and posting to message boards, important information may be uploaded or posted and thereby leaked.

■ Countermeasure points

To prevent external leakage of important information from organizations' networks, organizations must take measures concerning information devices.

1. Organizations must not allow the installation and use of software not authorized by the organization (e.g., file sharing software) on the PCs and other information devices of officers and employees. Organizations are to decide what software is allowed. In the case of requests by users for certain software, organizations must decide whether to allow its use.
2. With regard to Web access, it is advisable to install contents filter, and to restrict access to SNS, upload services, message boards, etc.
3. With regard to e-mail, it is advisable to confirm that e-mail software is not configured to forward business e-mails to personal e-mail addresses. Moreover, to prevent mistaken e-mail transmissions which could lead to the leakage of information, it is advisable to install mechanisms that recheck sent outbound e-mails and/or require supervisors approvals, and a mail system that does not allow the transmission of unencrypted attachments.
4. To protect PCs and other information devices, organizations are to implement general security measures such as installing antivirus software and applying security patches.

(13) Transfer and Protection of Important Information

1. The transfer of important information to contractors or other parties concerned must be appropriately managed at all steps from transfer to disposal.

2. Considering the possibility of mistaken transfer of important information to persons other than intended parties during the transfer of important information via transmission over the Internet or via storage media, the important information must be protected using encryption or other means.

■ What risks are there?

In the transfer of important information by e-mail, storage media, etc., if important information is not prevented from being taken from the premises other than when necessary, insiders may improperly take the important information. Moreover, if the transferred important information is not protected, important information may be leaked due to mistaken transmission of e-mail or due to theft or loss of storage media.

■ Countermeasure points

Steps are to be managed as follows, from the transfer of important information to parties concerned, to the disposal of the important information by said parties.

1. With regard to the transfer of important information, organizations are to establish internal procedures[*Q&A6:P68] and approval measures matched to the degree of importance, and are to make contractors and other parties concerned comply with these.
2. Organizations are to record activities related to transfers of important information to parties concerned.
3. Organizations encrypt information related to transfers of important information to relevant parties through the Internet or hand delivery of storage media.
4. When important information has been disclosed to parties concerned, organizations are to obtain from the parties records concerning the disposal or deletion of the important information.
5. Organizations must have subcontractors as well as contractors comply with the above arrangements[31].

[31] With regard to the oversight of entrusted parties, Article 22 of the Act on the Protection of Personal Information stipulates, "When entrusting the handling of personal data in part or in entirety to another party, a business operator handling personal information must perform necessary and appropriate oversight of the entrusted parties, to ensure the safe management of the personal data for which handling was entrusted.".

(14) Protection of Information Devices and Storage Media taken from the Premises

When mobile devices (laptop PCs, smartphones, etc.) and portable storage media (USB storage, CD-Rs, etc.) that store important information are taken from a physically protected location per (8), the important information must be appropriately protected through technological measures.

■ What risks are there?

When information devices or storage media storing important information is taken from the premises without the implementation of technological measures such as encryption or password locking, the important information may be leaked in the event of theft or loss.

■ Countermeasure points

When mobile devices (laptop PCs, smartphones, etc.) and portable storage media (USB storage, etc.) that store important information are taken from an organization's premises, the organization must take appropriate measures.

1. When information devices are used, organizations are to configure them to perform authentication via user ID, password, etc. Moreover, it is advisable to set BIOS passwords, HDD passwords, etc. for laptop PCs.[32] It is also advisable to install encryption software for protecting important information.
2. It is advisable to use tools or services allowing remote deletion of information on information devices in the event of loss of information devices storing important information. It is also advisable to use tools that delete important information when password lock authorization fails a set number of times.

[32] When devices (e.g. smartphones, tablet PCs, etc.) other than the organization's standardized devices are among the information devices being able to access important information, organizations must implement the same level of security measures on those devices as those for the organization's standardized devices .

(15) Protection of Important Information in Work Outside of the Organization

When performing work using important information outside of physically protection locations per (8), organizations must appropriately protect the important information, taking the surrounding environment, network environment, etc. into account.

■ What risks are there?

When work is done in a public place, important information may be leaked if viewed by surrounding persons. Moreover, if the organization's network is accessed via a public wired or wireless LAN and the communication is not protected, eavesdropping of the important information on the network may occur and the important information may be leaked. When working at home, important information must be restricted to be accessed and/or stored in PCs depending on the confidentiality of the important information. Otherwise important information may be stored in personally owned PCs which are not under control of organizations, or may be accessed by people other than the worker him/herself (e.g. family members and/or visitors) and that increases the risk of important information leakage.

■ Countermeasure points

In work involving important information outside of the organization, screens must be appropriately protected from unwanted viewing in the usage environment, and connections must be limited to approved network environments.

1. Care is to be taken against unwanted viewing of screens on trains, in cafes, etc. Moreover, it is advisable to protect screens from unwanted viewing by using privacy protection film, etc.
2. Organizations are to determine whether to allow connection to hotel wired or wireless LANs, public wireless LANs, and other networks shared by unknown users[33].
3. When accessing the organization's networks from an approved network environment, important information must be encrypted and communication must be encrypted using a VPN[34], etc.
4. It is advisable to store as little data as possible in PCs when connecting organization's networks from outside[35]. When allowing access to important information in the organization, precisely allocate access rights to prevent access to unnecessary information.

[33] It is advisable to implement user authentications using IDs and passwords, multiple authentications including terminal authorization using physical address, and access prohibition from outside the organization according to the confidentiality of important information. It is also preferable that the usages within the organization be similarly restricted.

[34] Depending on the confidentiality of important information and external parties involved, it is advisable to encrypt data and communication even within the organization.

[35] This includes desktop virtualization. Once desktops are virtualized, users can connect the organization's networks from outside to read and edit organization's data without storing them on local computers (or clients) so that the information is not to be left on PCs.

(16) Confirmations of Contractors Services (Including when using services provided by third parties)

Depending on services to be entrusted and importance of the important information, organizations and contractors must confirm and agree on security measures before contracting; afterwards, the organizations must regularly and irregularly check whether the contractors implement information security measures according to the contracts.

■ What risks are there?

If contracts are made without confirming needed security measures based on the services to be entrusted and importance of the important information, the important information could be leaked out due to the contractors' insufficient security measures. Also, depending on the contents of agreements, damages caused by important information leakage may not be compensated.

Information leakage caused by the contractors' insufficient security measures may not be prevented if organizations do not make sure that contractors are implementing security measures according to the contracts. Also investigations on internal improprieties could be difficult if the agreement does not state that the contractors must provide logs.

When using services provided by third parties (including cloud computing), if organizations do not determine which information may be handled via services provided by third parties and which may not, they may entrust sensitive, business-related information to the third parties, and should the leakage of such information occur, they may not be able to continue their operations.

If contractors involve operations related to handling of important information, the contractors must be incorporated in partnership structures when appropriate, depending on the importance of important information. When considering outsourcings, organizations must weigh efficiency advantages and increasing risks of internal improprieties.

■ Countermeasure points

When entrusting services to contractors, organizations confirm in advance any matters necessary for the safe management of important information, and incorporate these into agreements. During the contract periods, organizations must check regularly and irregularly whether the security measures are implemented according to contracts[36]. Specifically, organizations must confirm the contents of services from the following standpoints (depending on the importance of the important information), and make sure the contents of the security measures.

1. Before entrusting services, organizations must make sure the required security measures for handling of important information to be correctly implemented. For this it is advisable that according to the services to be entrusted, organizations check the contractors' service systems and business scales, availabilities of audits for provided services, and conduct on-the-spot inspections if necessary so that the supervising managers or division managers can appropriately evaluate the findings.
2. Organizations regularly and irregularly inspect whether contractors security measures are sufficient for safe management. It is preferable that supervising managers or division managers properly conduct results evaluation including possible contract revision.

[36] Case Studies for Appropriate Protection of Personal Information, reported by The Ministry of Economy, Trade and Industry (March 2010) could be a useful reference for supervising contractors.

3. When contractors subcontract services, it is advisable that contractors in advance require subcontractors to provide information of service contents and rules for handling of important information, or obtain approvals for them. During the contract periods, contractors, or if necessary organizations themselves conduct inspections or audits regularly and irregularly[*Q&A9:P69] .
4. It is preferable to make sure beforehand that subcontractors provide logs in cases when internal improprieties are suspected, and it must be clearly stated in the agreements between contractors and subcontractors.
5. When using services provided by third parties (including cloud computing), organizations decide if the third parties can handle the important information in the entrusted services. Organizations also make sure if the service levels and management requirements are appropriate for business continuity.
6. During contract periods, organizations may consider changing contractors or even terminating contracts if contractors or third parties who provide services are found failing in conducting appropriate internal improprieties countermeasures according to the organizations' basic policies.

4-5. Securing Evidence

(17) Recording and Storage of Logs and Trails[37] in Information Systems

From the standpoints of early discovery of internal improprieties (27) and the scope of the effects of follow-up measures, it is advisable to record and store logs and trails including the history of access to important information and users' operation history, and then securely preserve them.

■ What risks are there?

If logs and trails are not recorded and checked periodically, the actions in logs and trails that are signs of improper activity may not be uncovered, meaning that detection may be delayed and damage may be major when detected.

Moreover, if information systems division does not preserve logs and trails, then in follow-up measures (27) after incidents of internal improprieties, they will have difficulty identifying the causes of internal improprieties or investigating the trail of the perpetrators of the internal improprieties or the scope of effects. Also they may not be accepted as the grounds for punishment stated in (22) or evidences necessary for possible contract disputes or lawsuits.

■ Countermeasure points

From the standpoints of early detection of internal improprieties and follow-up measures, information systems division is to record logs[38] and trails and securely preserve them as follows.

1. Logs are to record histories of access to important information and the operation history of users (web access logs, histories of sending/receiving e-mails, etc.).
2. Trails are to record information other than that in the above logs, including date, user, operation terminal, content of operations, and content of transmissions, based on established policies.
3. Logs are to be reviewed on a regular basis. It is advisable to check for non-routine work performed by officers and employees, including access to a large number of files or to the files that are not relevant to their work. If the case has been confirmed, organizations are to strengthen monitoring or take other measures.
4. It is advisable to take users' privacy into account and obtain agreement from the labor union and other parties concerned as to collecting such logs and trails.
5. In general, it is preferable to notify employees of the fact that user logs and trails are preserved, since it is considered effective for deterring internal improprieties.

---

[37] Records of events occurring in information systems and networks. In these Guidelines, "logs" are logs of activity taken on a system, and "trails" are collected according to policies determined for monitoring and auditing.

[38] Consider not only server logs but also client logs[*Q&A 10:P69 *Q&A 11:P70] are necessary.

6. Logs and trails preservation period is decided by balancing risks and costs. It is preferable not to inform the preservation period to insiders for the purpose of deterring internal improprieties[39].
7. For checking logs and trails it is advisable to take measures including preventions of falsification and unauthorized deletion, and restrictions that enable only specified system administrators' accesses. It is preferable to require supervising managers or system administrators' permissions when conducting checks.

[39] Except when necessary to inform it considering the systems development or operations inside organizations. Information systems division must consider the period for storing logs from various standpoints, including the importance of the information to be logged, cost, business type, business form, etc. Relevant laws and regulations include, with respect to the preparation of rules for requesting the preservation of electromagnetic records of (5) communication history under the partial revision to the Code of Criminal Procedure, include the following: "A public prosecutor, public prosecutor's assistant officer, or judicial police officer, when deeming seizure or seizure with demand for recording to be necessary, are to identify necessary items in electromagnetic records of communication histories recorded for business purposes, and may request in writing that these not be deleted for a period not to exceed 30 days (extensible to a period not to exceed 60 days in the case of particular need).".

(18) Checking of System Administrators' Logs and Trails

Information systems division is to record and store logs and trails of the access history and operation history of system administrators, and, along with logs and trails per (17), must have persons other than system administrators periodically perform checks of the content of logs and trails of system administrators.

■ What risks are there?

As system administrators bear considerable privileges, if persons other than system administrators do not check and monitor work reports by system administrators, it will be difficult to check the correctness and authenticity of tasks and to detect internal improprieties by system administrators.

■ Countermeasure points

Information system logs must log not only failures, but also normal administration and operation work. Specifically, information systems division is to establish the following, and record and protect work logs.

1. Information systems division is to record logs of work concerning information system configuration changes and operations[40], with the content of the work logs periodically checked by the supervisors of the information system administrators or by supervising administrators[41].
2. When collection of logs and trails can not be performed in systems, the work content of system administrators is to be documented, and is to be periodically checked by the supervisors of the information system administrators or by supervising administrators.

[40] Logs that must be obtained and preserved by system administrators at least include communication logs for devices (firewall, router, detection system, etc.) closely located to network boundaries, access records of various servers (web, proxy, database, DHCP, etc.) and records indicating activation of functions specific to each server (authentication, processing, allocation, etc.).

[41] Companies and organizations which perform internal impropriety countermeasures and which have internal audit systems in place are to consider methods of checking and operating as audit items for internal audits.

4-6. Human Management

(19) Dissemination of Internal Impropriety Countermeasures through Education

1. Organizations must provide education for all the officers and employees, and must disseminate policies concerning the organization's internal impropriety countermeasures, procedures for handling important information, etc.

2. It is advisable to repeat the education periodically. Moreover, organizations must review and update the content of the education, and disseminate the updated content to insiders.

■ What risks are there?

If organizations do not provide education for all the officers and employees, officers and employees are not able to conduct appropriate management. Moreover, if organizations do review the content of the education, measures toward new threats may not be taken, and internal improprieties may occur.

Organizations that do not provide education may be unable to pursue the liability of persons committing internal improprieties. Moreover, doubt may be cast onto the management responsibility of the company or organization.

Note that, with respect to contractual parties to whom important information is presented, if organizations do not sufficiently inform the officers and employees directly handling said information of the fact of the important information and the handling of important information, information may be leaked by the contractual party.

■ Countermeasure points

Organizations must inform all officers and employees about important information and the handling of it to raise their understanding and awareness of internal impropriety countermeasures, and must implement education that enables insiders to conduct countermeasures.

1. Organizations are to provide education concerning matters to be followed by insiders, the background to these, and so on[*Q&A7:P68]. It is advisable to repeat the education every year so its content is not forgotten.
2. As evidence of the education having been conducted, organizations are to record the fact that participants underwent the education and understood its content.
3. Organizations are to periodically review and update the content of the education, and disseminate the updated content.
4. It is advisable to conduct the education at appropriate levels and with appropriate content based on the privileges and duties of the participants, including position (managerial, non-managerial, etc.) and form of contract (employee, temporary worker, etc.). It is particularly advisable to provide education aimed at heightening consciousness of rules in system administrators.
5. Division managers or persons in charge continuously collect information from outside sources[42] and attend trainings so that they can gain necessary knowledge and improve their abilities in response to technical and social changes including information communication technology development and emergence of new threats or newly enforced laws.

[42] For example, IPA provides the latest information related to information security countermeasures at http://www.ipa.go.jp/.

(20) Personnel Procedures for Conclusion of Employment

To prevent the occurrence of important information leakage or other internal improprieties by ex-officers and ex-employees after the conclusion of employment, organizations should require said employees to submit written pledges of confidentiality as required.

■ What risks are there?

If organizations do not conclude confidentiality agreements (including written pledges) at the conclusion of employment, the officer or employee may leave the organization without recognizing the criticality of the important information they obtained during their work. In this case, the risk of such important information being disclosed by ex-officers and ex-employees increases. Furthermore, claims for damages caused by said disclosure will not be recognized. Organization may conclude no-compete obligation agreements (including written pledges) as required, but must be careful not to obstruct freedom of occupational choice.

■ Countermeasure points

At the conclusion of employment, it is advisable that organizations conclude confidentiality agreements and no-compete obligation agreements (including the submission of written pledges) with officers and employees.

1. Confidentiality agreements must include descriptions which enable objective identification of the important information subject to confidentiality.
2. Any no-compete obligations must be of appropriate scope so as not to obstruct freedom of occupational choice.

(21) Return of Information Assets Due to Conclusion of Employment or Conclusion of Contract

At the conclusion of employment or work contracts, organizations must require officers and employees and contractors to return or completely delete all information assets that they were entrusted to handle. Moreover, organizations must delete information system user IDs and privileges granted to hires or contractors.

■ What risks are there?

If information assets (including important information) for which handling were entrusted are not returned or deleted, there is a risk of important information being leaked by ex-employees or ex-contractors. Moreover, if entry passes and loaned devices are not returned, or information system privileges are not deleted, improper entry into buildings, unauthorized intrusion into information systems via networks, and improper removal of information assets from the premises may occur.

■ Countermeasure points

Organizations must take the following measures at the conclusion of employment or contracts.

1. Written pledges or contracts must specify the return of information assets and the complete deletion of information assets from contractors' PCs, etc. at the conclusion of employment or contracts.
2. Organizations must confirm the return of all information assets for which handling was entrusted, and all entry passes[*Q&A8:P69].
3. Organizations must confirm the deletion of information system user IDs and privileges.
4. It is advisable to obtain conclusive evidence that all important information stored on contractors' PCs, etc. has been completely deleted.
5. As the removal of information and other internal improprieties occur more easily immediately prior to conclusion of employment, it is advisable to place PCs, etc. under the management of the system administration division, etc. for a set period prior to the conclusion of employment. (Examples: Restrictions on scope of access, restrictions on USB storage usage, etc.)

4-7. Compliance

(22) Preparation of Legal Proceedings

Organizations must take into account dismissal or other disciplinary actions for insiders committing internal improprieties, prepare rules of employment and other internal rules, and make provisions for official disciplinary proceedings.

■ What risks are there?

If disciplinary actions toward insiders committing internal improprieties are not incorporated into rules of employment or other internal rules, or if official disciplinary proceedings are not prepared, disciplinary actions may be rendered invalid by a claim of improper action from the insider.

■ Countermeasure points

When taking disciplinary action, it is necessary that items concerning disciplinary actions and confidentiality obligations be stipulated in internal rules.

1. Internal rules must note the internal improprieties (e.g., infringement of trade secrets, use of personal information for non-allowed purposes) that are subject to disciplinary action.
2. Internal rules must include descriptions which enable objective identification of important information for which confidentiality obligations hold.
3. Organizations must conduct dismissal and other disciplinary action within the framework of labor laws, based on internal rules that form the grounds for action.
4. In order to determine an appropriate disciplinary action, it is necessary to make the facts clear through a commission of inquiry, etc.
5. Organizations must make preparations for civil action and criminal prosecution legal proceedings.

(23) Requests for Written Pledges

In order to make obligations to protect important information understood by officers and employees, organizations must request them to submit written pledges of confidentiality.

■ What risks are there?

If officers and employees do not submit written pledges, organizations will be unable to instill understanding and awareness of the obligations to protect important information. Moreover, in the event of dismissal or other disciplinary proceedings against officers and employees committing internal improprieties, disciplinary actions may be rendered invalid by a claim of improper action from the officers and employees.

■ Countermeasure points

Organizations must ensure that the important information covered in written pledges of confidentiality can be identified objectively. Moreover, organizations must request written pledges of confidentiality at periodic intervals so as to instill awareness of the protection of important information.

1. Written pledges of confidentiality must include descriptions which enable objective identification of the important information subject to confidentiality.
2. In order to make obligations to protect important information understood by officers and employees, it is advisable that organizations request written pledges of confidentiality at periodic intervals in addition to the time of joining the company, such as at the time of changes in work duties due to advancement, personal relocation, etc., or at the conclusion of projects[43].

[43] If organizations request the submission of written pledges of confidentiality from officers and employees at their retirement, they may not accede to the request.

4-8. Workplace Environments

(24) Preparation of Impartial Personnel Evaluations

It is advisable that personnel division provides impartial and objective personnel and performance evaluations. It is also advisable to provide opportunities to explain how evaluation is carried out in personnel and performance evaluations. Moreover, it is advisable to conduct personnel assignments and reassignments to prepare appropriate work environments, as required.

■ What risks are there?

When officers and employees do not feel impartiality and objectivity in personnel evaluations and performance evaluations, discontent and dissatisfaction can degrade the workplace environment, which in turn may induce internal improprieties.

Moreover, if specific work is left in the hands of an individual without reassignment for long periods, important information may be handled only by the individual and improperly used. Moreover, if handling of the same type of important information becomes routine, awareness of the need for caution in handling the important information may lessen, heightening the likelihood of incidents occurring through careless mistakes or errors in operation.

■ Countermeasure points

The personnel division and persons in charge of personnel must take the lead in preparing evaluation systems for personnel evaluations and performance evaluations. Moreover, appropriate personnel assignments and relocation must be done.

1. It is important that personnel division impartially and objectively implement promotions, advancement, and organizational pay structure, while maintaining sufficient transparency. It is advisable that superiors or division heads provide explanations of the content of performance and other evaluations, as required.
2. As part of preparation for evaluation systems, it is advisable that organization encourage officers and employees to participate in education and training for skills and knowledge necessary for work.
3. When specific work is left in the hands of an officer or employee without reassignment for long periods, it is advisable to consider personnel relocation to avoid such situation.

(25) Promotion of Reasonable Work Environments and Communication

Organizations should promote environments that maintain good communication throughout the workplace, such as by preparing systems for promoting mutual work support and environments facilitating consultation, while also preparing suitable work environments through means such as normalization of workloads and working hours.

■ What risks are there?

If organizations do not prepare work environments with suitable workloads and working hours, specific officers and employees may be overloaded with work, and trying to reduce their workload and working hours, they may commit internal improprieties. Moreover, difficulties in executing work duties can heighten discontent in officers and employees and may lead to internal improprieties. When environments facilitating consultation or good communication are insufficient, work may continue under a situation of work-related worries or stress, and internal improprieties may occur.

■ Countermeasure points

In the preparation of workplace and work environments, the general affairs division and the persons in charge thereof must take the lead in normalizing workloads and working hours. In addition, they must prepare environments that facilitate consultation while considering trust relationships in the workplace, and at the same time, must promote support for work along with good communication with superiors and colleagues.

1. When workload is extremely high or working hours are long, including situations in which specific individuals cannot take time off or situations of overtime work, organizations must set appropriate scopes for workload and working hours.
2. Organizations must set work within a scope that is not harmful to physical or mental health, and must keep workplace environments safe and sanitary.
3. Superiors and division heads must discern the capabilities of staff members and subordinates and, to the extent possible, allot appropriate work content and workloads to these.
4. Superiors and division heads must consider systems and environments for providing as much support as possible to members and subordinates who require assistance with work and duties.
5. Organization must construct and maintain good teamwork among staff members, with staff members assisting each other with delays or problems on the job.
6. Organization must create and maintain an environment in which staff members engage in active exchange of information on the job and can also engage in consultations other than for work.
7. It is advisable that organizations promote work support and aid by persons.
8. In order to detect and rectify concerns over work or stress over personal relationships, it is advisable that organizations prepare environments that facilitate consultation not only with superiors but also with colleagues, and promote environments that maintain good communication throughout the workplace.
9. It is advisable that organizations create environments in the workplace that facilitate listening to problems. It is advisable to prepare environments in which when officers and employees find it hard to pour out their concern at the workplace (e.g. those related to their immediate superior), they can consult a consultation service outside their workplace that provides feedback to a big boss so that the situation is improved. To make consulters feel safe, organizations may handle concerns with anonymity depending on their content, with their feedback provided to a big boss.

(26) Management in Workplace Environments

It is advisable that organizations or the division in charge restrict independent work that is conducted apart from other officers and employees and disallows mutual monitoring.

■ What risks are there?

As independent work involves an environment in which the absence of other employees disallows mutual monitoring, the likelihood of internal improprieties occurring is high. When internal improprieties do occur, detection may be delayed and damage may spread. Moreover, when such independent work is performed, “(24) Preparation of Impartial Personnel Evaluations” and “(25) Promotion of Reasonable Work Environments and Communication” may be degraded.

■ Countermeasure points

1. As independent work involves an environment in which the likelihood of internal improprieties occurring is high, organizations need to check for the necessity of the work etc. and prepare procedures to track the work. For each independent work, the responsible manager etc. of the division concerned must check if the work really needs to be done independently and pre-approve it. Check items for the pre-approval are: the reason for "Why the work needs to be done in that period?" etc.; period/hours; and contents of the work. It is advisable to consider necessary assistance to avoid such independent work.
2. Independent work involves the risk of internal improprieties by the individual, so organizations need to perform after-the-fact check. Check items for the after-the-fact check are: consistency between the pre-approved work contents and the actual work contents; whether or not important information is handled during the independent work; and contents of modification, etc.

4-9. Follow-up Measures

(27) Preparation of Systems Required for Follow-up Measures

In order to identify the scope of the effects of internal improprieties, organizations must assess the concrete status of incidents and must implement measures to minimize damage and prevent the spread of effects. In addition, organizations must secure systems for cooperation with parties concerned inside and outside the organization, as required.

■ What risks are there?

Organizations that cannot identify the scope of the effects of internal improprieties may be unable to take prompt follow-up measures and may be unable to consider legal enforcement and other responses. Furthermore, when using third-party services (digital forensic[44] analysis, incident response[45] support, etc.) in the investigation or handling of internal improprieties, organizations that have not made provisions for the necessary information and means of communication may be unable to receive suitable support.

■ Countermeasure points

To construct systems required for follow-up measures, organizations must prepare the following content.

1. To minimize the damage caused by internal improprieties and prevent the spread of effects, organizations must determine in advance the required response procedures and reporting procedures. To assess the concrete situation surrounding internal improprieties and investigate the scope of effects, organizations must preserve verifiable evidence[46] concerning "who did what and when".
2. In responding to internal improprieties, organizations must cooperate with system administrators, persons in charge of incident response (including persons in charge of external incident response support), persons in charge of digital forensic analysis (including persons in charge of external support), attorneys, and internal auditors. Moreover, when receiving services, it is advisable that organizations determine the content and methods of communication in advance, so as to enable prompt provision of necessary information.
3. In cases where services are entrusted, organizations must develop systems in cooperation with contractors. Also cooperation systems after incidents should be specified beforehand in writings such as agreements.
4. Organizations must prepare systems for responding to cases that involve reporting requirements to the competent authorities.
5. Organizations having business continuity plan (BCP) and going to construct systems for internal impropriety countermeasures need to take into account the relationship with the BCP.

---

[44] A series of scientific investigative methods and techniques for conducting preservation of evidence, investigation, and analysis of electromagnetic records, along with analysis and information collection concerning falsification, damage, etc. of electronic records, in response to legal disputes, legal action, and acts such as improper use of computer and networks or obstruction of service.

[45] Follow-up response for the purpose of minimizing damage following information security incidents and accidents such as malicious attacks, viral infections, and theft of PCs.

[46] See "Documents proving the consistency of evidence preservation (Chain of Custody)" of the Evidence Preservation Guidelines issued by the Institute of Digital Forensics.

(28) Consideration of Punishment and Prevention of Recurrence

Organizations must consider the punishment to be applied to internal perpetrators of serious improprieties. Moreover, from the standpoint of preventing recurrence, while taking measures to prevent recurrence it is also advisable that organizations provide notification within the organization of cases involving internal improprieties.

■ What risks are there?

When organizations do not consider punishments for the perpetrators of internal improprieties, or do not take measures to prevent recurrence, similar internal improprieties may recur. Moreover, from the standpoint of preventing recurrence, when organizations do not perform internal notification and dissemination of cases involving internal improprieties, similar internal improprieties may recur.

■ Countermeasure points

To consider punishment for perpetrators of internal improprieties, and to consider the prevention of recurrence, organizations must prepare the following content.

1. To minimize the effects caused by internal improprieties, organizations must incorporate internal impropriety countermeasures into required response procedures, reporting procedures, and other business continuity management procedures. In order to consider punishments for perpetrators of internal improprieties, organizations must undertake consideration of legal action together with persons in charge of personnel, persons in charge of legal affairs, attorneys, etc., based on content established in the preparation of legal proceedings per (22) in these Guidelines.
2. Organizations must consider and implement measures to prevent the recurrence of internal improprieties.
3. It is advisable that organizations learn from the specific facts of incidents of internal improprieties, and, from the standpoint of preventing recurrence, provide notification of cases of internal improprieties within the organization, including the actions taken against the perpetrators.

4-10. Organizational Management

(29) Preparation of Whistleblower Systems for Internal Improprieties

Organizations or the division in charge must prepare whistleblower systems for the occurrence of incidents suspected of involving internal improprieties. Organizations or the division in charge must establish multiple whistleblower contact points to allow reports by officers and employees to parties concerned with internal impropriety countermeasures (Supervising Manager, etc.) other than their own divisions. Organizations or the division in charge must also secure anonymity for whistleblowers, as required. Organizations or the division in charge must also provide education on the specific usage and disseminate it.

■ What risks are there?

If organizations or the division in charge do not prepare whistleblower systems for the occurrence of incidents suspected of involving internal improprieties and do not provide education on the specific usage, internal whistleblowing will not function, response will be delayed, and signs of internal improprieties may be overlooked. Moreover, if organizations or the division in charge do not establish multiple whistleblower contact points for internal improprieties, then cover-ups may prevent information from reaching (i.e., being reported to) the Supervising Manager, etc. from divisions where the problems are thought to have occurred. Moreover, if organizations or the division in charge do not secure anonymity for whistleblowers, then due to the effects of surrounding human relations, etc., information thought to concern internal improprieties may not be obtained.

■ Countermeasure points

With regard to internal impropriety whistleblower systems, organizations or the division in charge must prepare content such as the following.

1. Reporting of internal improprieties must include the following information, etc. at a minimum: "Contact points (contact information and method)", "Targeted information or physical assets", "Time and situation of incident (e.g., improper use, destruction, etc.)", "How the incident became known", etc.
2. Organizations must develop systems stated in (27) to promptly conduct investigations in the event inquiries or reports concerning important information are made from outside.
3. Organizations or the division in charge are to provide education on the above systems for internal whistleblowing.
4. It is advisable for organizations or the division in charge to establish whistleblower contact points (including hotlines, etc.), in addition to the heads of the divisions to which officers and employees belong.
5. In order to secure anonymity and prevent whistleblowers from suffering disadvantages from the act of reporting, organizations or the division in charge are to consider establishing anonymous post office boxes and suggestion boxes, or to consider the use of third-party organizations.

(30) Implementing Checks Incorporating the Prevention of Internal Improprieties

Organizations must identify specific internal impropriety countermeasure items from the standpoint of preventing and deterring internal improprieties, and must regularly and irregularly conduct checks (including internal and other audits). Moreover, organizations must report the results of audits, following confirmation by the Supervising Manager, to the top manager, and must conduct reviews of countermeasures as required.

■ What risks are there?

If organizations do not conduct periodic and non-periodic checks and audits, including the monitoring noted under "(1) Clarification of the Responsibilities of the Top Manager", the organizations may be unable to confirm the status of internal impropriety countermeasures or problem points in the organization, and may be unable to conduct and review effective measures.

■ Countermeasure points

To conduct checks and audits (including internal and external audits) in terms of prevention and deterrence of internal improprieties, organizations must make plans considering the following items and conduct them accordingly. Once they are conducted, organizations must re-evaluate risks to review countermeasures and resource allocations under top managers' leaderships.

1. Organizations must make reference to items which are particularly advisable as internal impropriety countermeasures (items thought to be related in cases of internal improprieties, etc.), must confirm the implementation status, preparation status, etc. of specific countermeasures, and must report to top managers.
2. Organizations must check matters including whether differing management and handling are being applied to similar information, based on the work content of each division and dealings with parties concerned.
3. Organizations must confirm records concerning incidents thought to involve internal improprieties and related incidents, and must confirm that these are promptly reported following occurrence. Moreover, organizations must confirm whether any cases violate management procedures and handling methods for important information, and must confirm follow-up remedies, etc.
4. Internal improprieties countermeasures must be reviewed according to technical and social changes including information communication technology development, emergence of new threats and newly enforced laws. They should be continuously reviewed and improved.

Appendix I: Internal Impropriety Case Studies

Case studies from interviews surveys and case study surveys from the "Survey of Incidents Due to Improper Activity by Organization Insiders" by the Information-technology Promotion Agency, Japan and from the committee for the creation of "Guidelines for the Prevention of Internal Improprieties in Organizations" are presented below.

No	Overview	Items related to these Guidelines
1	A salesperson at a regional financial institution was embezzling funds from dormant accounts. Main cause: The salesperson was kept in a position without reassignment in order to maintain sales performance and no mutual monitoring was in place, which created an environment in which internal improprieties were difficult to detect.	(24) Preparation of Impartial Personnel Evaluations (26) Management in Workplace Environments
2	A system administrator in a small company changed settings on the president's PC to forward e-mail sent to the president to the account of the system administrator, who then read the e-mail. Main cause: Only one person in the company was in charge of the system administrator, creating an environment in which internal improprieties were difficult to detect. Moreover, this employee may have had low consciousness of the rules required for system administrators.	(7) Administrator Access Management (19) Dissemination of Internal Impropriety Countermeasures through Education
3	A system administrator employee in a company taken confidential information from the premises with the intent of working at home, but performed work on a home PC with file-sharing software (Winny) installed, resulting in leakage of information. Main cause: Confidential information was taken from the premises without informing anyone. The employee may not have fully known the severity of punishment for working at home without permission and leaking confidential information.	(12) Safety Management for Network Usage (19) Dissemination of Internal Impropriety Countermeasures through Education
4	A laptop PC was lost while left for a long period on a piled-up desk. Subsequent investigation revealed that the laptop PC had been sold, with the perpetrator unknown. Main cause: Laptop PCs were not managed, and could be taken away by anyone entering the floor.	(9) Asset Management and Physical Protection of Information Devices and Storage Media
5	An employee in a company took a CD-ROM containing confidential information from the premises, and sold the information. When taking confidential information from the information system, the employee had his subordinate create the CD-ROM containing the confidential information through official procedures, explaining to the subordinate that the action was part of work, and then engaged in cover-up. Main cause: Removal of CD-ROMs containing confidential information from the premises was not managed.	(9) Asset Management and Physical Protection of Information Devices and Storage Media

6	A developer in a company took development source code, etc. from the premises by uploading it to external online storage, out of belief that he owned the source code he developed and that the code would be useful in other projects. Main cause: The developer did not recognize that developed items belong to the company. Moreover, the company did not restrict the use of external online storage.	(12) Safety Management for Network Usage (19) Dissemination of Internal Impropriety Countermeasures through Education
7	A system administrator in a company repeatedly took confidential information from the premises and sold it. Each time, the employee escalated the severity of the act of removing confidential information from the premises. Main cause: The company was supposed to perform monitoring of system administrators' operations, but confidential information was repeatedly taken from the premises due to laxness on the part of the person in charge. Moreover, the privileges of system administrators were not distributed and may have been concentrated in a single person.	(6) Rights Management for System Administrators (18) Checking of System Administrators' Logs and Trails
8	A telecommuting employee in a company connected to the company's information systems from home via the Internet, and obtained and sold confidential information. As telecommuting makes work difficult to monitor, it more readily facilitates internal improprieties than does an office. Main cause: The company did not restrict access to its information systems and confidential information via the Internet by telecommuters, etc. Moreover, the company may not have been monitoring whether information other than that necessary for telecommuting was being accessed.	(15) Protection of Important Information in Work Outside of the Organization (17) Recording and Storage of Logs and Trails in Information Systems
9	Upon leaving a company, an employee downloaded a developed item and took it from the premises, with the intent of using it in a new place of employment. Main cause: There was a lack of awareness that developed items should not be taken from the premises and used at the new place of employment. Moreover, non-routine work performed by officers and employees such as access to a large number of files was not monitored and no measures were enacted.	(5) User access Management in Information Systems (17) Recording and Storage of Logs and Trails in Information Systems (20) Personnel Procedures for Conclusion of Employment
10	A salesperson in a company, leaving the company due to restructuring, changed a PC password without permission, and then claimed forgetfulness in not providing notice of the changed password. Main cause: Management rights for the PC were not placed with the company for a set period prior to the conclusion of employment.	(21) Return of Information Assets Due to Conclusion of Employment or Conclusion of Contract

11	A number of employees in a division of a company, retiring at the same time to form a new company, took customer data (a trade secret) from the premises for use in the new company. Main cause: The employees had poor awareness of the fact that the act of improperly removing trade secrets from the premises and using the information violates the Unfair Competition Prevention Act.	(20) Personnel Procedures for Conclusion of Employment (21) Return of Information Assets Due to Conclusion of Employment or Conclusion of Contract (23) Requests for Written Pledges
12	An employee of a contracted web site construction and operation company sold the customer data of a client company to a competitor, despite knowing the improperness of the act. The competitor used the customer data for its sales activities. Main cause: The company may not have confirmed that the information security measures of the contracted web site construction and operating company were sufficient.	(13) Transfer and Protection of Important Information (16) Confirmations of Contractors Services (Including when using services provided by third parties)
13	An ex-employee of a company manufacturing and selling products used the company's design drawings to manufacture and sell similar products at a competing company. Main cause: The company did not properly handle the return of important information upon departure of employees.	(21) Return of Information Assets Due to Conclusion of Employment or Conclusion of Contract
14	Personal information handed over by a company to a maintenance contractor was copied and sold by a part-time worker in a subcontracting company. Main cause: The company did not make the important information management systems of the contractor clear, and did not perform management extending to subcontractors.	(13) Transfer and Protection of Important Information (16) Confirmations of Contractors Services (Including when using services provided by third parties)
15	An ex-employee of a company used a remote access connection service for connecting to the company's network via the Internet, and taken confidential information from the company. Main cause: The ex-employee's account was not deleted from the remote access connection service.	(5) User Access Management in Information Systems

16	A teacher in an educational institution used USB storage to take grades and other student data from the premises. The student data was leaked when the USB storage was stolen. Main cause: The student data was not encrypted.	(15) Protection of Important Information in Work Outside of the Organization
17	In an educational institution environment allowing tacit permission for work usage of personal smartphones, an employee's personal smartphone was stolen and the personal information stored was leaked. Main cause: The institution did not set and operate an appropriate scope of usage, tacitly allowing work usage of personal smartphones.	(11) Restrictions on Bringing in and Using Personal Information Devices and Storage Media for Work
18	An employee in a contracting company providing a banking corporation with ATM maintenance and management service illegally obtained customers' card information from ATM transaction data. He forged cash cards using this information to withdraw money. Main cause: Privileges were heavily concentrated on the employee who was the project manager and that enabled him to forge the card only by himself. Also mutual monitoring system was not sufficient.	(6) Rights management for system administrators
19	An ex-employee in a business partner for a company illegally took out the company's research data and provided it to a foreign corporation he left for. Main cause: Dissatisfaction with working condition was one of his motives. Use of record media must have been restricted and access to important information must have been monitored through recorded access logs, as internal improprieties such as taking out information from premises tend to occur before resignation.	(24)Preparation of Impartial Personnel Evaluations (17)Recording and Storage of Logs and Trails in Information Systems (21)Return of Information Assets Due to Conclusion of Employment or Conclusion of Contract

20	An employee working for a company which is a group company of a contractor maintaining and managing customer database improperly obtained and brought out personal information from the premises for the purpose of selling. Main cause: Bringing personal belongings in the premises was not restricted. Countermeasures were implemented on business-use PCs to prevent record media connection, but the countermeasures failed when the latest smart phone was connected. The smart phone was accepted as record media and that allowed the employee to take out data. Also the company did not recognize that the security measures for the contractor's associate companies were insufficient.	(11)Restrictions on bringing in and using personal information devices and storage media for work (16)Confirmations of Contractors Services (Including when using services provided by third parties) (30)Implementing Checks Incorporating the Prevention of Internal Improprieties

Appendix II: Internal Impropriety Check Sheet

The internal impropriety check sheet in this appendix is a summary of the countermeasures presented in Chapter 4 in these Guidelines.

* □: Key person in charge / implementing division[47]; [ ]: Divisions confirming support / implementation aid[48]

No	Content	Check items
■Basic Policies		
1-1	Has the top manager formulated "basic policies" and disseminated these to officers and employees, for the purpose of showing within and outside the organization that internal impropriety countermeasures are the responsibility of the top manager? (See Appendix IV for examples of basic policies.)	□ : Top Manager(CEO)
1-2	Has the top manager made necessary decision and instruction to secure resources for implementing measures based on "basic policies"?	□ : Top Manager(CEO)
2-1	Has the top manager appointed a Supervising Manager for internal impropriety countermeasures, and is the top manager conducting approvals for management systems and implementation measures? (However, if the organization is one in which the top manager has a view of the entire organization and implements internal impropriety countermeasures on his or her own, it may not be necessary to construct management systems.)	□ : Top Manager(CEO)
2-2	Has the Supervising Manager constructed cross-organizational management systems in accordance with the basic principles, and formulated implementation measures?	□: Supervising Manager

[47] A division which, from the standpoint of its work content, is deemed appropriate to implement that countermeasure item in the check sheet.

[48] Divisions with which key person in charge/implementing division should cooperate in establishing and implementing the countermeasure item.

No	Content	Check items				
		Immediate division	Related divisions			
			Information Systems Division	General Affairs Division	Personnel Division	Legal Affairs and Intellectual Property Divisions
■Designation as Confidential						
3	Does the organization assess important information, assign it rating categories according to degree of importance, and set the scope of insiders allowed to handle the information?	□				
4-1	Do creators of important information select an established rating category for the information, and obtain confirmation of the selection from superiors, etc.?	□				
4-2	Are confidentiality marks, etc. understandable by insiders displayed on electronic documents containing important information?	□				
■Designation of Access Rights						
5-1	Do persons in charge of administering and operating information systems do so with procedures established for registration, change, deletion, and other settings concerning user IDs and access rights?		□			
5-2	Do persons in charge of administering and operating information systems promptly delete user IDs and access rights that have become unnecessary due to transfer or retirement?		□			
6	When there are multiple system administrators, does the organization assign an appropriate scope of rights for each system administrator ID and enable information system administrators to monitor each other? In addition, when only one person in the organization is in charge of the system administrator, does the organization monitor the administrator' operations through logs etc.?	□	[ ]			
7	Does the organization perform authentication using individual passwords, IC cards, etc. for individual users and system administrators, without using shared IDs, shared passwords or shared IC cards, etc.?	[ ]	□			
■Physical Management						
8	Does the organization physically protect locations where important information is stored, handled, etc. with walls and entry/exit management measures?	□	[ ]	[ ]		

No	Content	Check items				
		Immediate division	Related divisions			
			Information Systems Division	General Affairs Division	Personnel Division	Legal Affairs and Intellectual Property Divisions
9-1	Does the organization manage and protect information devices such as PCs and portable storage media such as USB storage to prevent theft, improper removal from the premises, etc.?	□	[ ]			
9-2	When disposing of information devices or storage media, does the organization confirm that important information has been completely deleted?	□	[ ]			
10	When mobile devices and portable storage media are taken from the premises, does the organization manage the approval, recording, etc. of the removal?	□	[ ]			
11	Does the organization restrict employees' bringing in and using personal mobile devices and storage media for work?	[ ]	□			
■Technological and Operational Management						
12	Does the organization restrict the use of file sharing software, SNS, external online storage, etc. on its networks, to prevent improper removal of important information?		□			
13-1	Does the organization manage the transfer of important information to contractors or other parties concerned, at all steps from transfer to disposal?	□	[ ]			
13-2	Does the organization take into account the mistaken transfer of important information to persons other than the parties concerned via the Internet or otherwise outside the organization, and protect the important information using encryption, etc.?	□	[ ]			
14	Does the organization limit the important information that can be used and handled outside the organization, and protect important information and information devices?	□	[ ]			
15	Does the organization take into account the surrounding environment, network environment, etc. when performing work using important information outside the organization?	□	[ ]			
16	Does the organization confirm and agree the security measures according to the services to be entrusted prior to the contract agreement, and make sure whether	□	[ ]			[ ]

No	Content	Check items				
		Immediate division	Related divisions			
			Information Systems Division	General Affairs Division	Personnel Division	Legal Affairs and Intellectual Property Divisions
	the security measures are practiced as specified in the agreement during the contract period?					
■Securing Evidence						
17	Does the organization safely protect logs and trails for a fixed period, including the history of access to important information and users' operation history?	[ ]	□			
18	Does the organization not only record and store logs and trails of the access history, operation history, etc. of system administrators, but also have the content of these periodically checked by persons other than system administrators?		□			
■Human Management						
19-1	Does the organization provide education for all the officers and employees, and disseminate policies concerning the organization's internal impropriety countermeasures, procedures for handling important information, etc.?	□		[ ]	[ ]	
19-2	Does the organization periodically repeat its education, and periodically review and update its content?	□		[ ]	[ ]	
20	At the conclusion of employment, does the organization require employees to submit written pledges imposing confidentiality obligations? (recommended)	□		[ ]	[ ]	[ ]
21	At the conclusion of officers and employees employment and termination of work contracts with contractors, does the organization have them return or completely delete all information assets which were entrusted to handle, and does the organization delete their user IDs and privileges from information systems?	□		[ ]	[ ]	[ ]
■Compliance						
22	Has the organization prepared rules of employment and other internal rules, and made provisions for official disciplinary proceedings?	□		[ ]	[ ]	[ ]
23	In order to make obligations to protect important information understood by officers and employees, does the organization request them to submit written pledges of confidentiality etc.?	□		[ ]	[ ]	[ ]
■Workplace Environments						

No	Content	Check items				
		Immediate division	Related divisions			
			Information Systems Division	General Affairs Division	Personnel Division	Legal Affairs and Intellectual Property Divisions
24	Does the organization promote impartial and objective personnel and performance evaluations as well as provide opportunities to explain how evaluation is carried out in personnel and performance evaluations? (recommended)			[ ]	□	
25	Does the organization as a whole promote environments that maintain good communication throughout the workplace, such as by preparing systems for promoting mutual work support and environments facilitating consultation, while also preparing suitable work environments through means such as normalization of workloads and working hours? (recommended)			□	[ ]	
26	Does the organization restrict independent work apart from other employees in environments that disallow mutual monitoring, and has the organization set necessary procedures for prior approval for independent work? (recommended)	□		[ ]	[ ]	
■Follow-up Measures						
27	In order to identify the scope of the effects of internal improprieties, organizations must assess the concrete status of incidents and must implement measures to minimize damage and prevent the spread of effects. In addition, organizations must secure systems for cooperation with parties concerned inside and outside the organization, as required. Does the organization do so?	□	[ ]			
28	Has the organization considered punishment for perpetrators of international improprieties, and has the organization considered providing notification of cases of internal improprieties within the organization?	□	[ ]			
■Organizational Management						
29	Has the organization prepared whistleblower systems for the occurrence of incidents suspected of involving internal improprieties, has it established multiple points of contact, and does it secure anonymity for whistleblowers, as required?	□	[ ]			

No	Content	Check items				
		Immediate division	Related divisions			
			Information Systems Division	General Affairs Division	Personnel Division	Legal Affairs and Intellectual Property Divisions
30	Does the organization identify internal impropriety countermeasure items, regularly and irregularly conduct checks (including internal and other audits), report the checked results to the top manager, and conduct reviews of countermeasures, as required?	□	[ ]			

Appendix III: Q&A

Q&A for assisting countermeasures (1)

Q-1. I do not know how to formulate basic policies. (4-1 (1))　(4-1(2))

A-1. The basic policies shown in these Guidelines assume the use of existing basic information security policies. If necessary, items concerning internal impropriety countermeasures should be added. The following are minimum items for the organizations having no basic information security policy.

In their basic policies, companies should set the following 3 items at the minimum, from the standpoints of thoroughly conducting protection and management of important information within the company, and of external accountability.

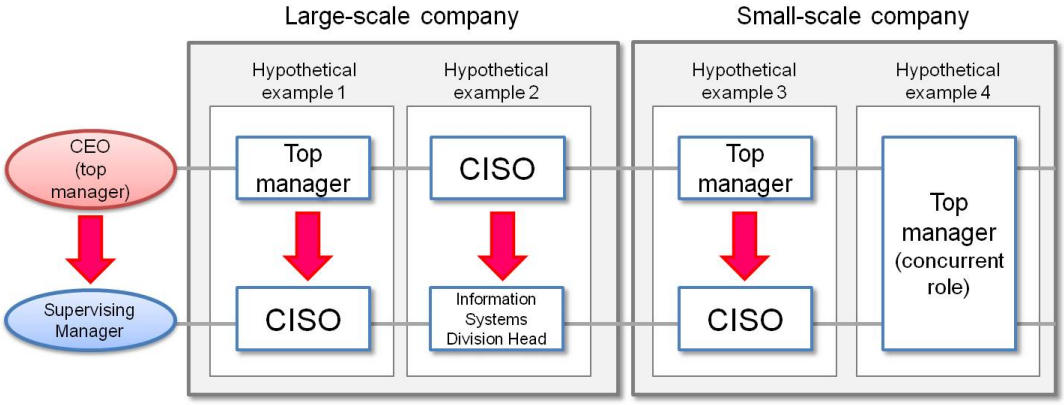
(1) The top manager shall recognize the need to conduct risk management as a management issue, and as a component of this, shall prevent internal improprieties and shall show the importance of protecting and managing important information.

(2) Basic policies shall identify important information that should be protected and managed, and shall indicate the business importance of this important information. Important information is the information which has considerable effects on the business of the company or group. Examples include manufacturing and development information or sales information, including strategic information and undisclosed intellectual property. Shared information obtained from parties concerned that are obligated to perform management of confidentiality is also included.

(3) Basic policies shall show implementation systems for the protection and management of important information, and while conducting reviews shall show that activities are ongoing. Implementation systems are to note systems that should be prepared in implementing internal impropriety countermeasures. The minimally responsible person must be indicated. Moreover, activities for improving countermeasures on an ongoing basis are to be shown.

For details, see the examples of basic policies in Appendix V.

The systems noted in basic policies assume a division into large-scale and small-scale companies, each with two types of systems. An overview of systems is described using the figure below.



In large-scale companies, a system with the top manager as the CEO and the CISO as the Supervising Manager (hypothetical example 1), and a system with the CISO as the CEO and the information systems division head as the Supervising Manager (hypothetical example 2), are assumed. In small-scale companies, a system with the top manager as the CEO and the CISO as the Supervising Manager (hypothetical example 3), and a system with the top manager as both CEO and Supervising Manager (hypothetical example 4), are assumed.

Q&A for assisting countermeasures (2)

Q-2. I do not know how to categorize important information. (4-1 (1))
A-2. First, information can be divided into two according to whether it is subject to protection. Information subject to protection should be managed with the organization setting rules for its handling. In actual work, when there is a need to change handling according to differences in the degree of importance of information subject to protection, the number of categories for managing the information can be increased. However, as too many categories can complicate management, about four categories are advisable.

Q&A for assisting countermeasures (3)

Q-3. I do not know what sort of information comes under important information. (4-1 (1))
A-3. Important information varies according to the work content and the information handled by divisions. For example, for a sales division this includes customer data and sales information restricted to parties concerned, and for a development division, important information may include developed items and specifications/design documents. In general, important information can be considered to be information that has an effect on the profits of the organization. However, the sharing of important information with parties concerned outside the organization is connected to profits in some cases, and varied handling and scopes of sharing can be considered depending on the work and status of the supervising divisions. Moreover, degree of importance may change by time: information with a high degree of importance can become public knowledge after a certain period of time.

Q&A for assisting countermeasures (4)

Q-4. I don't know what the special divisions and committees are.(4-1(2))
A-4. They are for example to set up “management committees” supervising handling of important information with divisions or managers as officials responsible for supervising handling of important information. “Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information” (2014 revised version) refers to “Establishment of the so-called Chief Privacy Officer (CPO) and Establishment of the responsible official for the operation and the limitation of operators in the handling of personal data” as preferable means to be taken for systematic security control measures.

Q&A for assisting countermeasures (5)

Q-5. I am trying to implement notification systems based on traffic to conduct monitoring, but do not know how to set criteria for the traffic to be reported (4-2-2(5)).
A-5. When monitoring through notification systems it is important to set and review the criteria according to the systems operations, since necessary notices are not provided if the criteria for notices is too lenient, while improprieties can be difficult to detect if notices are frequently made due to too strict criteria.

Q&A for assisting countermeasures (6)

Q-6. I do not know how to set user-managed password rules that prevent the use of simple character strings. (4-2-2 (7))
A-6. Simple character string passwords mean passwords identical to user IDs, user names or birthdays, or using keyboard arrays (such as "123456" or "QWERTYU"). To avoid users setting such simple character strings as passwords, organizations should set rules for passwords such as eight or more characters, with a mixture of upper-case and lower-case letters.

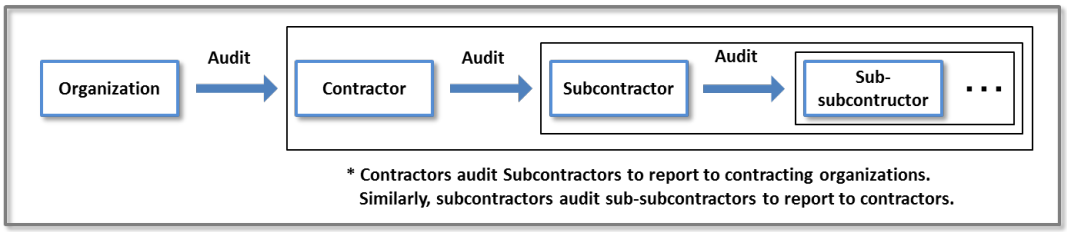
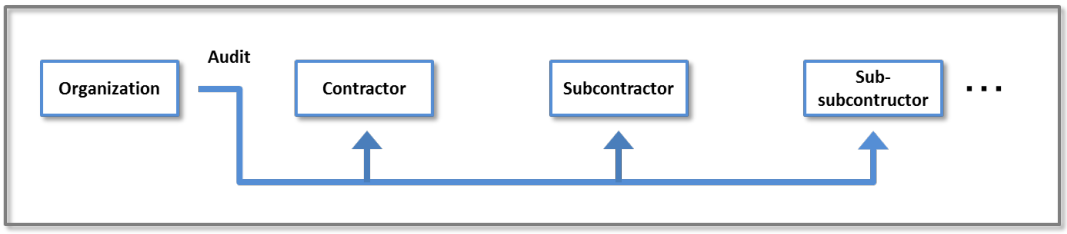
Q&A for assisting countermeasures (7)

Q-7. I do not know how to strengthen security for physically compartmented areas where important information is handled. (4-3 (8))
A-7. Organizations should restrict the persons who can enter physically compartmented areas (company grounds, buildings, rooms, etc.) where important information is handled, and should be able to identify targeted persons. Organizations should also record workplace or room entry/exit, and should appropriately manage and regularly and irregularly check the records. It is advisable to install equipment for automatically recording those histories, but when the installation or placement of such equipment is difficult, organizations should record workplace or room entry/exit history on their own, and then appropriately manage and regularly and irregularly check the records. It is important that the workplace or room entry/exit history not be viewable by other persons entering or exiting. With regard to IC cards which are used to enter or lock the compartmented areas where important information is handled, organizations must consider items such as the following. (1) Operation and management of keys and IC cards • Prohibit the loaning of keys and IC cards among officers and employees and keep records of the loaning and return of keys and IC cards under the confirmation of the responsible manager (the person in charge of the compartmented area). • Use dimple keys and IC cards that are hard to duplicate. • When keys and IC cards have become unnecessary for officers or employees due to transfers, retirements, etc., make sure that the keys and IC cards are returned. • Establish procedures (i.e., create manuals) for the loss of keys and IC cards, along with measures that can be taken immediately to invalidate lost keys and IC cards. • Carry out regular and irregular (i.e., surprise) checks of key/IC card possession, targeting persons to whom keys and IC cards are lent. • Not to store spare keys together with information identifying the keys' place of use. • Information identifying the place of use of spare keys with a given key number is to be handled as important information. (2) Confirmation of entry/exit history • Carry out regular and irregular checks of entry/exit records (including camera images) and make sure that the key operators (the owners of the IC cards) and those who actually entered and left the compartmented areas are identical. • Carry out regular and irregular checks of entry and exit information obtained through entry/exit management to detect unusual behaviors. (3) Others • Use cameras, etc. to monitor activities within compartmented areas where important information is handled, and communicate the fact of the monitoring. • Consider installing automatic security systems and other systems so that an intrusion through an intentionally-unlocked window, etc. is detected. • Establish rules for exemptions including emergency entry or entry of top managers or privileged persons, etc. who are in general not expected to enter the restricted areas.

Q&A for assisting countermeasures (8)

Q-8. I do not know how to set procedures for the handling (transfer) of important information. (4-4 (13))
A-8. Procedures for the handling (transfer) of important information, if via a network, differ depending on whether e-mail or online storage is used. For example, if an organization uses e-mail and may send important information as attachments, the organization should establish rules such as always attaching important information in encrypted format, and using telephones or other measures other than e-mail when transmitting decryption password. If the organization uses online storage, it must consider whether to limit the use of online storage to only that arranged by the organization. In that case, the organization is to establish rules such as the period during which download is possible, and the transfer of passwords when downloading. Moreover, when the organization uses an Internet-based online storage service, assuming that the service does not allow download by anyone, the organization is to establish rules such as always encrypting important information to be uploaded, and never sending the download destination and password in the same e-mail message.

Q&A for assisting countermeasures (9)

Q-9. I don't know the meaning of "organization's audit through contractors, or audit on their own if necessary". (4-4(16))
A-9. It means one of the two measures that follow. This figure shows case 1 as audit through contractors, case 2 as audit on their own if necessary. Procedures are the same for when subcontractors contract their services to sub-subcontractors. Case 1: Audit through contractors  Case 2: Audit on their own if necessary 

Q&A for assisting countermeasures (10)

Q-10. I don't know what to collect as client logs and how. (4-5(17))
A-10. Collect event logs showing at least users' operation dates, contents (logons and logouts) and the results (failures). Management tools can be used to collect logs for Windows.

Q&A for assisting countermeasures (11)

Q-11. What should I consider when configuring the settings for client logs to address internal improprieties? (4-5(17))
A-11. Default log settings for basic software (especially Windows) on client side are not intended to record all the operation logs. Thus for Windows clients especially storing important information, it is preferable to activate security audits to record almost all the operations.

Q&A for assisting countermeasures (12)

Q-12. I do not know what content to include in education. (4-6 (19))
A-12. In education, organizations should include content that heightens understanding and awareness concerning internal impropriety countermeasures, such as the following. (1) Describe specific case studies of the effects on the company or organization caused by internal improprieties. (2) Describe matters that should be followed concerning categories and management methods of important information indicated in operation regulations. Examples include rules to prevent faxes, printouts, and other documents recording confidential information from being left unattended for a long time, and reporting procedures in the event of detection of internal improprieties. (3) Describe disciplinary actions in the event of discovery of internal improprieties, based on company regulations and other internal rules. As an example, it is effective to describe the content of disciplinary actions for internal improprieties based on specific cases. (4) Explain that countermeasures are being implemented, while indicating management methods for important information. For instance, it is effective to explain the conducted countermeasures such as monitoring of e-mail archives, etc. (5) To deepen understanding of internal impropriety countermeasures, it is advisable to explain related laws and regulations (the Unfair Competition Prevention Act, the Personal Information Protection Act, etc.) that form the background to operation regulations.

Q&A for assisting countermeasures (13)

Q-13. What sort of information assets are there for which handling is entrusted, and what sort of privileges are granted? (4-6 (21))
A-13. Information assets for which handling is entrusted include the following information and hardware. (1) Important information • Customer data (including information not generally disclosed, such as information concerning purchasing and sales) • Information concerning the creation of program source code, design drawings, etc. • Information concerning information systems. (information system configuration information, etc.) * Information concerning undisclosed intellectual property (i.e., patents) held by the company. (2) Hardware • PCs (including laptop PCs), smartphones loaned by the company, CD-Rs, DVD-Rs, USB storage, etc. (3) Privileges granted • Entry passes • User IDs (and associated passwords) • Storage repository (safes, wagons, cabinets, etc.) keys

Appendix IV: Relationship with Other Guidelines, etc.

(1) JIS Q 27001 Supplementary Notes A

These Guidelines indicate measures for organizations to take in protecting information assets from internal improprieties. Information security management aims to maintain the confidentiality, integrity, and availability of information assets that should be protected by the organization, and contains many related items from the standpoint of protecting information assets. As such, for the reference of persons reading these Guidelines from the standpoint of information security management, the management measures of JIS Q 27001 Supplementary Notes A, which relate to the management measures of these Guidelines, are shown below. Note that as for "Workplace Environments" in these Guidelines, there are no corresponding JIS Q 27001 management measures.

Major item		Item name	JIS Q 27001:2014 Supplementary Notes A Related Items
Basic Policies		(1) Clarification of the Responsibilities of the Top Manager	A.5.1 Management direction for information security A.7.2 During employment
		(2) Appointment of the Supervising Manager and Construction of Cross-Organization Systems	A.6.1 Internal organization
Asset Management	Designation as Confidential	(3) Information Rating Categories	A.8.1 Responsibility for assets A.8.2 Information classification A.9.1 Business requirements of access control
		(4) The Application and Labeling of Rating Categories	A.8.1 Responsibility for assets A.8.2 Information classification A.9.1 Business requirements of access control
	Designation of access rights	(5) User Access Management in Information Systems	A.8.1 Responsibility for assets A.8.2 Information classification A.9.1 Business requirements of access control A.9.2 User access management
		(6) Rights Management for System Administrators	A.8.1 Responsibility for assets A.8.2 Information classification A.9.1 Business requirements of access control A.9.2 User access management
		(7) Identification and Authentication of Users in Information Systems	A.8.1 Responsibility for assets A.8.2 Information classification A.9.2 User access management A.9.3 Users responsibilities
Physical Management		(8) Physical Protection and Entry/Exit Management	A.11.1 Secure areas A.12.1 Operation procedures and responsibilities
		(9) Asset management and physical protection of information devices and storage media	A.8.3 Media Handling A.11.2 Equipment security
		(10) Management of portable information devices and storage media	A.8.3 Media Handling A.11.2 Equipment security A.12.1 Operation procedures and responsibilities

Major item	Item name	JIS Q 27001:2014 Supplementary Notes A Related Items
	(11) Restrictions on Bringing in and using Personal Information Devices and Storage Media for Work	A.6.2 Mobile devices and teleworking A.8.3 Media handling A.12.1 Operation procedures and responsibilities
Technological and Operational Management	(12) Safety Management for Network Usage	A.6.2 Mobile devices and teleworking A.12.2 Protection against malware A.12.6 Technical vulnerability management A.13.1 Network security management A.14.1 Security requirements for information systems
	(13) Transfer and Protection of Important Information	A.8.3 Media handling A.13.2 Information transfer A.14.1 Security requirements for information systems A.10.1 Cryptographic controls A.12.1 Operation procedures and responsibilities
	(14) Protection of Information Devices and Storage Media taken from the Premises	A.6.2 Mobile devices and teleworking A.8.3 Media handling A.9.4 Systems and application access control A.10.1 Cryptographic controls A.12.1 Operation procedures and responsibilities
	(15) Protection of Important Information in Work Outside of the Organization	A.6.2 Mobile devices and teleworking A.8.3 Media handling A.9.4 Systems and application access control A.11.2 Equipment security A.10.1 Cryptographic controls
	(16) Confirmations of contractors services (including when using services provided by third parties)	A.7.1 Prior to employment A.7.2 During employment A.7.3 Termination and change of employment A.13.1 Network security management A.15.1 Information security on suppliers side A.15.2 Management for suppliers services provision
Securing Evidence	(17) Recording and Storage of Logs and Trails in Information Systems	A.12.4 Collecting and monitoring logs A.12.7 Things to consider for information systems audit
	(18) Checking of System Administrators' Logs and Trails	A.12.4 Collecting and monitoring logs A.12.7 Things to consider for information systems audit
Human Management	(19) Dissemination of Internal Impropriety Countermeasures through Education	A.7.2 During employment
	(20) Personnel Procedures for Conclusion of Employment	A.7.3 Termination and change of employment A.18.1 Compliance with legal and contractual requirements
	(21) Return of Information Assets Due to Conclusion of Employment or Conclusion of Contract	A.8.1 Responsibility for assets A.18.1 Compliance with legal and contractual requirements

Major item	Item name	JIS Q 27001:2014 Supplementary Notes A Related Items
Compliance	(22) Preparation of Legal Proceedings	A.7.1 Prior to employment A.7.2 During employment A.7.3 Termination and change of employment A.18.1 Compliance with legal and contractual requirements
	(23) Requests for Written Pledges	A.7.1 Prior to employment A.7.3 Termination and change of employment A.13.2 Information transfer A.18.1 Compliance with legal and contractual requirements
Workplace Environments	(24) Preparation of Impartial Personnel Evaluations	—
	(25) Promotion of Reasonable Work Environments and Communication	—
	(26) Management in Workplace Environments	—
Follow-up measures	(27) Preparation of Systems Required for Follow-up Measures	A.6.1 Internal organization A.15.1 Information security on suppliers side A.16.1 Management of information security incidents and improvements A.17.1 Information security continuity
	(28) Consideration of Punishment and Prevention of Recurrence	A.7.2 During employment A.16.1 Management of information security incidents and improvements
Organizational management	(29) Preparation of Whistleblower Systems for Internal Improprieties	A.7.2 During employment A.16.1 Management of information security incidents and improvements
	(30) Implementing Checks Incorporating the Prevention of Internal Improprieties	A.5.1 Management direction for information security A.12.6 Technical vulnerability management A.12.7 Things to consider for information system audit A.16.1 Management of information security incidents and improvements A.17.1 Information security continuity A.18.2 Information security review

(2) Trade Secret Management Guidelines

Management of Trade Secrets specifies minimum required countermeasures for securing protection such as injunctions under the Unfair Competition Prevention Act. Comprehensive countermeasures to prevent and address leakages will be separately shown in Trade Secrets Protection Manual (tentative).

(3) The Guidelines for Economic and Industrial Sectors Concerning the Act on the Protection of Personal Information

The Guidelines for Economic and Industrial Sectors Concerning the Act on the Protection of Personal Information indicate necessary and appropriate safety management methods required by the Act on the Protection of Personal Information. The following are countermeasure items in this guideline related to “Matters to be taken” in Security Control Measures (related to Article 20 of the Act), Supervision of Workers (related to Article 21 of the Act) and Supervision of Trustees (related to Article 22 of the Act) for this guideline’s readers considering personal information protection. With regard to the improper removal of personal information from the premises by employees, the "Workplace Environments" section from these Guidelines offers items not found in the Guidelines for Economic and Industrial Sectors Concerning the Act on the Protection of Personal Information. Referring to "Points for Countermeasures" under "Workplace Environments" should be of aid in strengthening measures against the improper removal of personal information from the premises.

Security control measures (related to Article 20 of the Act)		Related items
Systematic security control measures	① Preparing the organization structure to take security control measures for personal data	(1) Clarification of the Responsibilities of the Top Manager (2) Appointment of the Supervising Manager and Construction of Cross-Organization Systems (27) Preparation of Systems Required for Follow-up Measures
	② Preparing the regulations, etc. which provides security control measures for personal data and operating in accordance with the regulations, etc.	—
	③ Preparing the means by which the status of handling personal data can be looked through	—
	④ Assessing, reviewing, and improving the security control measures for personal data	(30) Implementing Checks Incorporating the Prevention of Internal Improprieties
	⑤ Responding to accident or violation	(27) Preparation of Systems Required for Follow-up Measures (28) Consideration of Punishment and Prevention of Recurrence
Human security control measures	① Concluding the nondisclosure agreement with workers when signing the employment contract and concluding the nondisclosure agreement between an entruster and trustee in the entrustment contract, etc. (including the contract of supply of temporary laborer)	(23) Requests for Written Pledges
	② Implementing familiarization of workers with internal regulations, etc. as well as education and training of them	(19) Dissemination of Internal Impropriety Countermeasures through Education

Security control measures (related to Article 20 of the Act)		Related items
Physical security control measures	① Implementing the control for entering and leaving a building (room)	(8) Physical protection and entry/exit management (9) Asset management and physical protection of information devices and storage media
	② Preventing theft, etc.	
	③ Physically protecting equipment and devices, etc.	
Technical security control measure	① Identification and authentication for access to personal data	(7) Identification and authentication of users in information systems
	② Control of access to personal data	(5) User access management in information systems (6) Rights management for system administrators
	③ Management of authority to access personal data	
	④ Record of access to personal data	(17) Recording and Storage of Logs and Trails in Information Systems (18) Checking of System Administrators' Logs and Trails
	⑤ Countermeasures against unauthorized software regarding an information system handling personal data	(12) Safety management for network usage
	⑥ Measures when transferring and transmitting personal data	(13) Transfer and Protection of Important Information (14) Protection of Information Devices and Storage Media taken from the Premises (15) Protection of Important Information in Work Outside of the Organization
	⑦ Measures when confirming the operation of information system handling personal	—
	⑧ Monitoring an information system handling personal data	(17) Recording and Storage of Logs and Trails in Information Systems (18) Checking of System Administrators' Logs and Trails

Supervision of Worker (related to Article 21 of the Act)	Related items
An entity handling personal information, in order to make a worker observe the security control measures based on Article 20 of the Act, must exercise necessary and appropriate supervision over the worker (e.g. monitoring of employees).	(8) Physical protection and entry/exit management (17) Recording and Storage of Logs and Trails in Information Systems

Supervision of Trustees (related to Article 22 of the Act)	Related items
① Selection of trustees	(16) Confirmations of Contractors Services (Including when using services provided by third parties)
② Conclusion of entrustment contract	
③ Comprehension of the state of handling of personal data by the trustee	

Appendix V: Examples of Basic Policies

Examples of basic policies are indicated below. Add to and modify these for use as required.

Examples of Basic Policies

1. Significance of internal impropriety countermeasures

These basic policies (hereinafter "these Policies") are hereby established for the purpose of protecting important information and information systems handled by ○○○ (e.g. IPA) (hereinafter "the Organization") from threats by internal improprieties, and for the purpose of establishing necessary items for safely making use of these items in business. From here out the Organization will consider internal impropriety countermeasures an important issue for management, and will undertake these.

2. Protection of important information

These Policies designate ○○○, △△△, and □□□ (e.g. customer data) as important information to be protected by the Organization.

- ○○○ is ....
- □□□ is ....
- □□□ is ....
- (Example: To protect the advantages of products with respect to competitors, development information must not be leaked from important manufacturing contractors.)

The Organization takes appropriate measures for this important information according to work situations. The organization makes all officers and employees aware of implementation of these measures.

3. Implementation Systems

The Organization sets forth roles and responsibilities in order to establish systems of organizational countermeasures for internal improprieties.

- CEO…○○○ (e.g. president or other management team representative)
  The CEO conducting decision-making concerning internal impropriety countermeasures.
- Supervising Manager… • □□□ (e.g. president or other management team representative)
  The person responsible for deciding important matters concerning internal impropriety countermeasures, conducting checks and reviews of countermeasure status, and conducting checks of countermeasures and status when internal improprieties occur.
  * Note: ○○○ and □□□ may be identical.

3-1. Monitoring by the CEO

The CEO sets policies for internal impropriety countermeasures, and receives and evaluates periodic reports on those policies from the Supervising Manager on an ongoing basis. The CEO also reviews implementation systems and policies as necessary.

3-2. Countermeasure implementation and reporting by the Supervising Manager

The Supervising Manager drafts specific measures based on the CEO's policies, and periodically reports to the CEO on implementation status.

4. Review of basic policies

In order to maintain effective and efficient internal impropriety countermeasures, these Policies are to be periodically reviewed and revised as necessary.

Appendix VI: Five basic policies and twenty-five classifications to prevent internal improprieties

The following shows five basic policies and twenty-five classifications to prevent internal improprieties based on situational crime prevention, and examples of respective countermeasures as well as related countermeasure items in this guideline. “Major countermeasure items” indicate numbers corresponding to this guideline’s countermeasure items.

Source: Five categories and twenty-five classifications are created by IPA, based on page 191 of Environmental Criminology and Crime Analysis (Social Security Research Foundation).

Basic 5 policies and 25 classifications		Countermeasure examples※	Major items
Make crimes difficult (make harder to attempt): Strength countermeasures to make criminal activities difficult to conduct.			
	Strength countermeasures	Access control, password policy setting, revocation of resignees’ IDs, fixing PCs with security wires	(5)(6)(7)(9) (14)(21)
	Restrict entering/exiting facilities	Restriction of outsiders entrance, entrance/exit control	(8)
	Check at exit points	Checks for taking out of laptop PCs, etc., monitoring e-mails and networks	(8)(10)(17)(18)
	Block criminals	Restriction of entrance/exit based on physical levels	(8)
	Restrict information devices and networks	Prohibition against unauthorized bringing-in of PCs/USB storages, Restriction of uses of SNSs, uses of wireless LANs in hotels and public wireless LANs	(11)(12)(15)
Raise risks to be caught (detected if committed): Strength management and surveillance to raise risks to be caught.			
	Strength monitoring	Monitoring of access logs, working environment with multiple workers, information devices inventory, mobile devices management, monitoring of entrance/exit records	(6)(8)(9)(10) (17)(18)(30)
	Support natural surveillance	Development of reporting system	(29)
	Reduce anonymity	ID management, Removal of shared accounts, property management based on ledgers	(7)(9)(10)
	Implement operational managers	Restriction of one-man works	(26)
	Strength physical surveillance system	Setting up of surveillance cameras, Implementation of mechanical security systems	(8)
Reduce rewards from crimes (not worth doing): Hide or remove targets, or make it unprofitable to prevent crimes.			
	Hide targets (Unknown whereabouts)	Authorization of access rights, mobile devices storage with locks, application of privacy protection films	(5)(6)(9)(15)
	Eliminate targets (Eradicate existences)	Complete data deletion, physical destruction of record media, etc., disposal /deletion of information provided to persons involved	(4)(9)(13)(21)
	Specify properties	Property management for information devices and record media	(9)
	Decimate the market	Immediate reporting to police, (compliance to legal systems)	(27)
	Make it unprofitable	Encryption of electronic files, hard disks, telecommunications	(12)(13)(14)(15)
Reduce seduction of crimes (not to motivate): Deter crimes by dampening enthusiasm to commit crimes.			
	Reduce discontent or stress	Promotion of impartial personnel evaluations, appropriate working environment, smooth communication	(24)(25)
	Avoid conflict	Promotion of impartial personnel evaluations, appropriate working environment, smooth communication	(24)(25) (29)
	Control emotions	Promotion of impartial personnel evaluations, appropriate working environment, smooth communication	(24)(25)
	Mitigate pressure from co-workers	Promotion of impartial personnel evaluations, appropriate working environment, smooth communication	(25)
	Block copycat crimes	Recurrence prevention measures (Being careful to disclose the ways of incidents)	(28)
Not allow justification of crimes (not allow to excuse): Get rid of reasonings for criminals’ self-justification of their activities.			
	Decide rules	Development of basic policies, management and operation methods, services contracts, employment regulations	(1)(2)(16)(20) (22)(27)
	Post instructions	Posting of basic policies inside and outside organizations, education about the policies for employees	(1)(2)(19)
	Appeal to conscience	Indication of management levels, signing of pledges, posters for ban on bringing in personal devices	(3)(4)(11)(19) (20)(23)
	Support compliance	Education of compliance items and related laws	(19)(22)(23)
	Regulate drug, alcohol	(ban on drinking alcohol in workplaces, restriction of alcohol when holding important information)	-

※Bracketed countermeasure examples are examples not specified in this guideline.

Appendix VII: Countermeasures Classification

（1）Countermeasures for each environment

Countermeasures to be considered are shown here according to each environment (use of information devices and networks) in which a company or an organization is[49].

①Countermeasures any and all organizations using any information device or network environment must consider.

②Countermeasures to be considered when organizations do not have networks but information devices, though external connections such as e-mail services provided by telecommunication operators are available.

③Countermeasures to be considered when internal networks and external connections are both available in the organizations.

①Countermeasures any and all organizations must consider

Major item	Item name
4-1.Basic Policies (Responsibilities of the Top Manager and Governance)	(1)Clarification of the Responsibilities of the Top Manager
	(2)Appointment of the Supervising Manager and Construction of Cross-Organization Systems
4-2.Asset Management (Designation as Confidential, Designation of Access Privileges, Access Administration, etc.) 4-2-1.Designation as Confidential	(3)Information rating categories
	(4)The application and labeling of rating categories
4-3.Physical Management	(8)Physical protection and entry/exit management
4-4.Technological and operational management	(13)Transfer and Protection of Important Information※1
	(16)Confirmations of Contractors Services (Including when using services provided by third parties)※2
4-6.Human Management	(19)Dissemination of Internal Impropriety Countermeasures through Education
	(20)Personnel Procedures for Conclusion of Employment
	(21)Return of Information Assets Due to Conclusion of Employment or Conclusion of Contract
4-7.Compliance	(22)Preparation of Legal Proceedings
	(23)Requests for Written Pledges
4-8.Workplace Environments	(24)Preparation of Impartial Personnel Evaluation
	(25)Promotion of Reasonable Work Environments and Communication
	(26)Management in Workplace Environments
4-9.Follow-up measures	(27)Preparation of Systems Required for Follow-up Measures
	(28)Consideration of Punishment and Prevention of Recurrence
4-10.Organizational management	(29)Preparation of Whistleblower Systems for Internal Improprieties
	(30)Implementing Checks Incorporating the Prevention of Internal Improprieties

※1 Except for “Countermeasure points 3 (via the internet)”.

※2 Except for “Countermeasure points 5 (using cloud services)”.

[49] Since this guideline aims at security measures utilizing information systems, it can only be used as reference for countermeasures of organizations without information devices or networks.

②In cases organizations have information devices

Major item	Item name
4-3.Physical Management	(9)Asset management and physical protection of information devices and storage media
	(10)Management of portable information devices and storage media
	(11)Restrictions on bringing in and using personal information devices and storage media for work
4-4.Technological and operational management	(12)Safety management for network usage
	(14)Protection of Information Devices and Storage Media taken from the Premises
	(15)Protection of Important Information in Work Outside of the Organization

③In cases organizations have internal networks

Major item	Item name
4-2-2.Designation of access rights	(5)User access management in information systems
	(6)Rights management for system administrators
	(7)Identification and authentication of users in information systems
4-4.Technological and operational management	(12)Safety management for network usage
	(13)Transfer and Protection of Important Information※1
	(16)Confirmations of Contractors Services (Including when using services provided by third parties)※2
4-5.Securing Evidence	(17)Recording and Storage of Logs and Trails in Information Systems
	(18)Checking of System Administrators' Logs and Trails

※1 “Countermeasure points” 3 (via the internet)

※2 “Countermeasure points” 5 (using cloud services)

（2）Countermeasures for each type of impropriety

Countermeasures to be considered for each type of impropriety are shown here. This includes countermeasures related to early detection and actions after incidents.

①Basic countermeasures organizations must consider
②Countermeasures to be considered for each type of impropriety
③Countermeasures for reading signs and early detection of improprieties
④Countermeasures on the occurrence of internal improprieties

①Basic Policies

Risk factor	Countermeasure	Item name
Employees cannot tell whether the information is important or not	①Identification of important information	(3)Information rating categories (4)The application and labeling of rating categories
Cross- organizational management system is not developed Countermeasures are not refined or reviewed for new threats or laws	②Cross-organizational operations led by top managers	(1)Clarification of the Responsibilities of the Top Manager (2)Appointment of the Supervising Manager and Construction of Cross-Organization Systems (30)Implementing Checks Incorporating the Prevention of Internal Improprieties
Easy to enter floors where important information is stored Enter/exit records are not collected to identify individuals Inventory of information devices are not checked	③Physical management	(8)Physical protection and entry/exit management (9)Asset management and physical protection of information devices and storage media
More access privileges than needed for works are authorized	④Appropriate access privilege control	(5)User access management in information systems (6)Rights management for system administrators
Operation histories (logs) are not collected Collected logs are not periodically audited	⑤Periodic monitoring and auditing of operation histories	(17)Recording and Storage of Logs and Trails in Information Systems (18)Checking of System Administrators' Logs and Trails
Officers and employees are not familiarized with internal rules including handling of important information Officers and employees do not know internal management systems such as logs monitoring and disciplinary actions against improprieties	⑥Education to fully inform officers and employees	(19)Dissemination of Internal Impropriety Countermeasures through Education
Officers and employees do not understand that they are required to protect important information	⑦Instillation of compliance consciousness	(23)Requests for Written Pledges

②Countermeasures for each type of impropriety

a. Information leakage upon resignation

Risk factor	Countermeasure	Item name
Officers and employees (including expected resignees) are not monitored	①Strengthening monitoring of expected resignees	(10)Management of portable information devices and storage media (17)Recording and Storage of Logs and Trails in Information Systems (21)Return of Information Assets Due to Conclusion of Employment or Conclusion of Contract
Access to important information is not restricted		
Entrance admission cards and accounts obtained during employments are remain useable	②Preparation of resignation procedures	(20)Personnel Procedures for Conclusion of Employment (21)Return of Information Assets Due to Conclusion of Employment or Conclusion of Contract
Trade secret protection measures or non-compete actions after resignations are not prepared		

b. Improprieties committed by system administrators

Risk factor	Countermeasure	Item name
Privileges are concentrated Privileges are authorized to more employees than required	①Appropriate privilege management (minimization and decentralization of privileges, mutual monitoring)	(6)Rights management for system administrators (7)Identification and authentication of users in information systems
Uses of privileges are not restricted		
System administrators who accessed important information cannot be identified		
System administrators are not supervised	②Supervision of system administrators	(18)Checking of System Administrators' Logs and Trails

c. Information leakage from contractors

Risk factor	Countermeasure	Item name
Contractors operation systems and security measures are not checked before and during contract periods	①Contractors management for handling of important information	(2)Appointment of the Supervising Manager and Construction of Cross-Organization Systems (16)Confirmations of Contractors Services (Including when using services provided by third parties) (27)Preparation of Systems Required for Follow-up Measures
Necessary items for security management of important information are not included in contracts※	②Incorporation of security management items into contracts	
Delivery, disposal and deletion procedures for important information are not defined	③Protection for delivery of important information	(13)Transfer and Protection of Important Information (21)Return of Information Assets Due to Conclusion of Employment or Conclusion of Contract

※ including when using cloud services.

d. Improprieties induced by working environment

Risk factor	Countermeasure	Item name
Employees are not satisfied with their personal evaluations and have frustrations	①Impartial personal evaluation	(24)Preparation of Impartial Personnel Evaluations (25)Promotion of Reasonable Work Environments and Communication (26)Management in Workplace Environments
Specific works are left in the hands of specific employees for long periods	②Appropriate working environment	
Specific employees are overloaded with works		
Having no one to talk about work problems and being isolated	③Good communication	
Most woks are done without other persons' involvement		

e. Improprieties caused by imperfect enforcement of rules

Risk factor	Countermeasure	Item name
Officers and employees are not familiarized with internal rules including handling of important information	①Education to fully inform officers and employees	(19)Dissemination of Internal Impropriety Countermeasures through Education
Personally owned devices including smart phones and USB storages are not restricted to be brought in or used for works Rules are not clearly defined	②Information leakage countermeasures	(10)Management of portable information devices and storage media (11)Restrictions on bringing in and using personal information devices and storage media for work
Unauthorized applications or SNSs are not restricted to be used		(12)Safety management for network usage
Countermeasures are not implemented for possible information leakage to third parties		(14)Protection of Information Devices and Storage Media taken from the Premises (15)Protection of Important Information in Work Outside of the Organization

③Early Detection

Risk factor	Countermeasure	Item name
Having no idea where to report suspicious activities	①Implementation of reporting systems	(29)Preparation of Whistleblower Systems for Internal Improprieties
Logs are not periodically audited	②Periodic monitoring and auditing of operation histories	(17)Recording and Storage of Logs and Trails in Information Systems (18)Checking of System Administrators' Logs and Trails

④Follow-up Measures

Risk factor	Countermeasures	Item name
Having no idea of how to address internal improprieties In need of minimizing damages on the organization, customers and clients	①Preparation of acting and reporting procedures	(27)Preparation of Systems Required for Follow-up Measures
In need of preventing recurrences of internal improprieties	②Consideration of punishments and preventive actions for recurrence	(22)Preparation of Legal Proceedings (28)Consideration of Punishment and Prevention of Recurrence

■ Revision history (A Japanese version)

・Ver. 1.0 (March 25, 2013)

・Ver. 2.0 (September 26, 2014)

Updated countermeasure items, etc. based on case studies

・Ver. 3.0 (March 2015)

Updated based on users requests and relevant parts corresponding to revised standards/policies

Guidelines for the Prevention of Internal Improprieties in Organizations

Ver3.0（May 2015）

Information-technology Promotion Agency, Japan

16th Floor, Bunkyo Green Court, 2-28-8,
Hon-Komagome, Bunkyo-ku, Tokyo, 113-6591, Japan

URL : http://www.ipa.go.jp
E-Mail : isec-economics@ipa.go.jp