Guidelines for the Prevention of Internal Improprieties in Japanese Organization

Shigeyoshi SHIMA[1]* and Ayako KOMATSU[2]
[1] NEC Corporation
1753, Shimonumabe, Nakahara-ku, Kawasaki, Kanagawa 211-8666, Japan
shima@ap.jp.nec.com
[2] Information-Technology Promotion Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku, Tokyo 113-6591, Japan
a-koma@ipa.go.jp

Abstract

Information security incidents involving internal improprieties that threaten the very business of Japanese organizations have drawn attention. Internal improprieties are one of problems to be solved in Japanese organizations. However, it is difficult to share information about internal impropriety incidents and to consider the causes of and effective countermeasures for internal improprieties among Japanese organizations. Each organization enacts countermeasures based on its own experience, and most these countermeasures of Japanese organizations are insufficient. Thus, Information-technology Promotion Agency, Japan (IPA) created "Guidelines for the Prevention of Internal Improprieties in Organizations" which provides exhaustive countermeasure. This paper describes summary of these guidelines, and explains problems which are how to collect information and workplace environment to be hard to commit internal improprieties, and solutions of the problems.

Keywords: Insider threat, Internal Impropriety, Information security countermeasure

1 Introduction

Information security incidents involving internal improprieties that threaten the 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 taking out 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, one feature of incidents involving internal improprieties is that from 2005 to 2010 the number of incidents occurring due to internal crime and 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 [1]. 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

Journal of Internet Services and Information Security (JISIS), volume: 3, number: 3/4, pp. 81-93

*Corresponding author: NEC Corporation Central Research Laboratories / Cloud System Research, Tel: +81-(0)44-431-7686

[1] http://www.jnsa.org/result/incident/2012.html (in Japanese)

surveys by the Ministry of Economy, Trade and Industry , the vectors for leakage in companies experiencing leakage of trade secrets were reported[2] 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%)" (This is a multiple answer question). 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 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 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, the IPA created "Guidelines for the Prevention of Internal Improprieties in Organizations" (hereafter "these Guidelines") and made it available to the public. Organizations can download these Guideline (Japanese-language version) from the IPA website from March 2013. The IPA completed translating these Guideline into English (figure 1)[5]. This paper describes summary of these Guideline and explains problems to be solved for a creation of these Guideline.

2 Summary of Guidelines for the Prevention of Internal Improprieties in Organization

2.1 Outline

The aim of these Guidelines is the prevention of internal improprieties in organizations. The content of these Guidelines enables the preparation of effective internal impropriety countermeasures in companies (especially small-sized and medium-sized businesses) that have not yet thought about internal impropriety countermeasures. Moreover, these Guidelines also consider early detection and prevention of the

[2]http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/121211HP.pdf (in Japanese)

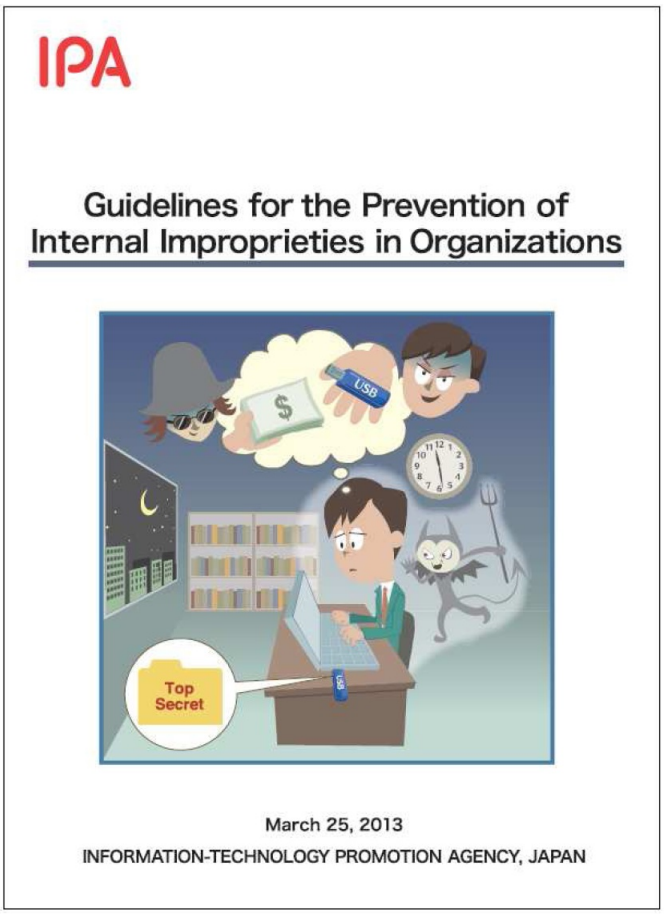

Figure 1: Guidelines for the Prevention of Internal Improprieties in Organizations (English-language version)

spread of damage following occurrences after the actual occurrence of internal improprieties.

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.

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 for Internal Improprieties” as the second half.

- Section 1: Background
- Section 2: Overview
- Section 3: Definition of Terms, and Related Laws
- Section 4: Model Management for Internal Improprieties
- Appendix I: Internal Impropriety Case Studies
- Appendix II: Internal Impropriety Check Sheet
- Appendix III: Q&A

- Appendix IV: Relationship with Other Guidelines, etc.
- Appendix V: Examples of Basic Policies

"Section 1: Background" and "Section 2 Overview" 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) 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". You will better understand the importance of countermeasures.

"Section 3: Definition of Terms, and Related Laws" shows internal improprieties and insiders of the scope to be treated in these Guidelines, and shows laws necessary to read these Guidelines and to implement countermeasures (see Section 2.2, Section 2.3).

"Section 4: Model Management for Internal Improprieties" 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" (see Section 2.4 in order to understand his or her role in the organization. The top manager (or management team) who is hard to establish Basic Policies can refer to template in "Appendix V: Examples of Basic Policies."

Persons charged with countermeasures should first assess the status of their organization's internal impropriety countermeasures by using the check sheet in Appendix II.

Organizations which have already taken countermeasures using other Guideline, refer to "Appendix IV: Relationship with Other Guidelines, etc." to grasp the status of countermeasures in the organizations. Other Guidelines are three following Japanese documents.

- JIS Q 27001:2006[6]
- Directives for Management of Trade Secrets[8]
- The Guidelines for Economic and Industrial Sectors Concerning the Act on the Protection of Personal Information[7]

To address items for which countermeasures are insufficient according to the results of the check sheet, consider specific countermeasures with reference to "Section 4: Model Management for Internal Improprieties" and "Appendix III: Q&A."

2.2 Definition of Insiders and Internal Improprieties

These Guideline referred to definition of the Cert Insider threat Center[3]. The Cert Insider Threat Center classifies insider threats in three, "Insider Fraud", "Theft of Intellectual Property", "Insider IT Sabotage."

Internal improperties of these Guidelines were referred to definition of "Theft of Intellectual Property" and a part of "Insider IT Sabotage" as follow because Information leakage of customer data and trade secret was one of serious incidents in Japanese organizations.

- Insiders
  Any persons corresponding to officers, employees, contract employees, 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.)

- 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 (customer lists, technical knowledge, etc.) 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.

2.3 Related Laws

Laws related to these Guidelines are provided below. If persons do not know those laws, they may establish inadequate countermeasures.

- Act on the Protection of Personal Information
  This act relate to personal data of customers to protect from internal improprieties.

- Unfair Competition Prevention Act
  This act relate to trade secrets to protect from internal improprieties.

- 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.

- Act for Securing the Proper Operation of Worker Dispatching Undertakings and Improved Working Conditions for Dispatched Workers
  This act is relate to obligations under labor contracts of dispatched workers.

- 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.

2.4 Countermeasure items for Internal Improprieties

These Guidelines comprehensively present countermeasures required from the following 10 standpoints in order to enact specific internal impropriety countermeasures within organizations. Based on these 10 standpoints, 30 countermeasure items 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.

- 4-1. Basic Policies
  (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
  (3) Information rating categories
  (4) The application and labeling of rating categories

(5) User access management in information systems
(6) Rights management for system administrators
(7) Identification and authentication of users in information systems

- 4-3. Physical Management
  (8) Physical protection and entry/exit management
  (9) Asset management and physical protection of information devices and storage media
  (10) Management and monitoring of the removal of information devices and storage media from the premises
  (11) Restrictions on bringing in and using personal information devices and storage media for work

- 4-4. Technological management
  (12) Safety management for network usage
  (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
  (16) Confirmations when Using Services Provided by Third Parties (Including Cloud Computing)

- 4-5. Securing Evidence
  (17) Recording and Storage of Logs and Trails in Information Systems
  (18) Checking of System Administrators' Logs and Trails

- 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 Environment
  (24) Preparation of Impartial Personnel Evaluations
  (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

2.5 Internal Improprieties Countermeasures Implementation Process

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 2, the countermeasures for the 30 countermeasure items are composed of the following 3 points. A example of structure of 3 points is shown in the appendix A.

- Countermeasure principles:
  Necessary countermeasures are shown in a box. These are also check sheet 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 clues to drafting specific implementation measures against the above-mentioned risks.

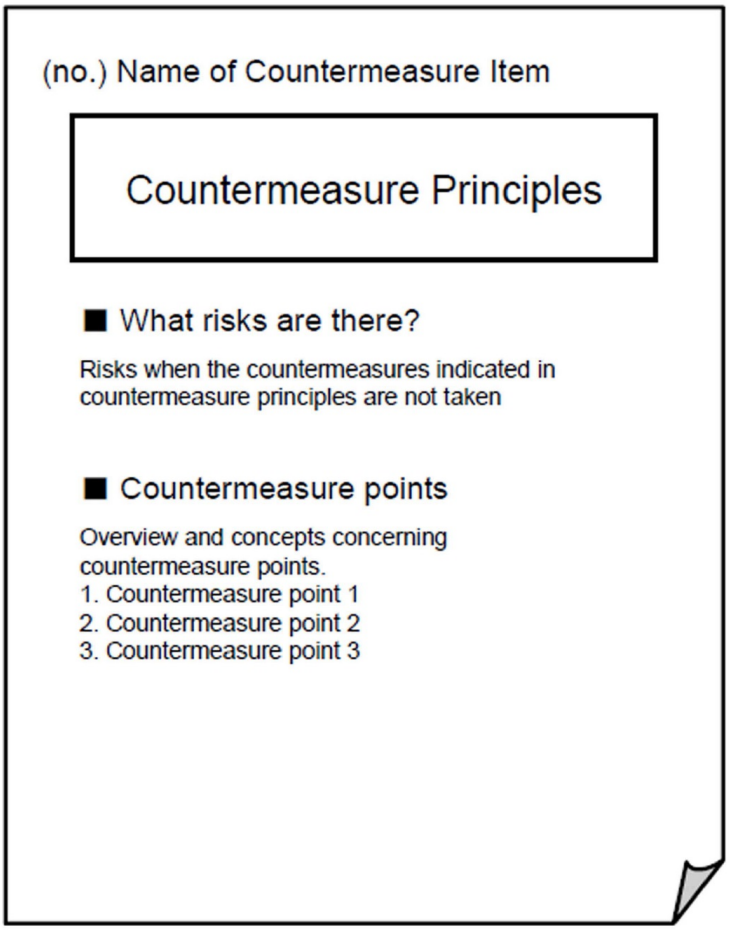

Figure 2: The structure of “Section 4: Model Management for Internal Improprieties”

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.

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 under these risks occur. If the effects on business are small and a risk is deemed allowable, it may not be necessary to enact countermeasures.

3. Read “Countermeasure points,” and, taking costs, resources, etc. into account, draft specific implementation measures based on the effects on business of (2). In “Countermeasure points,” countermeasures that use the term “advisable” in their text assume the case in which organizations wish to strengthen the countermeasures.

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 can be 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.

3 Problems and Solutions of Guideline Creation

3.1 Problems

The IPA published a report about intarnal improprieties[4]. The survey report is prior survey for creating these Guidelines, and two following problems were reached.

- Collection of information about internal impropriety incidents
  It was difficult to collect information about internal impropriety incidents by interviews of the survey. Even if IPA, public agency, propose interviews to organizations, most organizations are hard to disclose internal impropriety incidents. However, we should collect information as much as possible to grasp an internal impropriety situation in Japan.

- Establishment of countermeasure related to workplace environment
  Insiders officially have access rights to the organization’s information systems. The insiders can commit internal improprieties if the insiders intend to commit. Thus, it is necessary to reduce intentions of internal improprieties. We obtained that insiders were hard to commit internal improprieties in good workplace environment by the survey. However, we did not know what was elements of good workplace environment. Moreover, we were not able to refer to other guidelines described by “Appendix IV: Relationship with Other Guidelines, etc.” about workplace environment because the other guidelines were not described about workplace environment.

3.2 Collection of Information about Internatl Impropriety Incidents

We thought that we could not directly collect information about internal impropriety incidents from organizations which experienced those incidents. We looked for experts who had the knowledge of countermeasure of internal impropriety and asked the experts for cooperation of interviews, and could collect examples more than 30. We promised the experts to limit interview information sharing only to members who visited. IPA established “Committee to Consider Guidelines for the Prevention of Internal Improprieties in Organizations” because of analysis of internal impropriety cases and consideration of countermeasures. The committee limited participants (committee members, committee secretariat staffs, observers who was admitted by the committee) and did not disclose meeting contents because outsiders

of the committee prevent to infer organizations related to internal impropriety incidents from contents of meetings. The committee members consisted of CISO (Chief Information Security Officer), lawyer, academicians of information security and social psychology, analyst of information security. The Observers included academicians of social psychology, government official, etc. We could collect examples in the committee.

17 case studies from interviews surveys and case study surveys of the IPA's report[4] and the committee are presented in "Appendix I: Internal Impropriety Case Studies" of these Guideline. It is two case studies as following. However, these case studies do not describe detail information because of preventation to infer organizations related to internal impropriety incidents.

- case 1:
  A salesperson at a regional financial institution was embezzling funds from dormant accounts.
  (Major 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.

- case 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.
  (Major 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.

3.3 Establishment of Countermeasure related to Workplace Environment

An insider intention to commit internal improprieties increases if the insider dissatisfy with workplace environment. We decided to clarify workplace environment which insiders were easy to commit internal improprieties. There are two methods of a case analysis and a questionnaire analysis to clarify such an environment.

- Case analysis
  This method analyzes insiders' workplace environment which is human relations, organization cultures, positions of insiders, etc. in an incident, and look for elements related to internal improprieties.

- Questionnaire analysis
  This method sets up a hypothesis related to workplace environment for a questionnaire and analyzes results of the questionnaire.

The case analysis should collect detail information of an insider who committed internal improprieties. However, we were not able to hear detail information for case analysis from committee members because of a duty of confidentiality, and choice questionnaire analysis.

3.3.1 Questionnaire

9 categories of questionnaire items related to workplace environment are as follows. Questionnaire items were created in reference to 4 Japanese survey reports related to "mental health", "labor environment", "business management" and "internal fraud."

- Working conditions (8 items)
- Salary and treatment (6 items)
- Welfare (education and training) (4 items)
- Superior support (5 items)
- Co-worker support (5 items)
- Management Policy (3 items)
- Oganization rule (8 items)
- Oganizaiton commitment (11 items)
- Paternalism (9 items)

A period of the questionnaire was from January 15 to January 17 in 2013. As for the questionnaire, a Web questionnaire system of a market research company was used, and answers of the questionnaire was obtained from monitor members (respondents: n = 1024) of the market research company. "There is experience of committing internal impropriety" and "There is no experience of committing internal impropriety" were collected 512 each by a prior screening of the questionnaire.

3.3.2 Analysis of Questionnaire Results

For the purpose of obtaining elements of workplace environment difference to two groups, we used Mann-Whitney U test as statistical analysis method. Mann-Whitney U test evaluate the difference in questionnaire items of two groups. If an evaluation result of a questionnaire item is different in two groups ($p > 0.5$), a contents of the questionnaire item affect internal impropriety intention of respondents. Figure 3 shows the number of different questionnaire items for the number of questionnaire items in 9 categories.

It is surmised that 6 categories, "working conditions", "Salary and treatment", "Superior support", "Co-worker support", "Management Policy" and "Oganization rule", affect internal impropriety intention. 4 categories, "Salary and treatment", "Co-worker support", "Management Policy" and "Organization rule", were different in evaluation of all questionnaire items.

The following countermeasures related to workplace environment were established based on contents of affecting questionnaire items. Contents of these countermeasures did not contradict comments about effective countermeasures obtained from the interviews.

- (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.

- (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.

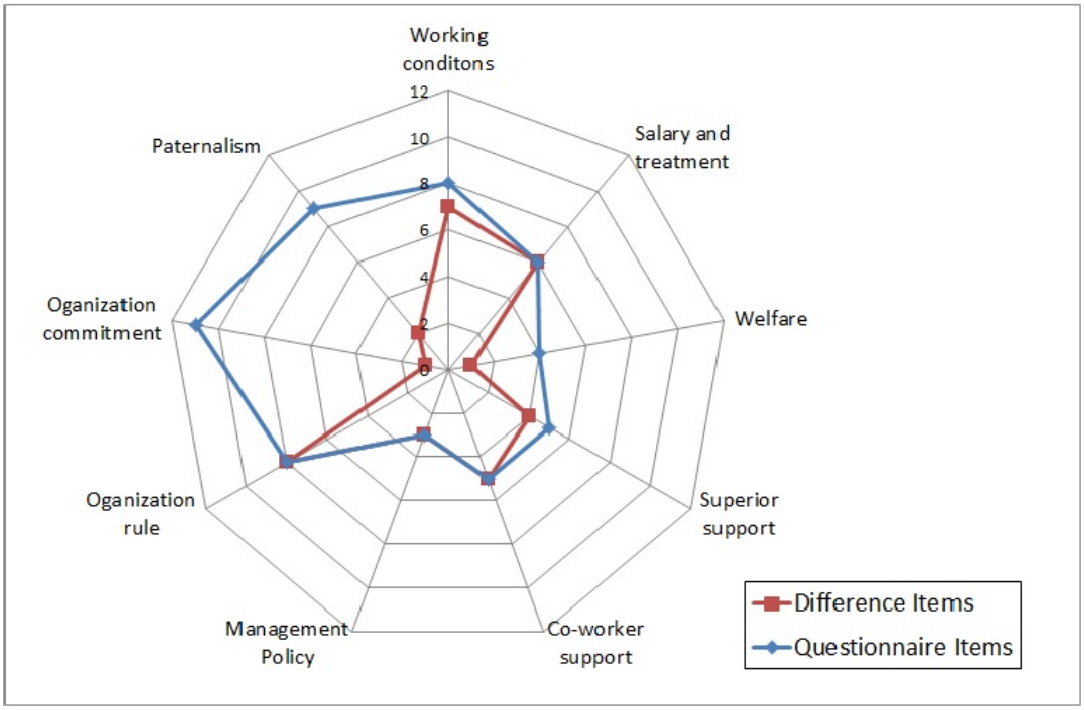

Figure 3: Radar chart based on result of Mann-Whitney U test

4 Conclusion

These Guideline created based on Japanese situations of internal improprieties, laws of Japan, culture and workplace environment of Japanese organizations. Other country organizations may refer to countermeasures of these Guideline except “4-7. Compliance” and “4-8. Workplace Environment” because “4-7. Compliance” was established based on laws of Japan and culture of Japanese oganizations and “4-8. Workplace Environment” was established base on workplace envirment of Japanese oganizations.

It may not be easy to collect information about internal improprieties in other countries. When such a country creates guidelines like this paper, we suggest that the country set up a committee. It is desirable to include at least one lawyer for legal responses and to include academicians of social psychology for a questionnaire of workplace environment in the committee.

There have been already guidelines for mitigating insider threats which include internal impropriety countermeasures [3]. The guidelines for mitigating insider threats describe countermeasures based on case studies of insider threats. We think that case studies are effective as promotion presentations for internal impropriety countermeasures because users can be easy to understand the case studies. We will refer to the guidelines for mitigating insider threats as our promotion presentation materials. The guidelines for mitigating insider threats classify countermeasures in following six.

- Human Resources (HR)
- Legal
- Physical Security
- Data Owners
- Information Technology (IT), including Information Assurance (IA)

- Software Engineering

The guidelines for mitigating insider threats describe mapping of these six countermeasures and countermeasures of standards[9][2][1]. We can apply the six countermeasures to 7 standpoints except "4-8. Workplace Environment", "4-9. Follow-up Measures" and "4-10. Organizational Management" in these Guidelines (see Section 2.4). However, "4-8. Workplace Environment" and "4-10. Organizational Management" may coincide with "Human Resources (HR)."

These Guideline will be used to promote and spread internal improprieties countermeasure by IPA, and will be revised from comments of users. We will strengthen countermeasure contents of those Guideline in reference to standards described in the guidelines for mitigating insider threats. We will cope with "Insider Fraud" as one of internal improprieties.

References

[1] American National Standards Institute. Information technology - Security techniques - Code of practice for information security management (ISO/IEC 27002), 2005.

[2] Carnegie Mellon University. CERT Resilience Management Model, Version 1.0, May 2010.

[3] Carnegie Mellon University. Common Sense Guide to Mitigating Insider Threats 4th Edition, December 2012. http://www.sei.cmu.edu/reports/12tr012.pdf, last viewed October 2013.

[4] Information-technology Promotion Agency, Japan (IPA). Report on Survey of Incidents Due to Improper Activity by Organization Insiders (in Japanese), July 2012. http://www.ipa.go.jp/files/000014169.pdf, last viewed October 2013.

[5] Information-technology Promotion Agency, Japan (IPA). Guidelines for the Prevention of Internal Improprieties in Organizations, March 2013. http://www.ipa.go.jp/files/000034260.pdf.

[6] Japanese Standards Association (JSA). Information technology – Security Techniques – Information Security management systems – Requirements. JIS Q 27001:2006, 2006 May.

[7] Ministry of Economy, Trade and Industry. The Guidelines for Economic and Industrial Sectors Concerning the Act on the Protection of Personal Information (in Japanese), October 2009.

[8] Ministry of Economy, Trade and Industry. Directives for management of trade secrets (in japanese), December 2011.

[9] National Institute of Standards and Technology (NIST). NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems and Organizations, August 2009. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf, last viewed October 2013.

Author Biography

Ayako Komatsu received Ph.D degree in the University of Electro-Communications in 2012. He is currently working as a principal researcher, Department of Central Research Laboratories, NEC Corporation, Japan.

Ayako Komatsu is a Laboratory Director of Security Economics Laboratory of Information-technology Promotion Agency Japan. She received her Doctor of Informatics degree from Yokohama National University.

A Example of Described Countermeasure Item in "Section 4"

4-4. Technological management

(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-ROMs, 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. It is also advisable to install encryption software for protecting important information.
  2. When sending and receiving important information by connecting to external networks, organizations are to encrypt important information.