Methods of Privacy Protection Certification Systems

KI-HO LEE, TAE-HEE CHO, KYU-CHEOL OH, DAE-YONG BYUN, SANG-SOO JANG
Korea Information Security Agency
78, Garak-Dong, Songpa-Gu, Seoul 138-803
Korea

Abstract: Recently, the collection and use of personal information by Internet service providers has increased sharply as Internet access becomes more commonplace in society. In addition, the illegal use and disclosure of personal information is occurring more frequently due to the special characteristics of the Internet such as its openness and non-personal nature. However, most enterprises in Korea pay only instantaneous attention to the issue of privacy whenever an issue arises, and have established piecemeal measures against it to date rather than organizational and systematic responses. For the mid-to-long term, systematic measures to prevent privacy infringement are required with the introduction of the certificate policy, such as ISO27001, KISA-ISMS (Korea Information Security Society – Information Security Management System) are required. This is also matched by the need for the increased participation and effort of the government and related enterprises. Although security certificate systems, such as ISO27001 and KISA-ISMS, have been introduced and implemented in Korea, a certificate system that certifies comprehensive privacy protection readiness of an enterprise is not yet in place. As a result, this paper proposes the basic direction for the development of a personal information certificate system.

Key-Words: personal information, ISMS (Information Security Management System), information security

1 Introduction

Recently, the collection and use of personal information by Internet service providers has increased sharply as Internet access becomes more commonplace in society. In addition, the illegal use and disclosure of personal information is occurring more frequently due to the special characteristics of the Internet such as its openness and non-personal nature. In particular, the economic value of personal information is increasing as economic activities of enterprises become increasingly focused on customers. In line with this trend, illegal privacy violations and misuse/abuse incidents are also rising. Starting with the illegal use of another person's name to access the Lineage game site in 2006 due to China-originated hacking activities, privacy infringement and misuse/abuse has caused a number of incidents – with large amounts of personal information leaking from a public agency website, the disclosure of job application information from LG Electronics, and information leakages from the National Health Insurance website.

To cope with these incidents, the Korean government and some enterprises have recognized the social impact and seriousness of privacy protection, and have proposed various countermeasures such as the establishment and institutionalization of incident handling organizations. However, most enterprises in Korea pay only instantaneous attention to the privacy issue whenever it arises, and have established piecemeal measures against it, rather than organizational and systematic responses. For the mid-to-long term, systematic measures are required to prevent privacy infringement and the active establishment and activities of professional, market-oriented, specialized information security services and technologies are becoming indispensable.

This is in addition to the need for participation and effort of the government and related enterprises. Unfortunately, the information security business is not being sufficiently promoted due to a lack of a strong driving force required to create a privacy protection market in Korea. Privacy protection is not being managed as one of the necessary information security business areas.

Various measures are required to enhance the enterprise-level privacy protection industry and to promote personal information security industry. In particular, it is expected that the establishment and application of the "personal information security certification system" will exert a significant impact on improvements in the levels of personal information security among enterprises.

At present, security certificate systems like

ISO27001 and KISA-ISMS (Korea Information Security Agency – Information Security Management System) are being implemented. However, a certificate system that certifies overall personal information security responses from an enterprise do not currently exist. If a system is in place whereby "authentication" is ganted by a certificate in a company with a well-established personal information security system and the public's trust, large conglomerate enterprises will be able to exert greater efforts to obtain this certificate, and most enterprises that handle personal information will gradually participate in any certificate system which will result in an enhancement of the privacy protection level in the nation.

Therefore, this paper proposes the basic direction for the development of a personal information certificate system. Firstly, the framework for personal information security certification will be presented. Secondly, the standard system for privacy protection certification will be proposed.

However, this paper does not cover the detailed checklist and operational methods required for privacy protection certification.

2 Analysis of Current Information Security Certification

2.1 Information Security Certification Systems - ISO27001 and KISA ISMS Certification

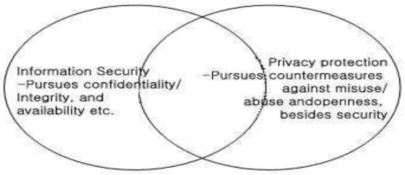
Currently, the representative information security system includes ISO 27001 and KISA ISMS (Table 1). Both certificates are specialized in "information security," based on "best practice in information security," and are not designed for "privacy protection." Therefore, it is unreasonable to apply the current security certification scheme to privacy protection certification. However, several major certification areas may be applied by converting "information security" to "privacy protection" Measures.

Table 1. Comparison of the Certification Area between ISO 27001 and KISA ISMS

ISO27001	KISA-ISMS	Possibility and limitation of privacy protection certificate application
Risk management	Information security management process	* Applicability: Not applicable if the current area and item are used.
Information security policy	Information security policy	
Information security organization	Information security organization	
	Information security for an external party	
Asset management	Classification of the information asset	
	Education and training on information security	
Personal resource security	Personal resource security	
Physical and environmental security	Physical information security	
Obtaining, development, and maintaining the information system	System development information security	
	Password control	
Access control	Access control	
Communication and operation management	Operation management	
	e-Commerce information security	
Information security incident handling	Information security incident handling	
Compliance	Review, monitoring, and audit	
Business continuity management	Business continuity management	

However, we cannot acknowledge the converted area as a certification scheme suitable for "privacy protection," even though the word "information security" is changed to "privacy protection," and although its coverage area and items are transplanted into a "privacy protection certification." Many people make the misunderstanding that the privacy protection issue can be resolved by security measures alone. Although "information security" and "privacy protection" do overlap in many areas, their basic concepts differ (Figure 1.). The former focuses on leakage and alteration prevention, whereas the latter focuses on leakage and alteration prevention as well as misuse/abuse prevention. For example, let us assume that a certain company collects customer information without their consent, and saves it with strong encryption measures. In this case, this company is acting properly in terms of "information security," but not in terms of "privacy protection." Therefore, the "misuse/abuse" issue should be reflected carefully in order to develop the "privacy protection certificate" area of concern.

Fig 1. Information Security & Privacy Protection Area



2.2 Comparison and Suggested Points of the Current Information Security Certification System

In summary, the current certification system cannot handle a "personal information security certification" system. To properly establish this, 1) a certification framework and criteria specialized for "privacy protection" should be developed; 2) a certification review scheme, (organization and process), is required, and; 3) education and fostering of the certification reviewer are required. Fortunately, KISA-ISMS or ISO27001 certification frameworks can be utilized for requirements ii) and iii). Therefore, the most critical issue facing the nation is to develop the certification framework and criteria specialized for "privacy protection" (i). The framework and contents of the existing KISA-ISMS or ISO27001 can also be re-used for this area. That is, the personal information security certification framework may utilize the security certification system (KISA-ISMS or ISO27001). In addition, most of the content of KISA-ISMS or ISO27001 can be reflected. However, there exist some differences in the basic concepts of the two systems, so some complementary measures are required.

3 Methods of Privacy Protection Certification System

Basic objectives and principles should be clearly defined so as to establish a privacy protection certification system. The following section describes the objectives and principles proposed by this paper:

3.1 Basic Principles

This paper aims to assess whether the target organization or business has established the management system for privacy protection and is able to repeat its operation rather than the effectiveness of privacy protection measures at a certain site.

- The scope of the certification should support the entire enterprise as well as the specific organization or business.
- The overall management system that processes personal information for the entire organization or service should be certified not only the specific site.
- The framework for the management system should include all areas related with personal information management.
- The privacy protection certificate should be able to cover information security as well as personal information misuse/abuse.

3.2 Certification Review Scheme

It would not be unreasonable to adopt the existing KISA-ISMS or ISO27001 certification system as the review scheme of a new privacy protection certification system. Rather, it would be more efficient and can produce a synergy effect if an organization running KISA-ISMS or ISO27001 also manages a privacy protection certification system. This is because the privacy protection certification system and KISA-ISMS or ISO27001 differ in the implementation content only, not in terms of the actual operation framework.

Therefore, it is desirable to apply the KISA-ISMS or ISO27001 certification system to a privacy protection certification system. It is desirable to associate a privacy protection certification system with the existing KISA-ISMS certification, and to temporarily name it the "KISA-PMS (Privacy Management System)," having it operated in a similar way to the current KISA certification scheme as described in Table 2.

Table2. Comparison of certification schemes

Certification Item	KISA-ISMS Certificate	KISA-PMS Certificate
Authority	KISA	KISA
Target	Enterprise-wide; Some organizations or services, if necessary	Enterprise-wide; Some organizations or services, if necessary
Procedure	KISA grants the certificate via a Certification Committee after review by the reviewer.	Adopts the same certification system as KISA-ISMS; However, reviewers and the Certification Committee should be organized independently from 'Security'

Reviewer	Person who has been trained in information security certification, passing;	Person who has been trained in privacy protection certification, passing
Committee	committee formed by experts and specialists in the information security area;	Committee formed by experts and specialists in the privacy protection area

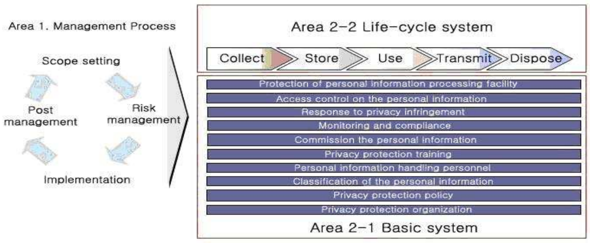
3.3 Criteria and Elements of Privacy Protection Certification Review

It is desirable to define the review area of the privacy protection certification system as described below:

a. Management process to establish and run the management system (Area 1 in Figure 2)

b. Privacy protection measures selected by the applicant via the management process (Areas 2-1 and 2-2 in Figure 2)

Figure 2. Criteria Area of Privacy Protection Certification


Area 1. Management Process
Scope setting
Risk management
Implementation
Post management
Area 2-2 Life-cycle system
Collect
Store
Use
Transmit
Dispose
Protection of personal information processing facility
Access control on the personal information
Response to privacy infringement
Monitoring and compliance
Commission the personal information
Privacy protection training
Personal information handling personnel
Classification of the personal information
Privacy protection policy
Privacy protection organization
Area 2-1 Basic system

Firstly, "a. Privacy protection measures selected by the applicant via the management process" is required to establish, operate, and maintain the privacy protection system, and is composed of activities described in the four steps below:

1) Management system scope setting: Sets the management scope to establish and run the management system, and studies the status of the information (or asset) related with privacy protection;

2) Risk management: Analyzes the privacy violation threat against the target information (or asset), and vulnerabilities in order to cope with them;

3) Implementation: Implements measures related with privacy protection;

4) Post management: Review, monitoring, improvement, and internal audit activities for the management system.

At this point, the method differing from risk assessment and risk management of "information security" should be used at the risk management stage described in 2). Generally, a risk assessment of "information security" focuses on the confidentiality, availability and integrity of the specific asset, whereas that of "privacy protection" is not suitable from this perspective. Therefore, one of the following two methods is practical for application:

The first is the simple method that analyzes vulnerabilities by performing a gap analysis based on the privacy protection measure in Area 2 which will be described later.

The second is the risk assessment method which focuses on the "threat" rather than on the "asset."

Therefore, it is more efficient to determine various privacy infringement threats against the information concerned or the business process, and to assess the occurrence possibility and impact for risk calculation rather than analyzing the "threats" and "vulnerabilities" of the specific asset, and subsequently calculating risk from the perspective of confidentiality, availability and integrity.

On the other hand, it is desirable to separate issues into the two areas described in Figure 2 so as to handle "b. Privacy protection measures selected by the applicant via the management process" – the basic management system area and the area for the personal information processing process.

The former is composed of ten sub-areas encompassing all areas from protection of the organization and policies related with privacy protection to the protection of the privacy protection area. These areas are similar to that proposed by KISA-ISMS or ISO27001 in terms of the operation scheme. However, the content items are quite different. The former focuses on "information security," whereas the latter focuses on "privacy protection." In addition, traditional "information security" areas such as password, communication, and operation management, as well as development management, e-commerce security and others are not the core issues in privacy protection. Therefore, these areas need to be excluded from any privacy protection certification scheme.

However, as described above, "privacy protection certification" deals with different areas from KISA-ISMS or ISO27001 certification schemes. That is, "privacy protection certification" should handle the misuse/abuse issue. It will be effective in handling this issue throughout the entire personal information processing process. Therefore, unlike KISA-ISMS or ISO27001, the operation scheme of "privacy protection certification" should cope with threats like misuse/abuse and disclosure as well as unauthorized personal information leakage and alteration from the perspective of the entire personal information lifecycle. As a result, control measures needed to be arranged for privacy protection certification criteria from the standpoint of the personal information processing lifecycle are required. This is an additional element that does not arise in the existing KISA-ISMS or ISO27001 certification schemes. Table 3 illustrates a comparison of control areas in the existing certification scheme and that of privacy protection certification.

Table 3. Comparison of Criteria Areas in ISO27001 and KISA-ISMS Certification Schemes and in Privacy Protection (Proposed)

ISO27001	KISA-ISMS	KISA-PMS	
Risk management	Information security management process	Privacy protection management process	
Information security policy	Information security policy	B A S I C S Y S T E M	Privacy protection policy
Information security organization	Information security organization		Privacy protection organization
	Information security for the external party		Commissioning personal information to the external source
Asset management	Classification of the information asset		Classification of the personal information
	Education and training in information security		Privacy protection training
Personal resource security	Personal resource security		Personal information handling personnel
Physical and environmental security	Physical information security		Protecting personal information processing facility
Obtaining, developing, and maintaining the information system	System development information security		
	Password control		
Access control	Access control		Personal information access control
Communication and operation management	Operation management		
	e-Commerce information security		
Information security incident handling	Information security incident handling		Personal information infringement response
Compliance	Review, monitoring, and audit.		Monitoring and response
Business continuity management	Business continuity management		
		L C S Y S	Collecting personal information
			Storing personal information
			Using personal information
			Sending personal information
			Disposing of personal information

Table 4 shows the classification at the 1st level for privacy protection certification criteria areas. The detailed control items fall beyond the scope of this paper, and will be examined at a later stage.

Table 4 Privacy protection certification criteria (Basic system area)

Large Category	Medium Category	Small Category
Basic System	Privacy protection organization	Organization Personal information manager Responsibilities and roles
	Privacy protection policy	Policy approval and announcement Policy system Customer privacy protection policy Policy maintenance
	Classification of privacy protection	List of personal information Classification Handling
	Personal information handling personnel	Responsibility assignment Duty minimization Eligibility review Documentation of accountability
	Privacy protection training	Education and training program Implementation and evaluation
	Commissioning personal information to an external source	Minimizing the scope of commissioning Commissioning contracts Reporting and management Notification to the user when commissioning Controlling re-commissioning
	Monitoring and compliance	Monitoring Periodical review Customer complaint recording and solving Independent review
	Infringement response	Personal information backup Infringement incident plan Infringement detection and recovery Post management
	Access control	Handling statistics Network access control System access control Post management
	Facility protection	Processing facility protection Processing equipment protection

Table 5 Privacy Protection Certification Criteria (LC System Area)

Large Category	Medium Category	Small Category
Life-cycle management	Collection	Constraint of data collection Public notice regarding collection purpose Consent regarding collection User rights Constraints of data collection about the users under14 years old

		User rights relief
	Trans- mission	Internal transmission Transmission to external companies
	Disposal	Disposal Public notice regarding disposal Reason for data retention
	Storage	List of storage status Data storage Saving document/file (Internal & External) Controlling the storage location
	Use	Allocating retrieval and use rights Defining objectives Minimized rights Non-disclosure Prevention of personal information leak Constraints on misuse Limitations on data retention Documenting the use purpose Accuracy of personal information Transfer notice

4 Conclusion

This paper reviewed the representative existing security certification, privacy protection certification systems, and developed some recommendations proposing a basic direction for establishing a privacy protection certification system.

In conclusion;

1) We may run the scheme and the procedure for privacy protection certification using a method similar to those employed in KISA-ISMS or ISO27001;

2) The criteria items for privacy protection certification are similar to those of KISA-ISMS or ISO27001. However, misuse/abuse is important in privacy protection, and this requires addition and emphasis. Therefore, privacy protection certification criteria should reflect the basic management system as well as the infringement issues throughout the personal information lifecycle – from its generation to its disposal;

3) Certification based on process, business and system is important in supplementing the insufficiencies of existing certification systems for privacy protection. If these lacking items are supplemented by a “privacy protection certification” system, certification will be better equipped to serve both enterprises and society.

This paper does not purport to outline a detailed checklist or certification operation procedure. Therefore, further research into these is required.

References:

[1] OECD (2003), 'Privacy Online: OECD Guidance on Policy and Practice', OECD.

[2] WPISP Report (2006) 'Proposed Next Steps for Cross-Border Privacy Law Enforcement & Cooperation', DSTI/ICCP/REG (2006)14.

[3] WPISP (2006), OECD Questionnaire on the Cross-Border Enforcement of Privacy Laws, http://www.oecd.org/dataoecd/5/30/37572050.pdf.

[4] WPISP (2006), Report on the Cross-Border Enforcement of Privacy Laws, http://www.oecd.org/dataoecd/17/43/37558845.

[5] Kang, Sin-won (2004), Major discussions and suggestion points of the Information and Communication Committee, ETRI, 2004. 12. 15.

[6] Kim. Chang-gon et al. (2004), Privacy Protection Whitepaper 2003, KISA.

[7] Kim, Hyeong-do (2002), Trends of OECD’s Security Guideline Revision, Overseas Information Security Trend, September Edition, KISA.

[8] Baek, Eui-seon et al. (2000), A Study on the Policy about Personal Information Distribution among Countries, Korea Information Security Center, Policy Study, December 2000.

[9] KISA (2004) Privacy Protection Whitepaper 2003, KISA.