

**2011 Modularization of Korea's Development Experience:
Information Security Activities
in Korea and Implications**

2012

2011 Modularization of Korea's Development Experience:
**Information Security Activities in Korea
and Implications**

2011 Modularization of Korea's Development Experience
Information Security Activities in Korea
and Implications

Title	Information Security Activities in Korea and Implications
Supervised by	Korea Communications Commission (KCC), Republic of Korea
Prepared by	Korea Internet&Security Agency (KISA)
Author	Jae Suk Yun, Korea Internet&Security Agency
Advisory	Jong In Lim, Director of Graduate School of Information Security, Korea University
Research Management	Korea Development Institute (KDI) School of Public Policy and Management
Supported by	Ministry of Strategy and Finance (MOSF), Republic of Korea

Government Publications Registration Number 11-1051000-000230-01

ISBN 978-89-93695-77-9 94320

ISBN 978-89-93695-27-4 [SET 40]

Copyright © 2012 by Ministry of Strategy and Finance, Republic of Korea



Government Publications
Registration Number

11-1051000-000230-01

Knowledge Sharing Program

2011 Modularization of Korea's Development Experience
**Information Security Activities in
Korea and Implications**



KISA



Preface

The study of Korea's economic and social transformation offers a unique opportunity to better understand the factors that drive development. Within one generation, Korea had transformed itself from a poor agrarian society to a modern industrial nation, a feat never seen before. What makes Korea's experience so unique is that its rapid economic development was relatively broad-based, meaning that the fruits of Korea's rapid growth were shared by many. The challenge of course is unlocking the secrets behind Korea's rapid and broad-based development, which can offer invaluable insights and lessons and knowledge that can be shared with the rest of the international community.

Recognizing this, the Korean Ministry of Strategy and Finance (MOSF) and the Korea Development Institute (KDI) launched the Knowledge Sharing Program (KSP) in 2004 to share Korea's development experience and to assist its developing country partners. The body of work presented in this volume is part of a greater initiative launched in 2007 to systematically research and document Korea's development experience and to deliver standardized content as case studies. The goal of this undertaking is to offer a deeper and wider understanding of Korea's development experience with the hope that Korea's past can offer lessons for developing countries in search of sustainable and broad-based development. This is a continuation of a multi-year undertaking to study and document Korea's development experience, and it builds on the 20 case studies completed in 2010. Here, we present 40 new studies that explore various development-oriented themes such as industrialization, energy, human capital development, government administration, Information and Communication Technology (ICT), agricultural development, land development and environment.

In presenting these new studies, I would like to take this opportunity to express my gratitude to all those involved in this great undertaking. It was through their hard work and commitment that made this possible. Foremost, I would like to thank the Ministry of Strategy and Finance for their encouragement and full support of this project. I especially would like to thank the KSP Executive Committee, composed of related ministries/departments, and the various Korean research institutes, for their involvement and the invaluable role they played in bringing this project together. I would also like to thank all the former public officials and senior practitioners for lending their time and keen insights and expertise in preparation of the case studies.

Indeed, the successful completion of the case studies was made possible by the dedication of the researchers from the public sector and academia involved in conducting the studies, which I believe will go a long way in advancing knowledge on not only Korea's own development but also development in general. Lastly, I would like to express my gratitude to Professor Joon-Kyung Kim for his stewardship of this enterprise, and to his team including Professor Jin Park at the KDI School of Public Policy and Management, for their hard work and dedication in successfully managing and completing this project.

As always, the views and opinions expressed by the authors in the body of work presented here do not necessary represent those of KDI School of Public Policy and Management.

May 2012

Oh-Seok Hyun

President

KDI School of Public Policy and Management



Contents | LIST OF CHAPTERS

Summary	16
---------------	----

Chapter 1

Background.....	19
1. Informatization Environment and Treats	20
2. Forecast for Information Security	21

Chapter 2

Main Policies of Information Security.....	25
1. Information Security System	26
1.1 National Information Security System	26
1.2 National Information Security Organizations.....	27
2. Main Information Security Policies and Strategies	31
2.1 Ubiquitous Information Security Strategies ('06.12).....	31
2.2 Long Term Comprehensive Plan for Information Security (July 2008)	33
2.3 Comprehensive Plans for Internet Information Security (July 2008).....	34
2.4 Comprehensive Plan for Promoting Knowledge Information Security Industry (December 2008).....	36
2.5 Comprehensive Plans for Smart Mobile Security (December 2010).....	37
3. Development and Status of Information Security Law System	38
3.1 History.....	38
3.2 Main Status.....	40

Chapter 3

Main Information Security Activities.....	45
1. Responses to Internet Attacks.....	46
1.1. Korea Internet Security Center (KISC)	46
1.2 Security Incident Response Process and the Roles of the KISA.....	48
1.3 Main Activities	49
2. e-government Security	53
2.1 Promoting the Security Level of e-government Services	53
2.2 Considerations for e-government Service Security Improvements	55
2.3 National Computing and Information Agency (NCIA) Establishment and Operation.....	58
3. Critical Information Infrastructure Protection	63
3.1 Overview of the System	63
3.2 Critical Information Infrastructure Protection Activities	66
3.3 Improvement of the Infrastructure Protection Systems.....	69
4. Implementation and Operation of a Safe Electronic Authentication System.....	70
5. Information Security Management System Certification.....	74
5.1 Overview.....	74
5.2 Main Activities and Project Accomplishments	76
6. Information Security Check	79
6.1 Background for Introducing the Information Security Check Service	79
6.2 Content of the Information Security Checkup Service	80
7. Information Security Product Evaluation	84
7.1 History of Information Security System Evaluation and Certification Service.....	84
7.2 Information Security System Evaluation/Certification Service and Procedures	85



Contents | LIST OF CHAPTERS

7.3 Operational Status of the Evaluation and Certification Service	87
7.4 Direction	93
8. Spam Prevention Activities	94
8.1 Overview	94
8.2 Cause of Spam Generation	95
8.3 Main Spam Prevention Plan	95
9. Personal Information Protection	99
9.1 Personal Information Protection System	99
9.2 Personal Information Protection Policy Activities	101
9.3 Raising Awareness of Personal Information Security	104
10. Copyright Protection	105
10.1 Importance of Copyright Protection	105
10.2 Enactment and Revision of the Copyright Laws	106
10.3 Efforts to Protect Copyright	108
10.4 Copyright Related Organizations and Their Activities	108
10.5 Copyright Protection Activities and Outcomes	111

Chapter 4

Information Security Basis Implementation Activities	115
1. Information Security Education and Training	114
1.1 Status of Information Security Manpower	114
1.2 Status of Information Security Training	115
1.3 Status of Information Security License	124
2. Information Security Industry Promotion and Technology Development	125
2.1 Information Security Promotion Policies in Korea	125
2.2 Status of Information Security R&D in Korea	130
3. Establishment and Operation of Information Security Organizations.....	133
3.1 Korea Internet&Security Agency (KISA)	133
3.2 e-Government Security Monitoring Center (G-Cert)	137
3.3 National Security Research Institute (NSRI).....	137
3.4 Electronics and Telecommunications Research Institute (ETRI)	138
3.5 KFTC (Financial Sector Information Sharing and Analysis Center)	139
3.6 KOSCOM	140
3.7 Financial Security Agency (FSA)	140
4. Information Security Awareness Promotion Activities	141
4.1 Status of Information Security Awareness in Korea	141
4.2 Overview of Activities to Promote the Awareness of Information Security in Korea	141
5. Information Security Cooperation Partner's Activities	150
5.1 Information Security Cooperation Activities in Korea.....	150
5.2 Overseas Information Security Cooperation Activities	156



Contents | LIST OF CHAPTERS

Chapter 5

Evaluation	161
1. Information Security Index and Policies: International Comparisons	160
2. Information Security Policy Accomplishments	162
2.1 Overview of National Information Security Index	162
2.2 Analysis of the Information Security Index Estimates	164

Chapter 6

Viewpoints	169
1. Importance of Government Leadership and Public/Private Sector Cooperation for Information Security	168
2. Threats in the Dramatically Evolving ICT Environment, and How to Cope with Them	169
3. Recommendation for Execution Plans to Promote the Level of Information Security	170
References	174

Contents | LIST OF TABLES

Chapter 2

Table 2-1 Long Term Comprehensive Plan for Information Security: Agendas and Task.....	34
--	----

Chapter 3

Table 3-1 Criteria for Designating the Critical Information Infrastructure.....	66
Table 3-2 Status of Designation as the Critical Information Infrastructures in Each Area.....	67
Table 3-3 Status of Accredited Certification Authority Designations	73
Table 3-4 Benefits from Obtaining Certificate of Information Security Management System.....	78
Table 3-5 Targets of Information Security Checkups.....	83
Table 3-6 Information Security Checkup Organizations	83
Table 3-7 Information Security Products' CC Evaluation and Certification Records.....	88
Table 3-8 25 Types of Information Security Products Subject to Domestic Evaluation and Certification	90
Table 3-9 Status of Evaluation Organizations in Korea.....	91
Table 3-10 Evaluation Fee Discount Policy (KISA)	92
Table 3-11 Main Policy to Prevent Spam in 2003~2005.....	96
Table 3-12 Main Spam Prevention Policies in 2006~2009.....	97
Table 3-13 Main Spam Prevention Policies from the End of 2009 to Present.....	97
Table 3-14 Number of Civil Appeals Registered as Personal Information Invasions.....	100
Table 3-15 Copyright Consignment Management Organizations	110



Contents | LIST OF TABLES

Chapter 4

Table 4-1 Manpower Breakdown for Information Security Business.....	114
Table 4-2 Status of Information Security Departments in Universities	115
Table 4-4 Status of Information Security Departments in Colleges.....	120
Table 4-5 Status of Information Security Departments in Informatization Education Centers ..	121
Table 4-6 Private Information Security Education Organizations.....	122
Table 4-7 KISA Academy Education Program	124
Table 4-8 Status of Information Security License	124
Table 4-9 Korean Information Security Market Size (revenue).....	126
Table 4-10 Korean Information Security Market Size (demand).....	126
Table 4-11 Korean Government's Policy to Promote the Information Security Industry.....	127
Table 4-12 Classification of Main Information Security Technologies.....	132

Chapter 5

Table 5-1 WEF Secure Server Statistics and National Ranking	161
Table 5-2 National Information Security Index System	163
Table 5-3 Estimates of the Information Security Index.....	164
Table 5-4 Description of Information Security Indices and Details of Estimates	166

Contents | LIST OF FIGURES

Chapter 2

Figure 2-1 National Information Security System	27
Figure 2-2 Basic Strategies and Vision for Information Security in the Ubiquitous Age	32
Figure 2-3 Comprehensive Goals and Strategies for Internet Information Security.....	35
Figure 2-4 Vision of the Knowledge Information Security Industry: Its Strategies and Detailed Tasks	36
Figure 2-5 Comprehensive Plans for Smart Mobile Security: Visions, Strategies and Detailed Tasks.....	37

Contents | LIST OF FIGURES

Chapter 3

Figure 3-1 Security Incident Response Process	48
Figure 3-2 The Role of KISA in Handling Cyber Security Incidents.....	49
Figure 3-3 Infected PC Cyber Cure System Organization Chart	50
Figure 3-4 DDoS Cyber Shelter Multiple Level Defense System	52
Figure 3-5 Security Level of e-Government Service in Each Year (2007~2010)	54
Figure 3-6 Security Level of Each Area of e-Government Service (2007~2010).....	54
Figure 3-7 Critical Information Infrastructure Protection System.....	65
Figure 3-8 Administrative Digital Signature Authentication System Diagram	71
Figure 3-9 Public Digital Signature Authentication System	72
Figure 3-10 ISMS Certification Criteria	75
Figure 3-11 ISMS Certification Procedures.....	76
Figure 3-12 Growth of certificates issued	77
Figure 3-13 Information Security Checkup Procedures (1)	81
Figure 3-14 Information Security Checkup Procedures (2)	82
Figure 3-15 Information Security System Evaluation/Certification Service.....	85
Figure 3-16 Information Security System Evaluation/ Certification Procedures.....	86
Figure 3-17 Certificate Effects Maintenance Procedures.....	87
Figure 3-18 Trends of Illegal S/W Copying	111

Chapter 4

Figure 4-1 Main Information Security R&D Areas	131
Figure 4-2 Examples of Information Security Ads	142
Figure 4-3 118 Paper Ads and 118 Songs, Everyday-song Music Video	144
Figure 4-4 Information Security Publicizing Activities.....	145
Figure 4-5 Information Security TV Program Rerun and Captures.....	147
Figure 4-6 Information Security SNS&Smartphone Apps.....	148
Figure 4-7 Information Security Publicizing Activities.....	149
Figure 4-8 Hacking Prevention Workshops.....	153

Chapter 5

Figure 5-1 Framework for the National Information Security Index.....	163
Figure 5-2 Annual Trends of Information Security Index Changes	165

Summary

Korea is ranked near the top in the world in all of the main informatization indices, and has the world's highest level of internet use as well. Recently, the use of wireless internet services through mobile handsets such as smartphones and tablets has been growing significantly. However, as informatization advances, related threats such as hacking, computer viruses, spam email, unhealthy information distribution and privacy invasions have also been increasing rapidly. Moreover, there is high concern over the potential damages to Korea's main national information communication infrastructures caused by cyber attacks.

As a result, the Korean government recognizes that information security activities have an equal level of importance to informatization when pursuing national projects. To enhance the national level of information security, the Korean government is working hard to implement a systematic foundation, and has been unfolding various types of information security activities.

First of all, the National Intelligence Service (NIS) takes comprehensive responsibility for the information security system in Korea, and each ministry of the Korean government supervises its respective area. The Korea Communication Commission (KCC) is responsible for the private sector and the Ministry of Public Administration and Security is responsible for the public sectors, while the Ministry of Defense takes the full responsibility for national defense. Also, the Ministry of Knowledge Economy safeguards the area of information security. The Korea Internet&Security Agency provides various professional supports to improve the level of information security at the national level. Many other stakeholders, including special organizations and private companies, are cooperating on this basis to promote the level of information security.

Korea's major information security policies and strategies include: the "basic strategies for ubiquitous information security (December 2006)," the "mid-term comprehensive plan

for information security (July 2008),” the “comprehensive plan for internet information security (July 2008),” the “comprehensive plan for knowledge information security industry promotion (December 2008),” and the “comprehensive plan for smart mobile security (December 2010).” On the basis of these policies and strategies, consistent efforts are being made to diagnose and improve Korea’s current level of information security.

On the other hand, the Korean government began to make aggressive efforts to cope with the threats accompanying informatization, a policy that had been nationally pursued since the ‘80s. In the early days, the well-known examples of these efforts are the “Framework Act on Informatization Promotion,” the “Digital Signature Act,” and the “Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.” Entering the year 2000, as the social and national dependence on the information communication system was emphasized the government began to find it necessary to repair the information security system from the perspective of national security. Therefore, the “Act on the Protection of Information and Communications Infrastructure” and the “Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.” were revised and enacted. Subsequently, to promote the information security industry, the “Act on Information Communication Industry Promotion” was enacted, and to protect defense/military information, the “Act on National Informatization Basis Implementation and Defense Information Resource Management” was enacted. Most recently, the “Personal Information Protection Act” was enacted in an effort to repair Korea’s overall legal systems.

Under the legal system mentioned here, the Korean government has been pursuing various types of information security activities. The most popular examples are: responses to internet attacks, enhancement the security level of e-government services, protection of the critical information infrastructures, digital signature certification management, certification of information security management systems, and evaluation of information security products, spam prevention, personal information protection and copyright protection activities.

To pursue such diverse information security activities, the Korean government is pursuing various ground-level tasks. The most popular examples of these include information security education, manpower training, promotion of related industries, technology development, and the establishment and operation of special organizations such as KISA. Also, to promote the spirit of information security, the Korean government is unfolding PR and campaign activities through various media.

But if the level of information security is to be improved, in addition to the government and the stakeholders in the public sectors, close cooperation among the various stakeholders in the private sector is required. In Korea, academic societies, associations and various discussion boards have joined forces with the government to pursue diverse activities such as conferences, workshops, and public campaigns, as well as cooperations with various

foreign and domestic organizations such as OECD, APEC, ITU, FIRST, and APCERT on information security issues.

Korea is recognized as a role model in the area of information security, as it has consistently been ranked very highly in the security server index of WEF (World Economy Forum), which evaluates the level of international information security based on various activities and cooperation among domestic and foreign organizations and systematic approaches to promote the level of information security.

By explaining the government's roles and efforts to promote the level of information security and to form a foundation for such promotion and its various activities and cooperation for information security, we hope to set out best practices that developing countries can benchmark.

2011 Modularization of Korea's Development Experience
Information Security Activities in Korea and Implications

Chapter 1

Background

1. Informatization Environment and Threats
2. Forecast for Information Security

Background

1. Informatization Environment and Treats

Korea is recognized as a country with one of the best internet environments in the world. It is ranked no. 3 in the information communication development index of ITU (International Telecommunication Union), and no. 15 in the network preparation index suggested by WEF (World Economic Forum). In addition, it is ranked very highly in other major information communication indices.

The status of internet use in Korea is the highest in the world. In 2010, there were 37.01 million internet users, and the rate of internet use was 77.8%. Nearly 100% of teenagers and adults in their 20s and 30s use the internet, and children (3~9 years of age) and adults in their 40s use internet at a rate of more than 85%. Recently, smartphones have become widely and rapidly available, and social network services (SNS) are gaining rapid popularity.

However, it should be noted that, with the rapid developments in internet services, related threats have also been on the rise. DDoS (Distributed Denial of Service) attacks, hacking, computer viruses, spam emails, and phishing or pharming to steal people's money have led to many crimes. Furthermore, the negative side effects of informatization such as unhealthy information distribution and privacy invasions are newly emerging social concerns.

It is important to note here that the damages caused by cyber attacks extend into the real world. In recent years, large-scale personal information leakage accidents that threaten individual privacy, damage a company's brand value and cause economic losses have occurred frequently. In July 2011, Nate and Cyworld, two of the most well known portals and SNS sites in Korea leaked personal information of more than 35 million users in a hacking accident, which led to increasing concerns over the potential for large scale cyber damage.

Each year, a new fraud technique emerges in a new internet environment, and more and more sophisticated and advanced hacking techniques appear. These new hacking techniques are not limited to cyber attacks on individuals and companies, but sometimes aim at the nation itself, which can lead to enormous damages and ripple effects. Intelligent attacks are making it difficult for organizations and internet users to resolve problems quickly. Many phishing crimes deliberately take advantage of social issues, and cause a great deal of damage.

In addition, with wireless internet becoming widely available and information becoming digitalized, there is a higher likelihood of illegal access to information and the leakage of confidential information. Through global connection online, Korea's well developed internet infrastructure is often abused as a bridge for foreign hackers who distribute viruses. Yet there is very weak law enforcement on cyber criminals who reside Korea.

More gravely, as the dependence on the internet for daily life is increased and the main national infrastructures are being managed and controlled by the information communication networks, hacking and cyber attacks can threaten national security. The fact has been giving many Koreans a sense of insecurity. Cyber terror attacks, such as Stuxnet and Ducus, that directly target major facilities, can be serious threats that endanger cornerstones of a country that heavily relies on the online "infrastructure." The best-known examples of such threat are the cyber attacks to the internet infrastructures of Estonia in 2007 and of Georgia in 2008. Also, similar cases can be found in the DDos attacks in Korea on July 7, 2009 and attacks on the nuclear facility of Iran in 2010.

2. Forecast for Information Security

As new services emerge in the future, such as smart-device based mobile services, wireless and wired cloud service, social network services (SNS) and the smart grid, we expect that informatization will advance further, which will lead to increased security threats.

Recently, with the wide availability of smart phones and mobile services, threats from the internet world appeared in the internet environment. More seriously, in the mobile world, since various network access routes exist, access control is very difficult, and intelligent hacking that takes advantages of the specific characteristics of the mobile world may take place. As mobile services are expanded, mobile malignant codes are on the rise, and the likelihood of personal information leakage or fraud due to a lost mobile device or hacking is increasing. In addition, spam threats via mobile devices are also expected to rise.

On the other hand, as cloud services are promoted, we can expect a rise in related security threats and damages. In the cloud service, there is the danger of personal information outflow due to ID/password leakage and vulnerability in the virtual environment. In particular, in mobile cloud services, there are many security threats including malignant

code distribution on mobile handsets, illegal access to the cloud service via lost mobile devices, and wiretapping in a wireless area.

Due to the wide availability of wired/wireless internet telephones, there will inevitably be more threats to security. In particular, it is expected that mobile internet telephone (m-VoIP) will experience various types of service failures due to wiretapping, DDoS attacks and mobile device hacking.

In addition, as IPTV and smart TV become widely available, malignant codes in the contents can infect set-top boxes and lead to system hacking. In particular, with mobile IPTV and smart TV, which use wireless networks, there is some potential to use packet collection tools in a wireless area to leak and falsify the multimedia contents, and enable access by unauthorized wireless handsets. Due to the characteristics of the wireless network, we can expect DDoS attacks with signal interference in specific wireless areas, and large-scale packet transmissions.

On the other hand, as various SNS such as Facebook or Twitter gains great popularity among users worldwide, there will be more cyber threats to SNS users. Since an SNS is easily used on a smartphone, the malignant code can rapidly reach mobile devices, as well as PCs. For location-based SNS, which combines the relationship management characteristics of an SNS information sharing characteristics of mobile, we can expect privacy invasions caused by location information leakages.

In the future, we can expect an increasing number of cyber attacks on the national infrastructures. Obviously, as the convergence of electrical power and communication proceeds further, the smart grid system implementation will expand over the entire world. Consequently, cyber attacks on the main systems of the smart grid, such as hacking to the smart meter connected to the network, can cause large-scale damages, including blackouts and the like.

The content of this report was prepared in the following order to facilitate systematic and broad understanding of the Korean government's experience in information security development.

First of all, as the main execution policy for information security, we will describe the superintendent organizations and the national information security support system. Moreover, we will provide an overview of how the main strategies and policies pursued by the government and the relevant laws and systems have been developed so far. After that, as the main information security activity, we will explain the responses to internet accidents, e-government security, and protection of main ICT infrastructures, digital signature certification management, information security management system certification, information security diagnosis, information security product evaluations, spam prevention, personal information protection, and copyright protection activities and so on.

Also, as exemplary activities to implement the basis for information security, we will take a glance at education and manpower training, industrial promotion and technology

development, professional organization establishment and operation, promotion of recognition on information security, and activities performed by cooperation organizations.

After that, we will evaluate the accomplishments of the efforts to promote the information security level in Korea. Finally, we will propose a roadmap that can clearly show the importance of the government's leadership and private-government cooperation for information security, threats emerging in the drastically evolving ICT environment and the future direction of handling these threats, and the systems and activities performed by developing countries to promote information security.

2011 Modularization of Korea's Development Experience
Information Security Activities in Korea and Implications

Chapter 2

Main Policies of Information Security

1. Information Security System
2. Main Information Security Policies and Strategies
3. Development and Status of Information Security Law System

Main Policies of Information Security

1. Information Security System

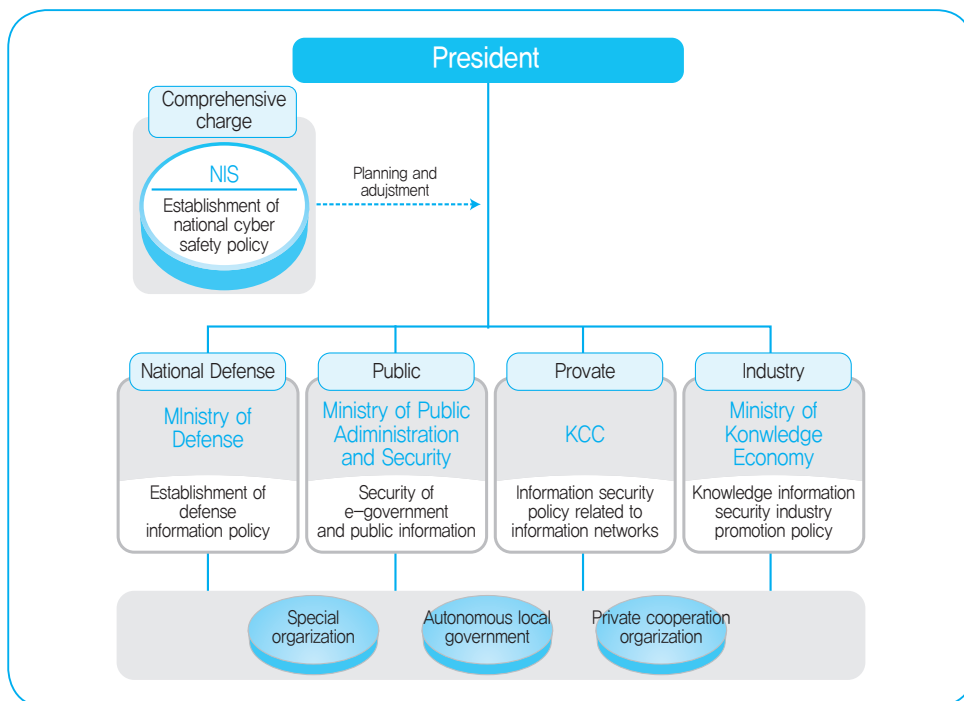
Before introducing Korea's information security system, we would like to introduce the reader to the central administration organizations in each area—defense, public, private, industry and finance—at the uppermost level of the national security system, and then discuss their roles, activities and relevant rules.

1.1 National Information Security System

In Korea, the NIS (National Intelligence Service) takes comprehensive responsibility for information security, and each administrative organization is in charge of its respective area. According to the 「Act on NIS」 and the resulting 「Rules for information/security business planning, adjustment」, the NIS plans the information security business and adjusts the information security business among the information investigation organizations and the administrative organizations. On the other hand, according to the “Security business rules,” it takes charges of the national confidential protection business.

Each administrative organization performs security-related business in its respective area—defense, public, private, industry or finance—according to the applicable laws. It establishes and executes its own security plan within the department, manages and supervises security businesses pertaining to its lower-ranked affiliates and self governing local governments, and provides support if necessary. In addition, it operates private cooperation organizations so that it can establish and execute policies through discussion with various stakeholders.

Figure 2-1 | National Information Security System



Source: National Information Security White Paper (2009~2010) reorganized

1.2 National Information Security Organizations

1.2.1 National Intelligence Service (NIS)

According to the “Act on NIS,” the “Security business rules,” the “Act on the Protection of Information and Communications Infrastructure,” and the “e-Government Act,” the NIS comprehensively takes charge of national information security businesses, including the planning, adjustment, establishment and execution of security policies. In particular, according to the “National Cyber Security Management Rules” enacted in January 2005, the head of the NIS has the privilege to comprehensively adjust and discuss national cyber safety policies and management with the heads of the central administration organizations. As a result, his authority as the head of national security business was further strengthened. In practice, the head of the NIS is in charge of the ‘National cyber security strategy meeting,’ which reviews the main issues arising in relation to national cyber security. For the efficient operation of the meeting, the ‘national cyber security plan meeting’ is hosted to review the national cyber security plans and decisions made at the ‘national cyber security strategy meeting.’ In addition, the national cyber security center was established to form cyber security plans, to support the operation of the national cyber security strategy/plan meeting, to collect, analyze and distribute the information related to cyber threats, to check

the safety of the national information communication network, and to prepare and distribute the 「national cyber security manual」. In the event of a severe emergency, this organization takes comprehensive control over the private/government/military to cooperate with relevant organizations.

1.2.2 Ministry of National Defense

As the scope of cyber terrors and crimes has been advancing rapidly beyond personal damages to a level that can destroy the national infrastructure and security networks, the Ministry of National Defense is trying hard to cope with this futuristic information warfare and to improve the level of online information security by establishing defense cyber crisis management systems.

According to the “National Cyber Security Management Rules,” the Ministry of National Defense performs cyber security activities in the area of national defense. Accordingly, the Ministry of National Defense operates a national information warfare center to take the full responsibility for cyber security at the level of national defense. Safety checkup, alarm issuance, investigations of crimes and relevant reporting on each unit’s information communication networks are performed separately.

The national cyber warfare center started off as the “information warfare team,” and was established by the Army HQ in July 1998 to support the protection of the main military information system. It was later reorganized and expanded on November 1, 2003.

In January 2007, the national defense information security education center was opened to train the special manpower for national defense and all the personnel in charge of information security at the army. CERT members are provided with special training on information security.

1.2.3 Ministry of Public Administration and Security

According to the “Framework Act on Informatization Promotion,” the “e-Government Act,” the Digital Signature Act, the “Act on the Protection of Information and Communications Infrastructure, and the ”Act on the Protection of Personal Information Maintained by Public Agencies,” the Ministry of Public Administration and Security carries out information security measures in the public sector and the personal information protection business.

To strengthen the capacity of the national organization to respond to cyber attacks, the NCIA (National Computing and Information Agency) and the regional development centers and the cyber invasion response centers were implemented in 16 cities and provinces. Since the DDos attack of July 7, 2009, it has been cooperating with relevant organizations to establish a large-scale cooperation system spanning the entire government.

To strengthen the information security and certification systems, a systematic integrated certification and privilege management system spanning the entire government is managed according to the degree of importance of each information system and the appropriate level of security, and the separate user certification and privilege management systems existing for each service are integrated with each other. Many other efforts are made to create a certification environment that is suitable for the advancement of the e-government service. In addition, to ensure the authenticity of all the e-documents throughout the phases of production and distribution, the e-document authenticity confirmation center is implemented and operated.

The Ministry of Public Administration and Security enacted and announced the “Personal Data Protection Act,” which suggested the principle threat personal information handling applied to all public and private sector companies (law no. 10465, proclaimed on March 29, 2011, executed on September 30, 2011) and prepared the enforcement ordinance for the same law in order to ensure the legal system is able to protect the privacy of individuals and prevent the unauthorized collection, leakage, misuse and abuse of personal information.

In addition to adjusting the legal systems to make sure that the right to personal information protection is ensured, the government is also strengthening its activities in the area of checking and managing personal information. The government diagnoses the degree of personal information protection at each target organization and strengthens the degree of personal information protection at the web sites that are the main routes of personal information leakages by implementing and operating an early-alarm system. Also, the government is currently operating a personal information invasion report center for private and public sectors, where the victims of personal information breaches can receive quick and fair help quickly and fairly. In addition, a ‘personal information disputes arbitration commission’ facilitates peaceful resolutions between parties to disputes.

Moreover, to strengthen the abilities of the persons in charge of information security, training is provided to information security officers in central and local self-governing organizations, workshops are hosted for the CPO (Chief Privacy Officer) at each organization, and various types of training video are distributed to government officers and carriers.

On the other hand, the National Police Agency, under the supervision of the Ministry of Public Administration and Security, has established and operated the CTRC (Cyber Terror Response Center) to unfold various necessary activities such as main hacking crimes prevention, criminal arrests, digital forensic officer education, and international cooperation related to cyber terrors.

1.2.4 KCC

The KCC (Korean Communication Commission) is responsible for information security in broadcasting and communication in the private sector, and helps all Koreans to enjoy a safe cyber environment by quickly responding to diverse threats in this dramatically changing environment, where broadcasting and communication are becoming seamlessly converged.

The KCC's cyber safety activities in the private sector are based on the "Act on Promotion of Information and Communications Network Utilization and Information Protection, etc." The KCC determines and posts guidelines for information security, manages and supervises organizations that diagnose the security and information security, and carries out the business of certifying information security management systems.

First of all, to improve its capacity to provide advice on information security, KCC launched its internet information security discussion board in 2009 with the aim of deriving plans to handle the newly-emerging information security issues. In July 2008, KCC announced the 「Comprehensive Plan for Internet Information Security」 and in December 2010, it announced the "Comprehensive Plan for Smart Mobile Security" in order to respond to the potential security threats related to the widespread use of the mobile internet. The KCC is currently pursuing many projects to protect services, infrastructures and users, as well as to establish the basis for protection.

To better handle and prevent internet attacks, KISC (Korea Internet Security Center) was established within KISA (Korea Internet&Security Agency) in December 2003, to respond to internet attacks in the private sector. Currently, a cooperation system has been established with security companies and internet service providers.

In addition, to promote the level of information security for those subject to information security diagnosis and to improve their capacity to respond to incidents, simulations of internet security incidents are provided. To unify the safety diagnosis system with the ISMS (Information Security Management System) at a higher level, the government prepared the revision of the "Act on Promotion of Information and Communications Network Utilization and Information Protection, etc." To reduce the potential for personal information exposure, KCC aggressively pursued an alternative to the use of resident registration numbers for website registration, called i-PIN. By strengthening its technical capacity and checking the status of personal information management, KCC is making every effort to provide on-site inspections for internet service providers, portal companies, mobile communication carriers, companies with large amounts of personal information in the DB and companies who already experienced information exposure incidents.

From a legal perspective, beginning with the DDoS attack on July 7, 2009, many lawmakers began to revise and enact laws related to information security. To prevent the generation and distribution of Zombie PCs and sites used as the source of malignant codes, great efforts were made to enact the 「Act on Prevention of Distribution of Malignant Programs」.

1.2.5 Ministry of Knowledge Economy

Under the 「Act on Information and Communication Industry Promotion」 and the 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」 The Ministry of Knowledge Economy fulfills its responsibility to promote the knowledge information security industry and train special manpower. The Ministry of Knowledge Economy recognizes the global market demand in information security industry and the social requirements for globalization, functional integration and convergence. Thus, the Ministry newly defines the ‘information security industry’ as the ‘knowledge information security industry.’ In 2008, to make the knowledge information security industry a driving force that can create new markets, the ministry established the “Securing Knowledge Korea 2013” plan. This plan is a comprehensive plan for acquiring global technology abilities, expanding the markets and manpower, and improving the competitiveness of exports, which can enable Korea to achieve its vision of becoming one of the world’s top three knowledge information security countries. Many efforts are being made to expand the market to KRW 18 trillion by 2013.

First, to acquire the necessary global technology abilities, the ministry is pursuing policies that promote the development of key original technologies and improve the R&D capacity of Korea’s small and medium-sized knowledge information security companies. In addition, the ministry is promoting the commercialization of R&D outcomes and security technologies developed by companies. Step-by-step plans to transfer the national security R&D outcomes to the private sector are being pursued.

In addition, security consulting in areas such as vulnerability analysis is being provided for small and medium-sized companies that have poor IT security infrastructure but hold key technologies. By expanding the market demand for products and providing information security consulting, the best efforts are being made to promote the industry. On the other hand, the “knowledge information security MS program with employment contracts” and the “demand-customized industrial site key manpower training program” are contributing significantly to resolving the imbalance between supply and demand in the field of knowledge information security, while laying a foundation for industrial growth.

From the perspective of improving the competitiveness of exports, the ministry is providing translation help for exports and advertising support for domestic knowledge information security companies, and is hosting business consulting sessions and exhibitions to lay the stepping stones for foreign market exploration.

2. Main Information Security Policies and Strategies

2.1 Ubiquitous Information Security Strategies (’06.12)

As Korea has rapidly advanced into the era of ubiquitous environment, which has seen many innovations that affect the daily lives of Koreans, including the advancement of the

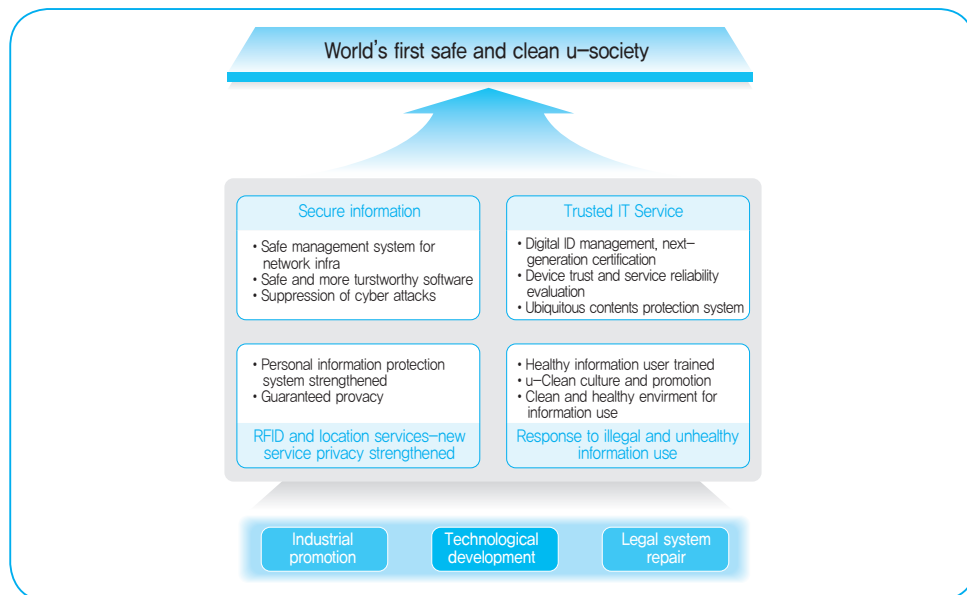
information society and the convergence of ICT with other industries, there have also been many adverse effects, such as the gap between technology and culture and invasions of privacy.

Therefore, it became necessary to suggest a comprehensive policy that could help Koreans benefit from various ICT services in the ubiquitous environment with its many new threats. So, in December 2006 the Korean government established the 「Basic Strategies to Protect Information in the Ubiquitous Age」 which can help Koreans safely use ICT services in the areas of finance, medical service and education, while protecting their privacy and promoting the healthy use of information.

The basic strategies for ubiquitous information security were expanded to comprehensively cover information security in u-Security, u-Privacy, u-Trust, and u-Clean. The strategy proclaimed that information security should be considered as a synthesis in the ubiquitous age, rather than an obstacle, from the perspective of user protection.

In terms of the main execution details, first of all, u-Security establishes the security plan for preventing cyber attacks and improving the response systems. u-Privacy prepares a protection plan to allow all Koreans to safely join the ubiquitous society. u-Trust is about preparing a reliable service system to allow the users to trust the broadband convergence system they are using. Finally, u-Clean implies that all the service users in the ubiquitous age can independently select good information and use it properly based on the national information ethics prepared by the government. The final goal is to implement a ubiquitous society by executing these detailed goals.

Figure 2-2 | Basic Strategies and Vision for Information Security in the Ubiquitous Age

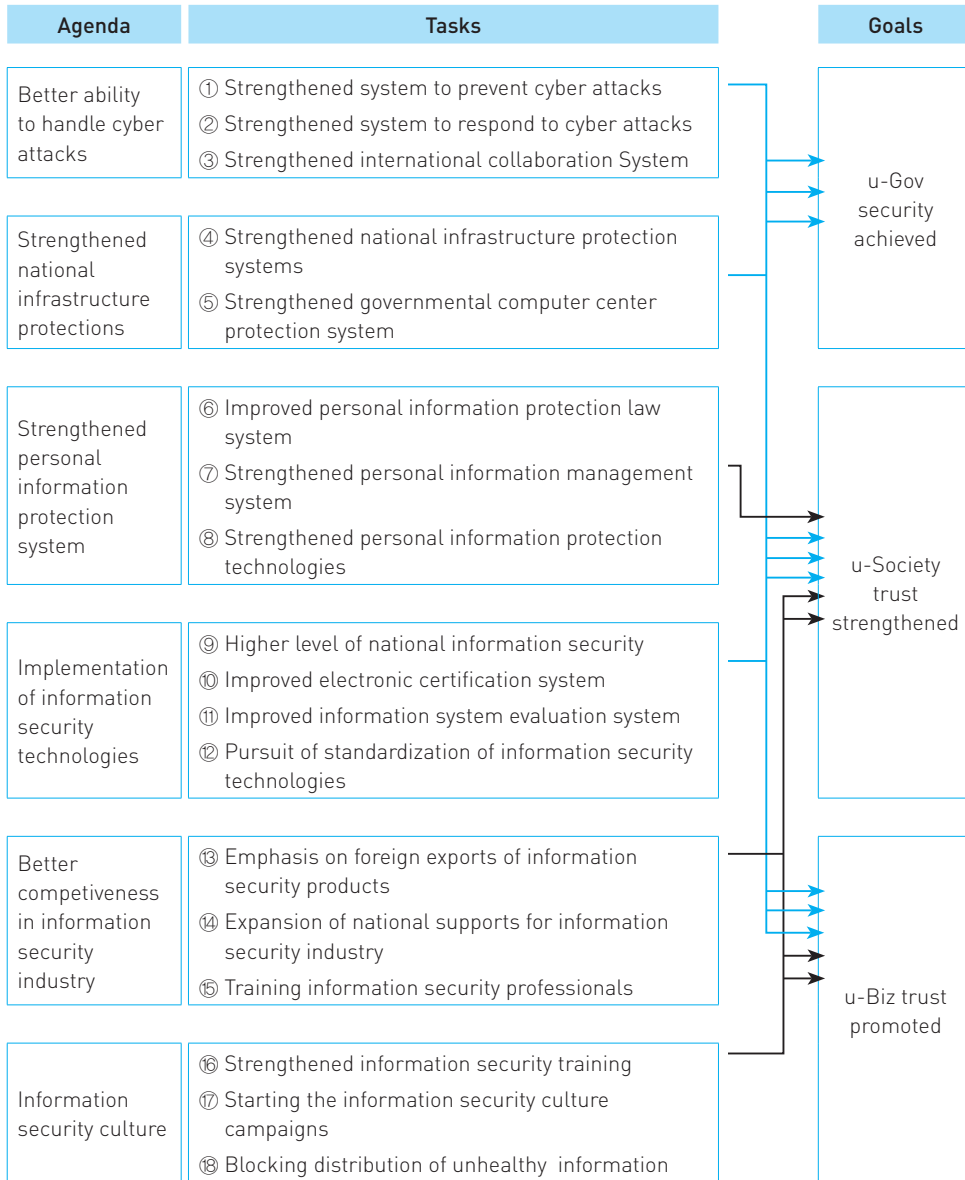


2.2 Long Term Comprehensive Plan for Information Security (July 2008)

The Korean ICT environment is advancing to reach the world's highest level with the help of various efforts, such as the implementation of the ultra high speed IT network, the promotion of relevant industries and the pursuit of e-government. As various network technologies are converged and interconnected, we are now entering the phase of convergence with non-ICT areas, such as BT or NT. However, due to the exposure of confidential information through hacking, social confusion increased. As a result, it has become necessary to establish a systematic, national plan for information security. Since the mid-80s, Korea pursued an informatization plan and it now seems that we have settled in a stabilization period, but information security has been pursued singularly since the mid-2000s. It was concluded that the system/financial scales and the relevant infra and R&D efforts are all very poor. Thus the government decided to implement the key infrastructure step by step using a comprehensive plan. In July, 2008, the government finally established the 「Long Term Comprehensive Plan for Information Security」.

The long term comprehensive plan for information security is comprised of six agendas, including 1) improving the capacity to handle cyber attacks, 2) improving protection of national infrastructure, 3) strengthening the personal information protection system, 4) implementing an information protection infrastructure, 5) improving the competitiveness of the information security industry and 6) implementing an information security culture, as well as 18 main tasks and 73 detailed tasks (See the table below). Under this plan, the government envisions its ambition to establish a safe and trustworthy ubiquitous society by ensuring the security of the e-government service, at the same time eliminating the anxieties of citizens and achieving confidence in business activities.

Table 2-1 | Long Term Comprehensive Plan for Information Security: Agendas and Task



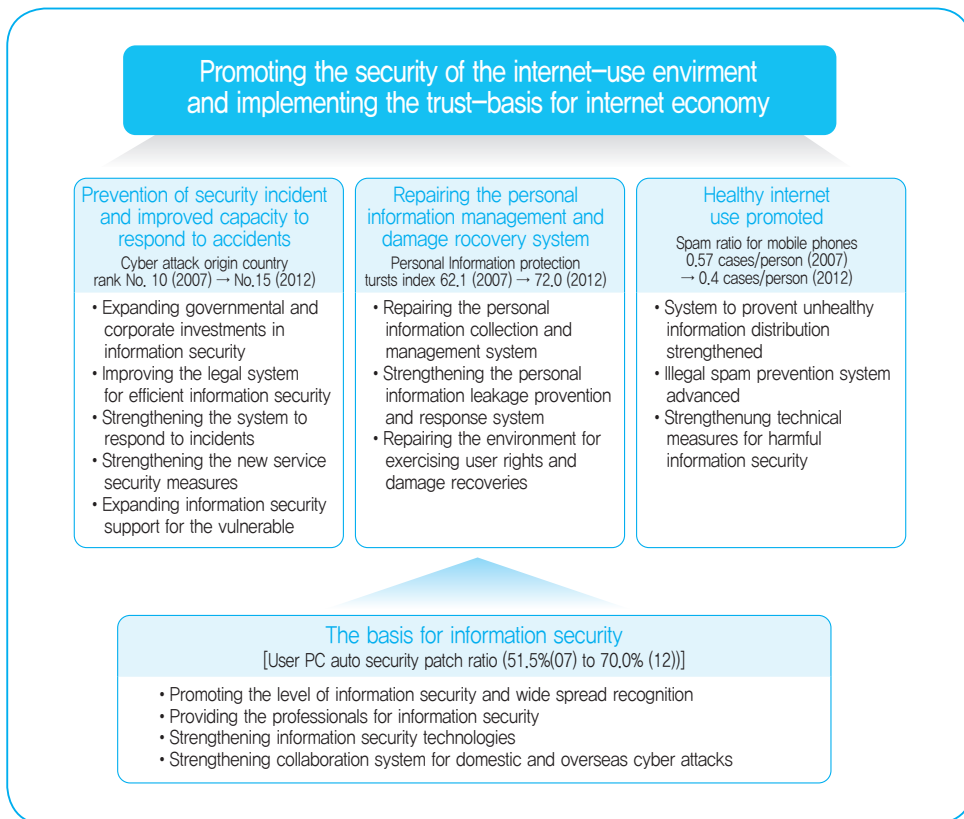
2.3 Comprehensive Plans for Internet Information Security (July 2008)

Despite the fact that Korea is a leading country in ICT infra implementation, the trust basis for internet use proved to be very weak, as indicated by many incidents, such as the shutdown of a stock trading company’s webpage through DDoS attacks, information leakage from a financial institution through wireless LAN hacking, large-scale personal

information leakage due to the hacking of an internet shopping mall, and others. Therefore, the Korean government announced the “Comprehensive Plan for Internet Information Security” in July 2008.

This plan sets the goal of promoting the security of the internet-use environment and implementing the trust basis for the internet economy, and establishes four major strategies—accident prevention, improving ability to respond to accidents, repairing the personal information management and damage recovery system and implementing the information security basis. These are accompanied by the detailed tasks to achieve these strategies.

Figure 2-3 | Comprehensive Goals and Strategies for Internet Information Security

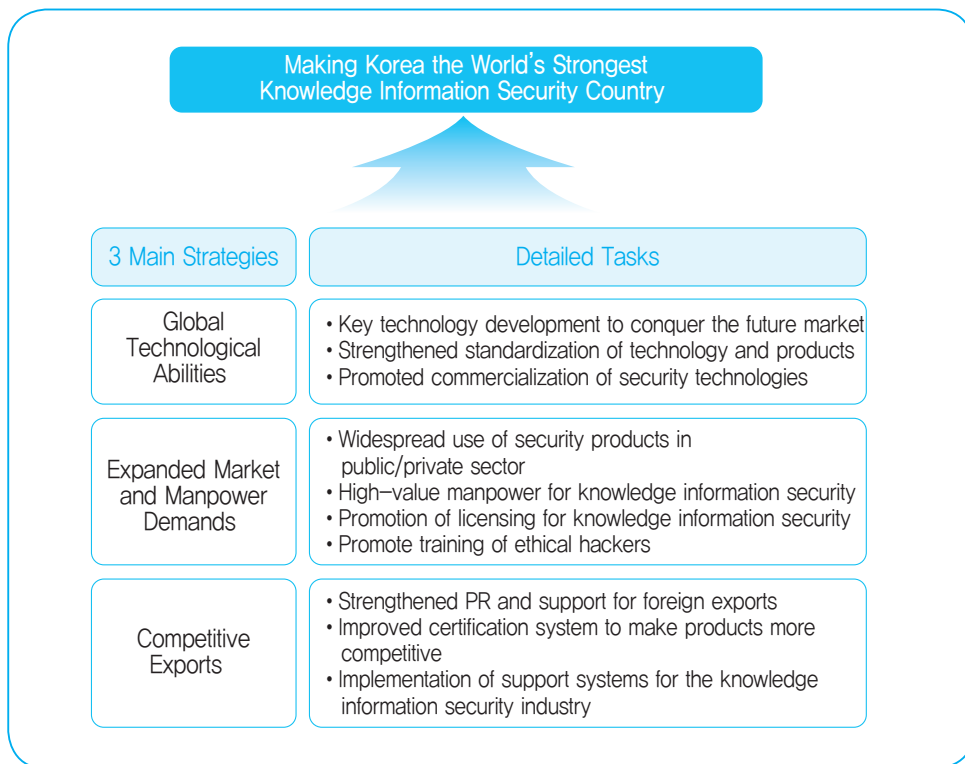


2.4 Comprehensive Plan for Promoting Knowledge Information Security Industry (December 2008)

Although the world's knowledge information security industry market has been growing at a high annual growth rate of more than 10%, as the USA and the EU occupy most of the market, the imbalance in the market share has been very severe. As the ICT industry develops, the security functions are being incorporated into various fields of industry. As a result, the knowledge information security industry is emerging as a new blue ocean, which requires the support of the Korean government.

The 「Comprehensive Plan for Promoting Knowledge Information Security Industry」 announced by the Korean government in December, 2008, aims to construct a strong knowledge information security country. The plan has three major strategies; acquisition of technological abilities, expansion of market/manpower demand and strengthened competitiveness in exports. These goals are accompanied by detailed tasks.

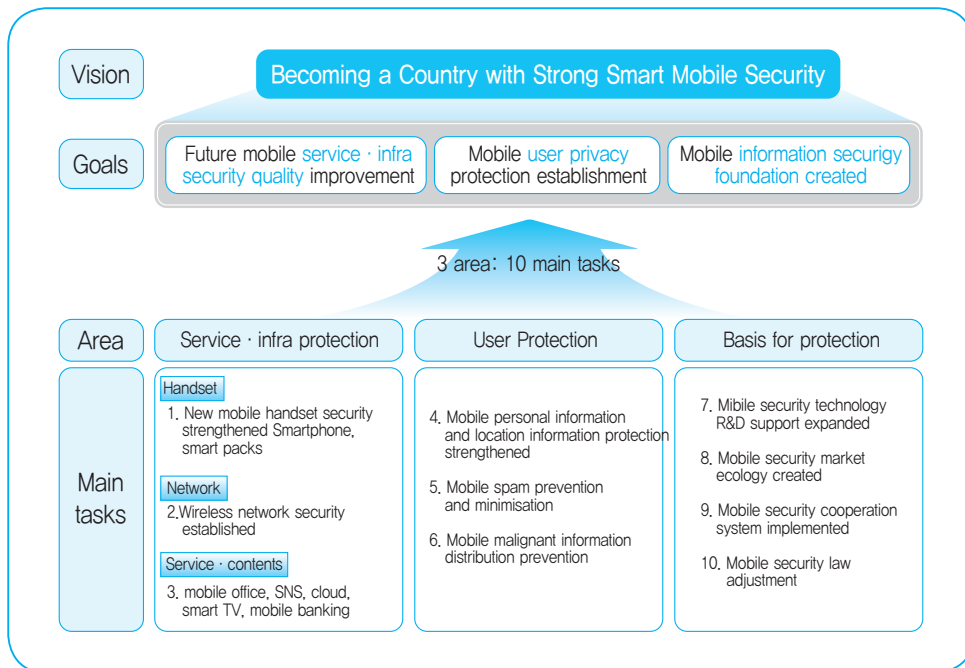
Figure 2-4 | Vision of the Knowledge Information Security Industry: Its Strategies and Detailed Tasks



2.5 Comprehensive Plans for Smart Mobile Security (December 2010)

The total number of accumulated smartphone subscribers in Korea is expected to exceed 30 million users in 2013 and 40 million users in 2015. This paradigm of shift to the mobile internet is also causing new security threats, which calls for more strict social requirements for mobile security. Therefore, the government has decided to pursue ten main tasks for service/infra/user protection and establishment of the foundation for protection under the three main goals: improvement of the future mobile service, infra security quality and establishment of mobile user privacy protection guidelines, and establishment of the basis for mobile information security.

Figure 2-5 | Comprehensive Plans for Smart Mobile Security: Visions, Strategies and Detailed Tasks



3. Development and Status of Information Security Law System

Let us now introduce the process by which Korea developed its information security law, then move on to the status of enacted and revised laws.

3.1 History

3.1.1 Early Phase of Information Society in the 20th Century (1980~2000)

With the informatization campaign pursued by the government since 1980, the adverse effects have also been emerging, forcing the government to work aggressively to amend the laws related to information security. The 「Act on Expansion of Dissemination and Promotion of Utilization of Information System」 enacted in 1986 is the first Korean law related to informatization, and defines the governmental policies and systems for informatization. This law includes some provisions related to network protection, but it does not recognize or focus on the importance of information security. It was the 「Framework Act on Informatization Promotion」 enacted in 1995 that emphasized the importance of information security in the public sector, and various policies and announcements were made in relation to this. In addition to the contents related to informatization promotion, this law includes the basic rules for information security.

As the internet became widely available, the scale of online transactions expanded. In 1999, to protect the information distribution and the main information of individuals and companies, the “Digital Signature Act” was enacted, and the “Act on Promotion, etc. of Utilization of Information System” was thoroughly revised to become the “Act on Promotion of Information and Communication Network Utilization and Information Protection, etc.” This series of legislative actions illustrate the government’s effort to redefine the rules to contain the adverse effects of informatization.

3.1.2 Phase of Entering the Advanced Information Society (2000~2006)

As Korea entered the year 2000, the national and social reliance on the IT system deepened. As a result, it became necessary to repair the information security law system from the perspective of national security. This was essential to avoid potential destruction of the national and social key information and IT systems threatened the national security, caused social and economical losses, and threatened personal freedoms and rights.

In 2001, to protect the important IT infrastructures for our society and country in the fields of finance, communications and energy, the “Information&Telecommunication Infrastructure Protection Act” was enacted. Also, a new criminal law was made to punish

the criminals who steal from others properties by entering false information or unlawful commands in a computer or information processing device. The existing “Act on Promotion, etc. of Utilization of Information System” was renamed the “Act on Promotion of Information and Communication Network Utilization and Information Protection, etc.” in an effort to strengthen the rules for information security. The same law was significantly modified following the large-scale internet incidents that occurred in January, 2003, to respond properly to such incidents. In addition, the punishment rule to minimize the victims of personal information leakages or advertisements transmissions was further strengthened.

In 2005, to protect the national IT network from cyber attacks that can threaten the national security, such as hacking and viruses, the “National Cyber Security Management Act” defining cyber security organizations and operation was issued under the president’s order. In addition, as Korea advanced to become a knowledge information society, various information systems were introduced and operated. However, there was no proper system to systematically manage them, causing investment overlap and poor compatibility between each system. To resolve these problems, the “Act on the Efficient Introduction and Operation, Etc. of the Information Systems” was enacted. As a result, information system supervision became available using the IT architecture.

Also, in 2006, in cases in which a national core technology leakage can severely affect the national security, or in cases in which exports of key national technology are not reported or are falsely reported, various actions such as interrupted exportations, prohibition or recovery of the key technology became possible under the “Act on Prevention of Divulgence and Protection of Industrial Technology.”

3.1.3 Phase of Implementing the Knowledge Information Society (2007~2011)

During this period, Koreans began to realize that implementation of the so-called knowledge information society is the main goal of national informatization-sharing the information resource to improve the national competitiveness and the quality of life. Therefore, in 2007, the existing “Act on the Promotion of the Electronic Administrative Services for the Realization of the Electronic Government” was renamed the “e-Government Act,” and other efforts were made to implement the e-government. In addition, the “Information&Telecommunication Infrastructure Protection Act” was revised to improve the system for checking the execution of protection measures for the main communication infrastructure, and the “Basic Logistic Policy Act” that describes the implementation of the national integrated logistic DB was revised.

In 2008, as the government organizations were reorganized, the responsibilities of the Ministry of Information and Communication were handed over to the KCC, the Ministry of Public Administration and Security and the Ministry of Knowledge Economy. The names

of the information security related departments were changed to reflect many changes in the informatization and information security systems.

In 2009, as the government became more interested in information security, the informatization-related laws were amended, and various efforts were made to strengthen information security. The “Framework Act on Informatization Promotion” was integrated with the “Act on the Efficient Introduction and Operation, Etc. of the Information Systems” and finalized in the “Framework Act on National Informatization.” The “Act on information communication industry promotion” was enacted to create the foundation for information security industry promotion.

In 2010, the “Act on Establishment of Basis for National Informatization and Defense Information Resource Management” was enacted to reflect the further development of information security in the area of national defense. In addition, the “e-Government Act” was completely revised, and endless efforts were made to improve the system for information security development.

In 2011, the “Personal Information Protection Act” was enacted to cover the private and public sectors, and to yield a principle of personal information handling that satisfied international standards. By strengthening support for damages resulting from personal information breaches, individual privacy could be protected and the rights and benefits of personal information could be guaranteed.

3.2 Main Status

Depending on the objectives of enactment and the functions, Korea’s information security laws and systems can be classified into national security protection related laws, laws related to the prevention of the leakage of important information to foreign countries, digital signature and certification related laws, laws related to the protection of information and communication networks and information systems, laws related to punishment of breaches, and personal information protection related laws, as follows:

3.2.1 National Security Protection Related laws

The laws related to national security protection govern the protection of national secrets or information that if leaked to foreign countries can threaten the existence of the nation, its safety and its democratic order; the classification of such secrets; and, the security business on such documents, materials and facilities pertaining to national secrets. On the other hand, the use of passwords, which were often used as a means to protect the national secrets in the past, is increasing in the private sector due to the development of communication tools and electronic transactions over the information and communication networks, which is leading to the reinforcement of the relevant legal systems. Password-related laws include: the “Security Business Rules,” the “Framework Act on National Informatization,” and the

“Framework Act on Electronic Commerce,” while the laws related to the illegal use of passwords include the “Military Criminal Act.”

3.2.2 Laws Related to the Prevention of Leakage of Important Information to Foreign Countries

The most frequently-cited law enacted to prevent the leakage of important domestic industrial, economical and scientific technologies, such as security information related to the national security, and advanced technology or devices, developed in Korea, to foreign countries is the “Act on Prevention of Divulgence and Protection of Industrial Technology.” This law states designation and change, approval of exports and prohibition of illegal leakages and invasions of key national technologies with very high technical or economical value in the Korean and overseas market that can have significant negative impacts on the national security and the development of national economy if leaked to the foreign markets.

The “Technology Transfer and Commercialization Promotion Act” prohibits the disclosure of a company or research institute’s confidential information by a person involved in technology transfers and commercialization. The “Promotion of Technology Projects for Joint Civilian and Military Use Act” grants the responsibility for maintaining the confidential information that a person learns while participating in joint civilian and military projects.

In addition, the “Unfair Competition Prevention and Trade Secret Protection Act” defines the type of punishment for a person who exposes important company confidential information to a third party in order to gain unfair profits or cause damages to the company, knowing that it will be used in foreign countries, actually using it in a foreign country, or preparing and planning to commit such a crime. As a result, the leakage of such information is heavily punished, and thus has proved to be effective in prevention.

3.2.3 Digital Signature and Certification Related Laws

As the information system and the information and communication network are developed further, transactions and businesses between remote places are promoted. This has made it necessary to reinforce the digital signature and certification related laws that can guarantee the safety and reliability of e-documents prepared by the information processing system, and promote the use of such e-documents. The digital signature and certification related laws include the “Digital Signature Act,” which can classify the scope of public certification for a non-profit organization depending on the purpose of establishment, in order to create a fair competition environment and support the balanced development of the public certification market, and the “e-Government Act,” which defines the administrative digital signature and certification.

3.2.4 Laws Related to the Protection of Information and Communication Networks and Information Systems

Due to hacking, virus distribution and other cyber-attacks, there has been an increasing number of threats to the national and private information and communication networks and information systems. As a result, it has become necessary to prepare systematic protection measures at the national level.

The laws related to the protection of information and communication networks and information systems include: the 「Framework Act on National Informatization」, the “Act on the Protection of Information and Communications Infrastructures,” the “Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.” the “e-Government Act,” the “Framework Act on Electronic Commerce,” the “National Cyber Security Management Rule,” and so on. The “Framework Act on National Informatization” suggests information security and personal information protection as the main principles of national informatization, and includes them in the establishment of the comprehensive plans. The “Act on the Protection of Information and Communications Infrastructures” defines the protection systems and procedures for the main national information communication infrastructures. The “Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.” defines the necessary systems and procedures for achieving the security of information communication networks and personal information protection. The “e-Government Act” establishes the plan for improving the safety and reliability of an information system, and orders the preparation of security measures for electronic public services. The “Framework Act on Electronic Commerce” defines the plan for achieving security in electronic commerce. The 「National Cyber Security Management Rule」 defines the roles of cyber security management systems and each department responsible for the information communication networks of the central administrative organizations, the local self-governing organizations and the public organization.

3.2.5 Laws Related to Punishments of Attacks

Various laws contain punishment guidelines for those who cause national and social damages by stealing or falsifying information and attacking the information systems and the information communication networks through hacking, viruses and DDoS attacks.

The “Act on the Protection of Information and Communications Infrastructures” provides the guidelines for the punishment of invasions into the critical information infrastructure, while the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. provides the guidelines to the punishment of violations of the responsibility to maintain confidentiality, invasions into the information and communications networks, and so on. In addition, the “Act on the Electronic Trade Promotion” states the punishment guidelines for those who falsify the trade information

entered in the DB or electronic trade documents recorded on a computer file of a trade organization. The “Basic Logistic Policy Act” provides the punishment guidelines for those who falsify an electronic document, or use a falsified electronic document knowing that it was falsified, or who invade, misuse, leak or cause damages to the logistic information processed, stored and transmitted by the comprehensive logistic information network or the national logistic integration DB, or who invade or cause damages to the protection measures for the comprehensive logistic information network or the national logistic integration DB. In addition, the “Criminal Act” defines the punishment for those who commit fraud with computers.

3.2.6 Laws Related to Personal Information Protection

Of the various types of information that needs protection, personal information represents a significant portion. With the recent development of information communication technology, personal information security breaches have been on the rise. As public awareness of this problem grew, efforts were made to repair the relevant legal systems.

In March 2011, the “Personal Information Protection Act” was enacted. In September 2011, the same law was enforced. The “Personal Information Protection Act” was prepared to guarantee the rights and profits pertaining to personal information by eliminating grey areas that existed in personal information protection due to a lack of accepted principles of personal information protection and handling that govern the overall society.

The main content of the Act states that the scope of the “Personal Information Protection Act” covers all the personal information handlers in the public and private sectors, and it installs the personal information protection committee and prepares the protection criteria at each phase of personal information collection, use and supply. In addition, it strengthens the restriction of unique identification information processing and prepares the basis for restrictions on the installation of video information processing devices. Finally, it introduces the personal information impact evaluation systems, the personal information leakage notice and report systems, the group dispute arbitration system and the group law suit systems.

The personal information protection laws for the public sector include: the “e-Government Act,” the “Resident Registration Act,” the “Passport Act” and others. There also are individual laws for the private sector, and these include: “Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.,” the “Use and Protection of Credit Information Act,” the “Act on Real Name Financial Transactions and Guarantee of Secrecy,” Internet Address Resource Act,“ the “Framework Act on Electronic Commerce,” the “Digital Signature Act” among others.

Main Information Security Activities

1. Responses to Internet Attacks
2. e-government Security
3. Critical Information Infrastructure Protection
4. Implementation and Operation of a Safe Electronic Authentication System
5. Information Security Management System Certification
6. Information Security Check
7. Information Security Product Evaluation
8. Spam Prevention Activities
9. Personal Information Protection
10. Copyright Protection

Main Information Security Activities

1. Responses to Internet Attacks

1.1. Korea Internet Security Center (KISC)

1.1.1 Purpose of Establishment of KISC, and the Legal Background

To implement a unified cooperation system for organizations operating networks and support the handling of security incidents on computer networks in Korea, and to provide a single account for handling global incidents, the Korean government established KISC (Korea Internet Security Center) in 2003. The responsibility for this center is based on Article 48, Clause 2 of the “Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.”

Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.

[Article 48 Clause 2] To properly respond to invasion incidents, the KCC should perform the business defined in each of the following clauses, and if necessary, it can hand over all or part of such business to KISA. <Revised: 2009.4.22>

1. Collection and transmission of the information related to invasion incidents.
2. Forecasts and alarms related to invasion incidents.
3. Emergency actions on invasion incidents.
4. Other necessary actions on invasion incidents determined by presidential order.

1.1.2 History of KISC

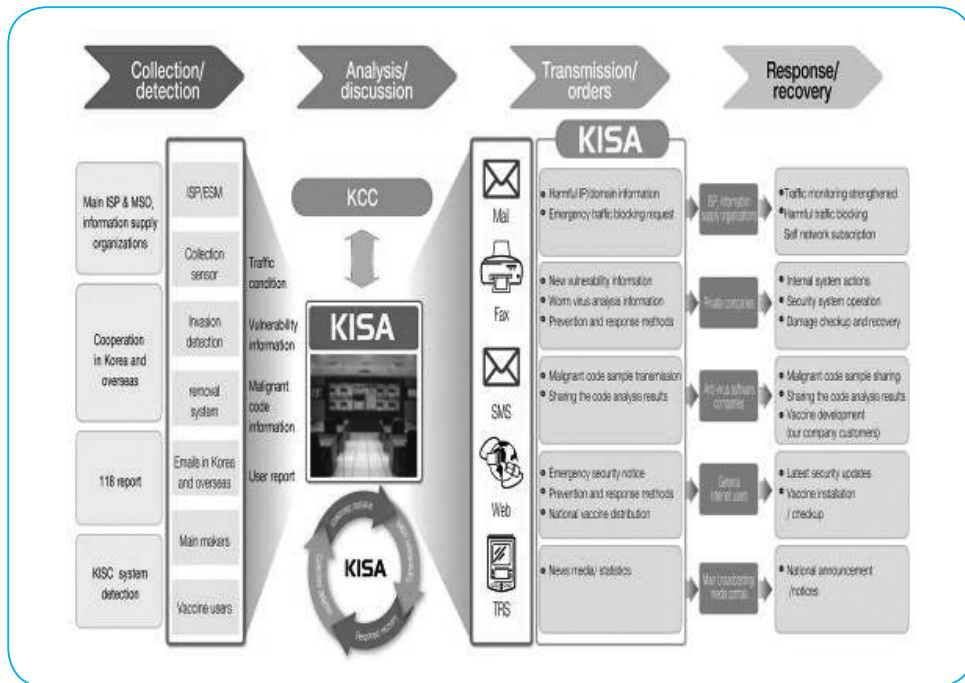
- 2003: Jan 25 Internet invasion incidents and opening of KISC (Dec. 2003)
- 2009: July 7 DDoS attacks responded to by KISC (36 sites under attack were causing access problems)
- 2010: Opening of comprehensive control room for KISA (Dec. 2010)&DDoS response projects pursued.
- 2011: Mar 4 DDoS attacks responded to (40 sites under attack returned to normal)

1.1.3 Main Business of KISC

- 24-hours and 365-days non-stop operation of comprehensive control room for early response and discovery of internet invasion incidents.
- Internet incident prevention and analysis, and strengthening of technology to prepare a quick response method for S/W security vulnerability and malignant codes abused in hacking.
- Hacking incident analysis, technical support and response capacity improvement to prevent and handle hacking damages in Korea.
- Common cooperation on domestic and foreign incidents for information sharing on internet incidents and prevention of further damages.

1.2 Security Incident Response Process and the Roles of the KISA

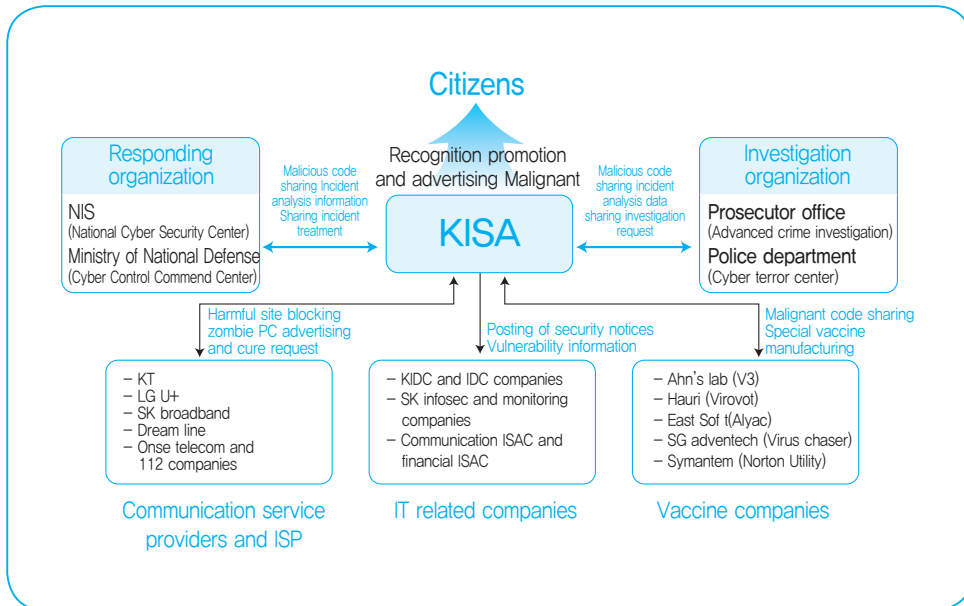
Figure 3-1 | Security Incident Response Process



More than 95% of all internet infrastructures are located in private networks, which indicate cyber security of the areas is of the most importance (targets of protection in the private sector: ISP, communication service providers, private companies, internet users). For cyber security in the private sector, KCC and KISA are maintaining close relations with communication service providers and security companies, and playing the following roles.

- Network protection:** By monitoring 24 hours a day for the signs of internet incidents in Korea, potential damages can be minimized and prevented from spreading.
- User protection:** Implement a “PC health” system for malignant code infections caused by hacking and worm viruses. Promote awareness of information security to strengthen user protection.
- Service protection:** Implement a comprehensive protection system that covers all new convergence services such as VoIP, cloud computing, smart mobile etc.

Figure 3-2 | The Role of KISA in Handling Cyber Security Incidents

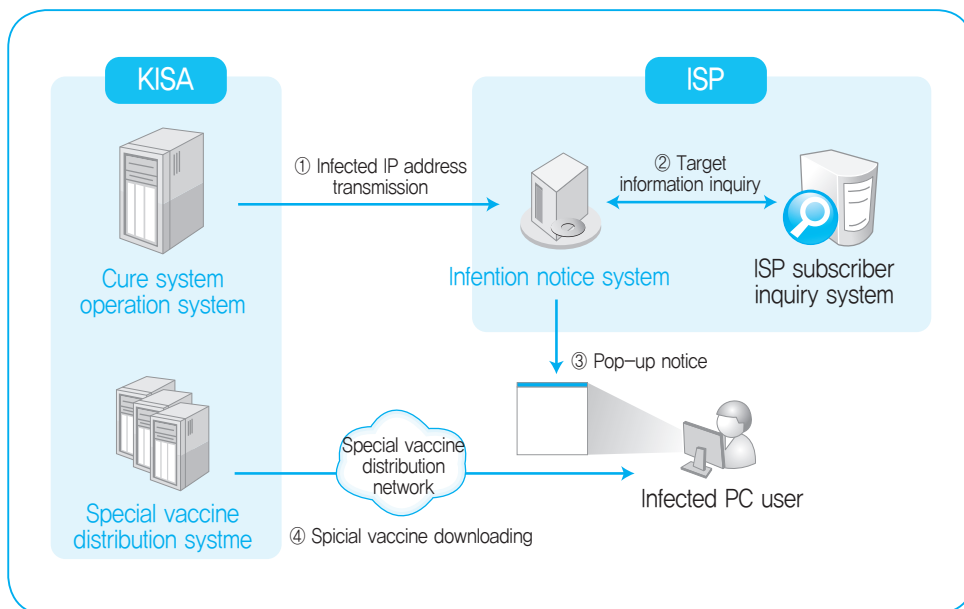


1.3 Main Activities

1.3.1 Infected PC Cyber Cure System Implementation and Operation

The July 7th DDos attack occurred in 2009 involved the use of approximately 115,000 zombie PCs over 3 days. The most important thing was to cure the infected PCs. After this incident, it became very crucial to implement a system that would immediately notify PC users of infections and provide means of cure. Therefore, in 2010, in cooperation with ISPs, the 「Infected PC Cyber Cure System」 was implemented. The infected PC cyber cure system uses a pop-up window to notify PC users of the fact that their computer has been infected by malignant code, and provides a customized special vaccine as means of cure.

Figure 3-3 | Infected PC Cyber Cure System Organization Chart



The details of the implementation and operation of the infected PC cyber cure system are shown as follows:

- Implementation and operation of a system that can quickly collect the IP addresses suspected to be infected by malignant codes, or the source of of DDoS attack.
- Implementation and operation of a system that can quickly inform the users of infected PCs of their PC's infection through interconnections with the ISP, so that they can receive proper treatment.
- Implementation and operation of a cure system in which the user who has been notified of his/her PC's infection can receive a special vaccine to remove the malignant codes.
- Implementation and operation of a special vaccine distribution system (server, networks) that can distribute a special vaccine to all Korean users from the vaccine company homepage in the event of an urgent incident.
- Pursuit of expanded detection of malignant bot control servers (C&C) by using vaccine companies through customized vaccine distribution business, as a way of performing virus curing and zombie PC curing simultaneously to speed up the response time.

1.3.2 DDoS Cyber Shelter Implementation and Operation

Frequently, DDoS attacks occur in a complex way over multiple ISP networks. As ISPs are sensitive to the security of their own networks but reluctant to take care of the internet interconnection regions (IX) where ISPs exchange internet traffic with each other, they can be directly exposed to DDoS attacks.

For this reason, by providing temporary shelters for those small companies that are unable to implement their own countermeasures for DDoS, greater service availability can be achieved, and the damages to small companies that lack good protection can be minimized.

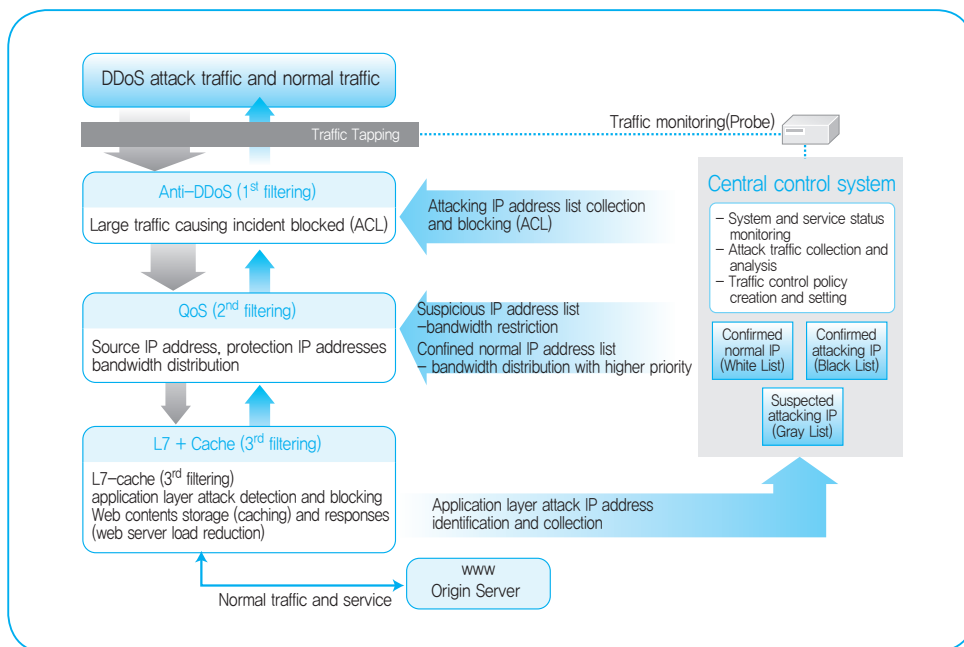
The details of the implementation and operation of the DDoS cyber shelters are as follows:

- The government provides DDoS shelter services for small companies unable to implement their own countermeasures for DDoS so that the damages from DDoS can be minimized.
- Implementing a network traffic detour system to provide DDoS emergency shelters.
- In the event of a DDoS attack, the traffic is redirected to emergency shelters so that the DDoS response system can remove the traffic and send the remaining traffic to the site under attack.

1.3.3 Strengthening the Level of Web Security to Block the Source of an Attack

Many web sites with security vulnerabilities are being abused as the source of malignant code distribution to cause DDoS attacks, personal information exposure and the like. To prevent potential internet invasion incidents and to promote the level of security for domestic web servers, KISC provides a remote inspection service for web vulnerability, WHISTL, CASTLE and other web security strengthening tools. By providing such services, KISC is helping administrators to improve the level of security for their web servers.

Figure 3-4 | DDoS Cyber Shelter Multiple Level Defense System



The details of the work performed to strengthen the web security level are as follows:

- Remote inspection service for web vulnerabilities to prevent web hacking incidents at small companies, non-profit organizations and penny traders who lack information security budget or management manpower.
- Distribution of web security strengthening tools such as WHISTL and CASTLE.
- Management, reporting and requests of detection results and pattern updates by providing the web shell detection patterns.
- Provision of web strengthening tools such as web security documents, and video information and hosting seminars for web site administrators and developers.

1.3.4 Implementation of a VoIP Service Incident Response System

To create an environment safe for users, that is robust against the security threats arising from widespread VoIP service, and establish perfect protection measures for smooth market settlement and service expansion, development of response technologies and improvement of legal systems to prevent security VoIP threats should be done in advance.

The details of execution by KISC to prevent VoIP service incidents are as follows:

- VoIP traffic monitoring system implementation and service security plan improvement.

- Environment implementation and operation, including developing a VoIP traffic monitoring sensor and collection technology.
- Development and distribution of VoIP incident response guidelines.
- Technical support for poor VoIP special category business to strengthen security.
- VoIP incident response discussion board organization and operation.

2. e-government Security

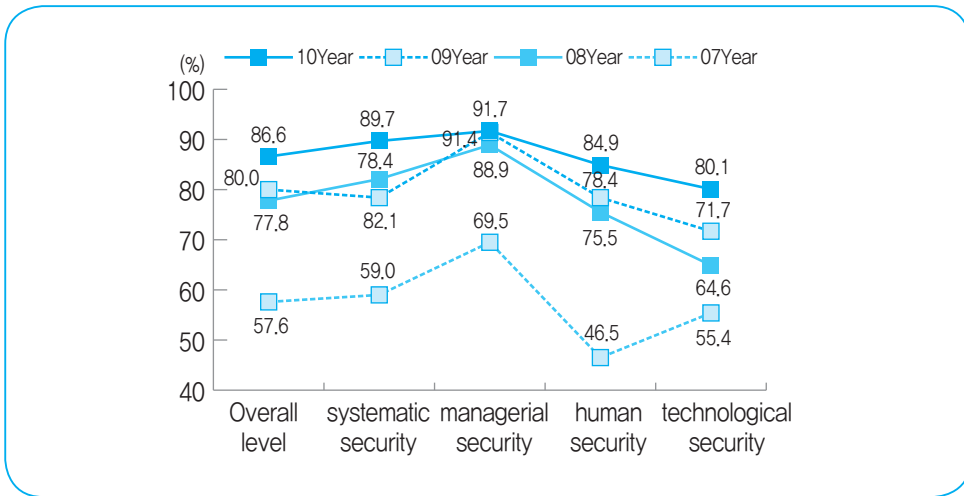
2.1 Promoting the Security Level of e-government Services

To improve the level of information security for e-government services in the areas of taxation, trade, bidding, and resident appeals (G4C, G4B, G4G) implemented and operated by the administrative organizations, the Ministry of Public Administration and Security performs annual investigations of the security level of e-government service according to Article 22, Clause 24 of the “e-government Act,” and establishes and executes a comprehensive security level improvement plan on this basis.

In 2007, in the very first annual investigations of the security level of e-government services, 295 central governments/local self-governing organizations nationwide were surveyed on a total of 501 services, either through written surveys or by visits, to investigate managerial/systematic/technical security levels. The results indicated that the overall technical security level was 55.4%, a very poor record. Thus, to address the vulnerabilities and prepare actions to improve each service, each administrative organization was asked to implement the security infrastructure.

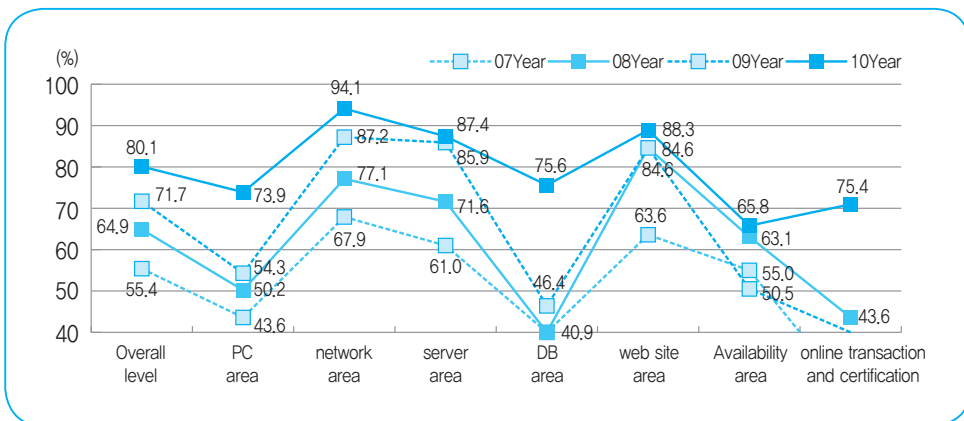
At the same time, in June 2009, the Ministry of Public Administration and Security revised the “Information Communication Security Business Rules” (Order of MoPAS) which was applied to the Ministry of Public Administration and Security and local self-governing organizations, in an effort to strengthen the security systems.

Figure 3-5 | Security Level of e-Government Service in Each Year (2007~2010)



In December 2009, the Ministry of Public Administration and Security published the web program development guidelines for web vulnerability improvement and pursued the ‘DDoS response system implementation project in cities and provinces’ as part of their efforts to strengthen the security level of e-government service.

Figure 3-6 | Security Level of Each Area of e-Government Service (2007~2010)



Through such efforts, from October 2010 to December 2010, the Ministry of Public Administration and Security investigated the security levels of 1,579 main e-government services operated by the central government and the local self governing organizations. The results indicated that the technical security level was improved to 80.1% from 71.7% in 2009, an improvement of 8.4%, and that the overall security level was improved to 86.6% in 2010, from 80% in the previous year.

Based on these results, the Ministry of Public Administration and Security has made a consistent effort to improve the security level by supplementing the security infrastructure. The ultimate goal is to improve the technical security level to 90% by 2012, so that all Koreans can use safe and reliable e-government services.

2.2 Considerations for e-government Service Security Improvements

By computerizing business procedures that used to be done using paper documents, e-government can implement a paperless work environment, improve business productivity and facilitate information and data production, accumulation, searching, sharing and transmissions. The ultimate goal is to provide the general public and governmental departments with increased business efficiency and convenience.

However, information security is emerging as the most critical issue in the process of actual e-government implementation. As 1) the diverse IT applied to implement an e-government has inherent vulnerabilities, 2) the heterogeneous-model-multiple-distribution environment causes an increase in complexity, 3) mutual compatibility requests are increased, and 4) a large number of unidentifiable people can access the e-government system and data over the wireless and wired network, the need to eliminate vulnerabilities and strengthen security has emerged.

Therefore, although in the early phase, e-government implementation mostly considered business productivity and convenience, as the issue of information security arose, security measures were gradually added to e-government. Since information security was not considered in the early phase, there have been difficulties adding new security requirements to the existing systems, and information security has not quite been systematic.

Considering many examples of actual e-government implementation in many countries, the following elements should be considered for the security of e-government:

- Establishment of the process for e-government service and information security
- Establishment of governance for e-government service and information security
- Establishment of technical architecture for e-government service and information security

2.2.1 Establishment of the Process and Governance for e-Government Service and Information Security

In general, the phrase ‘e-government’ may refer to computers and various IT devices that produce, process, store and share data. In practice, this is not completely wrong. However, to systematically implement and manage e-government services and information security, before introducing specific technologies and solutions, we must understand in advance what the desired business to be achieved by e-government is, what outcomes will be achieved, and what kind of values and responsibilities will be delivered.

It is obvious that IT is an indispensable element for improving productivity and competitiveness in this age of intense global competition. However, we must pay attention to what outcomes and values can be achieved by providing which service to whom, and by aiming at which goal. This process is necessary prior to guaranteeing that the e-government service and information security introduced can perform the desired functions. Therefore, such considerations and discussions are prerequisites to the execution of e-government service and information security.

The establishment of the process for e-government service and information security can only be successful if we carefully review the business content and the business process, and fully understand the roles/responsibilities and privileges of each stakeholder. Through such systematic and objective reviews, we can derive the advantages and disadvantages and the points of improvement for the existing business, and the resulting responsibilities that can be the essential basis for decision-making and judgment when starting the implementation of the e-government system and information security.

The establishment of the process for e-government service and information security should involve every stakeholder in e-government in order to share opinions, and the uppermost person in charge should be available for supervision. The process of such discussions and agreements should apply due procedures, rules, and verified methodologies if possible, and invite the participation of experts. Of course, in this process, unnecessary lobby by political groups or distortion of the original goals and intention by specific interest groups should be eliminated.

2.2.2 Establishment of Technical Architecture for e-Government Service and Information Security

To actually implement e-government service and information security, various IT methods are used and applied. The first goal is to provide service by computerizing the government business, which involves many stakeholders from different walks of life. Suburbs and big cities, central governments and local self-governing organizations, local small administrative organizations (resident centers), central government organizations-you

name it, all stakeholders have different types of jobs with different scales. As a result, there are many different types and levels of technologies applied to e-government service and information security.

Therefore, in such an organization and business environment, we are often faced with the heterogeneous-model-multiple-distribution environment, which leads to very strict technical integration, management and operation requirements. In addition, due to the dramatic advancement of technologies, the life cycle of IT is becoming shorter and shorter. As a result, the aging of existing technology is accelerating more rapidly, and there is always the possibility of being pressured to introduce new technologies and replace/abandon existing technologies. These varying technical innovations and environmental changes demand timely and accurate responses that utilize the limited technical abilities, costs and time to achieve the integration, management and operation of e-government services and information security.

Therefore, to be able to make the best of limited time, costs and system resources and continuously provide the best services for various stakeholders, we must introduce and apply a technical architecture for e-government services and information security. This technical architecture can be developed independently or introduced from the outside. The introduction and application of technical architecture for e-government services and information security require professional understanding and capacity, so we need to get advice from experts, or ask experts to systematically manage e-government services and information security by applying technical architectures.

Whether they are developed independently or introduced from the outside, the technical architectures should be verified, and if possible should have many references from other web sites. In addition, we must check whether such technical architectures can be handled in a cost efficient and timely manner. If we need to periodically revise technical architectures based on the environmental and time changes, then we must carefully examine whether the system can facilitate the management of such revisions and supplementations.

The department and personnel in charge of e-government services and information security should perform consistent technology introduction, operation, management, integration, disposal and detail/configuration management of such a technical architecture. All necessary businesses for e-government service and information security should be documented in standard formats based on this architecture, and properly observed.

In addition, the solutions and the products introduced to implement e-government service and information security could be used as a reference from the standpoint of a vendor, so they should support technical neutrality, interoperability, common use and stability, and fully comply with the international technical standards and specs. The process of introducing, procuring and contracting the solutions and the products should be done on a fair basis, and special attention should be paid to ensure that no specific vendor's solution or product is excessively introduced or purchased without a fair reason, as this will lead to

excessively high rates of market share, which in turn leads to the subordination of restriction of e-government service and information security to certain products or solutions.

2.3 National Computing and Information Agency (NCIA) Establishment and Operation

2.3.1 Background to the Establishment of NCIA

Since the second half of 2004, there has been consistent demand to accommodate information systems due to the increasing availability of computerized business for government organizations, and there also have been many organizations that are expected to have degraded administrative service quality and reliability, as the existing data room space/facility/equipment are lacking. In addition, as various e-government services such as G2B, G4C, and G2G were diversified and concentrated, and the implementation of e-government became a reality, the reliance of administrative works on the information system became more significant, and most of all, the demand for reliable and consistent service increased.

For this reason, it became necessary to efficiently use informatization investments and the operation and management budget for each organization, as well as to reduce the costs by adjusting the duplicate use of informatization budgets and commonly utilizing the computer environment, so that the reduced costs could be invested into new service development. In addition, it became very crucial to commonly utilize diverse information systems and their information, and as a result, it also became necessary to implement a systematic computer environment management plan, including the preparation and standardization of the service basis and information sharing.

Accordingly, the government took on the project to implement the National Computing and Information Agency (NCIA), which could reliably operate and manage the computer data resource for government organizations, and established the following directions for project execution.

- Implementation of the optimal e-government service basis by implementing the government integrated data center.
- Creation of an environment that members of the public and companies can access easily and conveniently.
- Allowing all government employees and members of the public to commonly use the knowledge and information of individual administrative organizations in order to improve the knowledge level of the entire society.
- Achieving economies of scale for data operation by common use of the data resource at the government level.
- Ensuring efficient protection of the important information system and implementation of backup systems to achieve reliability in national management.

2.3.2 Establishment of the Information Security System at the NCIA

As soon as the project to implement the National Computer Information Agency (NCIA) was confirmed, many organizations and experts expressed concerns over security issues. In particular, in the process of physically and logically integrating the e-government services many security issues were raised as follows:

- Potential of invasions and physical thefts at the NCIA building from the outside.
- Potential of damages to the NCIA building, such as forceful entry by criminals or terrorist attacks.
- Potential for external hacking of the operation server at the NCIA over the internet.
- Information leakages from the main organizations operating at the NCIA.
- Potential for simultaneous interruption of services to multiple organizations, such as Single Point Failures in the event that the NCIA experiences a failure.

To resolve such issues, the NCIA designed systematic and consistent management activities that can effectively handle the diverse security threats to information assets, such as hacking and viruses. By improving the security and reliability of the information asset and systematically managing and operating the procedures and processes, the basic goals of information security, such as confidentiality, integrity, and availability, can be achieved. For this purpose, perfect implementation of the information security system is required when opening the NCIA. In addition, an external protection system against physical invasions was implemented to protect the NCIA from terrorists' attacks.

When implementing the NCIA, the government designated it as the main national security facility to provide the utmost physical and technical protection measures. Prior to opening the NCIA, private security organizations such as the NCSC inspected the security level in order to eliminate potential security vulnerabilities existing in the process of establishing the NCIA.

2.3.3 Implementation of the Security Management System for the NCIA

The NCIA established the information security system to manage the security of the data network. The integrated security management system was established as an information security management system to establish managerial, physical and technical security measures in advance, and to apply systematic security controls as a foundation for a safe and trustworthy e-government. Therefore, by establishing information security measures for the NCIA against cyber attacks, and performing real-time analysis of harmful traffic such as worms and viruses and illegal access, the NCIA is able to protect information resources from external threats. In addition, by managing the status of security threats

to the information resource, vulnerabilities were analyzed and prevented in advance; by guaranteeing security, the existence of the data system was allowed. For this purpose, it is necessary to perform an analysis on events occurring in various security systems, such as entry blocking systems, entry prevention systems and password equipment, harmful traffic occurring over the network and security vulnerabilities in the information resource, so that the security policy can be complied with and integrated security management can be enforced.

Finally, the early detection and alarm system that could immediately detect security threats was established. By integrating automated security incident processing, an early response system for threats alarms and security information sharing was implemented. By processing a variety of event information and tracking the analysis information, the knowledge DB was implemented to manage the preceding records. Descriptions of each of the system are as follows.

a. Organization of the Information Security Management System

The NCIA established various policies and guidelines for the information security management system. First, through a quantitative and qualitative analysis of the information resource, one new security policy and eleven security guidelines were prepared. These include the following contents:

- Suggestion of efficient security operation guidelines for the safe operation of the NCIA.
- Reflection of each department guideline in the security policy and guidelines.
- Establishment of the information security guidelines and operation plans for the safe operation of the system.

By identifying the main information assets of individual departments expected to reside at the NCIA, a list of resources was prepared and the value of information security was assessed. Also, a plan was established for handling various threats and information security related to various departments and e-government project executions.

b. Implementation of the Integrated Security Management System

The most important goal of the NCIA is to provide a safe data environment for e-government service. Accordingly, to guarantee the security and reliability of the network, the NCIA had to make the following efforts.

- Guaranteeing security by additionally implementing the administrative networks in each line for internet access to public service and administrative services.
- Implementing efficient access control by implementing the public services web and the internet DB security areas, and the administrative business web and the administrative DB areas.

- Permitting communication between groups (organizations or tasks) in each security area, while prohibiting communication between different groups, in order to guarantee independence and security for residing organizations and e-government tasks.
- Guaranteeing safety with physically separated network structures, and duplexing by installing an invasion blocking system in each security area.
- Implementation of analysis systems and detection of harmful traffic to detect hacking, DDoS attacks and so on.
- Web/DB application's malignant code detection, blocking and web/DB server's illegal access control and audit record maintenance.
- Server security for system access control of insiders and unauthorized users.
- Automatic diagnosis of permanent vulnerability through analysis of resource vulnerability and vulnerability-based security incident correlation analysis.

Also, a security hacking analysis system that could prevent attacks after analyzing and detecting hacking attempts on the NCIA was implemented as follows:

- Collection of events from the security equipment for integrated monitoring, and correlation analysis of collected events to assess security threats and standardize events.
- Real-time monitoring of collected events and monitoring of the interconnected equipment's operation status.
- Correlation analysis to classify security incidents and vulnerability correlation analysis that compares the vulnerability analysis results, and invasion detection information to eliminate the possibility of false detection.
- Interconnection and management of security equipment for the resident organizations within the NCIA, and security equipment for the NCIA.

A very large-scale network is implemented in the NCIA for the execution of the described goals. In addition, with the government organization functioning as a gateway for internet connection, the analysis and removal of harmful traffic is indispensable. When there is harmful traffic, there are no normal services between the user and the server. In other words, the traffic contains malignant codes generated by attackers, or attack commands. Such traffic may mean an attack itself, but since the goal is to collect the information of the target before launching an attack, it must be detected and removed appropriately. The harmful traffic analysis system has the following functions.

- Real-time monitoring of the traffic trends by collecting the traffic information.
- Automatic detection of known and unknown harmful traffic and analysis of its origins by using the harmful traffic analysis functions.

-
- Provides interconnection analysis information of harmful traffic detected based on the vulnerability DB.
 - Auto registration of abnormal service details and classification of harmful traffic in abnormal services based on the network profiling details.
 - Using the invasion detection details and the harmful traffic trends to provide the organization administrators with real-time monitoring and the statistical data search functions.
 - Estimates of harmful traffic, trend analysis and correlation analysis (IP, port, events) with respect to all traffic.

For the e-government services of government organizations, the NCIA provides the network and server environment. The diverse data environments of the government organizations contain many vulnerabilities and risks. For this purpose, the threat management system is implemented to pre-detect the following potential vulnerabilities and risks that can arise.

- Event analysis information, and traffic analysis information and correlation analysis for comprehensive threat management at the NCIA.
 - Interconnection with other security products, such as the invasion blocking system and the invasion prevention system.
 - Resource value and security incident based risk evaluation management and invasion alarm setting.
 - Risk evaluation and map/graphic based monitoring of each equipment/group subject to supervision.
- Comparisons of each domain for comparative evaluation of the degree of risk, and setting of the reference values and various illustrations.
- Real-time search of the lasts analysis of security incidents in an integrated list.
 - The security processing results should be managed in the internal knowledge DB so that they can be used as reference later when processing similar incidents. Also, additional management is available, as the best practice.
 - Monitoring of the processing status of security incidents (# of processed /unprocessed cases)
- Graphical representation of unprocessed/processed security incidents for each type/degree of risk.
- Preventing event and analysis results (worm, security hacking, availability) from spreading and reoccurring in real time by performing detailed analysis, analysis result processing and early transmission.

- Providing comprehensive status diagrams (overall, by organization, tasks) for events and traffic.

As mentioned above, the NCIA design considers security issues at the time of implementation, and is systematically managed and operated.

3. Critical Information Infrastructure Protection

3.1 Overview of the System

3.1.1 Overview of Execution

As businesses that used to rely on existing offline infrastructures, such as e-government service, internet banking and industrial control systems, continue switching to online operations, reliance on IT and service is further intensifying.

The critical infrastructure and services that the government and the citizens are using are very tightly interconnected across the information communication infrastructures, so there is a very high likelihood that invasion incidents occurring in the information communication systems in the areas of administration, broadcasting, energy, and finance will spread further to those in other areas. In particular, the information communication infrastructures that connect the national infrastructures and significantly affect each information system can have a severe impact on the entire nation if they are invaded. For this reason, the government began to recognize information communication infrastructure protection as the main element required for social and economical stability and development. In 2001, the Korean government enacted the “Act on the Protection of Information and Communications Infrastructure.” The Act states that intense efforts should be made to manage the important information and communication infrastructures designated as the critical national infrastructures, and that their vulnerabilities should be evaluated and analyzed by the management organization so that short term and medium and long term protection measures can be established and executed.

Based on this law, many important information systems and communication networks were designated as critical information infrastructures, and their vulnerabilities were assessed and protection measure and plans were established in order to prevent electronic invasions in advance and establish the foundation for handling and recovering from incidents.

3.1.2 Execution System

To effectively respond to electronic attacks on the critical information infrastructures, the facility management organization should cooperate closely with the central administration organization (responsible departments).

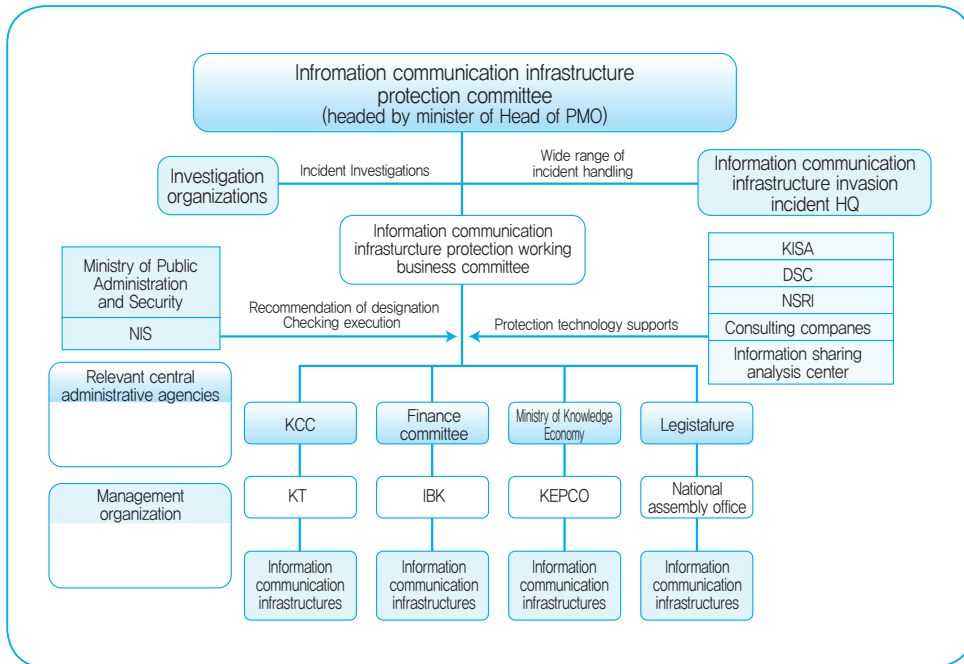
For this purpose, according to the “Act on the Protection of Information and Communications Infrastructure,” the Information Communication Infrastructure Protection

Committee supports reliable management and operation of the critical information infrastructures. The committee's responsibility is to comprehensively adjust and control the establishment and execution of information communication infra protection policy, so that the central administrative organizations can closely cooperate in the prevention and handling of invasions. This committee is headed by the head of the Prime Minister's Office (PMO), and the central administration organization's vice ministers have become active members of the committee. The main responsibilities are to adjust the critical information infra protection policies, to comprehensively adjust and execute the critical information infra protection plans, to improve the systems related to critical information infra protection and to review the main policies.

On the other hand, with the efficient operation and support of the information communication infrastructure protection committee, the information communication infrastructure protection working business committee was organized. This working business committee helps the efficient operation of the information communication infrastructure protection committee by reviewing the issues submitted to or consigned from the information communication infrastructure protection committee or the instructions received from the committee's head.

If an attack on the critical infrastructure covers a wide range of areas, then the information communication infrastructure invasion incident HQ is operated temporarily under the information communication infrastructure protection committee to provide emergency actions, technical support and damage recovery.

Figure 3-7 | Critical Information Infrastructure Protection System



The relevant central administrative organizations designate the critical information infrastructures and review the information communication infrastructure protection plan submitted by the management organizations before establishing and executing the plans.

The management organizations hold the primary responsibility for protecting the critical information infrastructures. To prevent attacks and handle them properly, they evaluate and analyze the vulnerability of the facility and establish protection plans. In addition, when an incident occurs, they notify the central administrative organization and the investigation organizations and recover the facility.

The supporting organizations for critical infrastructure protection includes: the Ministry of Public Administration and Security, the NIS, the Ministry of National Defense, the Police department and KISA. They provide technical support for the establishment of the protection plans and prevention and recovery from incidents. The NIS and the Ministry of Public Administration and Security support protection of the national and public organization and guidelines for preparing the main communication and information infrastructure protection plans, while the prosecutor’s office and the police department support criminal investigations.

3.2 Critical Information Infrastructure Protection Activities

3.2.1 Designation of the Critical Information Infrastructures

Those facilities subject to designation as critical information infrastructures include facilities operated by the private sector, as well as facilities operated by national and public organizations. They also include electronic control and management systems and information communication networks in the areas of national security, administration, national defense, defense, security, finance, broadcasting, transportation and energy, which can greatly affect the basic living conditions in Korea, including national security and economic stability, when they are attacked by hackers.

The Minister of Public Administration and Security and the head of the NIS can recommend the head of the central administration organization to designate a private or public information communication facility operating as the critical information infrastructure, if they believe it to be necessary.

The head of each central administration organization can designate it as the critical information infrastructure according to the five criteria, including its business value.

The five criteria suggested in the “Act on the Protection of Information and Communications Infrastructure” are shown in the following table.

Table 3-1 | Criteria for Designating the Critical Information Infrastructure

Classification	Designation criteria
1	Social and national importance of the business executed by the management organization.
2	Reliance of the business executed by the management organization on the information communication infrastructure.
3	Interconnection with other information communication infrastructures.
4	Scope of damages to society, the economy and national security in the event that invasion occurs.
5	Possibility of invasion occurrence, and ease of recovery.

Since the enactment of the “Act on the Protection of Information and Communications Infrastructure” in July 2001, the following facilities have been designated as critical information infrastructures: 23 facilities from 4 departments (1st, 2001), 66 facilities from 5 departments (2nd, 2002), 7 facilities pertaining to the Ministry of Information and Communication (3rd, 2004), 1 facility under the supervision of the National Election Committee (4th, 2005), 5 facilities pertaining to the Ministry of Information and Communication (5th, 2006), 10 facilities from 3 departments (6th, 2007), 8 facilities from

2 departments (7th, 2008), 21 facilities from 4 departments (2009), and 28 facilities from 4 departments (2010). As of August 2011, 11 central administration organizations and 103 management organizations are managing 153 designated facilities. In particular, in 2007, as serious incidents occurred such as VoIP service hacking and wire tapping, additional designations were made on the critical information infrastructures to strengthen the protection for the VoIP service.

Table 3-2 | Status of Designation as the Critical Information Infrastructures in Each Area

Administration	Administrative business system, etc.
Broadcasting	Internet access networks, etc.
Finance	Internet banking systems, etc.
Energy	SCADA systems, etc.
Construction and transportation	Navigation management systems, etc.
Social welfare	Insurance management systems, etc.
Other	Legal information systems, etc.

3.2.2 Vulnerability Analysis/Evaluation

Within six months after the management organizations designate a facility as the critical information infrastructure, its vulnerabilities should be evaluated and analyzed. In the short run, the management organization needs to remove the identified vulnerabilities of the critical information infrastructure, and in the long run, it should analyze the effects of invasion incidents in order to establish economical and effective protection plans by performing vulnerability analysis.

The vulnerability analysis/evaluation should be performed once every other year. In the medium term, a simplified vulnerability evaluation/analysis is carried out. Based on the “Act on the Protection of Information and Communications Infrastructure,” the management organization establishes a vulnerability analysis/evaluation team that can analyze and evaluate the vulnerability of the facility under their supervision. In addition, the management organization consigns the vulnerability analysis/evaluation business to other organizations such as KISA, the ETRI research centers, the information sharing analysis center or the knowledge information security consulting companies.

3.2.3 Protection Measures and Establishment of Plans

The head of the central administration organization that supervises the critical information infrastructure should establish and execute the protection plans each year according to the “Act on the Protection of Information and Communications Infrastructure.” The final

protection plan is prepared by comprehensively adjusting the protection plans submitted by the management organizations for the critical information infrastructure. The head of the central administration organization submits next year's protection plan to the information communication infrastructure protection committee for it to review. Once submitted to the committee, the protection plan is comprehensively adjusted and supplemented in the review process, which systematically reviews the direction of the protection plans announced earlier, compliance with the main considerations, items requiring supplementation and modification, and best practices that can be applied to other departments.

The critical information infrastructure protection measures and plans are very similar to each other, since they basically serve the same purpose from a managerial, physical and technical perspectives: to protect the critical information infrastructures. However, the protection measure consists of specific and detailed information security measures and businesses to reduce the risks identified by the vulnerability analysis and evaluation, while on the other hand, the protection plan actually includes the integration of such information at higher levels, or the selection of role model businesses from among the specific protection measures for wide application to the management organization. In other words, the protection plan is different from the protection measure, in that the central administration organization re-summarizes the protection measures submitted by each management organization.

The protection plan prepared by the central administration organization is based on the protection measures submitted by the management organization. A series of processes from vulnerability analysis evaluation to the establishment and execution of the protection plans can be illustrated as follows.

Each year, the management organization establishes the critical information infrastructure protection plan and submits it to the central administration organization. Since the enactment of the "Act on the Protection of Information and Communications Infrastructure" in 2001, it has been submitting the protection plan every year. In 2002, a total of 17 management organizations submitted protection plans for a total of 23 facilities. In 2009, 78 management organizations submitted protection plans for 109 facilities, while in 2010, 90 management organizations submitted protection plans for 126 facilities.

A protection plan can be broadly divided into two sections: first, it describes this year's accomplishments in comparison with the previous year. Second, it describes the next year's plan. In the next year's plan, the status and accomplishment section describes the details of the execution of the previous year's plan for the prevention, handling and recovery of invasion incidents and the related evaluation results. In general, the project plan included in the protection plan often involves the management organization directly or indirectly, as well as the central administrative organizations. In this sense, it is actually an integrated summary of the accomplishment from the protection measures. Also, the information security projects to be pursued in the following year are derived by reviewing the project plans for each management organization contained in the protection measures, and include the projects that have been selected for execution by the central administration organization.

3.2.4 Checking the Execution of the Protection Plans for the Critical Information Infrastructures

The Minister of Public Administration and Security and the head of the NIS can check the execution of the protection plans prepared by the management organizations.

3.3 Improvement of the Infrastructure Protection Systems

3.3.1 Changes in the System

Recently, as various electronic invasions techniques such as hacking, computer viruses and distribution of malignant code became more and more sophisticated, the scope of damages is broadening further. Amidst such threats, to protect the critical information infrastructures quickly and effectively, the weaknesses discovered during system operation have been continuously addressed.

First, the government prepared a new legal requirement that allows the Ministry of Public Administration and Security and the NIS to recommend the designation of the critical information infrastructure to the central administration organizations, so that the designation and recommendations functions can be executed smoothly. To implement a post management system for the protection plans, the Minister of Public Administration and Security and the head of the NIS can now check the execution of the protection plans. As there are only the procedural items governing the establishment of the protection measures by the management organizations, with no definition of the post check-up procedures, the management organization's protective measures could be merely documentation. For this reason, necessary action was taken to improve the effectiveness of the infrastructure protection measures. In addition, the range of technical support that the management organization could request was broadened, and the range of candidates for receiving technical support was expanded from the management organizations that included chairs of the local self-governing organizations to every management organization.

3.3.2 Direction of Future Execution

As mentioned above, though the system has been improved consistently, there are still problems that require attention. First of all, it is necessary to clearly define the role assignments between the NIS and the Ministry of Public Administration and Security. By clarifying their responsibilities in the comprehensive business governing the public and private infrastructure, we can implement a system that is fully committed to supporting the management organizations' duties to protect the critical information and communication infrastructures. In addition, by transferring the responsibility for making or cancelling the designation of the new critical information infrastructures to each department, the role of the central administration organization can be strengthened. But to prevent blind abuse of rights, when making or cancelling a designation, some kind of stipulation needs to be added

to the discussions between the NIS and the Ministry of Public Administration and Security. Currently, the NIS and the Ministry of Public Administration and Security are privileged to check the execution of the protection plans. A good solution to strengthen the role of the central administration organization could be to allow each department to check execution and notify the central administration organization. Finally, to reduce the burden of operation on the management organizations due to the designation of the critical information facilities, new financial supports should be provided, including tax or tariff exemptions or electricity bill discounts for the management organizations. As a result, we can prepare the basis for demanding stronger protection measures from the private management organizations. In addition, the private companies that are not designated can benefit from the system when they are newly designated.

4. Implementation and Operation of a Safe Electronic Authentication System

As the administrative environment for e-government has switched from being paper-based to e-document-based, the likelihood of attacks by hackers and exposure, falsification and damage of important data increased. Consequently, the reliability and safety of the e-government service became the number one priority. In addition, the government sought ways to guarantee the consistent distribution and safe recovery of the e-documents exchanged between the various administrative branches by preventing losses due to missing or damaged encryption keys.

The administrative digital signature authentication system was introduced in December 2000 when its system was implemented and operated. In December of 2002, the implementation of the public/private digital signature interconnection and authentication systems led to the completion of the actual e-government authentication systems. In February of 2006, the encryption key consignment and recovery management system was implemented to secure the continuity of administrative works and safe recovery.

In 2007, the advancement project for the administrative digital signature authentication system began to expand the scope of candidates for administrative digital signature certificates to public and financial institutions, and implement a reliable administrative digital signature authentication service by implementing the optimal system to replace aging equipment as demand was increased. In addition, to provide a certificate issuance service and online password use service for government employees, various projects were pursued, such as the implementation of security gateways, the advancement of the encryption key management system, the introduction of a load control/management system for integrated verification and privilege management, and the acquisition of extra disc space.

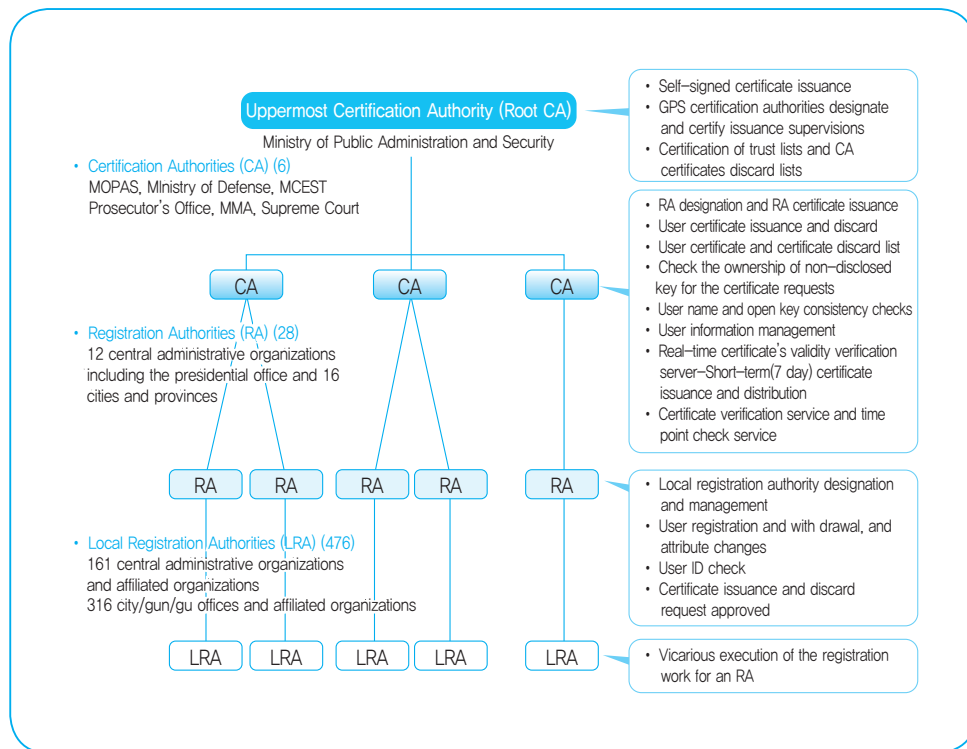
In 2009, the 'Next Generation Integrated Authentication System Informatization Plan' was established, and integrated authentication gateways were implemented to achieve the standardization of the integrated authentication framework. By 2012, these will be

distributed to all administrative branches. Considering the latest technological developments and business changes, the government is strengthening the security of the e-Government services, through means such as securing the authenticity of digital signatures and expanding the verification systems.

At the present, the Korean administrative digital signature authentication management system is comprised of the uppermost certification authority, six certification authorities designated by the Minister of Public Administration and Security, 28 registration authorities, and 476 local registration authorities operated and designated by the six certification authorities.

According to the ‘2011 National Information Security White Paper’ issued by KISA, as of December 2010, the total number of users for the administrative digital signature authentication system exceeded 1,318,682, and nearly 1,107 businesses are utilizing it.

Figure 3-8 | Administrative Digital Signature Authentication System Diagram

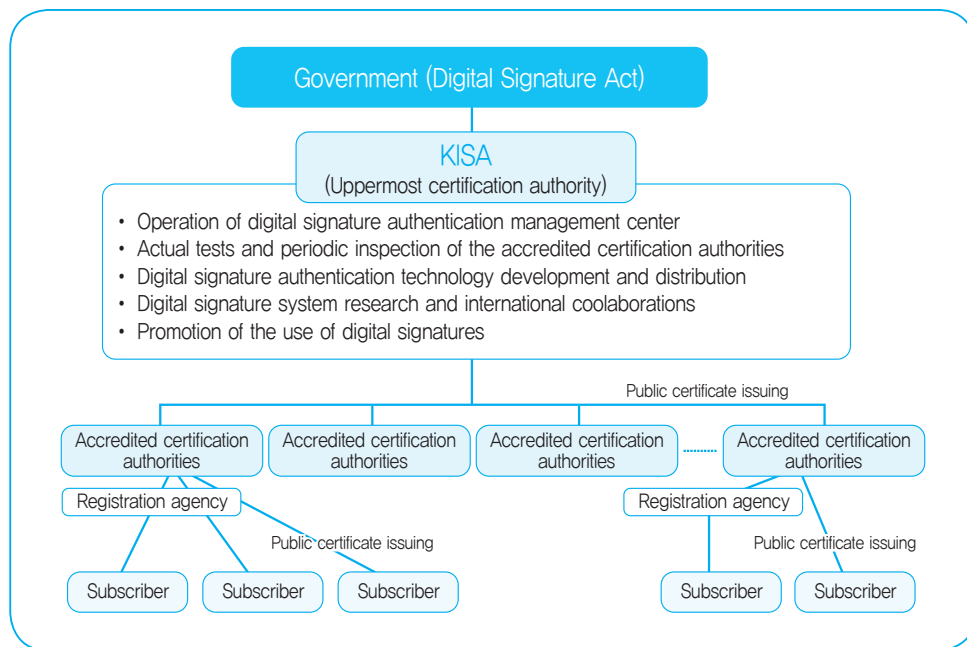


Source: Ministry of Public Administration and Security, Administrative Digital Signature Authentication Management Center

On the other hand, the Korean government enacted the “Digital Signature Act” in February of 1999, to create a safe for electronic transactions environment, to ensure the safety and reliability of e-documents in the private sector, and to efficiently manage the accredited certification authorities. Under this law, KISA was designated as the uppermost certification authority, and the complete public digital signature authentication system to issue and manage public certificates was implemented. In addition, to ensure convenience for public certificate users, a public certificate interconnection system was introduced in December 2001, in order to support electronic transactions for all banks by using one public certificate.

Since Signgate and KOSCOM were designated as accredited certification authorities in 2000, a total of five accredited certification authorities have been operating. An accredited certificate authority is designated by the Minister of Public Administration and Security, who reviews the candidate’s technical power, economic ability, and ownership of facilities and equipment that enables the candidate to safely implement and manage a public certification system.

Figure 3-9 | Public Digital Signature Authentication System



Source: KISA Korea Certification Authority Central (KCAC)

Table 3-3 | Status of Accredited Certification Authority Designations

Organization Name	Date of Designation	Goals of establishment	Characteristics
Signgate	February 2000	Public certification service	CO.
KOSCOM	February 2000	Stock trading computer system implemented	Co.
KFTC	April 2000	Bank-to-bank transactions	Non-profit organizations
Cross Cert Co.	November 2001	Public certification service	Co.
KTnet	March 2002	Automated trading	Co.

As the use of public certificates has been expanded to all electronic transactions due to the government policy to promote the use of public certificates, as of December 2011, a total of 26.55 million public certificates have been issued.

The volume of Korea's Internet banking was KRW 29 trillion 457.7 billion (the Bank of Korea, January 2010) and the average number of daily transactions was 28 million as of 2010. The number of Internet banking users accounts for 118.3% of the total population, which is significantly higher than 18.5% (based on the number of households) of the US and 35% of UK.

In the early phase of introduction, public certificates were mostly used for internet banking and online stock trading and other electronic financial areas. Recently, the scope of application is broadened to include all the areas of electronic commerce such as internet housing application, electronic civil appeals, end-of-year financial settlement and income tax report, electronic procurement, etc.

In addition, to strengthen the reliability of the ubiquitous environment, the device certification system that could detect and certify of various IT devices such as home devices, network cameras (CCTV), internet phones as well as human users and perform communication area encryption was implemented and operated.

Meanwhile, Korea had 14 Internet banking accidents reported and the amount of losses was KRW 0.23 billion from January to August 2009, while the US had the amount of losses of approximately KRW 135.2 billion in the 3rd quarter of 2009 alone. UK had the amount of losses of approximately KRW 66.4 billion in the 1st half of 2009 alone.

Government-led enforcement using public certificates has significantly contributed to growth of the Internet economy in Korea, however, PC-based Internet banking services, which were provided via MS Windows, used by most of the citizens faced a new obstacle,

Active X, as IT technologies including smart phone technologies have advanced and the patterns of Internet use have changed.

Due to high penetration of smart phones uses in access to domestic banks, security firms and shopping malls, they shifted their focus on the online banking and transaction market via wired Internet to mobile Internet. As mobile banking and transaction services significantly affect activation of mobile businesses and user conveniences, the policy of mandating use of public certificates (Article 7, the Rule on E-Financial Supervision, May of 2003) has emerged as a social issue in the mobile environment.

MS IE (Internet Explorer) accounts for over 98% of web browsers in Korea, so uses of public certificates has a relevance to MS IE. To use public certificates with MS IE, a user is required to install a plug-in called Active X, and smart phones do not support Active X of MS, casting challenges to operation of mobile Internet transaction services in the domestic market. Large credit card firms have suspended mobile transaction services, and domestic businesses are likely to fail in the competitions with overseas businesses like Amazon or eBay and be isolated in the global market due to difficulties in mobile transactions.

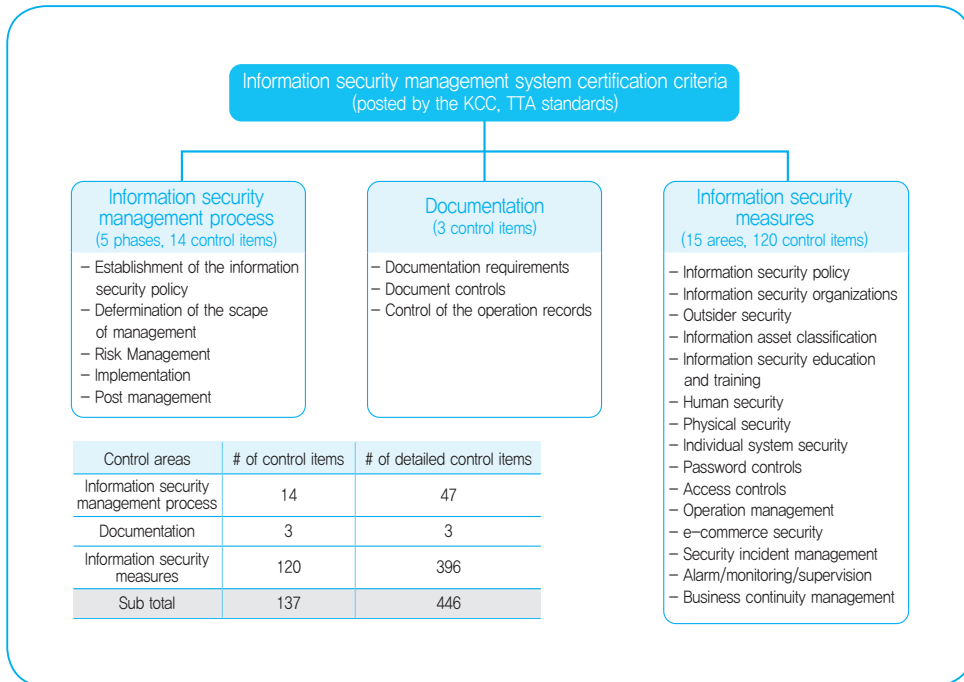
To this end, the government changed the banking services based on public certificates, as part of its efforts to respond to changing Internet banking environment. As the technical standards for public certificates have already been tech neutral, software of public certificates was completed with various technologies such as Java. The government encouraged uses of Java-based public certificate software for minority users using Safari, Opera and Firefox. The government also developed a dedicated program (common apps) for smart phone users to build a safe smart phone banking environment by distributing public certificate software completed with non-Active X technologies.

5. Information Security Management System Certification

5.1 Overview

The ISMS (Information Security Management System) is a comprehensive information security system that has the purpose of achieving reliability and trust in the information assets belonging to an organization. The ISMS certification criteria are shown in the following figure, and are comprised of the information security management process, the documentation, and the information security measures. To implement and operate the ISMS, you must first identify the information assets of the organization. Next, you need to analyze the risks of the identified information assets, and select and implement the information security measures. Finally, through post management such as consistent monitoring and internal supervision, you need to make steady efforts to improve the system during operation.

Figure 3-10 | ISMS Certification Criteria

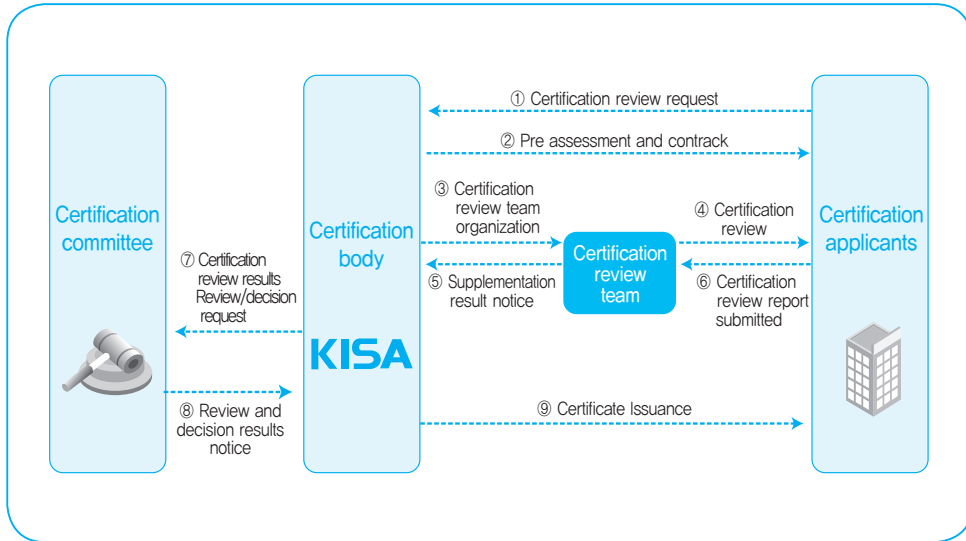


Source: KISA, isms.kisa.or.kr

The Information Security Management System (ISMS) certification service determines qualifications for certification by reviewing the compliance of the company establishing and operating the ISMS. This system has been enforced since 2002 based on the 「Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc.」, and at the present KISA is designated as the certification body to perform the certification business.

The ISMS certification procedures are shown in the following figure. A company that wishes to obtain a certificate should establish the ISMS and operate it for a certain period, and then apply for a certificate from the certification body. Then, after pre-assessment, a review contract is signed and the review team is organized to evaluate once. A company under review should resolve the defects pointed out during a review within a certain period of time, and submit the details of improvement to the certification body. Finally, the review results are reviewed by a certification committee composed of information security experts, after which a certificate may be issued.

Figure 3-11 | ISMS Certification Procedures



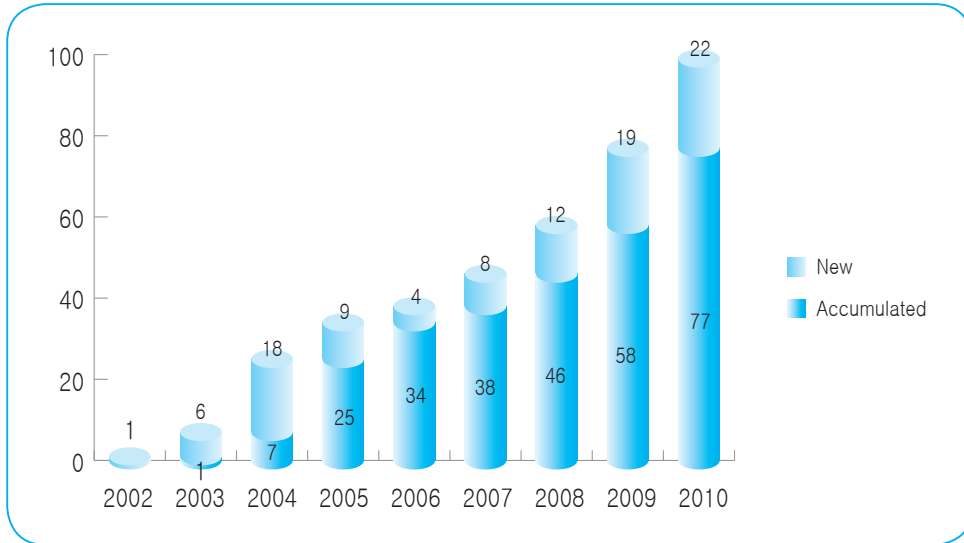
Source: KISA, isms.kisa.or.kr

The issuance of an ISMS certificate is not the end of the information security business, but the beginning. As it involves the establishment of a systematic process of information security, it is mandatory to consistently operate and supplement the ISMS. For this purpose, a company that receives an ISMS certificate is subject to post management reviews every year while the certificate is valid period (3 years), and must pass a test to maintain its certification status.

5.2 Main Activities and Project Accomplishments

Since the first enforcement of the system in 2002, the number of certificates issued has been steadily increasing, with a total of 99 certificates issued in 2010. The ISMS has now secured its position as a mandatory certification for companies interested in information security.

Figure 3-12 | Growth of certificates issued



Source: KISA, isms.kisa.or.kr

The scope of those who are subject to certification has been expanded from information security and IDC in the early phase to online universities, broadcasting and shopping malls. In 2010, Shinsegae and its affiliates (Shinsegae Mall, EMART Mall, Shinsegae I&C) received certification, and NHN and its affiliates (NBP, NHN I&S, Green Web Service, Internet Communications, Gplus) also received certifications. This indicates that there is a stronger need for a company to share customer's information with its affiliates. As the phenomenon may create synergy effects of information security activities, it may be used as a best practice from now on.

In addition, to create an environment for voluntary ISMS certification, the benefits of certification have been consistently improved. As shown in the figure below, ISMS-certified companies can get full scores in confidential security when applying for a candidacy for public organization S/W and information system planning, implementation, and operation. In addition, when the Korea Corporate Governance Service (KCGS) evaluates a listed company's ESG (environment, society, corporate governance) index, they can receive full scores in the consumer item. This indicates that the ISMS certification system is fully trusted and used as an evaluation index in various fields.

Table 3-4 | Benefits from Obtaining Certificate of Information Security Management System

Classification	Organizations	Details of benefits
Bonus points granted	Ministry of Knowledge Economy	Full scores in an item (confidentiality security) when selecting a public sector information system planning/implementation/operation company, S/W development company selection.
	KISA	Extra points when selecting information security targets, bidding and task evaluation.
	Credit rating organizations	Extra points when KIBO evaluates a company's credit rating.
	Korea Corporate Governance Service (KCGS)	Extra points in the consumer item when evaluating a listed company's ESG (environment, society, corporate governance).
Fee discounts	Insurance companies	Discounts on subscription to information security related insurances (liability insurances) (AIG, LIG, Green Insurance, Dongbu Insurance, Lotte Insurance, Meritz Insurance, Samsung Fire, First Fire, Hanwha Insurance, Hyundai Insurance, HK Fire)
Exemption	KCC	Exemption from safety diagnosis for the certification period (one year)
Recommendation	Ministry of Science and Technology	Recommends ISMS certification for remote education facilities.
	Ministry of Land, Transportation and Maritime Affairs	Recommends ISMS certification for ubiquitous city infrastructure.
ISMS certification fee discounts	KISA	Discounts for company that receives the information security grand prize (grand prize, excellence award, special award, 100~50%)
		Discounts for small companies (company with less than 50 permanent employees or revenue of less than KRW 5 billion, 50%)

Source: KISA, isms.kisa.or.kr

6. Information Security Check

6.1 Background for Introducing the Information Security Check Service

To promote reliability and trust in the information communication networks provided by information communication service providers, in January 2001, Ministry of Information and Communication prepared the recommendations for the execution of the “Information Security Measures” called the “Information Communication Service Protection Guidelines,” and recommended measures to be carried out by Internet Service Providers (ISP), online shopping malls and the like. However, with the 1.25 internet attack incident of 2003, the low level of security among ISPs and internet shopping malls emerged as a social issue.

As many people pointed out the need to strengthen the 「Information Security Measures」 for information communication services, on January 29, 2003, the “Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.” was revised to implement a safe environment for using information communication services, and the “Information Security Check Service” was introduced to mandate full compliance with the minimum protection standards proposed for the reliability and trust of the information communication network.

Since introducing the information security checkup service, the public awareness of information security has improved. As a result, interests in the information security checkup service increased, and with the DDoS attacks of July 7, 2009, which caused significant economic losses as reported in the news media, public acceptance of the information security checkup service was improved.

○ Execution details

- March 2003: Hosted policy hearing on ‘Information Communication Networks Protection Plans’
- March 2003: President’s annual business report
- June 2003: Open hearing for revisions of the “Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.”
- December 2003: Information sessions for the relevant companies (ISP, IDC, etc.)
- January 2004: Announced the enactment of the “Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.”
- September 2004: Information sessions to support the information security checkup.
- October 2004: Announcement and publication of explanations of the “Guidelines for the Information Security Measures and Security Checkup Methods, Procedures and Fees”

-
- March 2006~: Announcement of additional revisions to the “Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.” and execution of the system

6.2 Content of the Information Security Checkup Service

6.2.1 Target and Period of Information Security Check

The information security check service asks the main information communication service providers, Internet Data Centers (IDC) and shopping mall business companies to fully execute information security measures, and receive confirmations each year from the information security checkup organization. To reduce the burden on those who are subject to the checkup, the information security checkup criteria only recommends the minimal mandatory requirements. Only shopping mall services or multiple service providers with revenue earned through information communication service of more than KRW 10 billion in the previous year, or an average number of daily users for the last three months as of the end of the previous year of more than 1 million, are subject to the information security checkup.

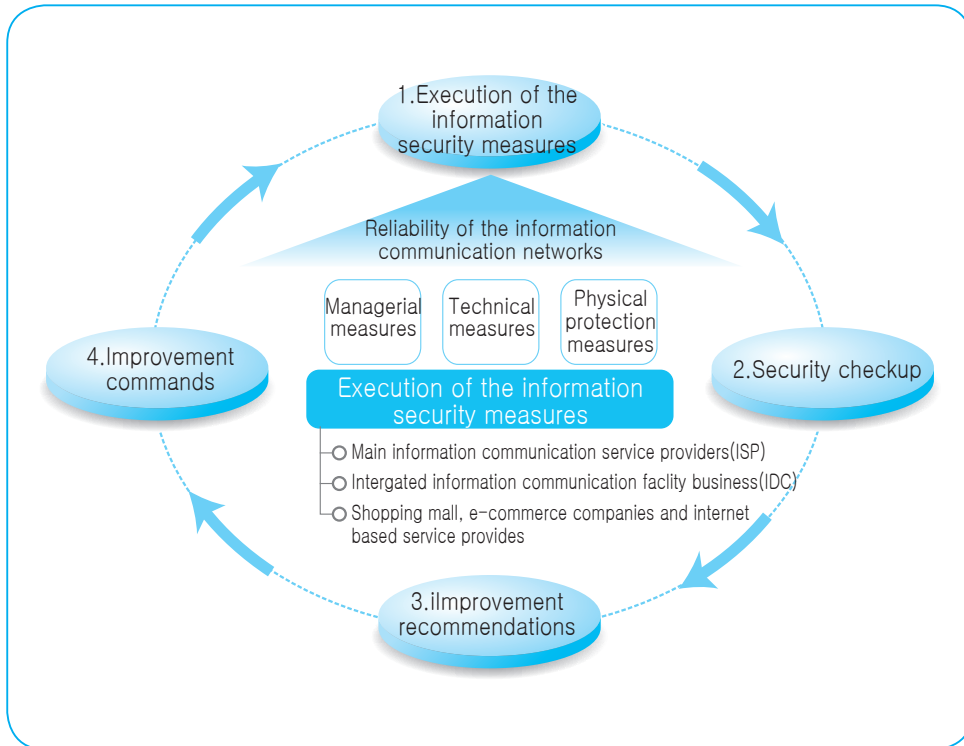
- Main information communication service providers
 - Internet access service providers, electrical communication line facility or network service providers
- Integrated information communication facility business
 - IDC operators (space rental service, server rental, network service, etc.)
 - VIDC (resells the rental from the IDC)
- Shopping mall and information communication service providers
 - Internet portal, internet e-commerce (shopping mall), internet broadcasting with revenue earned through information communication service of more than KRW 10 billion in the previous year, or an average number of daily users for the last three months as of the end of the previous year of more than 1 million
- Checkup period and items
 - Once per year, information security measures (managerial, technical, physical protection measures (48 items))

6.2.2 Concepts and Procedures of Information Security Checkup

This system states that the information security checkup organization should ensure that those who are subject to the annual information security checkup fully comply with the 「Guidelines for the Information Security Measures and Security Checkup Methods,

Procedures and Fees, which are the mandatory guidelines. As shown in the figure below, targets of inspection must fully execute the managerial, technical and physical protection measures for information security, and receive approval from the information security checkup organizations, so that the reliability and trust in the information communication networks and service can be guaranteed.

Figure 3-13 | Information Security Checkup Procedures (1)



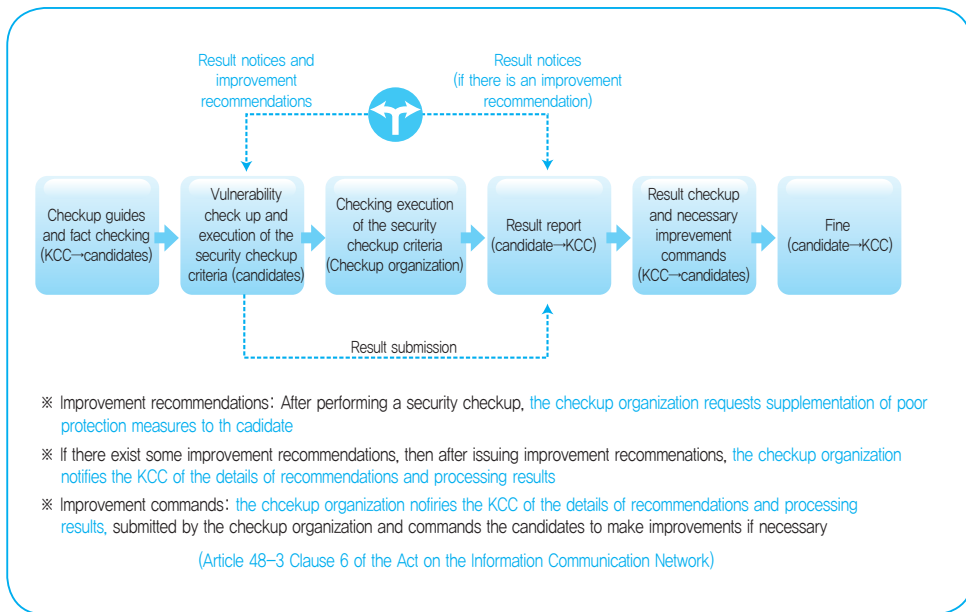
○ Information security checkup methods and procedures

The information security checkup organization directly visits those subject to the information security checkup, performs a paper-based review and on-site inspections, and checks whether or not the organization fully complies with the information security measures.

- Paper review: Paper based checkup of compliance with the information protection measures, based on relevant documents and evidences.
- On-site inspections: Includes vulnerability checkup, simulation hacking, log analysis, visual inspections and interviews.

According to the information security checkup procedures, a company subject to the information security checkup fully executes the information security measures and prepares a report after the information security checkup so that a certificate can be issued as follows.

Figure 3-14 | Information Security Checkup Procedures (2)



6.2.3 Target and Execution Organization of Information Security Checkup

Table 3-5 | Targets of Information Security Checkups

Classification	Number of companies subject to checkup					
	2005	2006	2007	2008	2009	2010
Main information communication service providers (ISP)	13	12	12	15	15	11
Integrated information communication facility business (IDC)	63	69	90	93	102	113
Information communication service providers (3 companies)	66	79	105	124	130	148
Total	142	160	207	232	247	272

Table 3-6 | Information Security Checkup Organizations

Classifications	Companies designated as information security checkers
Knowledge information security consulting companies (7)	A3 Security, Ahn's Lab, Secu I, STG Security, Infosec, Lotte IT, Cyber One
Accounting firms (2)	Deloitte Anjin LLC, Ernst and Young Advisories
Audit firms (3)	CAS, KCA, Korean IT Audit Consulting
Security companies (5)	Oulimelses, Infosec, Encoding Pass, Igloo Security, KCC Security
SI company (1)	KTIS Co.
ISP company (1)	KT Co.

6.2.4 Accomplishments of Information Security Checkup

In the early days of information security checkup services, the level of information security at those companies subject to checkup remained as low as 39%, but by 2010, it had improved to 98%. This accomplishment is due to consistent inspections and the

enhancement of information security activities, such as policy establishment, organization forming and implementation of the information security system.

In addition, if one takes a look at the results for information security checkup, one will find that there is higher interest in information security than in the previous year, and that more efforts were made to fully execute the technical protection measures. In addition, the newly joining candidates for information security checkup had opportunities to establish their own security systems.

In 2010, the 240 companies subject to information security checkup (subject to checkup in 2009) were surveyed on the efficiency of the system. Many companies responded that the security checkup gave them an opportunity to improve the awareness of employees, establish a security management system and strengthen security abilities.

7. Information Security Product Evaluation

The information security system evaluation/certification service can improve the level of information security at an organization and protect the main assets against the threats of informatization by providing the security evaluation/certification results of commercial information security products for product users, who can then select products with verified safety and trust.

7.1 History of Information Security System Evaluation and Certification Service

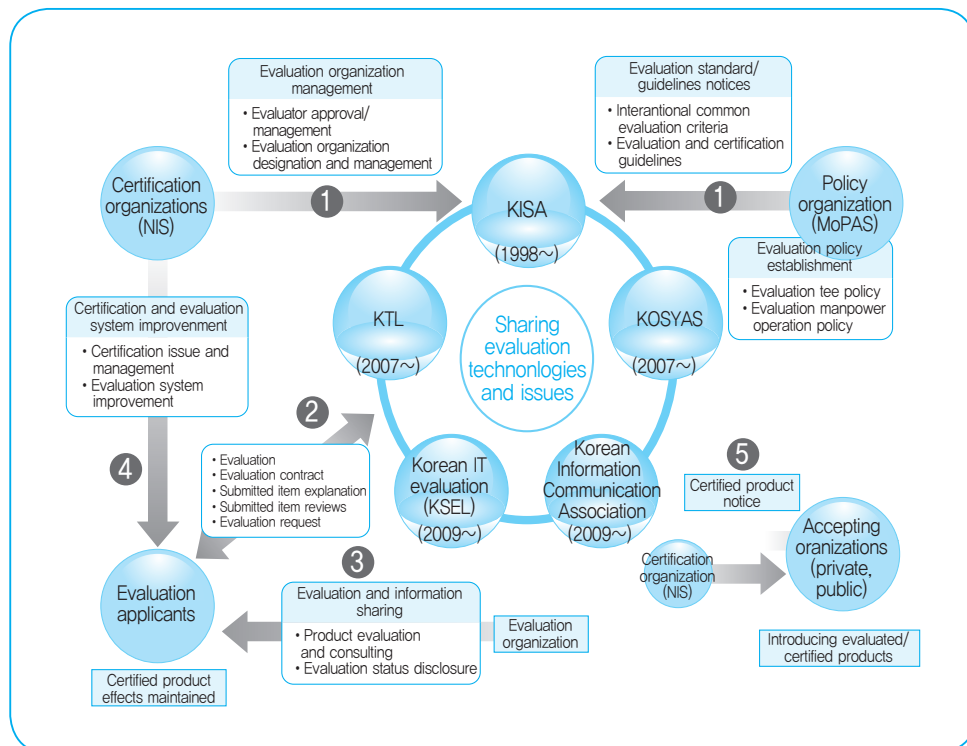
When the evaluation criteria suitable for Korea (K criteria) was developed and announced in February 1998, aggressive efforts were made for evaluation. The scope of systems subject to evaluation was expanded to include entry blocking systems in 1998, invasion detection systems in 2000, private networks in 2002 and OS security systems, fingerprint recognition systems and smart cards in 2003. In 2005, all of the information security products were subject to evaluation in order to respond to the global trends of integration and functional diversification. In addition, in 1999 a number of advanced countries including the USA, signed international agreements (CCRA) that ensured the mutual recognition of evaluation and certification results obtained according to common evaluation criteria (CC). Thus, to promote the internationalization of Korea's evaluation and certification system and the global competitiveness of our information security companies, the Korean government aimed to join the CCRA. In May 2006, the Korean government was finally admitted to the CCRA, and was entitled to issue certificates. In April 2007, the CC-based domestic evaluation and certification system was prepared, the evaluation period was reduced, and the burden on small information security companies was alleviated. In September 2008, Jeju Island hosted the CCRA general meeting and the 9th ICC (CC related international conference), with this event, Korea's reputation as a certificate issuing country was strengthened and domestic

information security companies had opportunities to promote their excellent technology to the world. In July 2010, the domestic evaluation system was improved to alleviate the burden on applicants for evaluation, and the security of the information security products in Korea was further strengthened. In January 2011, 25 types of information security products subject to evaluation and certification were selected.

7.2 Information Security System Evaluation/Certification Service and Procedures

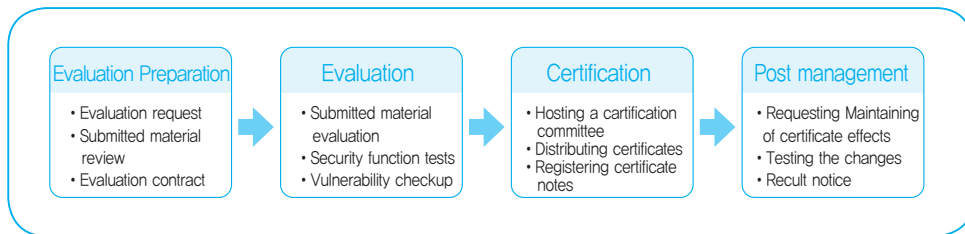
The information security system evaluation and certification service can be divided into policy organizations, certification organizations and evaluation organizations depending on the roles and responsibilities. As a policy organization, the Ministry of Public Administration and Security posts the standards and guidelines for evaluation and establishes certification-related policies, and the certification organization acts as a certificate issuer by approving evaluators and designating evaluation organizations, as well as managing evaluation organizations and establishing certification execution guidelines. Also, the five evaluation organizations, including KISA, play various roles, such as performing the evaluation of the information security products.

Figure 3-15 | Information Security System Evaluation/Certification Service



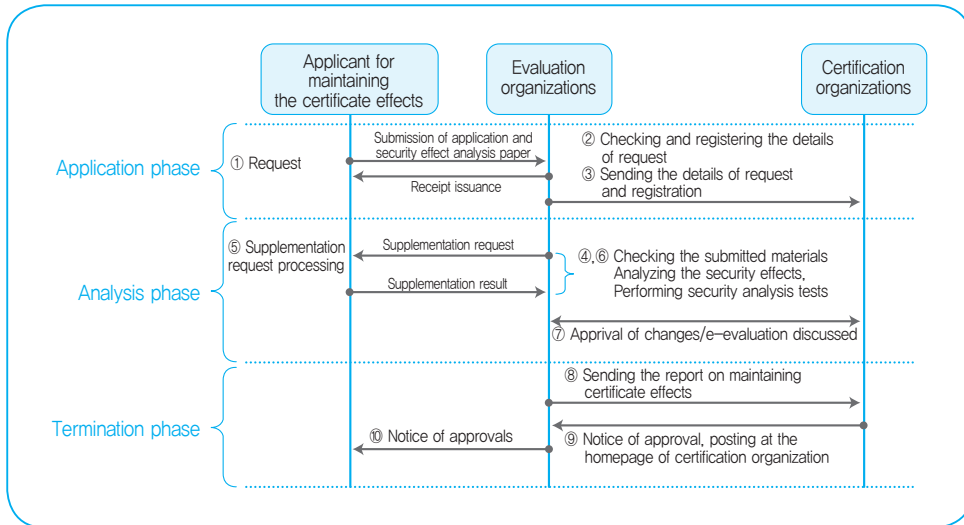
The information security system evaluation and certification procedures can be classified into the phases of evaluation preparation, evaluation, certification and post management. In the phase of evaluation preparation, an applicant for evaluation requests evaluation and signs an evaluation contract. In the phase of evaluation, the submitted material is evaluated, including a check for design error, to verify the safety and reliability of the commercial information security products, and the test of security functions and the vulnerability checkup are performed. In the phase of certification, the evaluation is terminated and a certificate is issued. In the phase of post management, a company that owns a certificate requests and tests to ensure continued compliance, in order to maintain the certified class of the product when the configuration of the product has been changed in some manner.

Figure 3-16 | Information Security System Evaluation/ Certification Procedures



With the revisions to the information security product evaluation and certification rules on January 1, 2010, the procedures for maintaining the effects of certificates saw some changes. The subject who requests and executes the maintenance of certificate effects was changed from the “certification organization” to the “evaluation organization.” A company who requests the maintenance of certificate effects submits a request to the evaluation organization that evaluated the product in order to carry out the procedures.

Figure 3-17 | Certificate Effects Maintenance Procedures



7.3 Operational Status of the Evaluation and Certification Service

Five evaluation organizations including KISA have evaluated a total of 110 products (certificate dates: January 2010~July 31, 2011) as of July 2011. These products include VoIP security, harmful traffic blocking and personal information security products, and various other new products. In particular, as the demands for internet telephony have increased dramatically, many harmful VoIP traffic blocking and detection products were evaluated. Also, as we experienced 7·7&3·4 DDoS, and system failures at domestic bank, Nonghyup and other kinds of large-scale security incidents, harmful traffic blocking products emerged as a new product group. As the IT environment becomes diversified, many new products are emerging daily. Amidst such changes, KISA has developed educational simulation products and deliverables to support preparation applicants who prepare for CC Certification. The educational simulation product was developed as a server/client-based invasion blocking system to help beginners to understand CC certification, and the deliverables were prepared with the aim of providing an educational simulation product. Domestic and international versions are available depending on the class.

Table 3-7 | Information Security Products' CC Evaluation and Certification Records

(As of July 31, 2011)

Classification	2003	2004	2005	2006	2007	2008	2009	2010	2011	Total
Invasion blocking system	-	-	1	-	-	1	-	-	1	3
Invasion detection System	-	-	3	5	-	1	-	-	1	10
Private networks	-	-	1	-	-	1	-	1	2	5
Access control system	-	-	9	4	3	4	2	7	-	29
Fingerprint recognition	-	-	1	-	-	-	-	-	-	1
Smart cards (COS)	-	-	-	1	-	-	1	1	-	3
Invasion prevention system (IPS)	-	-	-	5	10	4	4	1	1	25
Integrated security management system	-	-	-	1	1	-	7	3	2	14
Web firewall	-	-	-	-	1	7	4	1	-	13
Virus vaccine	-	-	-	-	2	4	3	3	-	12
Data leakage prevention system	-	-	-	-	-	2	2	-	2	6
Smart cards (IC chip)	-	-	-	-	-	1	1	-	-	2
Smart cards (e-passport)	-	-	-	-	-	3	-	5	1	9
DB Access control	-	-	-	-	-	2	5	3	-	10
Wi-Fi LAN certification	-	-	-	-	-	2	-	2	2	6
Spam mail blocking	-	-	-	-	-	-	3	1	-	4
Vulnerability check tools	-	-	-	-	-	-	5	1	1	7
Security USB	-	-	-	-	-	-	11	1	1	13
Networks Access control	-	-	-	-	-	1	4	2	-	7
Stored data fully deleted	-	-	-	-	-	-	2	-	-	2

Classification	2003	2004	2005	2006	2007	2008	2009	2010	2011	Total
Digital composite machine	-	-	-	-	-	1	-	8	-	9
Mail/messenger security	-	-	-	-	-	1	-	-	-	1
Classification	2003	2004	2005	2006	2007	2008	2009	2010	2011	Total
Abnormal traffic response system	-	-	-	-	-	-	2	-	-	2
Harmful site blocking	-	-	-	-	-	-	1	-	1	2
Security management system	-	-	-	-	-	-	-	2	2	4
DDoS response system	-	-	-	-	-	-	-	7	-	7
Email security	-	-	-	-	-	-	-	1	-	1
Integrated log management	-	-	-	-	-	-	-	2	1	3
Personal information protection	-	-	-	-	-	-	-	2	2	4
VoIP firewall	-	-	-	-	-	-	-	3	3	6
Multiple area security	-	-	-	-	-	-	-	1	1	2
Web contents Security	-	-	-	-	-	-	-	1	-	1
L2 security System	-	-	-	-	-	-	-	1	2	3
PC security	-	-	-	-	-	-	-	1	1	2
PC data Leakage prevention	-	-	-	-	-	-	-	-	1	1
Smart cards (USIM)	-	-	-	-	-	-	-	-	1	1
Integrated products	2	9	2	4	3	7	13	17	3	60
Total	2	9	17	20	20	42	70	78	32	290

7.3.1 Improvement of the Evaluation and Certification Service

As of July 1, 2010, the evaluation of the selected security function according to the domestic evaluation and certification service was expanded to all products including products without security functions in order to strengthen the product security. On January 1, 2011, 25 types of information security products subject to evaluations and certifications were designated so that the five evaluation organizations including KISA could evaluate the information security products supplied to national and public organizations. The scope of designation is expected to expand annually.

Table 3-8 | 25 Types of Information Security Products Subject to Domestic Evaluation and Certification

Product (module) name	Use
Invasion blocking	Network inbound and outbound traffic control
Invasion detection	Automatic detection of harmful traffic on a network
Invasion prevention	Harmful traffic invasion detection and automatic blocking
Integrated security management	Integrated monitoring and analysis of security events
Security management server	Central control of multiple security products
Web firewall	Web-based harmful traffic detection and blocking
DDoS response	DDoS attack detection and blocking
VoIP security	Internet phone related harmful traffic detection and blocking
Wireless invasion prevention	Unauthorized wireless equipment detection and blocking
Wireless LAN certification	Permission of wireless LAN use only for authorized users
Virtual private networks	IPSEC or SSL type virtual private networks
Network access control	Restricting network access permission to a PC with a security program
Spam mail blocking	Spam mail blocking and hacking mail tests
Virus vaccine	Virus and malignant code detection and deletion
PC media control	USB and media control and screen capture prevention
PC invasion blocking	Control of installation on PC and inbound/outbound traffic at PC

Product (module) name	Use
Web-based contents security	Detection and blocking of information leakages due to malignant codes and installation on the network
Data leakage prevention	Document security with server-based computing and virtualization
e-mail security	Mail/messenger attached file monitoring
Server security	Access privilege control and main file security setting
DB access control	DB access privilege control and access history management
Multiple area classification	Data and information flow control in security and non-security areas
Smart cards	Smart card chips and OS
Security USB	USB memory access control and auto deletion in case of loss
Composite machine fully deleted	Deletion module for the HD inside a composite machine

Table 3-9 | Status of Evaluation Organizations in Korea

(As of JULY 31.2011)

Logo	Organization	Date of establishment	Size of evaluation staff
	KISA	April 1996	8
	KTL	July 2007	13
	KOSYAS	August 2007	13
	KSEL	August 2009	10
	TTA	October 2010	14

7.3.2 Improvement of the Domestic Evaluation and Certification Service for Information Security Products

Initially, the domestic evaluation and certification service was introduced in 2007 to resolve the number of pending evaluation cases. As the number of evaluation cases increased from 20 in 2007 to about 70 in 2009, a 3.5-fold increase, while the types of products evaluated increased from 12 to 25 during the same period, the promotion of information security product markets was finally necessitated. However, since the introduction of evaluated and certified information security products in July 2009 to improve the security vulnerability in the operation environment (outside the scope of CC evaluation), the domestic evaluation and certification service was improved. The improved evaluation and certification service shifted from document-based evaluations to more function and vulnerability oriented tests, and the scope of evaluation was expanded to cover entire products, so that all aspects of vulnerability occurring in all product functions could be successfully removed. In addition, an applicant only needs simplified documents that can be used for functional and vulnerability tests, and the evaluation organization omits the submission of duplicate or substitutable deliverables in order to reduce the time spent for evaluation.

Through execution of the improved domestic evaluation and certification service, the security of information security products could be strengthened, the security level of national and public organizations introducing the products could be improved, and evaluation costs could be reduced. Eventually, the burden on small domestic information security companies was alleviated.

7.3.3 Evaluation Fee Discount Policy Operation

Since August 2008, KISA has been pursuing a discount policy to offer small companies one discount with 50% off on domestic evaluation fees. The purpose of this discount is to reduce the economic burden on small information security companies, which represent a significant portion of the information security companies in the marketplace. Thus far, about 31 companies have enjoyed benefits of 1 billion in evaluation discounts.

Table 3-10 | Evaluation Fee Discount Policy (KISA)

Classification	Details
Main contents	<ul style="list-style-type: none">• One case of discount with 50% off for small domestic companies.
Application period	<ul style="list-style-type: none">• Since August 2008~※ Application period is subject to change depending on the evaluation environment.

7.3.4 Strengthening and Promoting the Global Competitiveness of Korean Evaluations

To perform international standardization activities that could enhance Korea's reputation as a CCRA certificate issuing country, the certification organizations attended the CCRA international meetings comprised of the CCDB (development committee), the CCES (execution committee), and the CCMC (management committee), where they gave a presentation on the status of domestic security product evaluation and certification and analyzed the international evaluation technologies and the trends of evaluation policies. To promote information sharing among Asian CCRA members on evaluation and certification policies and technologies and to strengthen international cooperation, particularly in the area of support for Asian countries joining the CCRA, in 2009, the AISEC (Asian IT Security Evaluation and Certification) forum was launched. In July 2010, at the AISEC meeting held in Malaysia, KISA gave a presentation on the international e-passport evaluation results for EAL5+ class, which was an opportunity to showcase Korea's capacity and experience as a country with high-level evaluation technology. Currently, there are only seven countries that have received high-level evaluation and certifications for smart cards. The smart card evaluation requires professional technologies and abilities in all phases of S/W development, including design, development, test, and vulnerability analysis. In Asia, Korea, Japan and Taiwan have smart card evaluation technologies, and systematic efforts are also being made by Malaysia to obtain the smart card evaluation technology under its five-year plan.

7.4 Direction

Let us take a look at the main improvements that have been made to the evaluation and certification service. First of all, in terms of the system, to lessen the burden on information security product developers, the following efforts were made to amend the common evaluation criteria (CC): 1) simplification of the change approval procedures 2) minimal manpower injection for evaluation guarantee class (EAL2) 3) simplification of deliverables to be submitted and development of educational evaluation deliverables 4) 50% discount on evaluation processing fees for small companies. In addition, to promote the exchange of information between information security product developers and the actual consumers, persons in charge of security at national and public organizations, the '2011 information security products evaluation and certification conference' was held. This conference provides the opportunity to experience the various security technologies and products of 28 information security product developers in one place.

Following the system improvement in 2010, in 2011, the focus was placed on the quality of information security products and evaluation technologies to operate the evaluation and certification system. First, the product evaluation criteria were developed to enable the five evaluation organizations to consistently evaluate the information security products. The product evaluation criteria were provided, for utilization by developers and the evaluation

organization. The ‘information security product evaluation and certification technology review meeting’ is held each month to discuss all of the issues arising in the course of evaluation.

8. Spam Prevention Activities

8.1 Overview

8.1.1 Status

Spam is a kind of undesired email that consistently delivers unsolicited information, which most users find to be a major annoyance. In general, spam is defined as a profit-oriented advertisement that you receive on an electronic device, when using email or a mobile phone. It has the following three characteristics. First, it is unwanted or unsolicited. The defining property of spam is that the recipient does not want it. This is the most fundamental element for determining spam from the perspective of the recipient who is the final destination of the spam. Although there is no relationship between the sender and the recipient, transmission is forced. Second, it is commercial. If the information sent has some kind of commercial aspect in it, it can be classified as spam. However, since there may be some commercial information that the recipient desires to receive, this can't be the absolute standard for determining spam. However, profit-oriented information is sent blindly on a large scale more often than non-profit oriented information, so it is frequently classified as ‘unwanted spam.’ Third, it is sent as bulk mail. There are numerous applications and technologies that can be used to send a large number of email messages over high-speed information communication networks, and as a result, it is very easy to send several million spam emails to a large number of general users. Besides transmission, email address collection and creation are now fully automated to facilitate the transmission of spams. A large amount of spam can consume lots of network resources and increase the social costs involved in blocking the spam. Moreover, recently, spam has been going beyond the simple scope of advertisement. It is interconnected with hacking, malignant code distribution, and personal information exposure, the common threats of informatization. Due to the dramatic development of information and communication, spam distribution has also increased rapidly, but at the same time, technologies to prevent or filter out such spam have also been developed. The use of various filtering technologies is reducing the number of spam messages arriving in your email inbox, but spammers are now trying to send even more spam, which in turn increases the number of spam messages distributed worldwide. Recently, the media of spam distribution has been diversified to include instant messenger, internet BBS and blogs, email, and mobile phones. Also, today's sophisticated and advanced spam technologies include the use of botnets or illegal phones to avoid tracking and filtering.

8.1.2 Legal Background to Spam Prevention

According to the 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」, in Korea, mobile phone and fax advertisements need to be approved before being sent to the users (Opt-in). Also, email advertisements cannot be sent again if the user declines to receive them later (Opt-out). KISA is responsible for preventing spam, and for handling civil appeals in relation to spam.

8.2 Cause of Spam Generation

Various advertisement media include: information communication media such as TV, radio, internet, and email, or paper media such as newspaper, brochures and magazines. Among them, mobile phones and email are preferred because they are cost-efficient. It is cheaper to send advertisements over a mobile phone than advertise on TV, but it offers better advertising effects than paper-based ads. So, small companies are constantly tempted to transmit spam using mobile phones. For instance, in the case of loan advertisements, it is estimated that one out of 1000 cases receives a response from the user, and 20% of these respondents ultimately decide to take the loan, a success rate of 1/5000. Thus, mobile phones are regarded as the advertisement media with the most immediate and interactive media among all advertisement media that exist. As loan, 060 adult mobile-dates and chauffeur service companies compete fiercely in their respective sectors, illegal spam distribution is on the rise, despite the government's efforts to punish spammers. Moreover, the wide availability of caller number falsification, the diversification of spam transmission channels, and spam transmission friendly environments are the main causes of the rise in spam distribution. In other words, a person who transmits spam can use an illegally stolen or rented identity to sign a service contract with service providers, and use a device under someone else's name to send spam email. In such an environment, it is very easy to keep sending spam, and to avoid the government's efforts to track down spammers.

8.3 Main Spam Prevention Plan

8.3.1 Progress of Execution

As we were aware of the limits of post responses to spam messages, which are becoming more and more intelligent, Korean government prepared a comprehensive response plan to prevent spam. The detailed tasks included in the plan are analyzed each year in terms of effects, and supplemented and modified by considering the trends of technology development and the environmental conditions. In the past, the priority was put on handling spam that could cause increased social complaints, but a policy shift was made to a private sector participation based, prevention oriented policy.

① (2003~2005) As the high speed internet has become widely available since 2000, intense efforts were made to implement an infra against spam and to enable technical blocking according to the policy. Through these efforts, the number of spam messages was significantly reduced. ('03: 29.1 cases→'05: 6.9 cases→'10: 2.2 cases)

Table 3-11 | Main Policy to Prevent Spam in 2003~2005

Execution	Main policies
Jan. 2003	• Opened illegal spam response center
Jun. 2003	• Expanded the target of spam regulation (email ⇔ Tel/Fax ⇔ BBS)
2004~2006	• OECD spam workshop and "Anti-Spam Toolkit" development participation
Mar. 2005	• Opt-in system (pre-agreement) on Tel/Fax ads.
Apr. 2005	• Signed the 「Seoul- Melbourne multiple party spam MOU」.
Oct. 2005	• Spam report registration/handling process improved. (24-hour ARS with unattended help desk)
Dec. 2005	• Email blocking technology development and distribution. ※ Real-time spam blocking list (RBL), mail server registration system (SPF).
Dec. 2005	• Published and distributed the "Spam Mail Blocking Solution Utilization Guidelines."

② (2006~2009) Since the pre agreement (Opt-in) system was introduced in March 2005, the system was further improved to strengthen regulations on mobile phones spam messages that caused more significant inconveniences to users. As a result, the number of spam messages sent over mobile phones was significantly reduced. ('05: 0.74 cases→'09: 0.44 cases→'10: 0.43 cases)

Table 3-12 | Main Spam Prevention Policies in 2006~2009

Execution	Main policies
Mar. 2006	<ul style="list-style-type: none"> Introduced the user termination/contract cancellation of the service used for spam transmission.
Aug. 2006	<ul style="list-style-type: none"> Implementation of one-ring spam detection and blocking system by service providers.
Feb. 2007	<ul style="list-style-type: none"> Introduced simple reporting systems for mobile phone spam.
Apr. 2008	<ul style="list-style-type: none"> Cancellation of bills and restriction of use by illegal adult spam transmission companies.
Sept. 2008	<ul style="list-style-type: none"> Published the 「Spam Prevention Guidelines for Carriers (ex. guideline)」.
Sept. 2009	<ul style="list-style-type: none"> Strengthened investigations on harmful spam (gambling/loan/drugs) senders.

- ③ (End of 2009~) As the routes of spam generation became diversified and the sending methods more intelligent, a prevention-oriented comprehensive plan was prepared to eliminate the sources of spam generation and distribution.

Table 3-13 | Main Spam Prevention Policies from the End of 2009 to Present

Execution	Main policies
Nov. 2009	<ul style="list-style-type: none"> Limits the number of mobile phones per user. ※ General (3 units), Low credit (2 units), debtor /person with bad credit (1 unit)
Nov. 2009	<ul style="list-style-type: none"> Limits the number of daily SMS sent over the mobile phones to 500.
Nov. 2009	<ul style="list-style-type: none"> Provides consignment service to reject ads on mobile phones (chauffer service, adult ad companies)
Dec. 2009	<ul style="list-style-type: none"> Distributed posters and broadcast radio ads to prevent illegal phones.
Apr. 2009	<ul style="list-style-type: none"> Developed and provided intelligent spam blocking service for service providers.
Jul. to Sept. 2010	<ul style="list-style-type: none"> Developed and distributed educational material for youth to prevent spam (video materials).

8.3.2 Emerging Problems with Spam Prevention as the Environment Changes

a. Diversified routes of spam transmission(bubble effects)

With stronger actions taken against spam originating from mobile phones as of 2009, the number of spam messages sent via bulk SMS services (Biz-SMS, C2P, web messaging) increased, and the use of low cost internet phones (VoIP) gained in popularity. As a result, the abuse of such media for spam transmission was increased significantly.

b. Intelligent and adverse spam transmission skills

There have been many cases of damages caused by spammers who disguise themselves as renowned businessmen or acquaintances. For instance, by sending a phishing email saying “you have a photo mail,” a spammer enticed users to download adult photos, and illegally collected KRW 5 billion for information usage (KRW 2,990 per case).

c. Popularity of illegal and malicious spam

Spam in the five major categories of loans, gambling, drugs, adult entertainment, and communications services represents 77% of the total number of reported cases (Jan. to Dec., 2010). In particular, spam messages for unregistered loan companies’ loans, gambling and drugs are particularly harmful, since they can cause secondary crimes.

d. Lack of user awareness on spam prevention

As part of the comprehensive plan for spam prevention (October 2009), following the largest carrier in Korea, SKT, LGU+ and KT introduced the ‘intelligent spam prevention service’ in 2010. Despite the fact that it is a free service with great effects in terms of spam prevention, users are not willing to subscribe to the service as they lack an understanding of the service.

e. New spam problems continue to occur

There is an increasing amount of spam aimed at small-sized BBSs, where regulations are relatively less strictly enforced. Since there are many free services, it is very hard to manage them. In particular, operators of general hosting or free BBS, which are relatively poorer environments than large portals, have not implemented good plans to respond to spam messages.

8.3.3 Spam Prevention Strategies

a. Minimizing spam transmission by strengthening the sense of responsibility among carriers

Korean government plans to minimize the transmission speed for companies that generate large amounts of spam with large-scale SMS services (Biz-SMS, C2P), and share the information of spammers with carriers so that they also can restrict services. Also, we

will strengthen the voluntary regulations on spam prevention by managing internet phone (VoIP) companies' service launch and SMS transmission and by supervising and managing service providers in the user identification process, so that the use of mobile phones under false names can be eliminated.

b. Improving the efficiency of spam prevention by eliminating vulnerabilities in the transmission/receipt phases

Korean government encourages more mobile phone users to subscribe to the “Intelligent Spam Blocking Service” in order to improve the efficiency of spam blocking and immediately block off all spam SMS sent from confirmed spam numbers at the network level. In addition, harmful spammers will be identified as quickly as possible to restrict their use of the service by implementing a “real-time spam report/management system.”

c. Strict regulation of spammers

To improve the effects of law enforcement on spammers, Korean government plan to review ways to improve the current laws and update the guidelines for carriers, also make stricter regulations on adult content providers who illegally steal information use fees by sending unlawful spam while disguised as an acquaintance.

d. Spam response advancement and new spam prevention

Using the information communication networks, Korean government plan to implement the 『comprehensive monitoring and analysis system』 that can perform a real-time analysis of the spam status and take immediate action. In addition, periodical announcement of the amount of spam carried by certain email or mobile phone service providers will be done, in order to promote voluntary efforts to reduce the amount of spam. To prevent new spam, Korean government plan to develop a service to perform real-time/automatic analysis of BBS postings, and make it available for individuals, small companies and internet news media free of charge.

9. Personal Information Protection

9.1 Personal Information Protection System

The personal information protection system in Korea can be divided into personal information protection in the public and private sectors, as the legal basis and execution in the two sectors differ significantly. In the public sector, the Ministry of Public Administration and Security takes full responsibility as a superintendent organization, and manages the personal information owned by public organizations according to the “Act on the Protection of Personal Information Maintained by Public Agencies.” In the private sector, the “Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.” (“Information Communication Network Act”), the “Use and Protection of Credit Information Act” (“Credit Information Security Act”) and other individual laws are applied to protect personal information. KCC regulates information communication service

providers in the private sector, and the Ministry of Public Administration and Security regulates 22 types of businesses, including airliners, hotels and travel businesses, according to the Information Communication Network Act.

In addition, if a personal information invasion or dispute occurs, the personal information invasion report center and the personal information dispute arbitration committee are operated to resolve the related issues.

Table 3-14 | Number of Civil Appeals Registered as Personal Information Invasions

Classification		2007	2008	2009	2010
Consulting and reports		25,965	39,811	35,167	54832
Dispute arbitration	Request	90	172	145	191
	Arbitration established	13	44	72	37

However, in March 2011, when the “Personal Information Protection Act” was enacted to govern both the public and private sectors, many changes were made in the regulation system. The “Personal Information Protection Act” is a general law that governs personal information protection, and it is supposed to govern all private and public sector activity, including on/offline, unless other laws have special provisions that state otherwise. It is applied to all non-profit organizations, individuals, the national assembly and the courts, which had previously been processing personal information without any legal restrictions. Thus, a grey area of regulation that had previously been highlighted as a problem was eliminated.

In addition, the personal information protection committee under the president was implemented to review and vote on the main policies related to personal information protection, and the Ministry of Public Administration and Security was given the right to comprehensively adjust and control the personal information protection business. As a result, the overall level of personal information protection was improved. The act was enforced in September 2011, and the act on personal information protection by public organizations was abandoned after enforcing the 「Personal Information Protection Act」. However, the Information Communication Network Act and the Credit Information Security Act are enforced in the same manner as before.

9.2 Personal Information Protection Policy Activities

9.2.1 Distribution of Alternatives to the Resident Registration Number (i-PIN)

In Korea, many web sites are collecting resident registration numbers for the purpose of self-identification and confirmation. In the past, a resident registration number was typically used only to handle administrative works, but nowadays, it is collected and used in all areas of society, including public services, internet services, medical services and education. However, since the resident registration number itself contains gender, birthdate and birthplace information and contains a high level of individual identification, there is a high likelihood of abuse when the information is leaked.

For this reason, KCC introduced the i-PIN service to resolve issues of abuses and attacks occurring due to the excessive collection and use of resident registration numbers on web sites.

i-PIN is a means of identifying a person on the internet without using a resident registration number. It was introduced in 2005 to minimize the collection of resident registration numbers on the internet. As of July 2011, about 3.8 million units have been issued. i-PIN can be used to prevent leakage incidents, as no resident registration number is stored on the web site, and the details of use are reported to the issuer on a real-time basis each time the i-PIN is used, so that possible incidents can be monitored in advance.

From the perspective of the user, i-PIN can prevent identity fraud since no resident registration number is exposed, and from the perspective of the company, it is possible to confirm the user's identity, gender and age without storing a resident registration number, reducing the cost of personal information protection.

In June 2008, the Information Communication Network Act was revised to mandate acknowledgement of a method for subscribing to membership without using a resident registration number. Thus, all information communication service providers meeting certain criteria were told to provide an alternative method of joining a web site to requiring a resident registration number, which led to a legal basis for the promotion of i-PIN use. Moreover, in March 2009, the 'basic plan for using resident registration number alternatives (i-PIN) on the internet' was established, and the decision was made to gradually expand the distribution of i-PIN, so that by 2015, no resident registration numbers are used online.

9.2.2 Responses to Personal Information Leakages

Once personal information is exposed via internet, it is highly likely to be used for cyber crimes such as illegal spam transmission, voice phishing and the like. In Korea, to prevent additional abuses and misuses of personal information exposed on the internet, a range of policies have been enforced.

In 2006, using the Google search engine, the resident registration numbers exposed to domestic web sites were discovered and deleted. In November 2009, without using the search engines at portal companies, the “personal information leakage handling system,” which could directly search websites exposing personal information was implemented. Using the system, it became possible to search for leakages of nine personal information items, including account numbers and credit card numbers as well as resident registration numbers. In addition, a common response hotline was implemented to take necessary actions when a large-scale personal information leakage incident occurs. This hot line was launched with 24 companies in 2009, and as of the end of 2010, 103 companies are participating, including all of the major portals in Korea.

As Korean resident registration numbers have been exposed in foreign countries including China, the government is currently checking web sites in 45 countries, such as China and Vietnam. To immediately delete the exposed resident registration numbers, the government has implemented a cooperation system with the TWIA (Taiwan Internet Association), the TWNIC (Taiwan Network Information Center), the personal information protection supervision organizations in Hong Kong and Macau, the MIC (Ministry of Information and Communication) and the VNCERT (Vietnam Computer Emergency Response Team), and others.

In addition, the Ministry of Public Administration and Security is consistently monitoring leakages of personal information at the web sites of public organizations and complying businesses.

9.2.3 Distribution of the Personal Information Management System (PIMS) Certification Service

As the number of large-scale information leakage incidents has increased due to the widespread use of personal information by companies, it has become necessary to minimize the potential for personal information attacks by providing a management system for consistent and systematic personal information protection by companies. Thus, KCC introduced the PIMS (Personal Information Management System) certification service, under which a company can ask a trustworthy organization to check the level of personal information management and receive certification. In 2009, to introduce the PIMS certification service, proper implementation and operation methodologies and certification evaluation criteria were prepared. In 2010, based on the developed criteria, certification simulation was done on companies with different sizes (big, medium, small) to verify adequacy. In addition, a hearing and a vote by KCC were provided. In April 2011, many carriers and portal and information communication service providers received certification. To pursue international standardization, the standardization proposals will be made through international organizations, and case studies will be shared between organizations.

9.2.4 Responding to New IT Issues

With the advent of IT, the collection and use of various types of personal information, such as names and resident registration numbers, has been on the rise. In Korea, to respond to privacy invasions caused by new IT, diverse policies have been implemented.

First, to protect the public against location information leakages and abuse, and to promote the use of location information by creating a safe environment for its use, the 「Act on the Protection and Use of the Location Information」 was enacted in January 2005. However, as the mobile environment advanced, the use of personal location information was increased, and as it became necessary to promote emergency services using mobile phones in cases of emergencies or kidnapping, the government then made efforts to amend the relevant laws in order to alleviate restrictions on location information.

In addition, to promote the LBS (Location Based Service) industry and to improve the social safety networks, under the motto, ‘creating the world’s best environment for location information use,’ the government established the ‘plan for promoting the use of the location information for LBS industry development’ which defined three major goals-LBS industry promotion, social safety network advancement, and privacy protection-and nine detailed tasks, including legal system improvement, industrial support strengthening, R&D and standardization, implementation of social safety networks, etc.

In addition, to prevent personal information leakages in SNS (social networking services), which have recently been gaining popularity, KCC prepared protection guidelines for SNS companies and users.

9.2.5 Introducing the Personal Information Effect Evaluation System

The personal information effect evaluation is a system to establish a plan for necessary actions by evaluating the level of risk in all phases from collection to discarding of personal information, so that the potential risks of personal information breaches can be reviewed and the points of improvement can be derived in advance when pursuing an existing or new business that requires collecting personal information.

To introduce the system, the Ministry of Public Administration and Security and KISA performed test evaluations by considering the scale and sensitivity of the personal information collected and used in the course of informatization business. In 2009, a total of 10 informatization projects were evaluated, and in 2010, a total of 13 organizations were evaluated. In 2010, the “Guideline for Evaluating the Effects of Personal Information of Public Organizations” was revised in terms of detailed procedures and evaluation items. In addition, an effective evaluation program was developed, which public organizations can use to evaluate the effects on their own according to the procedures in the guidelines. In addition, a special training program on evaluation of the effects of personal information is

provided for personal information staffs and consultants at private companies and public organizations in order to train evaluation specialists.

9.3 Raising Awareness of Personal Information Security

9.3.1 Companies

To promote the level of understanding of complying businesses, the Ministry of Public Administration and Security pursued various types of education, including group education, special series visit education and instructor dispatch education. In 2010, the ministry opened and operated a total of 10 personal information education sessions, at which a total of 555 personal information protection officers were trained (June to December 2010). In addition, to respond to the large-scale personal information leakage incidents that occurred in March 2010, the ministry provided special visit education in the Seoul and Daejeon metropolitan areas, through which a total of 414 persons participated in education (April 2010). Also, to provide convenient education for complying business located outside Seoul, visiting education sessions were provided in the three areas of Busan, Jeju and Gwangju, where 488 personnel participated in education (October 2010). Finally, for companies that provided their own internal education programs, personal information protection instructors were dispatched thirty times to educate about 1,415 personnel.

In addition, to promote online education, the ministry developed an online program called 「Learning personal information protection with Manager Kim」. To allow companies to easily learn about personal information protection and apply the knowledge to the actual worksite, the ministry published a case-based textbook called “Personal Information Q&A.”

KCC also provided various on/offline education programs for information communication service providers. In 2010, quarterly group education on personal information protection measures and laws were provided to companies that violated laws related to the personal information protection related laws, through which a total of 802 persons were educated. In addition, personal information protection workshops were held for personal information managers at private companies so that they could learn the latest trends of personal information security and the governmental policies, while having opportunities to exchange information between companies. On the other hand, the ministry also prepared an online education program for small companies that had difficulties educating their own employees. A total of 401 persons received education.

9.3.2 Users

The government unfolded various education activities and campaigns to promote user awareness of personal information protection. In 2010, the Ministry of Public Administration and Security put up ads to emphasize the prohibition of personal information invasions and unfolded an online campaign to respond to large-scale information leakage incidents. In

December, to promote the practical rules for personal information protection, the ministry put up ads on subways and in local magazines, and distributed screensavers. In addition, the ministry made video materials that were played on the monitors at each subway station.

In addition, KCC interconnected with major web sites to protect the personal information of users, pursued the ‘i-PIN switching campaign’ (2010 April~May) and the ‘2010 self information security campaign’ (2010 October), and made efforts to advertise in various media, including radio, Twitter (SNS), subways, homepages, news media and so on. In particular, during the period of the ‘2010 self information security campaign,’ an idea contest was held to collect fresh ideas on how to promote the importance of personal information security. 591 posters, 63 UCC materials and 45 ideas were received from Korean citizens. During this period, a total of 13,465,774 passwords were changed, and a total of 21,670 users switched from resident registration numbers to i-PIN.

In addition, KCC worked with three major carriers to promote the ‘mobile phone application return campaign’ in various media such as radio, subways, BBS, agents, sales shops, etc. to publicize the importance of the right to retain mobile phone service applications containing personal information. In addition, the KT cultural foundation, which owns nationwide education networks, helped to provide “visiting personal information protection education class” for the parents of elementary, junior high and high school students, through which 125,066 were educated.

10. Copyright Protection

10.1 Importance of Copyright Protection

The world’s economy has passed the industrial age, in which only tangible assets such as real estate and capital existed, and entered the age of knowledge assets, in which non-tangible assets such as copyrights and patents bear much value. In particular, the rapid development of digital technologies is changing the social paradigm, and S/W is becoming more and more significant as it plays a critical role in changing the world’s economy. Such changes have positive aspects of bringing opportunities for industrial development, but they can also cause a crisis with attacks on the intellectual property right, a non-tangible asset.

Copyright is the driving force behind the cultural industry’s development, and is the basis for cultural industry. Without a healthy environment for copyrights, we cannot expect cultural development or the progress of industry. So, like many companies, the government also tries to respond to the need for global competitiveness by accumulating and developing knowledge assets, which are the source for the creation of a value-added economy. The implementation of a copyright protection environment implies that in this society, copyright holders are protected and can enjoy the fruits of their creativity. In other words, it implies that the users can now enjoy good quality contents.

However, in our society, the overall level recognition of copyrights is not yet very high. As the importance of copyrights is emphasized, there have been more campaigns and education on copyrights led by copyright holders than ever. But the actual efforts of users to protect and maintain copyrights are insufficient. In particular, with convergence media including smart phones and tablet PC emerging each day and becoming more widely available, we can easily see that the amount of illegally copied material distribution will also increase. Therefore, the establishment of a culture of lawful material use is more urgently needed than ever. In addition, the existing offline-based copyright system should switch to the new digital environment. Establishing copyright protection policies and systems requires much more than just producing good quality contents. Copyright is becoming an indispensable tool in terms of digital industry and S/W industry promotion, and contribution to the national economy.

10.2 Enactment and Revision of the Copyright Laws

10.2.1 Enactment of the Copyright Law and Its Objectives

The Korean government enacted the copyright act in 1957. Later, efforts were made to aggressively respond to the changes in the environment of digital material use and the development of digital technologies. As the domestic and international copyright environment changed, the copyright act was revised several times, including full revisions in 1986 and 2006. In 1986, as a special act on copyrights, the Computer Program Act was enacted to protect the computer programs as intellectual property. This effort was in line with the global trends, which began to protect computer programs as intellectual property according to international agreements. However, as the superintendent department handling computer program protection was changed from the Ministry of Information and Communication to the Ministry of Culture, Sports and Tourism, in July 2009 the computer program protection act was merged with the copyright act to establish the one unified copyright act that exists today.

The copyright act aims to contribute to industrial development by promoting the fair use of copyrighted materials and protecting the copyright holder's rights and other relevant neighboring rights. In other words, in addition to the protection of copyright holders, it creates an environment of fair copyright material use in order to ensure that copyrights can significantly contribute to industrial development. For this purpose, the copyright act specifies exceptions and limitations as well as rights pertaining to the copyright holders and the copyright neighbors.

10.2.2 Contents of Copyright Laws

A copyrighted material is defined as creative work that expresses a human's feelings or ideas. This can include literature, music, drama, arts, architecture, photos, video, geometric figures and computer programs.

Unlike patents, this can be protected only if registered, copyright protection starts at the time of creation, without executing any procedures or forms. Copyright includes the moral right of the author and the property right of the author. The moral right is the right to protect the author's honor and reputation as an author, and the property right is the right to protect the economic value pertaining to the copyrighted material. In general, it is very important to protect the right to publish, to display an author's name and to maintain consistency, as these are part of the moral rights of author. However, for S/W or computer programs, property rights are given greater emphasis than moral rights. Recently, the emphasis on property rights is greater than ever. The property rights of the author include: the right to copy, perform, broadcast, distribute, lend and to permit or forbid secondary creation. In other words, a copyright holder holds the right to copy and distribute the copyrighted materials, and to allow or prohibit distribution or copying.

The copyright act promotes the consistent production of contents by guaranteeing and compensating the rights of an author, but it has some important aspects related to the public good, since it involves political decisions to promote the use and develop the culture. Therefore, there is a certain protection period, after which anyone may use the copyrighted materials. Even during the period, the property rights of copyrighted material are fully protected. The protection period for copyrighted material extends to 70 years after the death of the author, unless it is specified otherwise.

10.2.3 Copyright Protection System

The copyright protection system based on the international standards and the copyright laws are being strengthened further, and the scope of its effects is also broadening. The Korean copyright protection system can be divided into two activities: first, copyright holders' activities to protect their rights, and second, the government's activities to establish a fair order of copyrighted material distribution.

A copyright holder can request civil damage compensation, criminal lawsuit or termination of illegal copy and transmission. Infringement of the copyright law is an offense subject to complaints, so although there are some exceptions, infringements are generally only punished if the copyright holder so requests. The government can investigate a case of copyright infringement and forfeit the illegally copied materials and take necessary actions. If copy (property) right is violated, the violator is subject to imprisonment of less than 5 years or a fine of less than KRW 50 million.

10.3 Efforts to Protect Copyright

10.3.1 Introducing the Web hard Registration System

The Korean copyright act strives to prevent the illegal distribution of copyrighted material online and to promote the creation of a lawful copyright environment. Currently, in cooperation with KCC, the government has introduced a registration system for special types of online service providers (OSP), such as web hard, which is the main route of illegal material distributed online, in order to eliminate the route for illegally copied material.

The Electrical Communication Business Act, which includes a registration system for web hard, will become effective on November 20, 2011. According to this act, all web hard-type companies should take technical measures to prevent the distribution of illegally copied materials and protect personal information. In addition, companies should display identification information, including the sender's ID and email address, and store the computer log files for more than two years. In addition, the act requires the residence of two or more monitoring persons for illegal material detection. If you want to register yourself as a web hard-type service provider, then capital of more than KRW 0.3 billion is required, and a user protection plan must also be submitted.

10.3.2 Protecting the Copyrighted Materials by Strengthening Administrative Actions

One of the unique things about the Korean copyright act is that it is a “three strike” system. Korea is the first country in the world to enforce an account suspension system that can strengthen the level of copyright material protection. In addition, Korea has also imposed the ‘account suspension’ and the ‘BBS termination’ system on heavy up-loaders.

While some believe that this series of administrative actions is an innovative system that can address the lack of social sensitivity to copyright infringement, some are concerned over the fact that the administrative organization has the right to punish the exercising of fundamental human rights, such as freedom of expression. However, it is indeed the most revolutionary law of its kind in the world, and many countries such as the EU are curious as to whether or not this system will settle itself as a norm.

10.4 Copyright Related Organizations and Their Activities

10.4.1 Ministry of Culture, Sports and Tourism

The Ministry of Culture, Sports and Tourism is responsible for maintaining the copyright protection policies. Its main activities include: improving the laws and systems for copyright protection, aggressive surveillance and preparation of comprehensive surveillance systems, support for consistent investigation of illegally copied materials online and offline,

strengthening international cooperation on current issues, and creation of an environment of fair copyright material use.

The Ministry of Culture, Sports and Tourism has a copyright policy officer under the supervision of the culture contents industrial room to operate the copyright policies department, the copyright industry department and the copyright protection department. Notably, it has a special private police force for copyright infringement, and is operating five offices nationwide (Seoul, Daejeon, Daegu, Gwangju, and Busan) that perform investigation in Korea.

In 2011, the Korean government's copyright protection policies aimed to create a stepping stone for transforming Korea into country with sense of awareness for fair use of cultural goods, and implemented five detailed tasks: ① 24-hour copyright protection system implementation, ② improvement of the recognition of copyright in daily life, ③ promotion of fair and convenient use of copyright-protected materials, ④ improvement of the laws/systems to meet the needs of the new digital environment.

10.4.2 Copyright Related Organizations

The copyright act identifies the Korea Copyright Commission as a copyright protection organization in Korea. The Korea Copyright Commission was launched in July 2009, by merging the Copyright Commission and the Computer Program Protection Committee. Its main tasks include: arbitration of disputes related to copyright infringement, research on copyrights, support for establishing copyright policies, technical protection measures, and support for establishing rights management information policies, recommendations to OSP, and requests for correction orders from the Minister of Culture, Sports and Tourism. It reviews the criteria for compensation paid for legal permissions to use copyrighted materials, the processing fees, and the amount paid to a copyright consignment manager. In addition, it carries out many programs to promote the awareness of copyright and develop the copyright systems.

The Korean Federation of Copyright Organizations was formed by various copyright organizations. It operates the copyright protection center with the support of the government, and according to Article 133 of the copyright act, it performs various works consigned by the Ministry of Culture, Sports and Tourism, such as the collection, disposal and deletion of illegally copied materials. In addition, it investigates the distribution of illegally copied materials, both online and offline.

In the private sector, there are copyright consignment management companies that represent various copyright holders. These include a total of 12 organizations: KOMCA (Korea Music Copyright Association), FOKMP (Federation of Korean Music Performers), KTRWA (Korean TV and Radio Writers Association), KVIA (Korean Video Industry Association), KBPA (Korean Broadcasting Performer's Association), KFPA (Korea Film Production Association), KRTRA (Korea Reprographic and Transmission Rights

Association), KSOA (Korean Society of Authors), and KSWA (Korean Scenario Writers Association). In addition to these, many private organizations such as KAOGI (Korean Association of Game Industry), KMPA (Korean Magazine Publishing Association) and KSCA (Korea Software Copyright Association) perform various activities to protect copyrights in various areas.

Table 3-15 | Copyright Consignment Management Organizations

Area	Organization name	Area of intense management
Music	KOMCA (Korea Music Copyright Association)	Rights of music copyright holders (composers, lyricists, publishers)
	KAPP (Korean Association of Phonograph Producers)	Rights of music record producers
	FOKMP (Federation of Korean Music Performers)	Rights of music performers
Literature	KSOA (Korean Society of Authors)	Rights of literature, arts and photo copyright holders
	KTRWA (Korean TV and Radio Writers Association)	Rights of TV/radio writers
	KSWA (Korean Scenario Writers Association)	Rights of movie scenario writers
	KRTRA (Korea Reprographic and Transmission Rights Association)	Right to copy and transmit literature
Movie	KFPA (Korea Film Production Association)	Consignment management of a filmmaker's right to transmit
	KVIA (Korean Video Industry Association)	Video and DVD performers' rights
Broadcasting	KBPA (Korean Broadcasting Performer's Association)	Actors' (talent, voice artists) rights
News	KPF (Korea Press Federation)	Consignment management of the news copyright holders' rights
Public contents	KOCCA (Korea Creative Contents Agency)	Consignment management of digital contents of public organizations

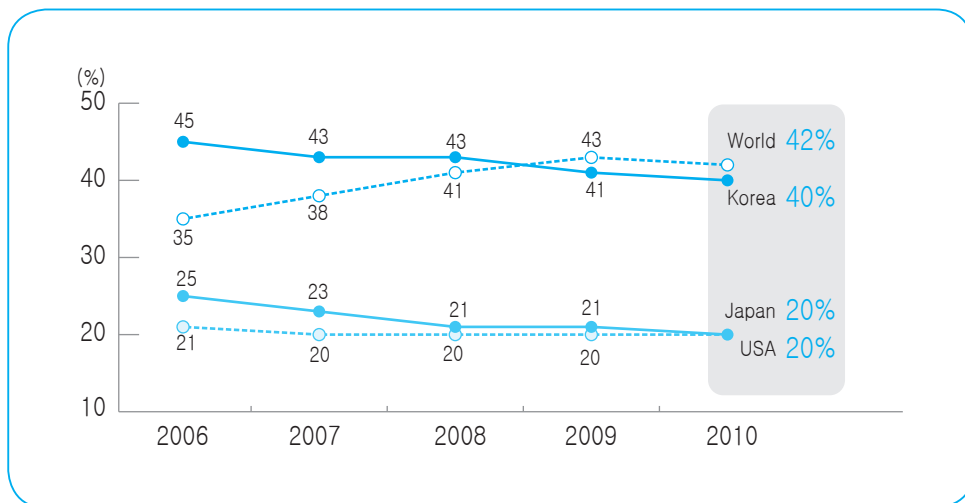
10.5 Copyright Protection Activities and Outcomes

10.5.1 Reduction of the Scale of Damages caused by Illegal Copying

Since 1989, the United States Trade Representatives (USTR) has been publishing the ‘Special 301 report’ each year. The US government uses this report to evaluate the level of intellectual property rights protection in each country, and announce the PWL (Priority Watch List), the WL (Watch List) and so on. Since 1989, Korea has been included in the PWL nine times and in the WL 11 times. However, since 2009, for three years in a row, Korea has not been designated as a country with suspicion of copyright infringement. This outcome is the result of the Korean government’s policy to protect copyrights, and gives Korea an opportunity to secure its position as a good trader who earnestly pursues copyright protections.

According to the global status report on the illegal software copying submitted by the BSA (Business Software Alliance), the ratio of illegal S/W copies in Korea amounts to 40%. This figure is lower than the global average ratio of illegal copying (42%) but it is much higher than the average ratio for OECD countries (28%). Also, it is twice as high as advanced countries in terms of copyrights, such as the USA or Japan. Considering the national competitiveness of Korea, this figure is quite embarrassing, even though it is better than the global average.

Figure 3-18 | Trends of Illegal S/W Copying



Source: BSA

The Korean government's efforts to protect copyright have been a very good example in the global market, and the rate of illegal copying in Korea has been consistently reduced. However, the scale of damages caused by illegal S/W copying in Korea is quite significant. According to the IDC, the total amount of damages caused by illegal copies in 2010 amounted to KRW 570 billion, while according to the investigations by the Korean S/W Copyright Association (SPC), there are more than 100 thousand cases of illegal S/W copies distributed online, representing a total loss of KRW 300 billion. This result was obtained by surveying 100 domestic open settlement protocols (OSP), so if you include companies and OSPs with servers in foreign countries, the amount will be even greater. This indicates that illegal copy distribution on the internet is still prevalent.

Besides hurting the copyright holder's rights, the distribution of illegal copies is also damaging the lawful contents distribution market. So, to eliminate the distribution of illegal materials, consistent surveillance and prevention activities are the most critical. In addition to activities that promote the awareness of copyright among the public, consistent surveillance activities are required, and the government should intervene more aggressively to establish the copyright protection laws and practices.

10.5.2 Introducing the system to suspend indictments by education

In addition to the protection of copyright holders, the copyright policy is showing some accomplishments in the area of user protection. For example, we can consider the system to suspend indictments by education. As blind lawsuits to collect settlement money on behalf of copyright holders had negative effects to the entire society, this temporary system was introduced to protect youth who were not fully aware of the significance of copyright protection. The Ministry of Culture, Sports and Tourism and the Prosecutors' Office introduced a temporary suspension of the indictment system for those who violated copyrights in minor cases but agreed to receive copyright education for a certain period of time. At the same time, efforts are being made to educate the public on copyright issues.

Information Security Basis Implementation Activities

1. Information Security Education and Training
2. Information Security Industry Promotion and Technology Development
3. Establishment and Operation of Information Security Organizations
4. Information Security Awareness Promotion Activities
5. Information Security Cooperation Partner's Activities

Information Security Basis Implementation Activities

1. Information Security Education and Training

1.1 Status of Information Security Manpower

According to our analysis of the information security workers in 2010, 5,812 persons had IT-related majors, while 3,171 were non-IT majors in their advanced education.

As of 2010, 8,983 individuals worked in information security related businesses, of which 10.1% were in the special workforce, 22.4% in an advanced workforce, 33.3% in an intermediate level workforce, and 34.3% in an entry-level workforce. If we classify workers by industry type, 37% are in R&D and implementation, 20% are in marketing and sales, 15.6% are in management and operation, and 12.4% are in strategy and planning.

Table 4-1 | Manpower Breakdown for Information Security Business

Classification	Special	Advanced	Intermediate	Entry level	Total		
					# of persons	%	
Strategy and planning	144	264	352	358	1,118	12.4%	
Marketing and sales	188	428	658	526	1,800	20.0%	
R&D and implementation	369	756	1,076	1,125	3,327	37.0%	
Education and training	15	92	95	115	317	3.5%	
Management and operation	134	261	514	488	1,398	15.6%	
Incident response	31	148	209	329	717	8.0%	
Evaluation and certification	23	59	85	139	306	3.4%	
Total	# of persons	904	2,009	2,990	3,080	8,983	100%
	Ratio [%]	10.1%	22.4%	33.3%	34.3%	100%	

In 2010, there were 1,005 newly-hired employees in information security related businesses, representing 11.2% of all information security employees. 45.9% of these, the largest portion of the manpower, were in the fields of R&D and implementation.

1.2 Status of Information Security Training

As of 2010, there are 19 universities and four two-year colleges with some kind of information security related departments. 11 general graduate schools, 2 specialized graduate schools and 9 special graduate schools are also currently running information security related departments, and 902 graduates received degrees from professional graduate schools or higher in 2010.

1.2.1 Training Manpower in the Official Training Program

a. Universities

The first information security department at a Korean university was the computer safety management department at Joongbu University in 1996. In 2001, many universities began to establish their own information security departments. As of 2010, there were 19 universities with 5,064 information security related majors, and 118 instructors teaching a total of 658 students each.

Although they are more interested in the fields of information security, it seems that the computer or internet related departments provide information security training along with the computer fundamentals, which means that the number of independent information security departments is actually decreasing.

As of 2010, the number of students at information security departments at all universities was increased by 51%, the number of graduates was increased by 58%, and the number of full time instructors was increased by 48%. But it still seems that the number of full-time instructors is quite low relative to the number of students.

Table 4-2 | Status of Information Security Departments in Universities

University name	Department/ major name	Year of est.	# of students	Graduates in 2010	# of full time instructors
Konyang University	Information Security Department	2003	241	22	4
Korea University	Computer Information Department	1987	425	55	23
Daegu Haany University	Internet Information Department			1	-

University name	Department/ major name	Year of est.	# of students	Graduates in 2010	# of full time instructors
Daejeon University	Computer Information Security Department	2003	231	29	4
Tongmyung University	Information Security Department	2005	330	16	7
Dongyang University	Computer Information Warfare Department	2000	255	41	8
Mokpo University	Information Security Department	2002	207	31	5
Seonam University	Computer Information Department	2010	16	-	13
Seoul Women's University	School of Computer Information Security Major	2002	183	24	4
Sejong Cyber University	Information Security System Department	2002	285	60	3
Soonchunhyang University	Information Security Department	2001	278	36	4
Yongin University	Computer Information Department	2005	248	20	-
Woosuk University	Information Security Department	2006	127	7	3
Woosong University	Computer Information Department		203	57	
Joongbu University	Information Security Department	1996	192	27	3
Korea University of Technology and Education	IT Engineering Department	1993	941	140	21
Hoseo University	Information Security Department	2002	288	30	4
Hanbuk University	Computer Information Department	2004	174	14	4
Howon University	School of Cyber Crime Investigation Cyber Crime Investigation Department/ Major	2006	440	48	8
Total			5,064	658	118

Source : KEDI academy info, www.academyinfo.go.kr

b. Graduate Schools

Information security related education at the graduate school level is offered in three different types of schools-general graduate schools, professional graduate schools and special graduate schools. Two professional graduate schools and nine special graduate schools and cooperative programs offer information security related trainings and majors. In addition, eleven general graduate schools offer MS and PhD programs.

In 1998, Dongguk University introduced the first information security major at the graduate school level, and in 2000, many graduate schools began to offer information security related majors. Professional graduate schools include Korea University's information management engineering graduate school and the University of Science and Technology's graduate school. Soonchunhayng University has information security departments in both its general and special graduate schools.

As of 2010, the total number of students at the graduate school related to information security is 927 and the total number of graduates is 195.

Table 4-3 | Status of Information Security Departments in Graduate Schools

Graduate school name	Department/ major name	Degree programs	Date of establish- ment	# of students	# of graduates in 2010	# of full time instructors
Kyungpook National University, General Graduate School	Information Security Department	MS, PhD	2001	2	1	-
Pukyong University, Graduate School	Information Security	MS, PhD	2001	14	8	-
Chonnam University, Graduate School	Information Security	MS, PhD	2000	40	5	-
Chonbuk National University, Graduate School	Information Security Engineering Department	MS, PhD	2003	1	1	1
Kyonggi University, General Graduate School	Information Security Department	MS, PhD	2003	1	4	1
Kyonggi University, General Graduate School	Industrial Security Department	MS, PhD	2000	14	-	-
University of Science and Technology, Graduate School	Information Security Engineering	MS, PhD	2004	1	2	-

Graduate school name	Department/ major name	Degree programs	Date of establish- ment	# of students	# of graduates in 2010	# of full time instructors
Korea University, Information Management Engineering Professional Graduate School	Financial Security Department Information Security Department Information Management Engineering Department	MS, PhD	2001	264	58	23
Dankook University, Information Media Graduate School	IT Department	MS	1997	56	15	-
Graduate school name	Department/major name	Degree programs	Date of establishment	# of students	# of graduates in 2010	# of full time instructors
Daejeon University, General Graduate School	Computer Information Department	MS, PhD	2005	5	2	-
Dongguk University, International Information Graduate School	Information Security Department	MS	1997	146	27	-
Sungkyunkwan University, Information and Communication Graduate School	Information Security Department	MS	1995	165	23	1
Suwon University, Engineering Graduate School	Information Security Department	MS	2003	20	-	5
Sunchunhayng University, Graduate School	Information Security Department	MS, PhD	2002	50	1	-
Sunchunhyang University, Industrial Information Graduate School	Information Security Department	MS,	1999	2	-	1
Soongshil University Industrial Information Graduate School	Information Security Department	MS,	2004	43	18	5
Ajou University Graduate School	Knowledge Information Security Department	MS	2003	58	12	-
Hannam University, Management Graduate School	Information Security Department	MS	2004	2	2	8

Graduate school name	Department/ major name	Degree programs	Date of establish- ment	# of students	# of graduates in 2010	# of full time instructors
Hanseo University, Information Industry Graduate School	Computer Information Engineering Department	MS, PhD	2002	2	0	-
Hanseo University, Information Industry Graduate School	IT Department	MS, PhD	2003	34	9	-
Hanyang University, Graduate School	Information System Department	MS, PhD	2005	1	5	3
Hoseo University Graduate School	Information Security Department	MS		6	2	-
				927	195	48

Source : KEDI academy info, www.academyinfo.go.kr.

c. Two Year Colleges

The information security related departments at two-year colleges offer practical education on internet security, hacking and cyber crime investigations, and are very active in providing education on how to obtain licenses. At the two-year colleges, highly specialized departments and majors are available. In particular, Dongju College's cyber police administration department and Chosun College of Science and Technology's U-cyber security department are the most popular examples. The schools provide education on investigation methods based on information security supervision. In 2010, four two-year colleges have 268 students enrolled and have graduated 49 students, which is about three times higher than the previous year.

Table 4-4 | Status of Information Security Departments in Colleges

College name	Department/major name	Date est.	# of students	Record in 2010	# of full time instructors
Dongju College	Cyber Police Administration Department	2005	88	12	2
Daeduk College	Information Security&Hacking Department	2002	43	1	-
Chosun College of Science and Technology	U-cyber Security Department	2008	61	19	-
Korean National College of Rehabilitation and Welfare	Computer Information Security Department	2007	77	17	4
Total			269	49	6

Source : KEDI academy info, www.academyinfo.go.kr

1.2.2 Manpower Trained by Professional Organizations

a. National Public Education Organizations

Government officers are educated at the informatization education center of the Ministry of Public Administration and Security. The informatization education center hosts a contest to test the level of knowledge of government officers, and operates a program to comprehensively evaluate the informatization and knowledge level of government officers.

Table 4-5 | Status of Information Security Departments in Informatization Education Centers

Program		Operation records in 2010		
		# of programs	# of operations	Operation records
Group education	Informatization policy education	9	20	317
	IT special education	27	53	1,102
	Information utilization education	19	73	1,930
	Customized education	35	35	900
	Special education	1	6	784
	Sub total	91	187	5,033
Cyber education	Informatization policy education	7	13	1,368
	IT special education	12	30	3,497
	Information utilization education	22	39	4,525
	Sub total	41	82	9,390
Total		132	269	14,423

Source : Ministry of Public Administration and Security's education portal www.eacademy.go.kr

b. Private Education Organizations

Information security education in the private sector is diversified in terms of number and contents. In addition to short-term education for non-information-security majors, private sector organizations provide six-month course to help those who want to obtain professional knowledge.

As of 2010, there are 19 private education organizations involved in the field. Most of them offer short-term programs in addition to long-term information security expert education programs. One of the most popular programs deals with licensing for information security experts.

The license programs include the CISA (Certified Information Systems Auditor) license program, and the CISSP (Certified Information System Security Professional) license program. Also, there are many programs for preparing for an SIS (Specialist for Information Security) license.

In addition, as the scope of candidacy for information security diagnosis was further expanded in 2011, the introduction of a CISO (Chief Information security Officer) to large companies became mandatory, and as a result, some organizations began to offer a CISM (Certified Information Security Manager) program.

Table 4-6 | Private Information Security Education Organizations

Organization name	Education program	Homepage
Netcollege	Data communication security course	www.netcollege.co.kr
Wiseroad	CISSP, CISA, CISM programs, etc.	www.wiseroad.co.kr
Lyzeum	CISSP license programs, etc.	www.lyzeum.com
Lacademy	Information security experts license program	www.lacademy.co.kr
Bit Campus	Computer security theory	www.bitcampus.co.kr
Samsung SDS Multi Campus	CISSP license program, practical business for network security	www.multicampus.co.kr
Ssangyong IT Education Center	Security network program developer program	www.sist.co.kr
Sun Training Center	CISA license program	www.suntraining.co.kr
SSol Desk	Hacking security expert program	www.ssoldesk.com
System Education Center	Information security education program	www.sysedu.co.kr
IT Bank	Information security expert license program	www.itbank.net
IT Bank Education Center	Information security expert program	www.itbank21.org
Aegis One	Information security expert program	www.hackerscollege.co.kr
Insec Security	Practical responses to invasion incidents	www.insec-security.co.kr
KISEC	Information security expert program	www.kisec.co.kr
i2SEC International Information Security Education Center	Information security expert program	www.i2sec.co.kr

Organization name	Education program	Homepage
Korean HP Education Center	Fundamentals of information security	education.hp.co.kr
KH Information Education Center	Information security expert program	www.iei.or.kr

1.2.3 Advanced Manpower Training Program Funded by the Government

The Ministry of Knowledge Economy is driving the main axes of the advanced manpower training program funded by the government. In 2011, under the 「Knowledge Information Security Business Promotion Plan (2008.12)」, the employment contract based MS program for knowledge information security, the key manpower training program and the new job creation projects were pursued to train advanced information security manpower in the field.

The employment contract based MS program for knowledge information security provided by KISA is a project to train the advanced manpower the industry demands. A consortium formed by companies and universities recruits students. If a student joins the program, upon obtaining a MS degree, he or she may find a job at a company participating in the program. In 2009, the program was offered for the first time, and the first students graduated in February 2011. They found jobs at companies participating in the consortium.

As of 2011, four universities (Korea University, Ajou University, Yonsei University and Dongguk University) are operating seven consortiums, and are providing the courses in mobile security, convergence security, etc.

a. Key Manpower Training for Knowledge Information Security

Just like the employment contract based MS program for knowledge information security, the key manpower training program for knowledge information security is also being pursued according to the 「Knowledge Information Security Business Promotion Plan(2008.12)」 and is training 2,000 advanced experts in the fields of knowledge information security that can meet the demands of industry. KISA's knowledge information security academy has been expanded to 'KISA Academy,' which trains key workforce for the knowledge information security field.

By reflecting the demand for advanced manpower in the industry and developing the proper education program, this program can provide educational opportunities for the workforce at the worksite. As of 2010, the following curriculums are covered in the key training programs offered by KISA.

Table 4-7 | KISA Academy Education Program

Course name		#	Persons
Digital forensics course	Digital evidence acquisition techniques and procedures to respond to computer and mobile related cyber crimes. Utilization of forensic tools and the relevant legal knowledge.	6	120
Knowledge information security consultant course	Junior/senior program to develop consulting ability with professional knowledge in general information security, physical security and knowledge information security.	6	161
Skill upgrade course	Education program for workers who deal with practical business related to the latest issues.	2	57
Security monitoring course	Training security officers to meet new demands following the revision of the 「National Cyber Security Management Rules」. For those who are about to graduate or find a job at a security monitoring company.	4	196
OJT	On-site practical education for those who are expected to graduate as information security majors.	1	72

1.3 Status of Information Security License

As the importance of information security is being highlighted and the demand for the skill increased, our interest in information security licenses is higher than ever. As of 2010, there are six types of information security licenses in Korea.

Table 4-8 | Status of Information Security License

License name	Level	Superintendent organization
Specialist for information security (SIS)	1, 2 class	KISA
Internet security specialist	1, 2 class	ICQA
Information security manager (ISM)	-	CQMA
Hacking security specialist	1, 2, 3 class, junior	NAHS
Cyber forensic investigation specialist	-	KPS, CFPA
Digital forensic specialist	1, 2 class	KISA

SIS (Specialist for Information Security) is one of the most popular licenses offered in the field of information security in Korea, and is available in class 1 and 2, both of which are nationally approved licenses. Class 1 verifies information security policy establishment, risk analysis and planning, development of the information security guideline, etc. Class 2 requires the skills to utilize systems, networks and internet, and practical skills to take full charge of the implementation of security policies, the operation and monitoring of security systems, and information security training and education.

Internet security specialist's licenses are also available in class 1 and 2. These verify the license holder's ability to respond effectively to server hacking through means such as security setting, security analysis, hacking prevention and security recovery, and examine such overall information on security and operation systems. The information security manager license verifies the ability to respond to various types of attacks such as various information leakages, wire tapping and information falsification over the network.

The National Agency of Hacking and Security supervises hacking security specialist licenses available in classes 1 through 3 and a junior class. Depending on the class, a different level of hacking and security ethics, basic knowledge and practical knowledge is confirmed. In addition to private licenses, the government is pursuing the establishment of a new national technology license in the field of information security. The legal system reinforcement and item development will follow.

2. Information Security Industry Promotion and Technology Development

Since the mid '90s, due to venture company promotion, the dramatic development of IT, the expansion of investments on information security technologies and newly launched excellent products, despite having a short history of only 15 years, the domestic information security industry saw a radical development, after which domestic companies were fully in charge of information security in Korea. Along with the global level of technology and competitiveness, the export amount has also been gradually increasing. In this chapter, we would like to discuss the current status of information security industry and R&D in Korea, and promotion policies.

2.1 Information Security Promotion Policies in Korea

2.1.1 Status of Information Security Industry in Korea

There are about 200 information security related firms in Korea, and in 2010 the market size was estimated to be KRW 1 trillion, 131.4 billion. Of the total revenue, information security products represent 81% (KRW 916.8 billion), while information security services represent 19.0% (KRW 214.6 billion). If you categorize it by source of demand, public

organizations show the highest demand at 35.5%, followed by major conglomerates (21.9%), financial organizations (19.5%), education organizations (10.8%), and small companies (10.6%).

Table 4-9 | Korean Information Security Market Size (revenue)

(Unit: KRW million)

Classification	2009	2010	Increase (%)	Portion in revenue (%)
Information security products	757,130	916,803	21.1	81.0
Information security services	173,324	214,612	23.8	19.0
Total	930,454	1,131,415	21.6	100.0

Source: KISA (2010.12)

Table 4-10 | Korean Information Security Market Size (demand)

(Unit: KRW million)

Classification	Public organization	Financial organization	Education organization	Big companies	Small companies	Other	Total
Information security products	37.3	20.0	12.4	18.3	10.3	1.7	100.0
Information security services	26.8	17.0	3.5	39.1	11.7	1.9	100.0
Total	35.5	19.5	10.8	21.9	10.6	1.8	100.0

Source : KISA (2010.12)

2.1.2 Korean Government's Policy to Promote the Information Security Industry

With the accelerating advancement to the smart society with mobile and cloud computing, and as various security threats such as DDoS attacks and Stuxnet are becoming dramatically more intelligent and advanced, the Korean government realized that information security technology and the development of the related industry is a key element for the promotion of convergence IT industry and acquisition of the fundamental ability to protect information security. Thus the Korean government established the “Information Security Promotion Plan” with the relevant government departments.

Table 4-11 | Korean Government's Policy to Promote the Information Security Industry

Classification	Detailed execution tasks	Superintendent organization	Schedules
□ Legal system repair	1. Pursuit of the information disclosure system	Ministry of Knowledge Economy	2011 (first half)
	2. Announcement of the adequate repair and maintenance fee rate system	Ministry of Knowledge Economy	2012
	3. Improvement of the special company designation system	Ministry of Knowledge Economy	2011-2015
	4. Quality certification guidelines	Ministry of Knowledge Economy	2011-2015
	5. Execution of the demand forecast system	Ministry of Knowledge Economy	2011 (second half)
□ Public market creation	6. Legal system reinforcement, such as forensic legalization	Ministry of Public Administration and Security-KCC· Ministry of Justice	2011-2015
	7. Early public market creation	All the relevant departments	2011-2015
	8. Test-bed and company competitiveness strengthening	Ministry of Knowledge Economy	2011-2015
□ Foundational organization strengthening	9. Increasing the manpower for public organizations	Ministry of Public Administration and Security	2011-2015
	10. Training information security manpower for subordinate organizations	Ministry of Knowledge Economy	2011 (first half)
	11. Announcement of excellent information security organizations	Ministry of Public Administration and Security-KCC	2011-2015
	12. KISA team launch	Ministry of Knowledge Economy-KCC	2011 (first half)
	13. Information security association launch	Ministry of Knowledge Economy	2011 (second half)
	14. Proclaiming information security industry day	Ministry of Knowledge Economy	2011 (second half)

Classification	Detailed execution tasks	Superintendent organization	Schedules
□ Next-generation information security leader training	15. Employment contract based MS program	Ministry of Knowledge Economy	2011-2015
	16. Cyber security research center establishment	Ministry of Knowledge Economy	2011 (first half)
	17. Retraining program for employees	Ministry of Knowledge Economy	2011-2015
	18. Hacking defense contests	Ministry of Knowledge Economy-Ministry of Public Administration and Security-KCC	2011-2015
	19. Enhancing the level of national public certificates	Ministry of Knowledge Economy-Ministry of Public Administration and Security	2012
□ R&D investment expansions and strengthening of competitiveness	20. R&D investment expansions	Ministry of Knowledge Economy-KCC	2011-2015
	21. Launching commercialization technology development projects	Ministry of Knowledge Economy	2010 (second half)
	22. Hosting a tech transfer event	Ministry of Knowledge Economy-KCC	2011-2015
	23. Introducing secure coding systems	Ministry of Public Administration and Security	2011-2015
□ Overseas information security market exploration	24. Support for market customized exports	Ministry of Knowledge Economy	2012 (first half)
	25. Newly launching export mentor programs	Ministry of Knowledge Economy	2011 (first half)
	26. Signing information security MOU	Ministry of Knowledge Economy, Ministry of Public Administration and Security	2011-2015
	27. Laying the foundation for export promotion	Ministry of Knowledge Economy	2011-2015
	28. Strengthening PR and marketing	Ministry of Knowledge Economy	2011-2015
	29. Cultural exchanges between domestic and international partners	Ministry of Knowledge Economy	2011-2015
	30. Organizing export discussion boards	Ministry of Knowledge Economy-Ministry of Public Administration and Security	2011-2015

Source : Ministry of Knowledge Economy (2010.12)

1) For the purpose of legal system reinforcement, Korean government prepared detailed tasks, such as the “voluntary information security information disclosure system” that asks a company to disclose its own information security systems and the inspection results to stakeholders, the “adequate repair and maintenance fee rate system” that considers the special aspects of information security S/W such as invasion pattern updates, the “discarding of the special company designation system’s expiration period” to expand the scope of special companies and promote fair competition, the “similar quality certificate duplication request alleviation” that can be applied as regulations, and the “next year’s public ordered information security projects forecasts” that investigates the type and scale of public ordered information security projects. The ultimate goal is to improve the current legal regulations to correspond to the current situation of companies, so that domestic information security companies can grow on their own in respective fields.

2) For the purpose of public market creation, the following five tasks are established: the “digital forensics market” including digital investigation tool certification systems and establishment of the digital investigation technology support center, the “security monitoring market” including the designation of security monitoring companies to strengthen the competitiveness of monitoring companies, the “DDoS market” including the implementation of DDoS emergency shelters and broadband DDoS Test-Beds, the “personal information security market” including the introduction of the personal information security management system certification service and the designation and operation of a personal information security effect evaluation company, and the “convergence security market” including key technology development for IT convergence security and homeland security industry development strategy establishment. The ultimate goal is to raise new revenue amounting to KRW 400 billion in these markets.

3) To strengthen the foundational organizations, the following detailed tasks are executed: the “addition of professional information security manpower to public organizations,” which includes the designation of CSOs (information security officers) for the central government and the local self-governing organizations, as well as the launchin of a department in charge of information security industry promotion and associations to expand information exchanges among the various information security organizations. By such efforts, we can successfully strengthen the roles of industrial support organizations and promote the private discussion boards and organizations, so that the information security related organizations such as public organizations, industrial promotion organizations and private discussion boards and organizations can benefit from strengthened industrial capacity and manpower.

4) For the purpose of training the next generation of leaders, various licenses such as SIS have been upgraded as nationally approved licenses. By providing bonus points for employment, and hosting recruiting events for knowledge information security, college graduates are helped in their job search in this “employment connection program to resolve youth unemployment.” Also, by establishing the cyber security research center, the best manpower can be trained to fight cyber warfare, and the intense education program for

current employees will help train the key industrial workforce. The focus should be placed on how to train the next generation information security workforce with the spirits of leadership and creativity.

5) For the purpose of expanding R&D investment and strengthening competitiveness, by 2015, the portion of R&D investments in information security will be expanded to 10% of the entire IT industry. For the early commercialization of new products such as smart phones and cloud services, as well as IPv6, the “accomplishment promotion” tasks will be undertaken to newly establish commercial technologies. By upgrading and expanding the test beds for evaluating the performance of security products made by small companies (SME’s), the certification costs and periods will be reduced in the “foundation implementation” sub task. Pioneering and market oriented policy execution will improve the domestic information security technologies and promote the commercialization of relevant technologies.

6) In the area of overseas information security market explorations, the following efforts will be made. “Market condition customized export supports” will help establish appropriate strategies for each country (e.g. Japan, South Asia and the Middle East) and the “Company growth customized export support” includes the launching of a new export mentor program that classifies the degree of preparation for export into three levels, and interconnects them with the proper business support. The “overseas market information acquisition and marketing” sub-task includes the publicizing of excellent domestic security products in the popular overseas market and aggressive participation in international exhibitions. Finally, the “overseas export system strengthening” will implement and operate an expert discussion board for each country to share the strategies for each target country. By accumulating experience in countries that are relatively open to imports and pursuing the expansion of exports to neighboring countries, we can help small companies to successfully explore the overseas markets.

2.2 Status of Information Security R&D in Korea

2.2.1 Backgrounds

The information security R&D projects pursued by the Korean government are centered on KCC and the Ministry of Knowledge Economy. To implement safety/reliability based knowledge information society by 2015, about KRW 22.3 billion will be invested in (as of 2011) a project aiming to develop the world’s best security technology. To reduce the gap with advanced countries such as the USA and Israel, efforts are made to first discover original information security technologies and distribute them to private companies by considering technologies, marketability, urgency and public merit.

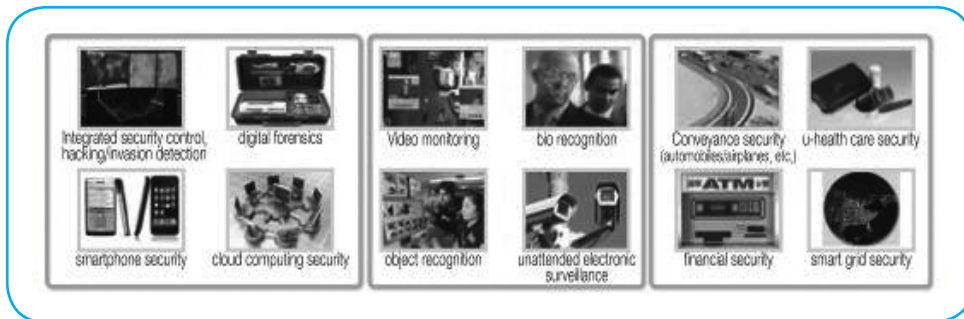
In addition, to respond to cyber attacks that are becoming more and more intelligent and cope with the dramatically changing ICT environment, themed/long-term R&D roadmaps for information security that include the milestones for technology development are established each year. Also, regular efforts are made to maintain consistency in the

information security policies by strengthening the relationships among markets&product/ technology&services to immediately discover new opportunities.

2.2.2 Main R&D Areas

The information security R&D pursued by the government can be classified into the following: network system based information security, physical security for safe daily living, and convergence security created by converging security technology with traditional industry. The original technologies in each area include common base protection, network/system security, service/applied security, physical security, and convergence security. In addition, by clearly distinguishing the roles of the government and the private sector, R&D efforts are strengthened, while the early development of key information security technologies will support test operation and strengthen verification efforts in the phase of service/infra implementation.

Figure 4-1 | Main Information Security R&D Areas



Source : ITEP (2010.10)

Table 4-12 | Classification of Main Information Security Technologies

Upper category	Lower category	Definition
Common base security	Password/authentication technology	Technology to guarantee the integrity and confidentiality of data and communication, and manage the identification and system access of authorized users.
	ID management	Technology to perform integrated and safe management of personal certificate information such as passwords and certificates, and the creation, change, distribution and deletion of IDs composed of personal characteristics, attributes and preferences.
	Sub channel attack prevention	Technology to prevent attacks that steal the confidential information through additional channels, EMI or power consumption of H/W devices.
	Personal information security technologies	Technology to guarantee anonymity and prevent privacy invasions in the lifecycle of personal information.
Network and system security	Network invasions responses	Technology (Firewall, IDS, IPS, ESM, and VPN) to prevent shutdowns due to abnormal operation of the network nodes or invasions of the network infra and to ensure continuous applied service.
	Malignant code responses	Malignant code is code that can have negative effects on your computer. Depending on its ability to duplicate itself and vulnerability for infection, it is classified as virus, worm or Trojan virus.
	Security OS	An OS that adds additional security functions to a general computer OS (kernel). It is an OS that can compensate for the vulnerability of kernels and grant access privileges.
	Digital forensic	Based on the digital data contained in an information device, this technology verifies the actual relationships. It describes a series of procedures and methods for data collection, storage and reporting.
	Security chip	By mounting the security functions in the H/W platform, this chip can safely protect applications stored in the computer memory against various attacks.
	Access security	This encrypts the necessary data for login for transmission. It protects this data from various threats over the networks.
	Security evaluation	Technology to evaluate security reliability. Can be classified into security evaluation criteria and system. <ul style="list-style-type: none"> - Security evaluation criteria: criteria to evaluate an information product's ability to respond to threats and the overall level of security. - Security evaluation system: rules governing management, procedures, subject and result of evaluation.

Upper category	Lower category	Definition
Service and applied security	Contents security	Technology to protect various convergence contents, such as digital video and contents generated in the convergence environment.
	Spam response	Technology to prevent/detect/block various types of spam in email, SMS, and blogs, and to identify zombie PCs that send spam.
	VoIP/IPTV/ LBS security	Technology to protect the safety of various broadcasting communication services. VoIP security to prevent internet phone wiretapping and hacking and IPTV set-top box hacking.
	Cloud security	Virtual platform protection, user data leakage prevention, illegal access prevention, service availability guarantees.
Physical security	Disaster monitoring	Disaster management technologies, including collection of disaster information such as security, seas, air and traffic accidents from communication terminals and status reports on disasters.
	Entry/exit controls	Technology for early discovery and immediate response to external invasions. Includes CCTV/DVR, exit/entry controls, security sensors, and search devices.
	Bio recognition	Technology to identify a person by extracting fingerprints, facial features, iris, cornea, hand shape, back of hand, vein or voice, which are different from person to person.
Convergence security	Conveyance security (automobile/ airplane)	Technology to respond to various security threats occurring in conveyance, and to provide comfort for the drivers and passengers in automobile and air conveyance.
	u-health care security	'Health care' is a technology to respond to various security threats. It can perform prevention, treatment, diagnosis and post-management anytime and anywhere with the help of IT-medical convergence.
	Financial security	Security technology to maintain safe and reliable electronic transactions, despite various security threats.
	Smart grid security	Technology to achieve reliability by performing physical security, access controls, subscriber information security and hacking prevention on the power networks.

Source : KCA (2010.7), ITEP (2010.10)

3. Establishment and Operation of Information Security Organizations

3.1 Korea Internet&Security Agency (KISA)

KISA (Korea Internet&Security Agency) was founded on July 23, 2009 through the integration of Korea's three existing organizations-KISA (Korea Information Security Agency), NIDA (National Internet Development Agency),&KIICA (Korea IT International Cooperation Agency).

Pursuant to Article 52 of the “Act on Promotion of Information and Communication Network Utilization and Information Protection, etc.”, KISA is executing various businesses,

including the creation of safe internet environments, the promotion of internet services, the advancement of IT networks, and the provision of efficient support for international cooperation in broadcasting and the exploration of foreign markets.

The original Korean Information Security Agency (KISA) was established as the Korean Information Security Center (KISC) in April 1996, as the government recognized the necessity of information security in the age of informatization. In 2001, it was officially upgraded to the Korea Information Security Agency (KISA). At the time of establishing KISC, vast efforts were made by the relevant government organizations, members of industry and academic partners to provide actual support, so that the overall awareness of information security could be enhanced. The first visible accomplishment was made in November 1996, when the Consortium of Computer Emergency Response Teams (CONCERT) was founded to implement the basis for immediate and systematic responses to the hacking of information systems. As CONCERT began to act, it became possible to take systematic and immediate action against hacking incidents, and in January 1998, the Korean government joined the Forum of Incident Response and Security Teams (FIRST) to enhance Korea's reputation in the global community and strengthen the efforts for international cooperation. At that time, as information systems were widely available, it was necessary to distribute information security systems that could support reliability while meeting the security requirements of the information system operation organizations; however, there was no system in Korea to evaluate the reliability of information security systems. Therefore, KISC prepared its own information security system evaluation criteria and guidelines, developed the relevant evaluation methods, and enforced the evaluation service in February 1998. Moreover, KISC also contributed significantly to the promotion of information security technology development and the standardization and preparation of information security industry promotion plans.

Since the integration of Korea's three internet organizations in 2009, KISA's main functions were 1) operation of the KRCERT/CC, implementation of the cooperation systems for security invasions in Korea and overseas, operation of the illegal spam response center, and prevention and handling of internet attacks; 2) operation of the personal information leakage response HQ and hotline, wide distribution of the alternative means of registration to resident registration numbers (i-PIN) and promotion of the level of personal security; 3) information security product evaluations, digital signature certification management, critical information infrastructure protection, protection of information security management systems (ISMS) in the private sector and the government; 4) execution of campaigns to create more mature internet culture, operation of the Korean internet dream team for early promotion of internet literacy for elementary and junior high school students, promotion of wireless internet, promotion of the use of '.한국' domains and distribution of IPv6 (IP version 6) addresses; 5) support for international cooperation to enhance the international reputation of Korean broadcasting technologies, cooperation with international organizations, support for exploring the overseas markets for broadcasting technologies, service and contents and enhancing the reputation of Korean broadcasting; 6) acting as an organization fully in

charge of internet information security by developing polices and technologies related to internet information security.

In particular, to prevent the threats of the internet such as hacking, viruses, personal information invasions and illegal spam and their related damages, KISA is operating a national public hotline 24/365, free of charge (☎118 call center), the personal information leakage/internet invasions response center (KISC) HQ, the digital signature certification management center, and the knowledge information security industry support center, to make significant contributions to the national information security.

3.1.1 Korea Internet Security Center (KISC)

KISC constantly monitors the domestic internet to discover possible vulnerabilities, security threats such as worms and viruses, or signs of abnormality as early as possible, and issue warnings to prevent incidents from spreading further. In particular, it regularly exchanges information with domestic information service providers (ISP), anti-virus software companies and security monitoring companies, and takes common measures to minimize the socioeconomic losses so that it can implement a safe environment for Koreans to enjoy reliable internet services.

KISC operates a comprehensive status room to strengthen its ability to immediately respond to invasions, and receives network information in real time from the major carriers such as KT, SK broadband and security monitoring companies, in order to perform 24 /365 monitoring. In addition, it executes various projects such as registration and handling of major hacking incidents like DDoS (denied distribution of service) and homepage falsification, and carries out technical consulting for hacking, viruses, worm infections and the like. In addition, it tracks down the origin of malignant code and gives real-time notifications to the relevant organizations and companies in order to minimize potential damages.

In addition, KISC collects information on worms, viruses and newly-emerging vulnerabilities, and uses an objective index to evaluate the risk level, such as the possibility of spread and effects. It issues alarms for the private sector depending on the level of severity, and transmits status notifications to facilitate immediate responses.

KISC makes such efforts to prevent possible incidents and the further spread of damages by performing consistent monitoring and responses, and provides the latest trends of the security industry and the statistics of such incidents on its homepage, KrCERT (www.krcert.or.kr) so that it can successfully support the government in establishing a good information security policy and promoting awareness of information security. In addition, it is pursuing international information exchanges by participating in international organizations such as APCERT and FIRST.

3.1.2 ☎118 Call Center

☎118 call center is an account to respond to Koreans who have inquiries or complaints about domain names, exposure of personal information on the internet or cyber space threats, such as hacking viruses, personal information invasions or illegal spam.

☎118 call center can provide various types of consulting on hacking, viruses, privacy invasions, and internet domains, anytime and anywhere, 24/365.

3.1.3 Knowledge&Information Security Industry Support-Center (KISIS)

KISIS (Knowledge&Information Security Industry Support-Center) is working to lay the foundation for industrial development by implementing and operating an infrastructure for SME's that struggle with knowledge information security due to the inability to afford expensive lab instruments.

In addition to security laboratories for traditional computer and network factors such as network/ system security, password authentication/ anti-virus security etc., KISIS is currently operating a convergence security laboratory for financial IC cards, resident registration cards and electronic passports, as well as a physical security laboratory for CCTV security equipment, and entry and exit control systems. Recently, KISIS implemented a large-capacity DDoS Test Bed. As mobile security has received consistent social attention, additional test environments for mobile security will be added in the future.

3.1.4 Korea National Biometric Test Center (KNBTC)

KNBTC (Korea National Biometric Test Center) is operating to promote the domestic bio recognition industry and the test/certification system for biometrics, and to implement a system that can meet issuing country requirements for mutually recognized certificates.

KNBTC is providing test services to verify accuracy and compatibility of domestic biometric products, such as facial and iris recognition products, and technical consulting services for test projects by the government of public organizations. Tests are performed according to the biometric system test methods suggested by international standards such as ISO/IEC JTC1 SC37. For this purpose, KNBTC prepared guidelines for the biometric test and certification procedures. In addition, KNBTC is promoting biometric products development to comply with the international standards, and is supporting exploration of the foreign markets with domestic biometric products. KNBTC also makes efforts to lead the international standardization and test technologies in the area of biometrics.

3.1.5 KISA Academy

KISA academy is working to improve public awareness of information security and to provide systematic education for training skilled workforce for the knowledge information security industry. At the same time, the education curriculum is developed and operated by reflecting the domestic and overseas requirements for new information security education.

3.2 e-Government Security Monitoring Center (G-Cert)

In September 2005, the Ministry of Public Administration and Security implemented the e-government security monitoring center to cope with cyber threats in real time, but the local self-governing organizations had no monitoring systems for cyber attacks whatsoever. Thus, in 2006, the national cyber security strategy meeting decided to organize an e-government invasion incident response committee through the joint efforts of the Ministry of Public Administration and the local self-governing organizations. In July 2007 the e-government act and the revision of the enforcement ordinance of the same act began to strengthen the security rules for e-government, so the ministry began in 2008 to implement security monitoring centers for 16 metropolitan local self-governing organizations, and started interconnection operation. In 2009, to strengthen the capacity of the local self-governing organizations to handle cyber attacks, the cyber attack response centers for the sixteen cities and provinces were implemented at KLID (Korean Local Information Research and Development Institutes).

These efforts made it possible to perform 24/365 monitoring and handling of threats on the information communication networks of the local self-governing organizations. In addition, to promote the security and reliability of the web service, which is the key public service of e-government, consistent efforts are being made to check and resolve the security vulnerabilities of 1,200 major web sites.

On the other hand, to improve the capacity of local self-governing bodies to respond to DDoS attacks, the nationwide response system was implemented, and simulation exercises are performed according to the 'DDos response manual.' To maximize the capacity of local self-governing organizations to operate the security monitoring centers, the staffs in charge of cyber attack handling are provided with security education on a regular basis.

3.3 National Security Research Institute (NSRI)

The NSRI (National Security Research Institute) is an information security research organization established to develop technologies to protect the critical information infrastructure, and to develop technologies and policies that can effectively respond to cyber attacks to the national and public organizations' information communication system and networks.

NSRI was established in 2000 pursuant to Article 8 Clause 1 of the “Act on Establishment, Operation and Promotion of the Government Funded Research Institute in Science and Technology,” and since its establishment, it has been performing research and development work to acquire cyber security related technology in the public sector. Thus, by researching national encryption technologies, developing hacking response technologies and information security technologies, supporting relevant policies and implementing the foundation and supporting activities, the NSRI has been contributing significantly to the development of national security technologies.

In addition, to strengthen the foundation of domestic information security and R&D, and to establish the basis for national communication and data information security, each year NSRI has been hosting the WISC (Workshop Information Security and Cryptography). Through such activities, it has been sharing the latest trends of information security with domestic information security businesses, such as the administrative department and their subordinates departments, the communication infra companies and academia. Through the implementation of organic, cooperative relationships, it has been contributing to the development of domestic information security. In addition, it is analyzing and collecting the information of the latest information security related technologies domestically and internationally and the shifting paradigm of policies for the relevant organizations.

On the other hand, NSRI has been operating the security monitoring technology support center to monitor the research institutions. The security monitoring technology support center was opened in July 2010, and has been maintaining 24/365 monitoring of 26 research institutes, including the NRCS (National Research Council for Economics, Humanities and Social Science) and its subordinate government funded research centers in order to provide a cyber security service that can monitor and prevent cyber attacks.

3.4 Electronics and Telecommunications Research Institute (ETRI)

The Electronics and Telecommunications Research Institute (ETRI) is operating a software knowledge information security research department. In 1999, to develop information security technology for the private sector, the information security technology research center was established, and has since been developing various information security technologies for the private sector.

The knowledge information security research department is making intense efforts to research and develop technologies in the fields of information security, physical security and convergence security, as the global IT security trend gradually shifts from “competition for information security in communication” to “competition for knowledge information security in daily living.”

First, in the fields of information security, it aims to implement a clean internet economy. It is currently developing security products and services that can prevent damages,

falsification and leakages of the information on personal PC's or networks. This includes hacking/invasion detection, forensics, digital intellectual rights protection, harmful information blocking, digital ID management and digital ID wallets.

Second, in the field of physical security, to provide a safe daily living environment, ETRI is developing security products and services that can prevent disasters and support the safe operation of the main infrastructures. This includes alarm monitoring, unattended electronic exit/entry controls and biometrics.

Third, in the field of convergence security, ETRI is developing security products and services in which physical or information security is combined and converged with non-IT or traditional industry. This includes national defense, financial security, transportation security (automobile, airlines), shipbuilding, medical and construction security, and surveillance security robots.

Moreover, the knowledge information security department has signed MOUs with relevant domestic organizations and is promoting technology exchanges and cooperative activities in order to strengthen its own capacity to develop technologies.

3.5 KFTC (Financial Sector Information Sharing and Analysis Center)

KFTC's financial ISAC (Information Sharing and Analysis Center) is a financial analysis center that is approved by the Korean government. Currently, it is providing various information security services, including real-time integrated monitoring, vulnerability analysis for the information communication infra, information sharing such as alerts on threats, and information security education for 20 financial companies (17 domestic banks, KFCC, Shyinhyp NCUFOK, NCFE).

KFTC's financial ISAC takes immediate action to handle various cyber attacks such as hacking and malignant code distribution, and issues an alarm depending on the threat level so that financial companies can respond to invasions on their own.

In addition, by analyzing the vulnerability of a financial company's information communication infra such as its internet banking system (including smartphone banking), it eliminates potential threats and supports safe electronic financial services, through emergency actions on the spot when necessary.

As DDoS attacks have become larger in scale, when an attack exceeds the defense capacity of DDoS attack response system is in place, the 'Financial ISAC DDoS Attack Response Center' is operated jointly by the KFTC and participating organizations.

In addition, to promote information security awareness among financial company employees and to encourage the exchange of information on information security, each year KFTC's financial ISAC hosts a technical seminar and workshops. It provides visit training

and group education (including practical education) and various other types of education programs suitable for the IT staff and employees of financial companies.

3.6 KOSCOM

KOSCOM's financial ISAC (Information Sharing and Analysis Center) is an information sharing and analysis center approved by the Korean government. Currently, it is providing various information security services, including real-time integrated monitoring, vulnerability analysis for the information communication infra, sharing of information such as threat information, and information security education for 70 financial companies (stock traders, future markets, and stock related organizations).

KOSCOM's financial ISAC analyzes the vulnerabilities of the cyber trading system at stock trading companies, establishes security master plans and provides electronic financial consulting and information security service for each company. Also, it provides system and network security infrastructure design and analysis, personal information protection and wireless mobile security analysis, as well as various other types of consulting.

In the future, it will strengthen its capacity to prevent and respond to new cyber attacks by increasing new members that use real-time alarms/analysis service, installing a new department in charge of invasion responses, and performing simulation hacking of electronic trade systems and DDoS simulation exercises.

3.7 Financial Security Agency (FSA)

The FSA (Financial Security Agency) was established in October 2006 to support the government in the information security business for the financial sector under the 「Comprehensive Plan for Promoting Stability of Electronic Transactions」.

The FSA implemented the OTP (one time password) integration certification center in June 2007 to improve customer convenience, eliminate duplicate investments and improve its efficiency. As of the end of December 2012, about 4.5 million OTP generators are being used. The OTP integration certification center processes an average of about 1.51 million transactions per day, contributing to the safe use of electronic commerce.

In addition, through mutual cooperation with the relevant organizations, the FSA supports the analysis and handling of emerging security vulnerabilities in the financial sector, while pursuing R&D in the financial security sector, including adequacy tests on security products applied to the dramatically developing financial IT environment.

In addition, the FSA hosts an annual event called the Financial Information Security Conference (FISCON), and holds an information security contest in the financial sector

in a joint effort with the financial information security committee. Strong efforts are being made to promote awareness of financial information security and to enhance the level of such activities.

4. Information Security Awareness Promotion Activities

To create a safe internet environment, the relevant laws and systems, technologies and processes are important. But most of all, each layer of society (government, organizations, companies and individuals) must be fully ready to practice information security. Considering that as almost all Koreans are using the internet, each individual's PC, smartphone or IT device can be abused for a large scale DDoS attack or malignant code distribution, it is critical to promote individual awareness of information security, and encourage people to practice information security actions.

4.1 Status of Information Security Awareness in Korea

According to the "2010 information security survey" announced in March 2011, about 99.5% individual internet users who were surveyed responded that they recognized information security and personal information protection on the internet as one of the most important issues. Also, each year, more people recognize the importance of information security. However, while many internet users know that information security is important, they seem to have difficulty in determining where to obtain the necessary information. In other words, it is necessary to unify the source of information security related information that is provided for internet users, while at the same time, it is necessary to publicize it in an interesting and intuitive way.

4.2 Overview of Activities to Promote the Awareness of Information Security in Korea

The most urgent issue in promoting the awareness of information security is to determine "how" to publicize "what." Regarding "what" to publicize, it is important to understand what is most urgent and fundamental depending on the status of IT and internet services in each country. Regarding "how" to publicize, as each country has a different IT infra and living culture, it is very important to determine what kind of approaches should be taken for what group of people, as all visible and audible things can be good tools.

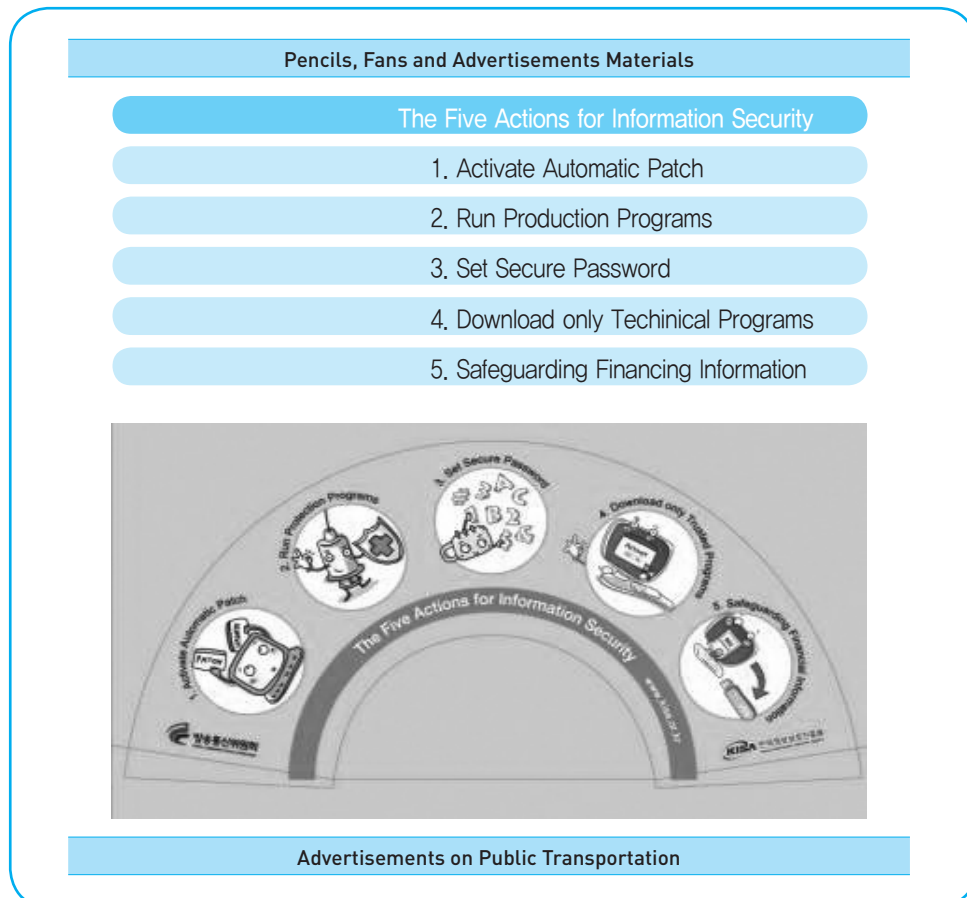
To allow the general public to easily access the necessary information, the Korean government has been using various on/off line methods for multi dimensional publicizing. In order to avoid difficult-to-understand and too-official policy advertisements, and to

promote an image of information security you can easily find in your daily life, customized information security publicizing efforts were made for each age group.

4.2.1 Establishment and Distribution of Information Security Practice Guidelines

Information security can easily be regarded by the general public as a tedious and difficult issue, so it is very important to deliver a simple message that conveys the mandatory information security guidelines. In 2001, the Korean government enacted and distributed the eight major practice rules for information security, and in 2005, they enacted the 10 major practice rules for information security by adding the new major incident types, such as spyware, phishing, P2P and messenger. In 2007, this was simplified into the five major rules, which were publicized via online posting, pencils, fans and public transportation ads, which can be easily seen in daily life.

Figure 4-2 | Examples of Information Security Ads





The practical rules for information security are aggressively publicized in overseas countries as well as in Korea, as many countries have enacted their own practical rules to suit local conditions.

4.2.2 Public Telephone Consulting Service (☎118) Operation and Publicizing

In 1988, the CIH virus infected about 300 thousand PCs in Korea and caused other large-scale damage. If a problem like this occurs in the information communication network, it can spread very quickly over the internet. Therefore, it is very critical to immediately register the current situation and make systematic efforts to handle the problem. For this purpose, the Korean government established a hacking virus consulting support center to consult and report cyber terrors and emergency cases by calling the hotline (☎118). On January 25, 2003, when the Slammer worm virus hit the entire world, many phone call reports were made to 118.

In the early phase of IT development, information security was left to information security experts and persons rather than the general public. However, as IT devices were diversified and the rate of internet use by all Koreans was increased, information security became a very critical problem that all Koreans should handle. However according to a survey of information security status, while many people recognize the significance of information security, they do not really know where to get the information that will enable them to apply security appropriately.

So on January 18, 2010, the Korean government expanded the 118 hotline, which used be the main line of communication for the information security experts, and made it available to all Koreans. In addition to information security, all internet-related consultations are made

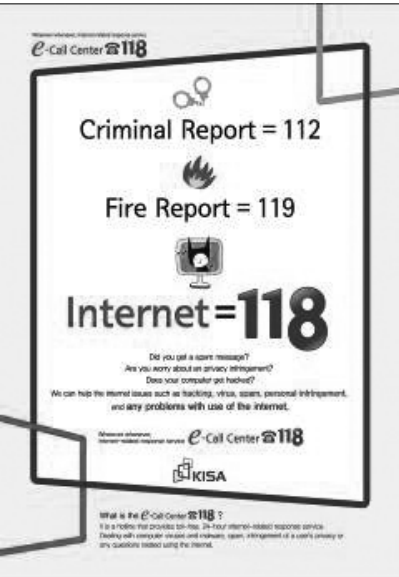


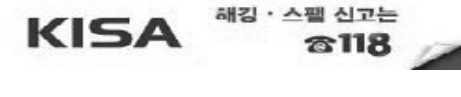
through that number. 118 is a three-digit number designated by the Korean government, and no matter what time it is or where you are, you can call the hotline to receive free consulting.

The government has been emphasizing the fact that you can call 118 anytime anywhere when you have a question about information security. Using the very easy-to-remember three-digit number, we can all easily remember this hot line, which is very similar to the emergency number, 119.

They also developed many types of advertisements, such as advertisements in newspapers and magazines, online banners, leaflets, etc., and popular ads like 118 songs and 118 dances. These popular ads attracted many youth who were interested in songs and dancing. Also, various information security methods, security patch updates and PC security methods were expressed in interesting songs and dances, so that children and youngsters could easily follow them.

118 song and everyday-song music video were posted on the internet to allow netizens to access them easily. Everyday-song was broadcast on a kids program on EBS in February 2010, and on that day many kids watched and followed the song and dance related to information security.

Figure 4-3 | 118 Paper Ads and 118 Songs, Everyday-song Music Video

118 paper ads (for all Koreans)	118 song music video (youth and adults)
	
	Everyday song music video (for kids)
	
	118 banner ads (for all Koreans)
	

In addition to online internet ads, great efforts were also made offline to publicize 118. Various performances were held to attract the attention of the public. 118 wave performances, subway station 118 performances, 118 national bike ride, and 118 world cup rallies were held to provide effective advertising. In addition, 118 participated in IT exhibitions, which were attended by many citizens, including youth, to publicize 118 in a friendly manner.

Figure 4-4 | Information Security Publicizing Activities

Contents	118 offline ad materials
118 dance performance, 118 wave performance	
118 national bike ride, 118 world cup rallies	

4.2.3 Textbook Used to Promote Youth Awareness of Information Security

To effectively deliver information security related knowledge to youth (junior high and high school students), the group most actively using the internet, education at school plays a very significant role. So, the Korean government modified the curriculum and included the subject of “information security and sharing” in the technology and housekeeping textbook for the 8th grade. Since 2011, junior high school students in Korea have been learning the subject of information security.

4.2.4 Use of Mass Communication such as Broadcasting

Newspapers and broadcasting are two of the most familiar media types to Koreans. In particular, for tough subjects such as information security, the news media plays a very significant role. Using the news media, the importance of threats such as hacking, viruses, spam and personal information invasions can be emphasized, and the government policies

on information security and the methods for handling and practicing information security can be aggressively promoted. As a result, a positive social consensus can be created.

To maximize the production of good quality information security news on the main news channels, radios and magazines, the best efforts should be made by providing news reporters with good information and cooperating with them very closely. So, for various information security topics such as personal information protection, safe methods for using SNS, and the seriousness of internet invasion incidents, articles, interviews and special TV programs were produced to promote an awareness of information security among Koreans.

In particular, as the PCs for general users were frequently infected by malignant code and abused as the source of internet incidents such as DDoS attacks, it became very important to notify users of the danger of malignant codes and provide a method for protecting their own PCs. As such necessity arose, KCC and KISA began to unfold large-scale TV campaigns that could promote the awareness of information security among Koreans.

To inform users of the danger of malignant codes and the method for protecting their own PCs, through close cooperation with the major broadcasting companies, various types of cultural programs, cable TV special news, and documentaries were produced to promote an awareness of information security. The average viewing rate for terrestrial TV programs was estimated to be around 6.7%. The most popular programs were *Sponge Zero*, and the documentary “Zombie PC wants you!” and these were rebroadcast over cable TV to allow more viewers to watch them. The subjects included zombie PCs, personal information security, mobile phone spam, SNS, wireless LAN, VoIP, Stuxnet and other various types of internet incidents and preventive measures.

The programs broadcast on TV were made available by KISA in various ways, including the protection world homepage

(<http://broadcast.boho.or.kr/UserView/UserView.jsp>) and on smartphones (iOS, android) information security apps, so that they can be available for students and employees in the area of information security, anytime and anywhere.

Figure 4-5 | Information Security TV Program Rerun and Captures



4.2.5 SNS Used to Promote Information Security Awareness

As various mobile devices such as smartphones began to gain popularity, in addition to traditional media such as TV, new information delivery media such as Twitter and Facebook began to emerge. According to a smartphone use survey performed in the first half of 2011, as of August 2011, in Korea there are about 15 million smart phone users, who use them for SNS 1.9 hours a day, on average.

KISA unified its Twitter, Facebook and blog IDs as 'Kisa118' and is currently delivering information on internet incidents as quickly as it can. When March 4th DDoS attack and large scale personal information leakage incidents occurred in 2011, the news was transmitted very quickly to prevent further damages and to notify the public of how they can prevent additional damages. Also, smart phone applications were developed and distributed to provide interesting quizzes on information security subjects.

Figure 4-6 | Information Security SNS&Smartphone Apps

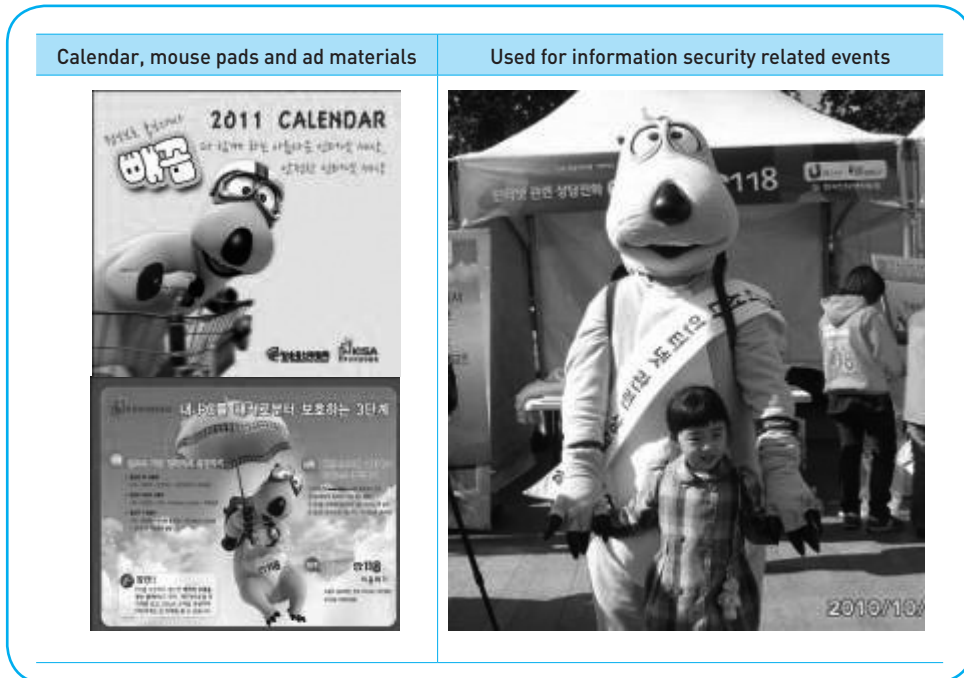


4.2.6 Friendly Information Security Advertising using Honorary Ambassadors

It is always a good idea to develop unique characters that are suitable for the subject of information security, but it is true that it takes some time and money to develop characters and publicize them in Korea. For this reason, it may be a good idea to utilize existing characters and personalities who are already popular among Koreans.

In Korea, utmost efforts were made to promote the subject of information security in a friendly manner. Animation companies who provide well-known animation characters for kids were contacted, and a nationwide campaign for information security was pursued to utilize the characters in an efficient way. This was much cheaper than hiring popular celebrities, and the characters could be utilized for various printed and video materials.

Figure 4-7 | Information Security Publicizing Activities



4.2.7 Promotion of Information Security Practice through Social Contributions

KCC and KISA have been pursuing an “internet information security campaign” to provide free PC repair services for social welfare organizations that seniors and the handicapped use since 2008. In 2010, they visited about 30 welfare centers including Gyeonggi-do, Chungcheongnam-do, Busan and Seoul to install Windows security patches and vaccine programs on PCs. Joint efforts are being made in conjunction with KUCIS (Korean University Clubs of Information Security). College students are trained in PC security and given the opportunity to provide social services on their own. Thus far, about 260 college students have participated in repairing more than 1,300 PCs.

4.2.8 Hacking Prevention Contests

To respond to the rapid evolution of hacking technologies, the ability of the staff in charge of information security is very important. Since 2004, KCC and KISA have been hosting hacking contests to promote the skill level of information security experts and to train ethical hackers. In this contest, unlike traditional hacking contests that measure the attacking abilities of contestants, contestants analyze a virtual server that is being attacked in order to evaluate their ability to track attackers, and determine the scope of damages

and the attacking methods. In 2010, the seventh hacking contest was held. In this contest, a traditional problem related to web hacking was quickly resolved, but the latest issues associated with smartphones were not properly resolved. The previous year's winner was eliminated in the early phase of the tournament, and the new high school teams advanced to the main events. A generational change was apparent at this event.

4.2.9 Information Security Grand Prize

To promote the level of information security in the private sector, since 2002 KCC and KISA have been offering the Grand Prize for Information Security to companies that show model information security practices. The purpose is to identify and reward companies that can be information security role models, and to publicize them aggressively so that the private sector's voluntary activities to promote information security can be supported, and companies CEOs are encouraged to increase their investments in information security. An ISA (Information Security Award) mark is given to the winning company so that it can be clearly displayed as a role model of information security practice.

5. Information Security Cooperation Partner's Activities

5.1 Information Security Cooperation Activities in Korea

5.1.1 Korea Institute of Information Security&Cryptology (KIISC)

KIISC (Korea Institute of Information Security&Cryptology) was established in December 1990 to contribute to academic and technological development and promotion in the fields of information security. KIISC is currently executing various types of business, including academic seminars on information security, academic and technological research and publication, research for the establishment of standards and specifications, the project for technology distribution and development, and the project to implement the basis for training experts.

To implement the basis for exchanging international academic and technological standards in the field of information security, KIISC has been hosting renowned international academic seminars each year that are participated in by more than 10 countries. The most popular of these include WISA (Workshop on Information Security Applications), which is specialized in network and service security applied technologies, and IWDW (International Workshop on Digital Watermarking), which mainly deals with copyright protection and watermarking technologies. As a domestic academic seminar, it has been hosting the NETSEC-KR every year since 1995 to take a leadership role in domestic information technology development and upgrades by promoting active information exchange in the fields of the latest domestic and foreign information security technologies and information security service industries.

In terms of academic research in each specialized area, various activities are being performed by about 18 research institutions, including: the Digital Identity Management Research Society, the Digital Forensic Research Society, the Linux Security Research Society, the Information Security Management and Policy Research Society, the Information Security Education Research Society, the Information Security Standardization Society, the Cloud Service Security Research Society and the Mobile Security Research Society. Each research society hosts regular workshops to discuss the latest research results and the domestic and overseas technology trends. The most popular examples include: the u-home security certification digital ID management common symposium jointly held by the Digital Identity Management Research Society and the Home Network Security Research Society, the digital forensics workshop to discuss the latest trends of digital forensics technologies and the utilization methods, and the information security education workshop, where experts in charge of information security education gather to present actual case studies.

In addition, the academic society magazine to introduce the latest information security trends and the proceeding of academic journals are published every other month. To address the latest issues in information security, discussion sessions are frequently held. In 2011, the personal information security act workshop was held to discuss the changes brought about by the enactment of the Personal Information Protection Act.

5.1.2 Knowledge Information Security Industry Association (KISIA)

KISIA (Knowledge Information Security Industry Association) is the only legal corporation that represents the domestic knowledge information security industry. It was initially launched as the information security industry committee in August 1997, and was re-launched as KISIA (Knowledge Information Security Industry Association) in September, 1998. With the growth in the importance of information security industry, and the emergence of the necessity to promote the relevant strategies, in September 2004, according to the “Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.,” it was shifted to a legal corporation, and in September 2009, according to the “Information Communication Industry Promotion Act”, its name was changed to KISIA. As of August 2011, its 150 active members include network security, anti-virus software, PC security, contents security, information security consulting, and physical security companies.

Its main activities include making suggestions for the efficient improvement of the information security related legal systems, academic/research/industry R&D for technology development, support for training special manpower, investigations of the trends and statistics of the information security industry, common resolution of hardships in industry, support for participating in information security exhibitions in Korea and abroad, and common research on information security by the government and the relevant organizations.

In 2010, KISIA investigated the market trends of the domestic knowledge information security and performed various activities such as the operation of SIS license and education programs, operation of knowledge information security technology forums, and support for overseas market explorations and marketing in order to promote specialization in information security.

In particular, KISIA executed various projects to support overseas market exploration that enabled domestic information security companies to enter Asian markets such as Japan. KISIA operated the Korean booth at Japan's most popular information security exhibitions, IST 2010 and Security Show 2010, and Vietnam's SecuTech Vietnam 2010, introducing excellent Korean information security products and companies to those countries. In addition, KISIA dispatched a market exploration team to Malaysia to offer 1:1 business consulting and more. In addition, to enhance their support for domestic companies expanding business networks in Japan, KISIA signed an MOU with Japan's most popular information security organization, the Japanese Network Security Association (JNSA), as well as the Japanese Information Security Audit Association (JASA) and others. KISIA also agreed to pursue business partnerships with the Malaysian information security control organization, CSM (Cyber Security Malaysia). Many efforts were made to broaden the scope of business cooperation with overseas organizations. In addition, to expand the domestic market for knowledge information security industry, joint efforts were made with the relevant organizations to host defense information security conferences and financial information security conferences. As part of its diversification efforts, a biometrics conference was held to promote the awareness of biometrics technologies among Koreans.

5.1.3 CONCERT

Consortium of Computer Emergency Response Teams (CONCERT) is a consultative group formed by voluntary participants such as the CER or the information security department within a private company or organization, and was established in 1996 under the motto, "I will protect my own information!" Reflecting the characteristics of the organization as one in which private companies and organizations participate voluntarily, in June 2005, it was re-launched as a corporation.

Its main businesses include: implementation of a contact system to transmit incident information among the members very quickly, mutual information exchanges on attacks on the information communication networks, the necessary works for handling invasions to the global information communication networks, supports for CERT organized by information communication network operators, education and seminars to improve the capacity to respond to incidents, investigation of the status of information security at each company, and preparation and distribution of reports on information security.

Considering the fact that members of the association are departments in charge of the information security of a company or organization, in addition to the information

exchanges related to incident response technologies, education and information exchange of management for information security strengthening has recently been emphasized. Membership in CONCERT is classified into three types-regular member (a company or organization who operates the CERT team or response department for the information communication networks that it is operating), associate member (a company or organization who is preparing to operate the CERT team or response department for the information communication networks that it is operating), and partner member (a company who manufactures and sells information security related service and systems). As of August 2011, there are 143 regular members, 169 associate members and 107 partner members, for a total of 419 members.

In 2010, the main activities include: small committees where security managers in the industry can share information and respond to current issues, a security round-up where 20 to 30 regular members join each other to discuss issues of information security in depth, a regular member workshop where about 150 employees at regular member companies participate for two days and one night, the 'CONCERT FORECAST 2010' seminar to draw forecasts on the trends of information security activities at a company, and the hacking prevention workshop called the Annual Security Users' Festival that investigates the cases and issues of information security activities committed by a company. In addition to these, the company information security status report and issue reports were published.

Figure 4-8 | Hacking Prevention Workshops



Source : CONCERT, www.concert.or.kr

5.1.4 KCSOA

KCSOA (Korea Association of Chief Security Officers) was established in June 2009 to promote cooperation and information sharing between CSOs (Chief Security Officers) in the private and public sectors. By collecting opinions from the CSO of each industry, practical and efficient information security policies can be established, as well as a desirable role model for CSOs.

For this purpose, KCSOA implemented private/public sector cooperation systems for cyber attacks, delivered response plans for the latest security issues and emergency information and shared information on them, hosted hearings and seminars to promote information sharing, published practical guidelines, periodic magazines and research data, and carried out publicity campaigns.

In 2010, KCSOA hosted a total of 10 CSO forums to discuss the roles of the public/private sectors in information security threats, the status and plans of internet fraud, the status of personal information management and the related political tasks, the status and forecasts of convergence security, the implementation plans for the security monitoring system depending on the changes in the type of cyber attacks, the response plans for second July 7th DDoS attacks, the role of the CSO in strengthening the national information security, the cause analysis and response plan for industrial espionage, and the status and plan of stuxnet.

In addition, in March 2010, about 800 persons representing the businesses to which the information communication act applies, the personal information security staff at the central government, local self-governing organizations and public organizations as well as the members of the KCSOA attended the ‘Smartphone Security Threats and Response Workshop’ to suggest a plan for the government and companies to handle the paradigm shifts to the smart age and the sudden increase in the number of smartphone users.

5.1.5 Korean CPO Forum

The Korean CPO Forum (Korea Chief Privacy Officers’ FORUM) was established in November 2007 based on the consensus that private companies are required to voluntarily strengthen regulations, so that issues of personal information security could be resolved properly. The Korean CPO Forum’s goals are to share the latest issues of personal information, as many VIPs in each layer of society such as academia, business and relevant organizations attend, while collecting and delivering opinions from the private sector for personal information security legislation and policy establishment.

Its main functions include: mutual exchange of personal information related information and technologies, issuance of personal information security specialist licenses, education and seminars on personal information security, collection and delivery of opinions from the private sector for personal information protection policy establishment, and international cooperation with the relevant organizations in foreign countries.

The main businesses executed in 2010 include the following. Monthly ‘Privacy Round Up’ events were hosted to provide the latest issues and trends of personal information security and privacy. Also, Privacy Global Edge 2010, the international personal information security symposium, was held to share domestic and overseas issues and trends of personal information security by inviting the main personal information security experts from each country. Notably, in December 2009, the Korean CPO Forum began to offer a Certified Personal Information Manager (CPPG) license test to suggest an objective index for measuring the ability of personal information management staff for companies and organizations, contributed to the education of personal information security experts, and promoted personal information security awareness among Koreans.

5.1.6 Korea Information Assurance Society (KIAS)

KIAS (Korea Information Assurance Society) was established in December 2001 by military, government, academic, industrial and research experts in order to promote professional knowledge among its members and to protect the main national information communication infrastructures by facilitating academic and information exchanges among domestic and foreign organizations, as well as by performing R&D on cyber terror and information warfare.

KIAS regularly hosts conferences and academic symposiums for the general public and industrial experts under the topic of ‘Cyber Terror&Information Warfare’. In addition, the customized digital forensic expert education is training forensic experts who can investigate and analyze illegal invasions, confidential information leakages and hacking incidents, both in the Police Department and in companies.

In Chungcheong Province and Gyeongsang Province, there are research societies in eight areas. Each year, four information security journals are published and two academic proceedings are held to discuss and give presentations on information warfare, and international conferences are hosted by inviting experts in cyber terror and information warfare from all over the world. In addition, KIAS cooperates with various organizations, such as the KISF (Korea Information Security Forum) and the GITSC (Gyeonggi Industrial Technology and Security Corporation), to perform research in the field of industrial security and provide symposiums and seminars.

In April 2010, KIAS hosted the ICISA2010 (International Conference on Information Science and Application) with the industrial technology protection center of Gyeonggi University and the ICHIT 2010 (International Conference on Convergence&Hybrid Information Technology) with the military and private engineering research center of Hannam University in August 2010 in order to provide opportunities to share the latest information security issues and the global trends of computer engineering.

In addition, in November 2010, KIAS hosted the ‘11th cyber terror information warfare conference’ with the Ministry of National Defense, and invited about 400 members of

information security divisions in the military, government organizations and companies to discuss the latest trends of cyber warfare, the multi-dimensional threats in the open age and the plans to respond to them, the responses to cyber attacks on the main national communication infrastructures, and the development direction of national defense information security plans depending on the changes in cyber attacks in the future.

5.2 Overseas Information Security Cooperation Activities

5.2.1 OECD WPISP (Working Party on Information Security and Privacy)

The OECD WPISP (Working Party on Information Security and Privacy) is one of the working parties under the supervision of the ICCP (Committee for Information, Computer and Communications Policy) and it is comprised of over 100 representatives that represent 34 member countries. The WPISP hosts a general meeting at the OECD HQ in France Paris twice a year to comparatively analyze the cyber security policy for each country, and develop policies in areas such as personal information security, digital ID management and internet economy promotion. The volunteer group and the focus group discuss specific subjects via email and conference calls.

5.2.2 ITU (International Telecommunication Union)

The ITU (International Telecommunication Union) adopted resolution 130 (Malaksh, 2002) and resolution 149 (Antalya, 2006) to expand its area of activities to cyber security. Resolution 130 (The role of the ITU in reliability and security implementation regarding the use of ICT) allows the ITU to perform various activities for reliability and security implementation in the fields of ICT (Information Communication Technology), while resolution 149 (Definition and Terms for Reliability and Security Implementation regarding the use of ICT) commands the ITU to organize and operate the working parties for the committee to summarize the common terms related to reliability and security implementation regarding the use of ICT.

The ITU-T's subordinate SG17 (Study Group 17) for information security organizes three working parties to develop the international standards: Network security areas (WP1: Working Party 1), applied security areas (WP2), and identity management and language areas (WP3). At each annual international meeting, Korea has submitted articles. The acceptance rate of Korea's articles is currently 40%, indicating that Korea is a very active member of the community.

5.2.3 APEC-TEL SPSG (APEC Telecommunication and Information Working Group: Security and Prosperity Steering Group)

The APEC-TEL (APEC Telecommunication and Information Working Group) supervises the SPSG (Security and Prosperity Steering Group) that discusses information security. It was established in 2006 to discuss the plans for suppressing cyber crimes such as spam and hacking in the international community and to share information on the network and IT security, and is hosting two general meetings each year.

At the 41st official meeting held in May 2010, the Seoul-Melbourne multi-party spam response MOU was renewed to extend the expiration period by three years, as it was about to expire in April 2010. Moreover, the scope of MOU participants was expanded to private companies such as ISPs and communications service providers, and it was decided that a face-to-face meeting would be hosted once per year. On the other hand, the APEC cyber terrorism seminar summary, which was jointly executed with the APEC CTTF (Counter Terrorism Task Force) under the leadership of the Ministry of Foreign Affairs and Trade, was selected as the deliverable of the project. At the meeting, many reports were submitted regarding cyber security awareness promotion activities in Korea, such as launching ☎118 hotline and carrying out awareness promotion and internet attack prevention.

5.2.4 FIRST (Forum of Incident Response and Security Teams)

In 1989, as the worm virus called Wank caused a huge damage, the need for the CERT teams to achieve smooth communication and control was emphasized. So in 1990, the FIRST (Forum of Incident Response and Security Teams) was finally organized, in which the CERT teams from many countries participate as members. FIRST is now a non-profit international organization in which 240 CERT teams from countries all over the world, including USA, EU, Asia-Pacific regions, and Africa.

The KrCERT/CC has represented Korea by attending the FIRST conferences since 1996. In 1998, Korea was the first Asian country to join FIRST as a regular member, and since then Korea has been performing various activities. As of the end of 2010, including the KrCERT/CC, 7 organizations (ASEC, ECSC, INFOSEC-CERT, KF/ISAC, KFCERT, KNCERT) are participating as regular members to the FIRST. In 2010, two domestic organizations (ECSC, KF/ISAC) became new members with support from KrCERT/CC.

From June 13 to June 18, 2010, The KrCERT/CC attended the annual general meeting and conference held in Miami USA and acted as a regular member by participating as an operation commissioner. At this conference, the latest trends of the evolving internet environment and IT were presented. The interesting topics included virtualization technology, and cyber threats in the cloud environment. Also, discussions were held on various topics such as virtual technology convergence, large-scale computing environments affecting information security, and the significance of personal information leakage.

5.2.5 APCERT (Asia Pacific Computer Emergency Response Team)

APCERT (Asia Pacific Computer Emergency Response Team) was established to encourage and support mutual cooperation among the CERT teams in the Asia-Pacific regions. Only countries within the longitude of 60 degrees defined by the APNIC (Asia Pacific Network Information Center) can join the organization. Unlike APEC, APCERT does not allow countries from the American continent to join the organization.

KrCERT/CC has been aggressively participating in APCERT activities as an operation commissioner, and during 2005 and 2006, it led international simulation exercises at the APCERT level twice. KrCERT/CC was reelected as an operation commissioner with the most votes at the annual meeting of APCERT held in Phuket, Thailand, March 2010. In 2011, it successfully hosted the annual APCERT general meeting and conference in Jeju-do. From March 22, 2011 to March 25, 2011, the APCERT general meeting and conference was held at Lotte Hotel, Jeju-do. At the meeting, the main topic was “prevention and handling of cyber attacks,” and the latest issues of information security, the trends of cyber attacks and the cooperation plans for implementing a cyber space that the Asian Pacific regions can use safely were discussed. In addition, KrCERT/CC was elected as the vice chairman of the APCERT at the general meeting.

2011 Modularization of Korea's Development Experience
Information Security Activities in Korea and Implications

Chapter 5

Evaluation

1. Information Security Index and Policies:
International Comparisons
2. Information Security Policy Accomplishments

Evaluation

1. Information Security Index and Policies: International Comparisons

Currently, the only index that can be used to compare the information security levels of different countries is the ‘secure server index,’ which is included in the network preparation evaluation items prepared by the WEF each year. It is also used by OECD, the World Bank and others. A secure server is the most fundamental protection measure that safely protects personal information against illegal invasions by only transmitting personal information such as resident registration numbers, ID and passwords in an encrypted form. According to the 2011 world ICT report (Global Information Technology Report 2010-2011) submitted by the WEF, Korea is ranked 12th among 137 countries, which is a slight improvement from its 14th place ranking in the previous year. For the past several years, the ranking of secure server distribution in Korea has been as follows: 51st in 2008, 16th in 2009, 14th in 2010, and 12th in 2011, showing an increase of 35 places in 2009 and a gradual improvement following that.

As mentioned earlier, the reason why the rate of secure server distribution was increased rather dramatically is because the government made aggressive efforts to investigate and publicize the actual condition of web sites handling personal information, and to help small and struggling companies to actively pursue secure server distribution policies. In particular, the 2007 revision of the “Technical and Management Protection Standards for Personal Information” clearly indicated the existing encryption measures as an implementation of the secure server, which prepared the basis for administrative actions. As a result, various secure server distribution policies pursued by the government led to a sudden increase in the number of secure servers distributed that year, which led to an improvement of the WEF secure server index of 2009 (actual stats are two years older than the WEF announcement).

Table 5-1 | WEF Secure Server Statistics and National Ranking

National ranking	2008	2009	2010	2011
1	1,258 (Iceland)	1,421 (Iceland)	1,562 (Iceland)	1,711 (Iceland)
2	859 (USA)	1,060 (USA)	1,174 (USA)	1,414 (Netherlands)
3	644 (Canada)	828 (New Zealand)	1,105 (Netherlands)	1,234 (USA)
4	596 (Denmark)	812 (Switzerland)	1,036 (Denmark)	1,212 (Australia)
5	584 (New Zealand)	812 (Canada)	993 (Australia)	1,166 (Denmark)
6	584 (Australia)	807 (Australia)	980 (New Zealand)	1,120 (Swiss)
7	582 (Luxembourg)	805 (Denmark)	977 (Swiss)	1,077 (Luxembourg)
8	580 (Swiss)	780 (Netherlands)	940 (Malta)	1,059 (New Zealand)
9	561 (UK)	753 (UK)	912 (Luxembourg)	1,011 (Norway)
10	486 (Malta)	737 (Luxembourg)	906 (Canada)	986 (Malta)
11	420 (Ireland)	698 (Malta)	904 (UK)	984 (Canada)
12	412 (Netherlands)	621 (Norway)	844 (Norway)	927 (Korea)
13	406 (Sweden)	600 (Sweden)	772 (Sweden)	905 (UK)
14	390 (Norway)	551 (Ireland)	696 (Korea)	857 (Sweden)
15	381 (Finland)	542 (Finland)	684 (Finland)	802 (Finland)
16	349 (Germany)	498 (Korea)	673 (Ireland)	744 (Ireland)
Ranking of Korea	51st	16th	14th	12th
Actual amount of distribution	2,903 units	24,177 units	33,816	45,172
(per million capita)	(60 units)	(498 units)	(696 units)	(927 units)

〈 Accomplishment of the secure server distribution expansion policies 〉

- Organization of the “Secure Server Special Consultative Group” to expand the basis for supplies (August 2006)
- Revision of the “Technical and Management Protection Standards for Personal Information” (January 2007)
 - * Defining the existing encryption measures as an implementation of the secure server, which prepared the basis for administrative actions. (Article 6)
- Investigation and education of the status of website secure server implementation (March 2007)
 - * In 2007: 21,656 points inspection and education, in 2008: 26,065 points, 13,865 points improvement, in 2009: 36,851 points inspection / 18,011 points improvement, in 2010: 51,452 points inspection / 8,884 points improvement

- Development and distribution of the secure server implementation guidelines for voluntary implementation by a company (February 2007, July 2008, December 2009)
- Self diagnosis of the secure servers and online domestic certificate distribution event (June 2007) free supply of secure servers for small web sites (August 2009, June 2010)
- Web hosting and company hearings to promote the introduction of secure servers (March 2008, between February and July 2009, between June and December 2010)
- The Ministry of Public Administration and Security, the Ministry of Science and Education and KCC made joint efforts to form a consultative group to expand the distribution of secure servers (December 2009)
- Secure server searching online events to promote the recognition of the need for secure servers (November 2006, between May and June 2008)
- Making and distribution of manuals and video for promoting use of secure servers (Between May and November 2010)

2. Information Security Policy Accomplishments

Although the secure server index is widely acknowledged as the only international index that can be used to compare the level of information security for many countries, secure server distribution alone cannot properly evaluate the information security level of a country or the accomplishments of the governmental policies. So the Korean government in 2004 took on a research project to develop its own information security index, and completed the development of the index system and the model by the end of that year. Since then, the Korean government has been deriving the index each year to measure the information security level of Korea and evaluate the outcome of policy execution to determine the future direction of government policies.

2.1 Overview of National Information Security Index

The national information security indices include the information security index used to measure the level of preparation for information security in Korea and the threat index used to measure the scope of damages caused by the threats related to informatization. The information security index is in turn composed of the basis index that measures the actual efforts and degree of practicing information security, the environmental index that measures the degree of preparation for the information security environment such as the introduction

of an information security system, the level of technology, and system implementation. On the other hand, the threat index consists of three elements-hacking virus, personal information invasions and spam mail.

Figure 5-1 | Framework for the National Information Security Index

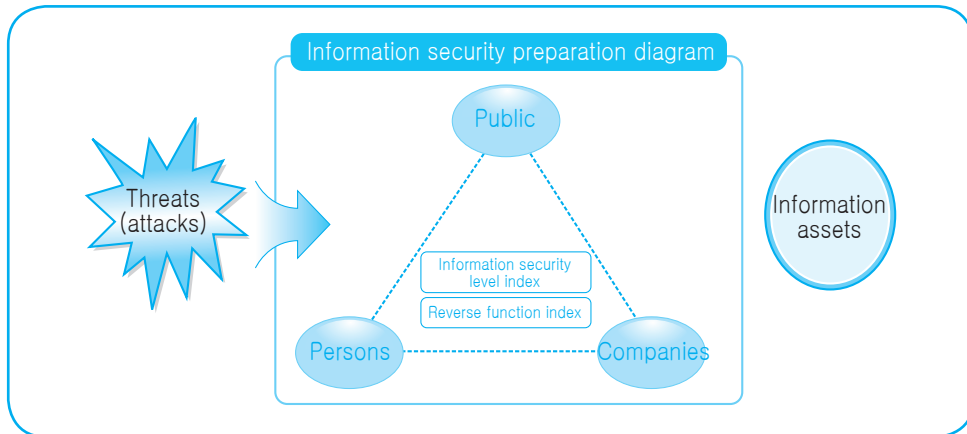


Table 5-2 | National Information Security Index System

Classification	Sub category	Detailed index
Information security index	Information security basis	Vaccine use rate
		Patch installation rate
		Public certificate distribution rate
		Firewall distribution rate
		IDS/IPS distribution rate
		Secure server distribution rate
	Information security environment	Information security budget rate
		Information security manpower rate
		Level of awareness of information security
Threats index	Threats of informatization	Hacking virus report rate
		Personal information invasion report rate
		Spam mail received rate

2.2 Analysis of the Information Security Index Estimates

2.2.1 Estimates of the Information Security Index in 2010

In 2010, of the 9 information security indices, seven were improved, yielding total points of 80.5, which showed a 6.6 point improvement. The basis index was improved from 73.4 in 2009 to 74.0 in 2010, an improvement of 0.6 points, and the environmental index was improved from 74.4 in 2009 to 87.0 in 2010, which indicates an improvement of 12.6 points.

Table 5-3 | Estimates of the Information Security Index

Area	Detailed index	Estimates of indices		Up/ down
		2009	2010	
Information security basis	Vaccine use rate	95.7	96.3	+0.6
	Patch installation rate	86.8	90.0	+3.3
	Public certificate distribution rate	59.9	64.1	+4.2
	Firewall distribution rate	75.4	70.1	-5.3
	IDS/IPS distribution rate	58.6	46.5	-12.1
	Secure server distribution rate	63.8	77.0	+13.2
	Basis index	73.4	74.0	+0.6
Information security environment	Information security budget rate	55.2	81.2	+26.0
	Information security manpower rate	69.9	80.3	+10.4
	Level of information security awareness	98.1	99.5	+1.4
	Environment index	74.4	87.0	+12.6
Information security index		73.9	80.5	+6.6

2.2.2 Reasons for an Increase/Decrease in the Index in 2010

The most significant improvement in 2010 can be seen in the secure server distribution rate, the information security budget rate and the information security manpower rate, all of which show more than a 10-point improvement compared to the previous year. The ‘secure server distribution rate’ was significantly improved over the past several years with the help of the policy to expand the distribution of secure servers, such as the provision of free certificate services pursued by the government, and the number of domestic secure servers was increased by 30.5%, from 49,358 in 2009 and 64,415 in 2010. The information security budget rate as a share of the entire informatization budget was also significantly increased, as the July 7th DDoS attacks forced the government to spend lots of money on the implementation of the national response system (2009: KRW 174.2 billion→2010: KRW

273.1 billion). The 'information security manpower rate as a share of total informatization manpower' was also increased, as the growth rate of information security was significantly increased, from 11.5% in 2009 to 21.6% in 2010, which led to an increase in employment opportunities in the area of information security (information security manpower 2009: 5,006 persons→2010: 5,748 persons).

On the other hand, the 'Firewall distribution rate' and the 'IDS/IPS distribution rate' declined compared to the previous year, mainly because of the change in the pattern of information security products use. The firewall use rate was reduced (2009: 75.4%→2010: 70.1%) because the use of web-firewall, a firewall alternative, was suddenly increased (2009: 38.1%→2010: 77.9%). Also, the IDS/IPS distribution rate was decreased (58.6% in 2009 to 46.5% in 2010) because the demand for single products was reduced due to the fact that the big companies' demand for integrated security products, such as UTM that supports integrated functions, was significantly increased.

Figure 5-2 | Annual Trends of Information Security Index Changes

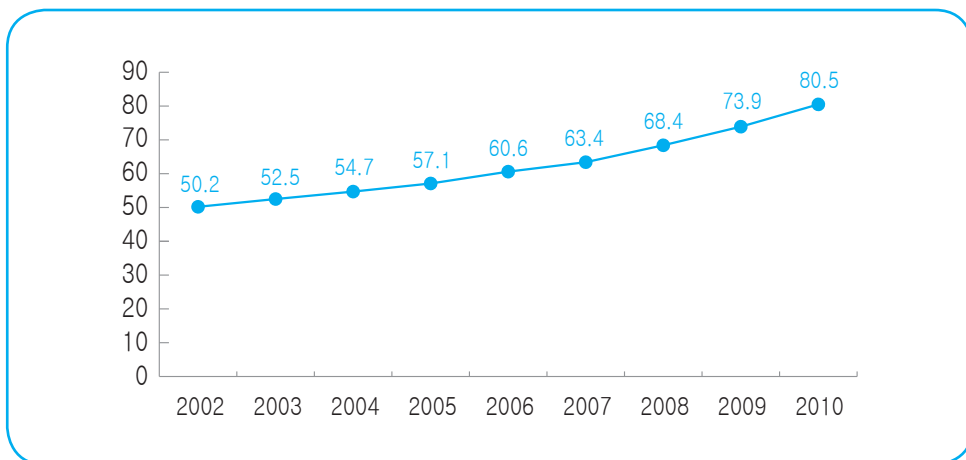


Table 5-4 | Description of Information Security Indices and Details of Estimates

Area	Detailed index name	Meaning	Index estimates		
			'09 (%)	'10 (%)	UP/down (%p)
Information security environment	Vaccine use rate	Rate of users among general internet users who install vaccine software on their PCs.	95.7	96.3	0.6(↑)
	Patch installation rate	Rate of users among general internet users who performs OS updates on their PCs.	86.8	90.0	3.3(↑)
	Public certificate distribution rate	Rate of users among general internet users who use public certificates.	59.9	64.1	4.2(↑)
	Firewall distribution rate	Rate of companies who use firewalls among companies with more than 50 employees and using networks.	75.4	70.1	5.3(↓)
	IDS/IPS distribution rate	Rate of companies who use IDS or IPS among companies with more than 250 employees and using networks.	58.6	46.5	12.1(↓)
	Secure server distribution rate	# of secure servers owned per 1 million capita.	63.8	77.0	13.2(↑)
	Basis index			73.4	74.0
Information security environment	Information security budget rate	The information security budget as a portion of the national informatization budget.	55.2	81.2	26.0(↑)
	Information security manpower rate	The information security manpower as a portion of the informatization manpower.	69.9	80.3	10.4(↑)
	Level of awareness of information security	The number of users who understand the importance of information security as a portion of general internet users.	98.1	99.5	1.4(↑)
	Environment index			74.4	87.0
National information security index			73.9	80.5	6.6(↑)

Viewpoints

1. Importance of the Government Leadership and the Public/Private Sector Cooperation for Information Security
2. Threats in the Drastically Evolving ICT Environment and How to Cope with Them
3. Recommendation for Execution Plans to Promote the Level of Information Security

Viewpoints

1. Importance of Government Leadership and Public/Private Sector Cooperation for Information Security

As the Korean government began to make great efforts for informatization in the early phase of informatization in the '80s, the information communication industry was able to continue its incredible growth each year.

However, as the national and social reliance on the IT system deepened, it became necessary to amend the information security law system from the perspective of national security. To cope with such problems, the Korean government prepared various legal systems and policies. In 1999, to protect the information assets and distribution of individuals and companies, the “Digital Signature Act” was enacted, and the “Act on Expansion of Dissemination and Promotion of Utilization of Information Systems” was fully revised as the “Act on Promotion, etc. of Utilization of Information Systems.” Starting with such repair works on the threats of informatization, in 2001, to protect the main national information communication facilities in finance, communication and energy, the “Act on the Protection of Information and Communications Infrastructures” was enacted. The existing “Act on Promotion, etc. of Utilization of Information Systems” was renamed the “Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.” to conclude the strengthening of acts related to information security. Moreover, in January 2003, as a large-scale internet invasion incident occurred, the internet invasion related regulations were fully revised, and in 2004 and 2005, the punishments for those who commit crimes by sending illegal spam or breaching personal information were strengthened.

Also, in 2006, the basic strategy for ubiquitous information security was established, and in 2008 the comprehensive mid-term plan for information security, the comprehensive plan for internet information security, and the comprehensive plan for knowledge information security promotion were pursued to improve the level of information security in the private

and public sectors. In addition, by operating various high quality education programs at universities, graduate schools, public and national organizations, and private education organizations, the best efforts were made to train information security specialists and promote technology development and industrial development, which can contribute to the national competitiveness.

Consequently, the Korean government is making gradual developments and accomplishments in terms of information security in the overall aspects related to the protection of information service providers, and is promoting an awareness of information security, including e-government information security, critical information facility protection, personal information protection, information security diagnosis and information security management systems (ISMS) certification, etc.

However, leadership by the government or public organizations may not be enough to for there to be sufficient accomplishments in the area of information security. What is needed is to implement the basis for enhancing the overall level of information security in the country by encouraging the participation of various stakeholders. Therefore, the Korean government is making multi-dimensional efforts to handle various information security issues by involving itself with various organizations such as KISIA, the Korea CONCERT, the Korean CSO Association and the information security development association, in which various private information security companies are participating.

As discussed earlier, the Korean government has established various legal systems and policies to support the information security systems, and the superintendent organizations to pursue diverse activities. A security threat can have significant impacts on our nation, so the most important thing is to take early action that can minimize the effects. For this reason, the most critical element for success is: establishment of legal systems and policies, establishment and operation of the superintendent organizations to pursue such legal systems and policies, and the governments extensive support and interest. These are also the mandatory elements for continuing the sustainable development of the internet economy. In addition, to maximize the readiness to respond to threats that exist in the grey area between the private and public sectors, and to expand mutual cooperation, the government and the private sector should make joint efforts. So, the most important thing from this perspective is to establish proper information security plans in a timely manner, establish a comprehensive governance system that can continue to support such plans, and strengthen the private and government cooperation systems.

2. Threats in the Dramatically Evolving ICT Environment, and How to Cope with Them

As smart phones gain in popularity, the mobile broadband infra and the social networking service environments are expanding. Therefore, new issues and security threats are emerging every day, the most popular examples of which include social and cultural threats such as

slander and stalking, and unhealthy information distribution; and technology-based threats, which include viruses and malignant codes, SNS phishing, spam, personal and confidential information leakages and privacy invasions. In particular, the social networking services that have been gaining popularity lately, such as Facebook and Twitter, are emerging as a new source of attacks that can replace the existing email-based spam and malignant code distribution. In addition, the so-called “hactivism” that is used to achieve a certain social or political goal is increasing every day, and its methods are constantly becoming more sophisticated. Such threats can damage the national security as they propagate to the main national infrastructure, going beyond invasions of personal information and a company’s confidential information.

The Korean government has established a comprehensive plan for smart mobile security in order to immediately respond to the increase in cyber crimes and attacks using new technologies such as smartphones, SNS, cloud computing and others. The plan was prepared under the motto “Reaching the smart mobile security country,” and the main goals are to improve the quality of the future mobile service infra security, to establish the protection of mobile user privacy, and to implement the basis for mobile information security. The government will select and execute 10 major tasks in the three main areas of service infra protection, user protection and implementation of the basis for protection. Thus, by preparing for possible security threats in the future, the social costs for handling such threats can be minimized, and the mobile service environment for safe and reliable use will be implemented. Eventually, user convenience and quality of life will be improved.

As the mobile broadband infrastructure is implemented in the future, the number of the relevant services is increased, and social networking services continue to evolve dramatically, it is important to establish and execute a proper information security plan in a timely manner. For this purpose, all stakeholders are encouraged to participate in strengthening the response system for invasion incidents and the capacity to advance information security in the age of IT convergence, and to pursue ethical campaigns to create a desirable internet environment. Eventually, we can expect to see a safer and more convenient ICT environment that can take us to a better world with great economic prosperity.

3. Recommendation for Execution Plans to Promote the Level of Information Security

To improve the level of information security, developing countries are recommended to establish and execute the following detailed execution plans under the three main pillars including ICT infra protection, application security and information security training and recognition promotion, so that they can finally improve the level of information security by using Korea as a role model.

- ICT infrastructure protection
 - Committee establishment and operation to establish the framework for information security law systems.
 - Information security managing organization, internet response organization establishment and operation.
 - Recommendation and development of the information security related guidelines.
 - Implementation and operation of the system to cooperate with the information security related organizations
 - Implementation and operation of the international cooperation system to prevent online invasions.
- e-Application Security
 - Password algorithm development
 - e-government security process establishment
 - Implementation and operation of the national public certification systems
 - PR activities to promote use of digital signatures.
 - Promoted information security product and service development and use
- Education and Awareness Activity of Information Security
 - Computer and information security literacy education expansions
 - Information security awareness improvement by public campaigns
 - Information security experts' education
 - International cooperation to expand the Culture of Security

The detailed strategies for execution and the management activities should be carried out by the departments and the organizations in charge of information security.

- KISA (2011), “2010 Hacking Virus Status and Responses”
 -----, “2011 National Information Security White Paper”
 ITEP, “2010 Knowledge Information Security R&D Development Strategy,” Aug. 2010
 KCA, “2010 Broadcasting Communication Technology Roadmap,” July 2010
 Ministry of Public Administration and Security, “Perfect solution for cyber attacks to the
 local e-government services,” 2009
 Consensus Korea, “e-government security, install a perfect defense system with the local
 self governing organizations,” 2007
 ITU, Measuring the Information Society 2011, Dec. 2011.
 WEF, The Global Information Technology Report 2010-2011, March 2011
 Korea Communication Commission (KCC), Basic Strategy for Ubiquitous Information
 Security, Dec. 2006
 -----, Comprehensive Plan for Internet
 Security, July 2008
 -----, Comprehensive Plan for Smart Mobile
 Security, Dec. 2010
 Ministry of Public Administration and Security(MOPAS), Mid-Term Comprehensive Plan
 for Information Security, July 2008
 Ministry of Knowledge Economy, Comprehensive Plan for Promoting Knowledge
 Information Security Industry, Dec. 2008
 Korea Information&Security Agency(KISA), e-Call center 118 Consulting Center
 Business Manual, Dec. 2009

Relevant URL

- KCC, <http://www.kcc.go.kr>
 Ministry of Public Administration and Security, <http://www.mopas.go.kr>
 Ministry of Knowledge Economy, <http://www.mke.go.kr>
 National Intelligence Service, <http://www.nis.go.kr>
 KISA, <http://www.kisa.or.kr>
 ETRI, <http://www.etri.re.kr>
 KTFC, <http://www.ktfc.or.kr>
 KOSCOM, <http://www.koscom.co.kr/>
 FSA, <http://www.fsa.or.kr>
 Cyber Terror Response Center, <http://www.ctrc.go.kr>

www.ksp.go.kr

Ministry of Strategy and Finance, Republic of Korea

427-725, Republic of Korea Government Complex 2, Gwacheon, Korea Tel. 82-2-2150-7732 www.mosf.go.kr

KDI School of Public Policy and Management

130-868, 87 Hoegiro Dongdaemun Gu, Seoul, Korea Tel. 82-2-3299-1114 www.kdischool.ac.kr



ISBN 978-89-93695-77-9

**Knowledge Sharing Program
Development Research and Learning Network**

- 130-868, 87 Hoegiro Dongdaemun Gu, Seoul, Korea
- Tel. 82-2-3299-1071
- www.kdischool.ac.kr