KCC announces 'Comprehensive Plans for Smart Mobile Security'

- Promoting 10 key tasks in 3 fields to preemptively prepare for security threats and to develop Korea into a powerful nation of mobile security in the era of 30 million smart phone users -

On the 24th, Korea Communications Commission (KCC) announced the mid to long-term 'Comprehensive Plans for Smart Mobile Security' (2011 ~ 2015) established in order to preemptively prepare for potential security threats in accordance with the explosive increase of mobile Internet use through smart phone, etc. and to secure competitiveness of Korea in the global mobile security market and therefore to develop Korea into a power nation of mobile security.

KCC and Korea Internet & Security Agency (KISA) have been organizing and operating 'Private - Public Joint Smart Phone Information Security Handling Team (Jan.)', 'Mobile Security Forum (Apr.)' and 'Future Convergence IT Service Security Search Group (May)' since the first half of this year. Through these efforts, KCC and KISA have been preparing preemptive security measures to handle the potential security threats in line with the increase of mobile Internet use.

With the recent increase of mobile terminals, such as smart phone and smart pad (tablet PC), etc., the smart phone subscriber count in Korea as of the end of November 2011 is

6.25 million (12% of mobile communications service subscribers). It is forecasted to exceed 7 million by the end of this year. As 'smart life' using a variety of smart devices including smart phone, smart pad and smart TV will accelerate in the future, the era of 'Smartciety' will begin in full scale. With this, the cumulative smart phone subscriber count is forecasted to exceed 30 million in 2013 and over 40 million in 2015.

※ Smartciety (smart + society): Smartciety refers to a society in which communications are carried out with various smart devices, such as smart phone, and smart technologies are used in various areas of the society, such as business operations, learning activities and medical services.

However, the shift to mobile internet paradigm triggers new security threats and this, in turn, increases the society's demand for mobile security. Accordingly, in preparation for the 'era of 30 million smart phone users', KCC decided to pursue 10 key tasks in the areas of service · infrastructure protection, user protection and protection base expansion under the 3 goals of ▶ quality improvement for future mobile service・infrastructure security ▶ establishment of mobile user privacy protection base and ▶ establishment of mobile information security base.

▶ For **(Quality Improvement for Future Mobile Service · Infrastructure Security)** KCC will ① activate mobile vaccines to strengthen security of new smart phone and smart pad terminals and establish the environments for safe application distribution and app genome projects to identify malicious applications, ② strengthen wireless LAN security management to ensure wireless network safety and implement the system to detect and handle wired · wireless linked network invasions and ③

establish environments to spread the use of mobile office by discovering and publicizing exemplary cases of mobile office introduction with consideration given to security, prepare mobile cloud standard SLA guidelines and support smart TV device · contents security solution development. Therefore, KCC will secure the basis for safe service by strengthening the security system of new mobile services.

▶ For **(Establishment of Mobile User Privacy Protection)**, KCC will ④ strengthen the responsibilities of providing and managing protection measures, such as personal information encryption, in order to increase personal information and location information security in mobile service and promote implementation of app privacy safety verification system and personal location info. self-control system, ⑤ minimize mobile SPAM by analyzing SPAM risks of new services and strengthening anti-SPAM services, such as intelligent filtering and ⑥ prevent distribution of harmful information through mobile devices by promoting development and distribution of applications blocking mobile harmful information and preparing app store monitoring system.

▶ For **(Establishment of Mobile Information Security Base)**, KCC will ⑦ strengthen support for development of source security technologies, such as low power · compact encryption, terminal and platform protection, wireless network protection and mobile contents protection, ⑧ establish win-win environment between large enterprises and small security businesses in order to form the mobile security market ecosystem, support commercialization and transfer of new security technologies to the private sector, lease

mobile security globalization by establishing 'Mobile Security Standard Research Center', etc. and promote development of core human resources. In addition, KCC will ⑨ strengthen domestic and international cooperation to prevent and handle mobile incidents, support a research organization specializing in the field of mobile security (think-tank) and promote expansion of mobile information security culture. At the same time, KCC will ⑩ promote improvement of the legal system in order to ensure safe use of new mobile services and smart devices by organizing and operating the '(tentatively named) Association of Smart Mobile Security Legislation Research'.

Once KCC's comprehensive plans for mobile security are implemented through organic cooperation among industrial, academic, research and government sectors, the national prestige of Korea will be enhanced together with the quality of living for the entire nation as the environments for safe mobile service will be implemented earlier on and the social cost will be minimized through prevention of mobile security threats of the future.

KCC plans to promote the 10 tasks by stages considering user demand, market-leading capacities of the infrastructure technologies and synergic convergence with new market creation, etc. Through these efforts, KCC will contribute to activating mobile security market and increasing competitiveness of the related industries. Accordingly, the scale of domestic mobile security market will increase from KRW 5.7 billion in 2010 to KRW 207.8 billion by 2015 so that Korea's global mobile security market share will increase to 7.3%.

Attachment: One copy of 'Comprehensive Plans for Smart Mobile Security (Summary)'

<Attachment>

Comprehensive Plans for Smart Mobile Security (Summary)

1. Promotion Background

o **(Expansion of Mobile Terminals)** The count of domestic smart phone subscribers is 6.25 million as of the end of November 2010 (12% of mobile communications service subscribers). The count is expected to exceed 7 million by the end of this year.

- The cumulative count of smart phone subscribers in Korea will exceed 30 million by 2013 and 40 million by 2015 (KISDI · KCC, Nov. 2010).

- The count of smart pad (tablet PC) users is also expected to increase from 180,000 in 2010 to approx. 9.82 million by 2015 (KISDI · KCC, Nov. 2010).

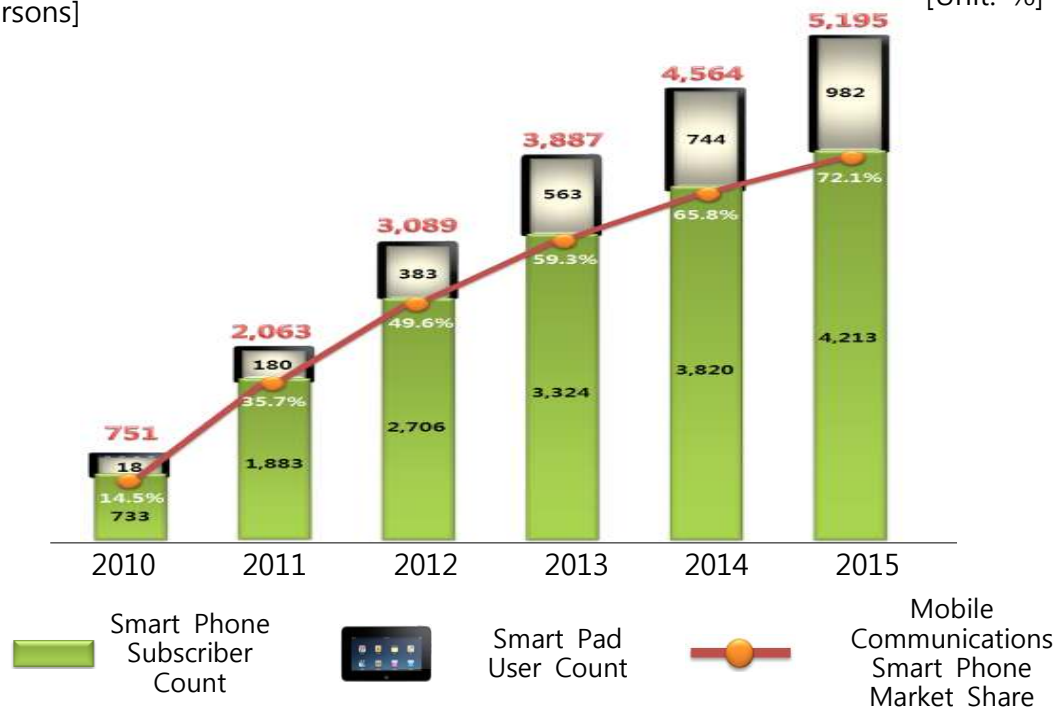
⇒ The acceleration of smart life using a variety of smart devices, such as smart phone and tablet PC, will lead to the era of 'Smartciety'.

※ Smartciety (smart + society): Smartciety refers to a society in which communications are carried out with various smart devices, such as smart phone, and smart technologies are used in various areas of the society, such as business operations, learning activities and medical services (the term used for the first time in the KCC comprehensive plans).

【 Forecast of Smart Phone and Smart Pad Distribution (Cumulative) in Korea (2010 ~ 2015) 】

[Unit: 10,000 persons]

[Unit: %]

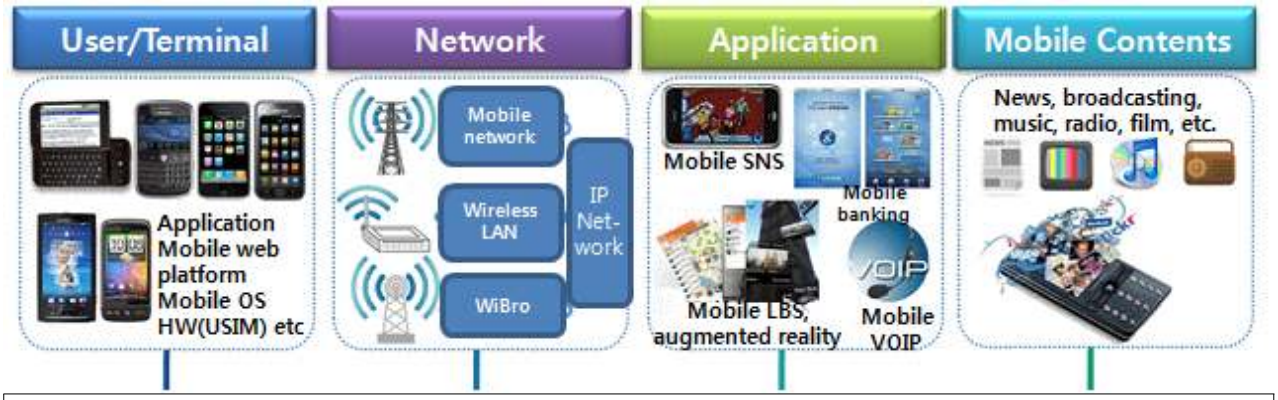


※ Source: Forecast by KISDI and KCC based on "Mobile voice and data forecast pack: 2010–15" OVUM (May 2010) and "2010 National Informatization White Book (NIA, Jul. 2010)" (Nov. 2010)

o **(Mobile Security Threat)** However, the shift to mobile Internet paradigm has resulted in new security threats together with service advancement and changes in lifestyle patterns.

- Since it became possible to collect, analyze and use personal information at all times with activation of new mobile terminal-based services of SNS and LBS, the apprehension for privacy invasion has also increased.
- With introduction of new convergence services, composite terminals and open platforms, new security issues that are difficult to predict will be raised continuously.
- In particular, mobile security threats can be divided into the 4 fields mobile terminal, wireless network, mobile-based new services and convergence contents.

【 Security Threats in the 4 Mobile Fields 】



• Malicious code infection (illegal billing) • Terminal operation failure • Terminal loss and information leakage	• Security vulnerabilities of wireless devices (sniffing and wiretapping) • Mobile DDoS • AP no-security setting • Connection to unauthorized devices	• Location/ personal information leakage (privacy invasion) • Mobile banking hacking • Mobile service suspension • Increase of illegal service use	• Contents DRM hacking • Mobile SPAM • Illegal/ harmful contents distribution

o **(Expansion of Mobile Information Security Market)** The scale of domestic information security market in 2010 is KRW 917.9 billion (estimation). The scale of mobile security market is approx. KRW 5.7 billion (0.6% of the information security market) (KISIA, Dec. 2009).

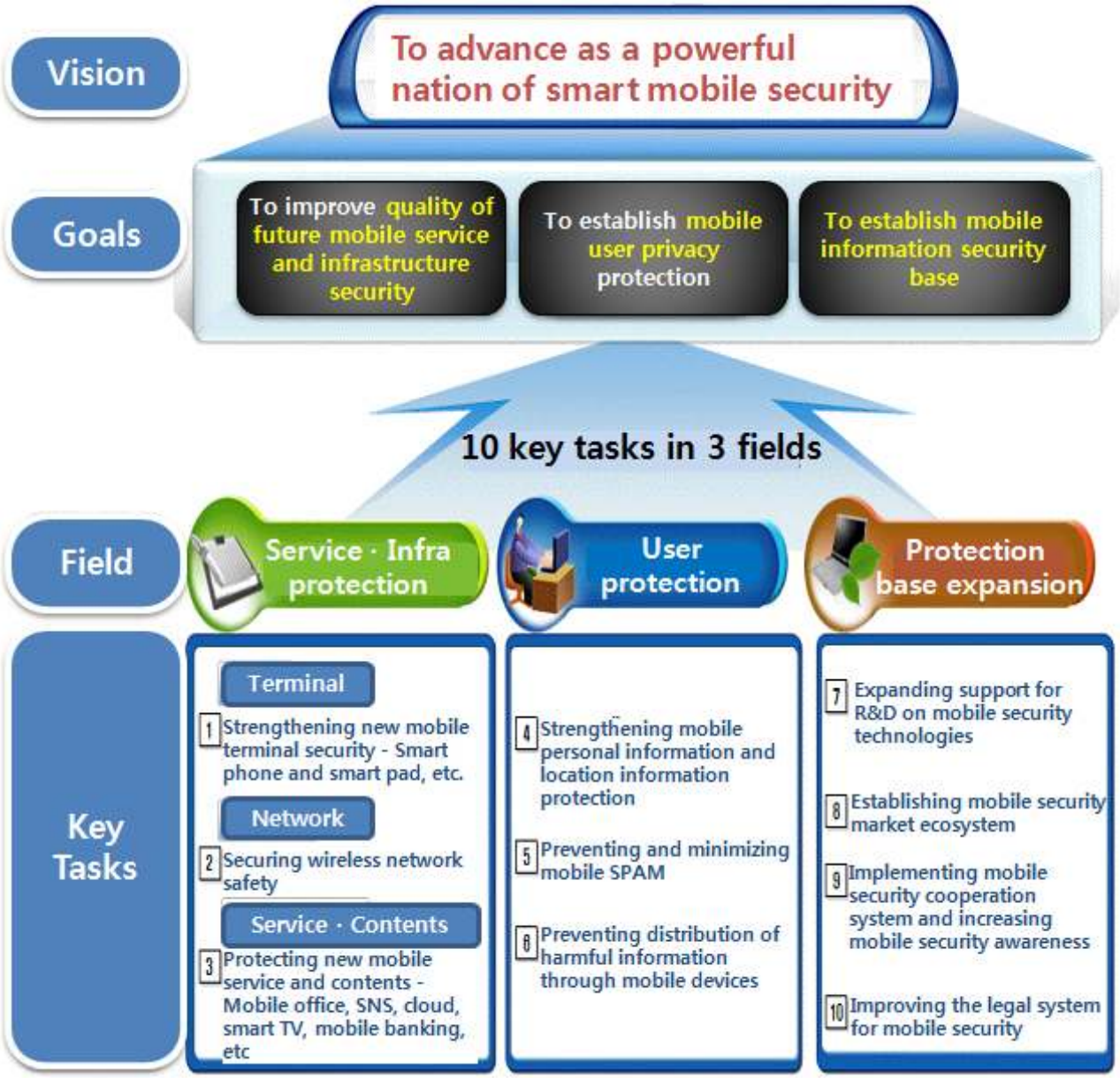
- Domestic mobile security market is expected to grow rapidly (annual average growth rate of 206%) supported by efforts in the private sector and the government's security policies. Therefore, the scale is forecasted to be approx. KRW 207.8 billion (12.9%) by 2015.

- The global mobile security market will grow by 2.2 times over 6 years (2009 ~ 2015) and will therefore reach the scale of approx. $2,864 million (approx. KRW 3 trillion) by 2015 (IDC, May 2010).

o In preparation for the 'era of 30 million smart phone users', it is necessary to establish preemptive measures for implementation of safe mobile Internet society.

- KCC has established and is promoting to implement the mid to long-term 'Comprehensive Plans for Smart Mobile Security' (2011 ~ 2015) in order to preemptively prepare for new security threats in the rapidly changing mobile Internet environment and to dominate the global mobile security market.

2. Vision and Promotion Strategies



3. 10 Key Tasks in 3 Fields

1. To Improve Quality of Future Mobile Service and Infrastructure Security

① To Strengthen New Mobile Terminal Security

o **(To activate mobile vaccines and strengthen malicious code inspection)** Discovering new business models for smart phone vaccine,

strengthening malicious code inspection, implementing security application and solution testing center, etc.

o **(To promote Korean style app genome project)** Identifying maliciousness of applications by analyzing functional characteristics and security threats of the applications and therefore using the information in developing vaccines and preparing the basis of determining malicious applications

※ Lookout, a U.S. mobile security company, promotes 'app genome project' to analyze approx. 300,000 applications (Aug. 2010).

o **(To establish safe environment for distribution of applications)** Preparing standardized verification criteria and procedures for smart phone applications and encouraging users to observe the criteria and procedures

※ Green Market Certificate: Government selects a market that observes security verification procedures and guidelines for applications and continuously administers follow-up management and certifies the market as a reliable application provider.

o **(To prepare terminal security guidelines for smart pad, etc.)** Preparing guidelines on vulnerabilities and the handling measures for development and distribution of safe smart devices

2 To Secure Wireless Network Safety

o **(To strengthen wireless LAN security management, etc.)** Developing wireless LAN security standard model, enhancing security awareness, improving wireless LAN security laws, etc.

- Periodically inspecting operation of public Wi-Fi zones and private wireless LAN security facilities based on wireless LAN security operation standard model

※ Inspecting change of the initial wireless AP password, security setting, authentication and conformance to encryption guidelines through field

survey

o **(Implementing linked security system for linked wireless zone)** Advancing the existing security system centering on wired network, such as DDoS response system, to the wireless network · IP backbone network linked zone

3 To Protect New Mobile Service · Contents

□ Preparing Mobile Office Security System

o **(Developing and Distributing Security Guidelines)** Developing and distributing information security guidelines for smart work security elements, such as terminal, system and legal issues

- Establishing security base to successfully promote smart work

o **(Improving the laws and systems)** Improving the related laws and systems in order to clarify legal responsibilities of mobile office service providers and to protect the rights and interests of users

- Preparing the uniformed legal base for personal information provision and entrustment and the legal criteria on compensation for personal information leakage and loss

- Preparing the base to assess security of products and technologies configuring mobile office and improving certification system

o **(Discovering and spreading exemplary cases)** Discovering and publicizing best practices of mobile office introduction considering security and establishing the environment to spread mobile office system

□ **To Strengthen Mobile SNS Security**

o **(Improving the legal system for SNS information leakage handling)** Preparing and promoting the legal system to prevent personal information (location information) leakage

- Notifying the risk of violation of personal information when collecting personal information and preparing plans to obtain consent for information collection

o **(Preparing technological handling measures)** Strengthening technological protection measures for vulnerabilities of mobile SNS through collaboration with domestic and international SNS providers

- Implementing domestic and international short URL-related information sharing system to prevent and handle malicious code distribution and phishing website distribution using short URL

□ **To Strengthen Mobile Cloud Security System**

o **(Preparing mobile cloud security base)** Developing 'mobile cloud forensic' technology to implement the integrated certification gateway base and to analyze the causes of accidents

o **(Standardizing services and implementing handling system)** Standardizing services and policies to protect mobile cloud service users, strengthening user education and handling system

- Preparing standard SLA guidelines to provide security service

differentiated per mobile cloud service type and information sensitivity

※ SLA: Service level agreement

- Preparing violation response system to share information on new threats among mobile cloud service providers and to promptly handle the new threats

□ Implementing Smart TV Security System

o **(Preparing smart TV device protection system)** Preparing the system to analyze vulnerabilities of smart TV devices and to diagnose security of the devices in order to protect smart TV system

o **(Promoting contents and personal information security plans)** Supporting copy guard solution development and preparing management guidelines according to the characteristics of mobile contents

□ To Establish Mobile Banking Security Base

o **(R&D on mobile banking security)** Researching mobile banking service security according to the release of new mobile devices and developing technologies to analyze security vulnerabilities

o **(Developing security guidelines and inspecting vulnerabilities)** Developing and distributing security guidelines for safe smart phone banking service provision and use

- Supporting inspection of safety and security vulnerabilities of

mobile financial services provided by financial institutes through cooperation with the financial authorities

2. To Establish Mobile User Privacy Protection Base

④ To Strengthen Mobile Personal Information and Location Information Protection

o **(Strengthening Management Responsibilities)** Strengthening responsibilities for provision and management of protection means, such as personal information encryption, preparing the legal system to prevent mobile personal information leakage

o **(Validating privacy safety)** Suggesting personal information protection guidelines for smart phone S/W development and portable terminal manufacturing, implementing app privacy safety validation system

o **(Implementing personal location info. self-control system)** Strengthening users' self-control of their location information so that they can have location information or location-based service providers check the details of location information use

⑤ To Prevent and Minimize Mobile SPAM

o **(Analyzing SPAM risk of new services)** Analyzing SPAM types and vulnerabilities in new services, such as SNS, conducting preemptive studies on legal and technological handling measures

o **(Expanding the use of intelligent filtering)** Strengthening anti-SPAM services, such as intelligent SPAM filtering as well as simplification of mobile SPAM reporting procedures through smart phone, etc.

6 To Prevent Harmful Information Distribution through Mobile Devices

o **(Developing applications to block harmful information)** Recommending development and installation of applications to block harmful information transmitted to young people through mobile devices

※ Encouraging the measure to install an application blocking harmful information as a default setting when selling terminal so that the terminal can be operated according to the user's age

o **(Strengthening harmful information monitoring for applications)** Investigating harmfulness, sensationalism and privacy invasion of smart phone applications in distribution

3. To Establish Mobile Information Security Base

⑦ To Expand Support for R&D of Mobile Security Technologies

o **(Developing Source Technologies)** Extensively supporting basic · source technology development for the common base/ terminal · platform/ wireless network/ service/ contents for mobile security

- Developing source technologies for protection of mobile terminal and infrastructures, such as security platform (terminal · platform), invasion detection and monitoring (wireless network)

- Developing technologies to ensure safety of smart mobile service, such as low power · compact encryption, mobile cloud and contents protection

⑧ To Establish Mobile Security Market Ecosystem

o **(Establishing win-win environment for mobile security)** Organizing and operating the '(tentatively named) Mobile Security Council' to resolve difficulties in cooperation experienced by mobile security companies, terminal manufacturers and mobile communications service providers

o **(Strengthening commercialization support)** Strengthening support for commercialization and transfer to the private sector of mobile security technology development outcomes from research organizations, such as KISA, ETRI and NSRI

- Establishing the '(tentatively named) Mobile Security

Commercialization Support Center' to promote integrated package-type support covering the entire stages from security product development to sale, maintenance and repair

o **(Supporting standardization and overseas market entry)** Preventing excessive competition · repetitive investments among businesses through standardization and organizing publicity road shows to support overseas market entry by small-scale security companies

- Establishing the 'Mobile Security Standard Research Center' through cooperation between industrial and academic sectors and therefore securing the related base technologies and promoting global standardization of domestic technologies

o **(Developing global mobile security human resources)** Supporting mobile R&D personnel development in universities and promoting educational programs through cooperation with the industrial sector and international research centers

9 To Implement Mobile Security Cooperation System and to Enhance Awareness

o **(Strengthening preventative cooperation system)** Implementing public - private cooperation system to prevent and handle incidents on various mobile devices including smart phone

o **(Developing and supporting think-tank in mobile security fields)** Analyzing new mobile threats and technological · social · cultural changes in the future society through support by expert group

※ Supporting the leading domestic research institutes and implementing

cooperative research system to lead research activities in the security fields

o **(Spreading mobile information security culture)** Promoting to enhance awareness using a variety of mobile devices and services in connection with the related organizations, manufacturers and mobile communications service providers

⑩ Improving mobile security laws

o Promoting improvement of the legal system in order to ensure safe use of new mobile services and smart devices by organizing and operating the '(tentatively named) Association of Smart Mobile Security Legislation Research'

4. Promotion System and Funding Plans

o **(Promotion System)** Promoting the Comprehensive Smart Mobile Security Plans by implementing organic cooperation system through role division per industrial, academic, research and government sector

o **(Funding Plans)** Securing budget from the government and private sectors in 2011 ~ 2015 and promoting the comprehensive plans by investing approx. KRW 99.8 billion of fund

※ KRW 51 billion from the government sector (General Account: KRW 19.5 billion, Fund: KRW 31.5 billion) and KRW 48.8 billion from the private sector

- Government budget is based on the budget estimated by KCC and is subject to change according to deliberations with the Ministry of Strategy and Finance.
- Budget from the private sector is subject to change according to the situations of participating companies.

5. Expected Benefits

o **(Lowered Future Security Threats)** Preparation for security threats possible to occur in the future will minimize social cost of the future caused by security incidents.

o **(Safe Mobile Society)** Implementation of environment for safe and reliable mobile service use will contribute to enhancing the quality of life for the entire nation.

o **(Politic Effects)** National prestige will be enhanced by developing new mobile security fields and upgrading the level of national information security.

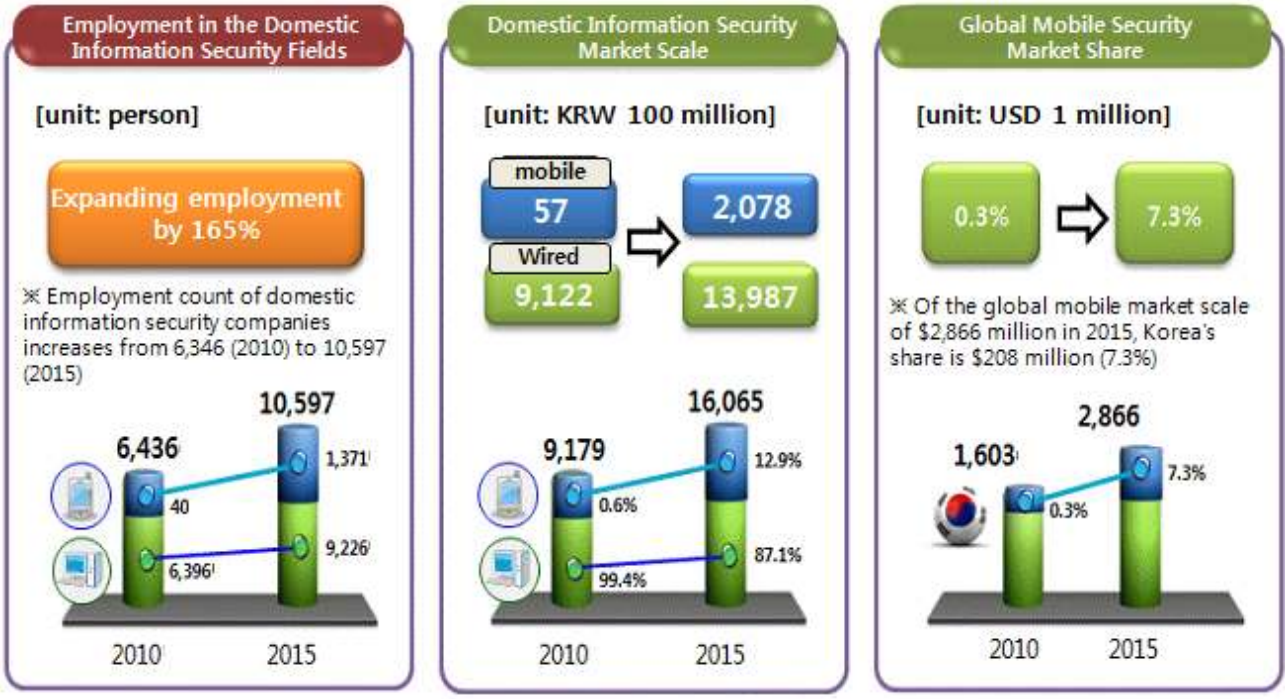
o **(Industrial · Economic Growth)** Together with resolving security-related apprehensions, security market activation will be promoted, industrial competitiveness will be enhanced and new jobs will be created.

- The total employment count in the information security field in 2010 is approx. 6,436. However, through market expansion, it will increase to 10,597 by 2015, which is an increase by 165% from 2010.

※ The percentage of employment in mobile fields is forecasted to increase from 0.6% (48 workers) in 2010 to 12.9% (1,371 workers) in 2015.

- The scale of domestic mobile security market will increase from KRW 5.7 billion in 2010 to KRW 207.8 billion in 2015. By 2015, Korea's global mobile security market share is forecasted to be 7.3%.

【 Industrially · Economically Expected Benefits 】



※ Source: Forecast by KISA (Nov. 2010) based on [New Recruitment] KISIA (Dec. 2009), Domestic Market Scale] Korea IDC (Jun. 2009) and KISIA (Dec. 2009) and [Global Market Share] IDC (May 2010)