(Tentative translation)

Study Group on Information Security Issues of Smartphone and Cloud Computing Final Report
- Measures to be Taken for the Safe Use of Smartphones -

June 29, 2012

Table of Contents

Introduction

Although the significance of information security is something that has generally been intimated in the past, information leakage and obstruction of business as a result of so-called cyber attacks on networks, have become serious social issues in recent years, further strengthening awareness of the pressing need to address these issues.

With the number of users increasing as a result of the merit the smartphone offers in combining both a conventional cell phone and personal computer (hereinafter referred to as PC) in a single device, the smartphone, including related areas such as applications, is an extremely fast-growing sector. However, as the market has expanded in line with rapid dissemination, [1]information security issues such as the emergence of malware targeting smartphones have come to the forefront. As expectations for the utilization of smartphones in a variety of different landscapes continue to escalate, an awareness of the need to tackle these issues before the damage spreads, prompted Ministry of Internal Affairs and Communications (MIC) to establish this Study Group and to start reviewing information security countermeasures in October last year.

If the public are unable to securely benefit from new technology and services, their confidence in those technologies and services will eventually be lost. Although the call for improvements in both convenience and information security levels is considered somewhat contradictory, rather than adopting an either-or mentality, it is important that the issue be examined from the view of what kind of information security measures need to be put in place, while maintaining the convenience factor.

In this respect, as a countermeasure to firstly improve smartphone information security levels and more particularly, to urgently tackle malware and cyber-attacks, the interim report from December last year compiled effective and reality-based policies including information security countermeasures where introduction should be considered by mobile phone operators and mobile device manufacturers, as well as the content and method of publicity to increase user awareness.

Since then, although some headway has been made in light of the interim report by relevant business operators and the government in terms of engagement in publicity and the establishment of technological countermeasures, on the other hand, requests for advice and reports received from users about actual incidents of security breaches

[1] Malware is short for malicious software. It is a generic term used to describe software programs such as computer viruses, that are created to cause damage.

would suggest that security risks are fast becoming a reality.

Based on these recent efforts and the new change in circumstances, this final report extends the content covered in the interim report, compiling the policies that need to be tackled by relevant business operators and the government, including the issues associated with the use of cloud services on smartphones and relevant countermeasures, and policies enabling the safe use of smartphones by utilizing cloud services.

Chapter 1 The Situation Surrounding Smartphones

Section 1 Dissemination of Smartphones

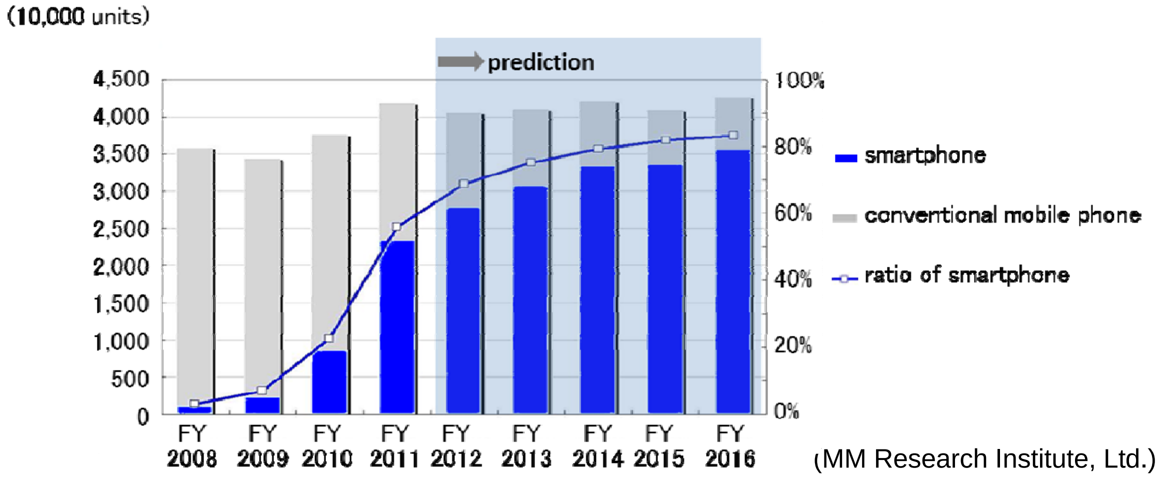
(1) What is a Smartphone?

Smartphones can be defined as hand-held mobile telephone devices that integrate advanced information processing functions with conventional mobile phone capabilities. With a large number of products equipped with touch screens, smartphones characteristically offer users the ability to customize their handset as they please, enabling unrestricted installation of desired applications in much the the same manner as a PC.

In an environment marked by the circulation of a diverse array of applications, expectations are mounting for the utilization of smartphones in a variety of different scenarios involving individual and corporate activity.

(2) Dissemination Status of Smartphones

The dissemination of smartphones is progressing rapidly. The volume of domestic shipments of smartphones in 2011 soared 2.8-fold on the previous fiscal year to 24.17 million units, accounting for 56.6% of all mobile phone shipments, with smartphones taking over the majority of shipments for the first time during the current fiscal year[2] (Figure 1). As the smartphone market enters a growth period, the strengthening of information security countermeasures is imperative, given the serious impact that potential information security incidences pose and also in light of the fact that requests for advice and reports about actual incidents of security breaches have already started to emerge.



(MM Research Institute, Ltd.)

Figure 1 Domestic shipments of mobile phone (conventional mobile phones + smartphones)

[2] MM Research Institute, Ltd. News Release (March 13, 2012) (http://www.m2ri.jp/newsreleases/main.php?id=010120120313500)

Additionally, at the end of December 2011, the number of domestic smartphone subscriptions according to operating system (hereinafter referred to as OS) market share tallied in at 58.1% for Android and 37.2% for iOS (Figure 2).

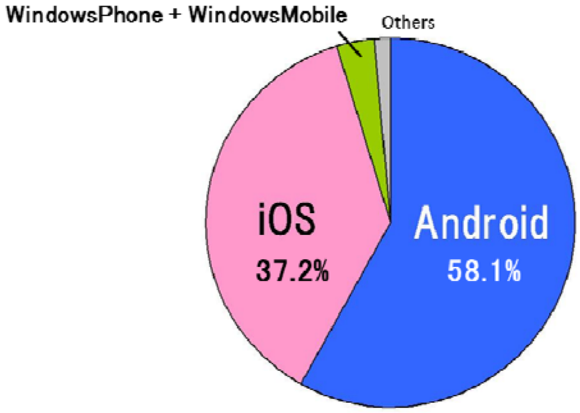
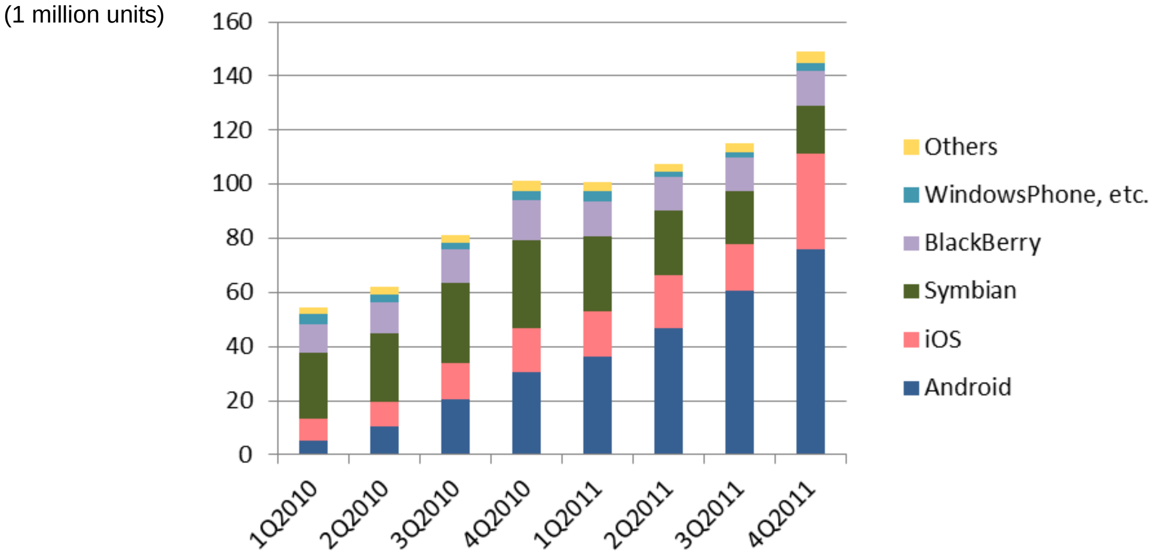


Figure 2 Number of domestic smartphone subscriptions according to OS market share

Unlike conventional mobile phones, smartphones boast a large number of global model handsets that have entered the domestic market, featuring OSes and terminals created to common global specifications. The Android and iOS platforms are expanding their market share[3] (Figure 3) on a global scale and in view of the conceivable possibility of overseas security risks spreading to Japan, the relevant issues and countermeasures need to be examined, including the risk of breaches in information security, a risk that has yet to emerge domestically.



(Created based on details sourced from Gartner, Inc. press release)

Figure 3 Number of worldwide smartphone, etc.[4] shipments according to OS

[3] Gartner, Inc. Press Release (http://www.gartner.com/it/page.jsp?id=1924314), etc.
[4] The figures for the Symbian OS include conventional handsets.

Section 2 Characteristics of Smartphones

(1) Difference with PCs

Compared to PCs, smartphones only offer minimal resources for protecting information security due to the limited processing capacity of the hardware on these devices and as the OSes assume a single user environment, authorization settings cannot be configured on an individual user basis. Smartphones are also not well equipped with functions such as the capacity to encrypt files and communication paths and based on the properties that are present in PCs but not on smartphones, it may become difficult to implement the same information security measures that are possible on PCs. On the other hand, aside from the verbal communication function, smartphones offer functions that are not available on PCs, including inbuilt cameras, GPS devices and other accessories, and in light of this, there is a need to be mindful of the fact that although smartphones offer a high level of convenience, there is always the possibility of new risks emerging or of current risks amplifying as a result of this convenience factor.

(2) Characteristics of Information Security Models

Information security models (sandboxes[5]) are employed by a large number of smartphone OSes and are designed to prevent fraudulent misuse of devices and data by ensuring applications can only operate within a limited scope. Thus in terms of design, smartphone OSes are generally considered to offer a higher level of security than PCs.

However, once users authorize an exorbitant range of access to the application, there is the down side that the relevant information security model will cease to function effectively.

(3) Diversified Communication Paths

Whereas conventional mobile phones basically only access the networks of mobile phone operators, smartphones can connect to the networks of both mobile phone operators and other telecommunications carrier networks that are accessed via a wireless local area network (LAN) (Figure 4).

[5] A sandbox in this context can be defined as an information security model designed to run programs from external sources within a protected environment, by utilizing technology that virtually simulates a multi-computer environment from the one computer. The use of a sandbox disables access to restricted areas by separate programs and therefore offers an effective method of preventing system misuse.

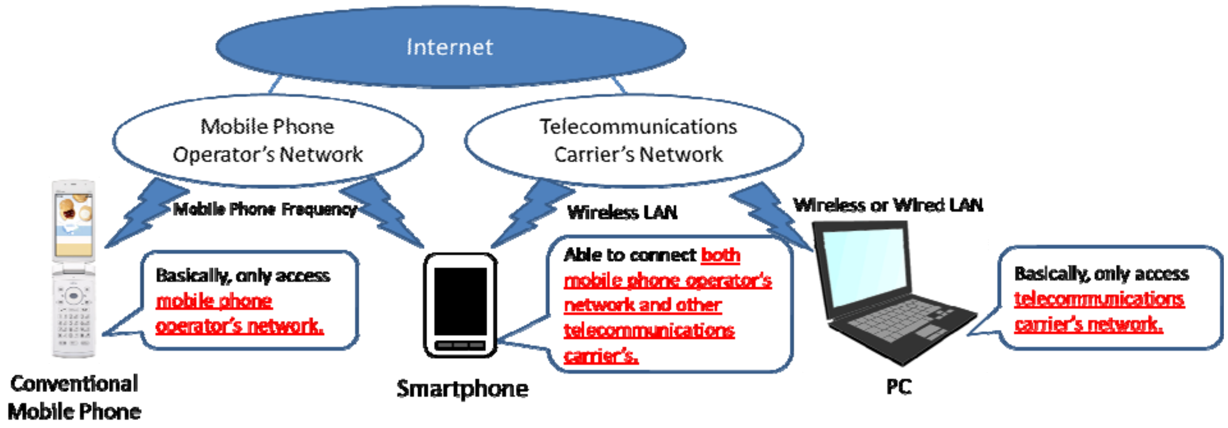

Internet
Mobile Phone Operator's Network
Telecommunications Carrier's Network
Mobile Phone Frequency
Wireless LAN
Wireless or Wired LAN
Basically, only access mobile phone operator's network.
Able to connect both mobile phone operator's network and other telecommunications carrier's.
Basically, only access telecommunications carrier's network.
Conventional Mobile Phone
Smartphone
PC

Figure 4 Diversification of Communication Paths

As user convenience improves in line with the diversification of communication paths, information security of wireless LAN networks present something of a problem.

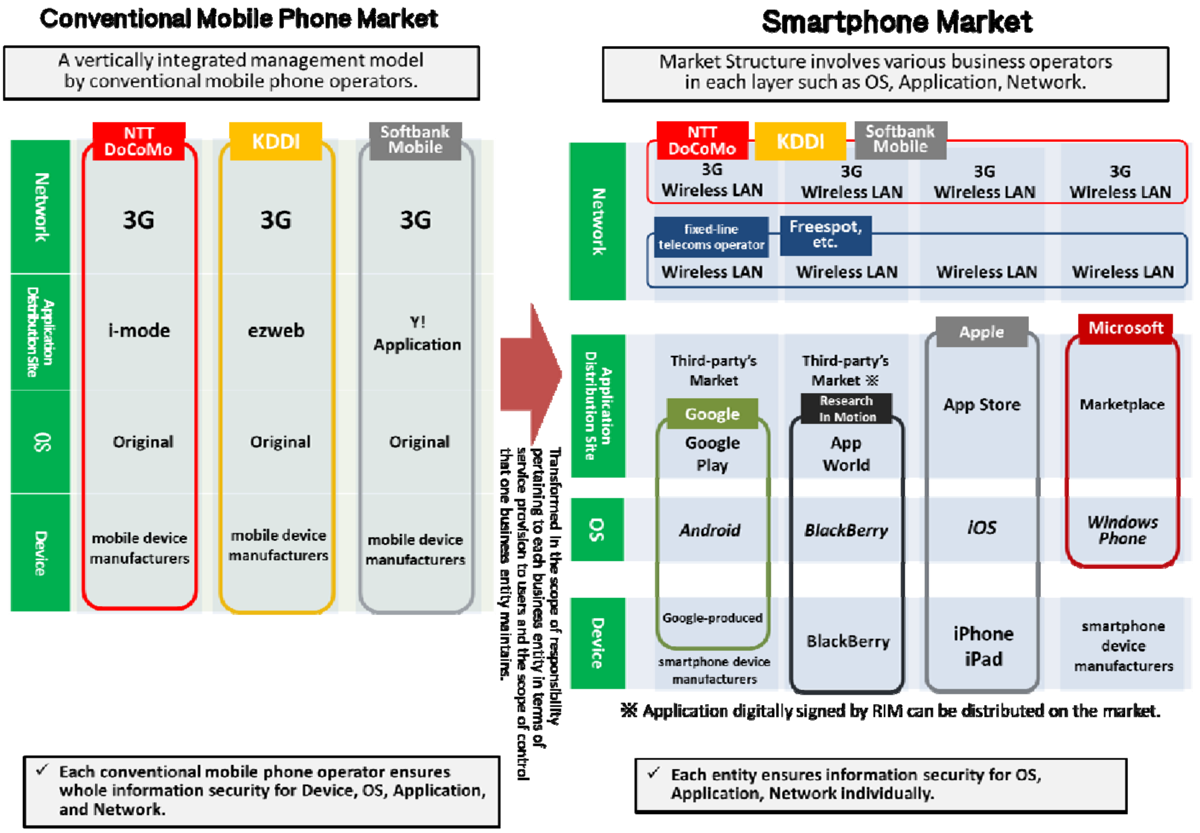
(4) Business Model Transformation

As a result of the rise in smartphones, the situation surrounding mobile phones in Japan has also undergone a transformation, progressing from a vertical integration model centered around conventional mobile phone operators, to a complex model involving a variety of players including OS providers, mobile device manufacturers and mobile phone operators, etc. (Table 1 & Figure 5) Moreover, OS providers and mobile device manufacturers have expanded their businesses globally and now supply global models of their products. A business model transformation like this has not merely involved changes in the scope of responsibility pertaining to each business entity in terms of service provision to users or the scope of control that one business maintains, but has also instigated changes in the nature of technological countermeasures.

Table 1 Status of market development according to OS (OS)

OS Classification	OS Provider	Number of Domestic Shipments in 2011 (10,000 units)※	Characteristics
Android	(US) Google	1,766	* As the OS, terminals and application distribution sites are deployed on a specialized horizontal basis, multiple business entities are involved in the manufacture of terminals and operation of application distribution sites. * As this is an open source OS, there is a great deal of flexibility in terms of customization by mobile device manufacturers. For this reason, even though the OS version may be the same, handsets often operate on a model-dependent basis.
BlackBerry	(Canada) Research In Motion	8	* As the OS, terminals and application distribution sites are essentially deployed on a vertically integrated basis, only OS providers engage in the manufacture of terminals. * Regarding the operation of application distribution sites, non-OS provider business entities are permitted to offer applications as long as the application is digitally signed by Research In Motion.
iOS	(U.S.) Apple	390	* As the OS, terminals and application distribution sites are deployed on a vertically integrated basis, only OS providers engage in the manufacture of terminals and operation of application distribution sites.
Windows Phone	(U.S.) Microsoft	12	* As the OS and application distribution sites are deployed on a vertically integrated basis, only OS providers engage in the operation of application distribution sites. * As the manufacture of terminals is deployed on a specialized horizontal basis, multiple business entities are involved. (There is presently 1 company in Japan)

(Secretariat data. However, ※ indicates data provided by Yano Research Institute Ltd.)


Conventional Mobile Phone Market
A vertically integrated management model by conventional mobile phone operators.
Network
Application Distribution Site
OS
Device
NTT DoCoMo
KDDI
Softbank Mobile
3G
3G
3G
i-mode
ezweb
Y! Application
Original
Original
Original
mobile device manufacturers
mobile device manufacturers
mobile device manufacturers
Transformed in the scope of responsibility pertaining to each business entity in terms of service provision to users and the scope of control that one business entity maintains.
Smartphone Market
Market Structure involves various business operators in each layer such as OS, Application, Network.
Network
NTT DoCoMo
KDDI
Softbank Mobile
3G Wireless LAN
3G Wireless LAN
3G Wireless LAN
3G Wireless LAN
fixed-line telecoms operator
Freespot, etc.
Wireless LAN
Wireless LAN
Wireless LAN
Wireless LAN
Application Distribution Site
Third-party's Market
Third-party's Market ※
Apple
Microsoft
Google
Research In Motion
Google Play
App World
App Store
Marketplace
OS
Android
BlackBerry
iOS
Windows Phone
Device
Google-produced
smartphone device manufacturers
BlackBerry
iPhone iPad
smartphone device manufacturers
※ Application digitally signed by RIM can be distributed on the market.

✓ Each conventional mobile phone operator ensures whole information security for Device, OS, Application, and Network.

✓ Each entity ensures information security for OS, Application, Network individually.

Figure 5 Business Model Transformation

Section 3 User Awareness of Smartphones

(1) General User Awareness

Many general users tend to purchase their smartphone device from the same store they purchased their conventional mobile phone at or otherwise choose a smartphone when upgrading from their conventional mobile phone. Based on this, it would appear that many users view the smartphone as an extension or an sophisticated version of the conventional mobile phone.

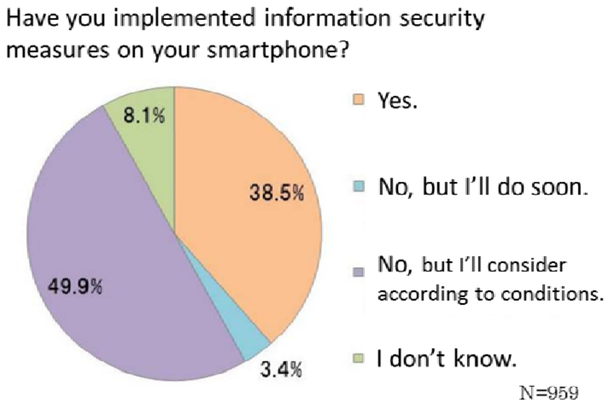
According to a survey conducted by a private research firm[6], approximately 40 percent of users take information security measures on their smartphone (Figure 6-1) and the reality is that there are a great number of users who believe that smartphones offer the same level of security as conventional mobile phones. Furthermore, these survey results reveal that more than 40 percent of those users who fail to implement appropriate security measures on their smartphone responded, "security measures are necessary, but I don't know what I need to do" (Figure 6-2).

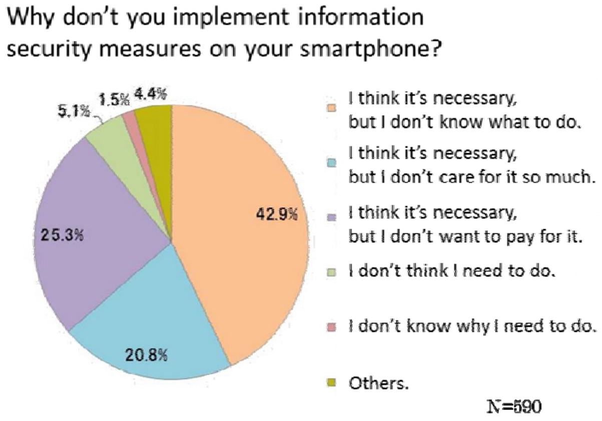
Accordingly, although mobile phone operators have continued to endeavor to educate users about information security measures for smartphones, there is a need to take the view that general users may not necessarily be sufficiently aware of the risks associated with smartphones and approaches to implementing the appropriate measures.

Users who fail to implement information security measures put not only their own smartphones at risk, but also jeopardize the network and other users, exposing both to potential damage as a result of invasion by malicious BOT viruses[7], and based on this, efforts need to be made to improve user awareness of information security measures.

[6] NetMile, Inc. "A Survey of Smartphone Security" (December 6, 2011) (http://research.netmile.co.jp/voluntary/2011/pdf/201112_1.pdf)

[7] A BOT infection refers to the state of a computer when infected with a self-propagating computer virus (BOT virus) designed to connect back to a remote source which is used to control the infected host computer. "BOT" is derived from the word "robot" due to the automated manner in which BOTs control the host.





(NetMile, Inc.)

Figure 6-1 Figure 6-2

User awareness of smartphone information security

(2) Business User Awareness

Smartphones are frequently being used in place of PCs, which were the prevalent tools of use in business environments until recently. Based on this we can assume that business users perceive smartphones to be the equivalent of a PC but with the added functions of verbal and Internet-based communication. The recent rapid proliferation of smartphones and the growing sophistication of smartphone capabilities would suggest that the business sector has not necessarily established a model of how to incorporate smartphone technology into business systems. Particularly in terms of smartphone usage in a business context, companies face the pending issue of whether to provide employees with a workplace supplied terminal or employ a strategy of having personal handsets used for business purposes (referred to as "BYOD"[8]), which then raises the issue of how to design the information security policy when the BYOD strategy is adopted.

It is against this backdrop that the "Japan Smartphone Security Association" (JSSEC)[9] was established by a group of companies and businesses involved in the smartphone sector, for the purpose of ensuring the safe utilization of smartphones and encouraging the dissemination of smartphone devices. JSSEC examines potential information security risks faced by the business sector, and considers relevant countermeasures to these risks, including measures against information leakage incurred as a result of smartphone usage for business purposes. As an indication of the progress that has been made, (on December 1, 2011) JSSEC published a set of guidelines designed with administrators in mind,

[8] Abbreviation for "Bring Your Own Device".

[9] Formerly a private organization known as the "Japan Smartphone Security Forum", JSSEC reformed in April 2012.

titled "Security Guidelines for using Smartphones and Tablets for Business Purposes - Advantages for Work Style Innovation - (Version 1)"[10]. The guidelines are intended as a reference regarding the utilization of smartphones in the business sector.

(3) Intended Users

Based on the above, this final report focus on general users and offers measures to be taken for the safe use of smartphones and compiles the policies that need to be tackled by relevant business operators and the government, including awareness promotion aimed at general users.

[10] http://www.jssec.org/dl/guidelines2012Enew_v1.0.pdf

Chapter 2 Smartphone Information Security Risks & Issues

Section 1 Smartphone Information Security Risks

(1) Applications that Pose Information Security Risk

Smartphone applications differ from applications created for conventional mobile phones in that users are able to realize a variety of functions under the access authority granted to users. As smartphones have rapidly infiltrated the market, a multitude of different applications have been created drawing on this attribute, however, some applications pose information security risks to users. Among those applications, the following applications appear to be prevalent: ① malware-inclusive applications, ② applications containing vulnerabilities and ③ applications that transmit personal information to external sources without specific intent on the part of the user.

a. Malware Targeting Smartphones

Malware targeting smartphones has become increasingly prevalent and there is a growing trend in the variety of malware in existence. At present, most of the malware contaminants that have been detected have been targeted at the Android platform and in the second half of 2011, the number of these contaminants demonstrated a dramatic increase[11] (Figure 7).

Meanwhile, based on survey results[12], a comparative analysis of the number of malware contaminants that emerged in 2011 for PCs and smartphones, would demonstrate that only one in several tens of thousands of smartphone malware contaminants exist against the several hundred that exist for PCs which would indicate that at present the smartphone malware situation has not progressed to a state involving the spread of serious damage.

[11] Trend Micro Incorporated. "Monthly Internet Threat Report" (June, First Half of FY2012) (http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20120706015002.html)

[12] A survey conducted by several information security providers.

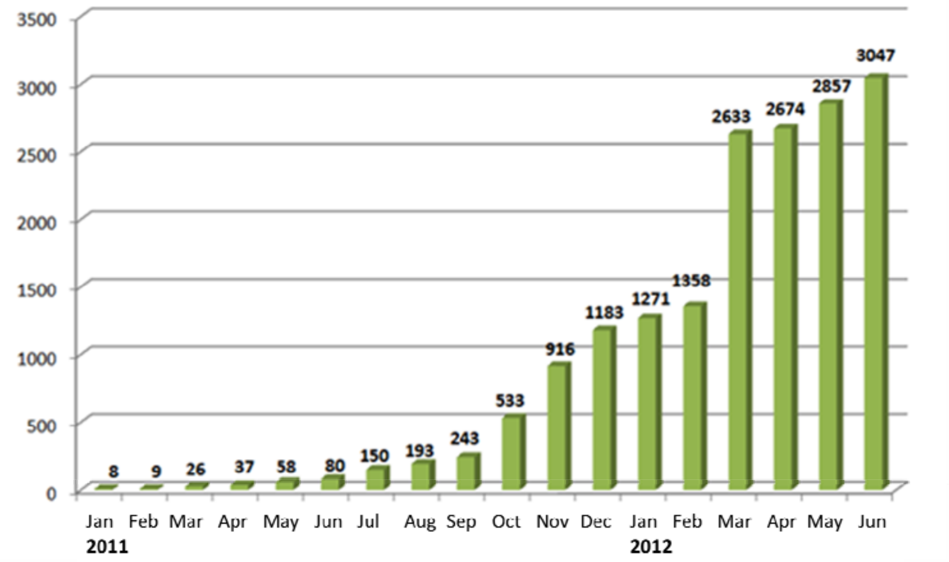


Figure 7 Number of Virus Pattern Files that Have Detected Malware[13] Contamination on Android Terminals (Trend Micro Incorporated.)

Of the malware detected thus far, there are some which have capacities of causing unauthorized charges, information leakage, fraudulent hacking and interception of administrator authority (Table 2).

Table 2 Actual Examples of Malware

Month/Year Detected	Company Name	OS	Overview	Note:
November 2009	ikee	iOS	A self-propagating worm that infects "jail-broken" (hacked) iPhones and changes the phone's wallpaper.	
August 2010	FakePlayer	Android	The first kind of malware to target the Android platform. Sends unauthorized SMS messages to premium rate phone numbers in Russia.	Only works on Russian networks so the SMS messages cannot be sent from outside Russia.
December 2010	Geinimi	Android	The first BOT virus to target the Android platform. After installation, the virus collects user information from the handset and waits for remote commands from the server.	The virus is spread by grafting the malware onto repackaged versions of legitimate applications. Contaminated Japanese versions of these applications also exist.
February 2011	DroidDream	Android	A BOT virus that attacks OS vulnerability, intercepting administrator authority. Communicates periodically with a remote server after launching and then runs commands and updates.	Distributed as a free application after being grafted onto legitimate applications. Also detected in applications available in the Android Market (now, Google Play).
May 2011	Lightdd	Android	Spies on the user without the user running the application, sending information back to an external	Also detected in applications available in the Android Market (now, Google Play).

[13] Definition/term varies depending on the information security provider.

			server after running a malicious code on the device when a call or message is received or a call ends.	
January 2012	FakeTimer	Android	Sends telephone number and email address details, etc. to an external source and then displays this stolen information on a pop-up window together with a request for payment of a fictitious usage fee.	Used on "one-click billing fraud" websites in Japan, this malware installs itself on the device, disguising itself as an application offering video playback ability when accessed. The Metropolitan Police Department apprehended the senior executives of a Tokyo based IT company in June, on suspicion of fraud involving the unlawful distribution of electronic records (virus distribution).
April 2012	the Movie	Android	Sends the names, telephone numbers and email addresses, etc. of individuals stored in the user's contacts list to an external source.	The Metropolitan Police Department searched the homes of Tokyo-based IT companies, etc. in May, on suspicion of unlawful distribution of electronic records (virus distribution).

(Secretariat data)

The threats posed by malware and the environment surrounding malware vary from one OS to another.

In the case of iOS and Windows Phone, these OSes have been designed so that, unless the users themselves remove the restrictions that have been set by default by the OS providers (a practice commonly known as “jailbreaking”), they will not be able to install applications from other sites other than from the official application download site operated by each OS provider. In the case of the BlackBerry, while users are able to obtain applications from sites other than BlackBerry’s official application download site, they will be able to install only those applications that have been digitally signed by the OS provider, Research In Motion. In addition, all of the official websites of the said OSes perform prior screening of all the applications that are offered through their websites to check their safety based on their own standards. Thanks to the way in which each of the OSes has been designed, and their capability to check applications in advance, there have been no confirmed incidents relating to any of the BlackBerry, iOS, or Windows Phone of malware infections among their standard devices, provided that no jailbreaking was performed on these devices.

As far as Android is concerned, a large number of applications have been created which are distributed through various application distribution sites (which are known as “third-party markets” [14] other than Google Play (the official

[14] There are various types of application distribution sites, ranging from sites that are operated by mobile phone operators, etc. to those sites that are run by individuals.

website that replaced Android Market), and users are able to install these applications by modifying the settings on their own devices.[15] Much of the malware that preys on Android that has been discovered thus far has come from third-party markets which operate in foreign countries.

Google, in the past, had a policy such that their official website did not pre-screen the applications that were made available on Android Market (which was their official website at that time), instead, application developers conducted self-examinations to ensure that their applications were in compliance with Android Market's rules for making applications available for download. Due to this policy, there were instances where applications that contained malware were available for download on the official website. However, as soon as these malware-containing applications were detected, steps were taken to delete them from the official website as well as from the devices of users that downloaded them. As a result, there were no confirmed reports of substantial damage from these applications as of the publication of our interim report. Further, in February 2012, Google announced through its official blog that the company had a system up and running for performing automatic analyses of applications [16] in order to eliminate malware, etc. from the applications offered through its official website.

On the other hand, in January 2012, a billing scam application that targeted Android users was discovered. The scam attempted to direct users to install the said application on a certain website. As of March 2012, consumer service centers, etc. received complaints about possible malware infections arising from the above application.[17]

b. Applications that contain vulnerabilities

In some cases, application vulnerabilities may be attributed to problems in coding[18] while in other cases they may be caused by, among other things, problems in specifications or design.

For example, it is possible to exploit a memory-related vulnerability in an application caused by a coding error in order to execute a malicious program for enabling an attack on OS vulnerabilities or illegal access to the data stored within a device. It is possible that administrative privileges may be taken over through an attack on vulnerabilities in an OS. In addition, illegal access to data may lead

[15] Android users can install applications from application distribution sites other than Google Play by checking the item "Applications from unknown sources" on the settings screen. (By default, the said item has not been checked off.)

[16] Google Japan Blog (article dated February 6, 2012) (http://googlejapan.blogspot.jp/2012/02/android.html)

[17] Newsletter issued by the Tokyo Metropolitan Government (http://www.shouhiseikatu.metro.tokyo.jp/sodan/kinkyu/120323.html)

[18] The process of writing a program based on software specifications and design.

to information leaks, or other such problems.

Furthermore, improper storage locations for important data, or inappropriate encryption caused by errors in specifications and design, may potentially result in information leaks.

c. Applications that can send out user information without the intent of the user

Smartphones, as is the case with conventional mobile phones, are usually carried around by their users on a daily basis, and are frequently used even while users are away from home. For this reason, users tend to spend more hours on smartphones than on their PCs, and because of the heavy use of applications and location data, a wide range of user-related information is stored on their smartphones.

It has been found that there are applications, daemon[19], and other programs that enable this user-related information to be sent out without the intent of the user. In April 2012, an application was found to exist that can send out the personal names, telephone numbers, e-mail addresses, and other such information registered in the address books of smartphones.

(2) Threats of information leaks, etc. caused by the loss or theft of a device

As far as the information being handled by smartphones is concerned, aside from applications that lead to information leaks, the information that each device saves internally may possibly be leaked or damaged as a result of the loss or theft of the device.

(3) Threats caused by the use of wireless LAN

When wireless LAN is accessed through a smartphone, the device will be exposed to the information security threats that commonly exist on the Internet, and therefore the device will become vulnerable to access point spoofing, and packet interception, as well as unauthorized access through identity theft that may result from such threats.

There are those who are of the opinion that smartphones, when they are used in the wireless LAN environment, are susceptible to the same types of threats as those relating to PCs. However, it must be kept in mind that, considering that smartphones have functional limitations and may gain access to the wireless LAN environment without the proper literacy or awareness on the part of users, the threats facing smartphones tend to emerge more easily than in the case of PCs operating in the wireless LAN environment.

[19] Daemon is a program that runs as a background process in a multi-tasking operating system.

Section 2　Information Security Issues Relating to Smartphones

In keeping with the emergence of information security threats such as those described in the previous section, the present section will outline those information security issues that need to be resolved. Figure 8 below illustrates those areas that are under close scrutiny, and the exchange of information among those areas.

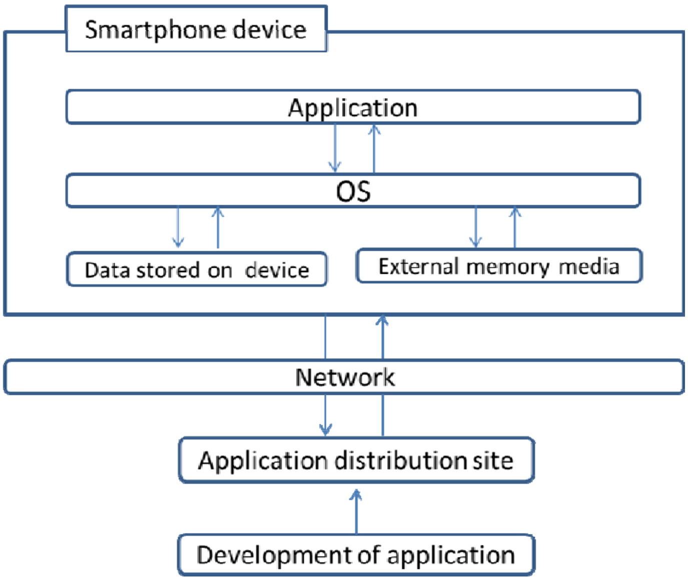


Figure 8　Areas under Close Scrutiny for Information Security Issues Relating to Smartphones

The symbols “A”, “B”, “i” and “W” which appear in the present section and sections thereafter indicate that each of the matters described below are associated with Android, BlackBerry, iOS, or Windows Phone, respectively. Note that the information presented herein is as of the time of publication of this report, and is therefore subject to change as new threats surface in the future.

(1) Issues relating to OSes

a. Issues relating to vulnerabilities (A, B, i, W)

Concerns have been raised that malware which exploits the vulnerabilities in an OS may take over the user’s administrative privileges without his or her authorization creating a risk that the OS itself or system files may be altered.

b. Issues relating to OS version upgrades and security patches (A, W)

Version upgrades for OSes are independently developed and released by OS providers, and can have a wide-ranging impact on the mobile device manufacturers that load the said OSes onto its devices, as well as mobile phone operators who offer the networks accessed by these devices.

In particular, in the case where a mobile device manufacturer customizes an OS on its own to enhance its convenience and the level of security, they need to customize an upgraded version of that OS as well, which requires a fair amount of worker-hours and time period.

Furthermore, there have been instances where security patches [20] released by OS providers take quite a while to reach to their users, as these security patches, after they are released by the OS providers, first need to be integrated by mobile device manufacturers into their systems, and reviewed by mobile phone operators. As a consequence, these mobile devices tend to become susceptible, for a longer period of time than in the case of PCs, to the risk of infection with malware that may exploit certain vulnerabilities.

c. Issues relating to the support period for OSes (A, B, i, W)

At the present time, the support period for the previous versions of some of the OSes remains unclear, and, therefore, their users are not certain about how long security patches for the previous versions will continue to be offered after a new version is released. There are concerns that when a smartphone is used over a long period of time, the user may not be able to upgrade to a new version of the OS due to the limitations set by the device, and so will likely continue to use the previous version of the OS. As a result, when the support period for the previous version of the OS ends, the user will have to continue to use the OS without security patches.[21]

d. Issues relating to the channels for providing support for OSes (A, B)

As a means for providing security patches for an OS, some mobile phone operators distribute security patches only through their own networks. The issue with smartphones loaded with this type of OS is that the users will not be able to, as a general rule, receive support for the OS after their service contract has ended with their respective mobile phone operators.

It has been pointed out that, in the case of sophisticated smartphones, some users continue to use, even after their service contract has ended with the mobile phone operator, the functions on the device, other than oral and data communication functions using the provider’s network. Among these functions, of particular concern is the wireless LAN function which users can continue to use after their service contract has ended. Since these users will no longer be able to

[20] Security patch refers to a program that fixes certain vulnerabilities in an operating system, etc.

[21] In some cases, certain smartphone specifications, security enhancement steps taken by mobile device manufacturers, and other factors can keep vulnerabilities in operating systems that should require security patches from materializing.

receive support for the OS on the device after the end of the service contract, they will be exposed to the risk of information leaks through malware infection, etc. [22]

(2) Issues relating to applications

Applications that come equipped with smartphones are different from those applications that normally come with conventional mobile phones, as they enable functions that freely make use of the privileges that are given to users. It is known that certain applications that exploit this feature have been created, and they can pose information security threats to users. It has been pointed out that at present the installation of these applications poses the most danger to users.

As stated in the previous section, the types of applications that pose threats to smartphone users are as follows: (1) applications that contain malware; (2) applications that contain vulnerabilities; and (3) applications that can send out user information without the intent of the user. Among these applications, there are issues relating to those applications that can send out user information without the intent of the user, over how the consent of users should be properly obtained upon installation of the applications, and how to establish criteria for objectively evaluating those applications that are considered problematic. These issues were raised in our interim, which stressed the importance of a debate over the information that needs to be protected, and therefore made a recommendation for establishing a forum to discuss these issues in detail. Subsequently, a discussion on these issues was held by the "Working Group on the User Information Sent through Smartphones", which is a subgroup organized under the "Study Group on Consumer Issues with ICT Services" within the Ministry of Internal Affairs and Communications. In view of the foregoing, the remainder of the present section will focus on the issues pertaining to the first two types of applications mentioned above: (1) applications that contain malware; and (2) applications that contain vulnerabilities.

a. <u>Issues relating to the creation of applications that contain malware or vulnerabilities</u> (A, B, i, W)

Applications that contain malware or vulnerabilities are normally created when malicious developers intentionally incorporate malware into the applications they are developing, or, in other cases, when developers who are lacking in expertise or knowledge, without harmful intent, incorporate modules, etc. that contain malware into their applications, or leave the applications with vulnerabilities. For this reason, actions are called for to improve the technical competence of

[22] Same as above.

developers and to provide them with morale training.

b. Issues relating to the circulation of applications that contain malware or vulnerabilities (A, B, i, W)

When insufficient checks are performed in screening applications that contain malware or vulnerabilities, these applications may be made available on application distribution sites in view of the fact that new types of malware and vulnerabilities will likely continue to be created in the future, it will be difficult to ensure a perfect screening capability against them. Nonetheless, it is important for all concerned parties to implement measures to prevent the circulation of these malware and vulnerabilities as much as possible.

c. Issues relating to the installation of applications that contain malware or vulnerabilities (A, B, i, W)

Another concern relates to the fact that users may install applications that contain malware or vulnerabilities.

As for the OSes for which anti-malware software are offered, the use of such software can prove effective to a certain degree against the installation of applications that may contain malware or vulnerabilities. However, because the security model for the OSes running on smartphones is characterized by the use of a sandbox configuration, issues have been raised over, the structural limitations of anti-malware software, which is a type of application, such that the software is unable, as a general rule, to monitor the behavior or contents of other applications.

(3) Issues relating to networks (A, B, i, W)

A surge in telecommunications traffic due to the widespread use of smartphones has overburdened the networks of mobile phone operators. As a result, mobile phone operators, in an attempt to enhance user convenience, have expanded the access points for wireless LAN in order to offload a portion of the data traffic (offloading [23]), and they have announced that they will offer, free of charge, wireless LAN services to their users. In addition, in many cities there are a number of public wireless LANs that have been set up by business operators other than mobile phone operators.

It is forecast that there will be more and more opportunities going forward for people to access public wireless LANs from their smartphones. However, there are

[23] The term “offloading” used herein refers to a means for reducing the network load burdening mobile phone operators by transferring their smartphone data communications traffic to the other communications networks, such as wireless LANs that are maintained by operators other than mobile phone operators.

worries that some of these public wireless LANs employ encryption methods and authentication methods that are known to possess vulnerabilities. In addition, while conventional mobile phones basically offer oral and data communications by using only the telecommunications facilities of mobile phone operators, smartphones enable their users to access public wireless LANs that have been established by operators, other than mobile phone operators. The problem here is that the measures that have been implemented by mobile phone operators alone cannot adequately address the information security problems associated with these public wireless LANs.

(4) Issues relating to the data stored on devices (A, B, i, W)

Since smartphones are carried around at all times, the risk of loss or theft of devices is much higher for smartphone users than for PC users. In addition, it has been recognized that, since personal information and other various types of information are stored on smartphones, there is a risk that the data stored on the device may be lost, or extracted by a third party in the event of loss or theft, of the device. Further, it is necessary to design smartphones so that they cannot be re-used by any person other than the authentic device user. At present, remote wipe, self-erase [24], and other functions are known as means for mitigating this risk. It must be kept in mind, however, that the remote wipe function can prove effective only when the device is on, and the conditions of communication are stable.

Also, SD (secure digital) cards are widely used as external memory media for smartphones; however, these cards can be stolen in the event of loss or theft of the device. Furthermore, it is difficult to control access from applications to the data that has been saved on SD cards. There is risk, therefore, that the said data may be extracted through the use of certain applications, or may be taken out when these cards are connected to a PC as an external memory medium.

(5) Effects of smartphones on external networks (A, B, i, W)

From the point of view of smartphone users, there are concerns over not only the protection of the users' own devices and information stored thereon, but also over the possibility that, due to a lack of adequate information security measures, their smartphones may be used in a variety of cyber attacks, or cyber crimes, as well as the problem of bandwidth overload brought about by communication through smartphones.

At the present time, there have been no reports of large-scale incidents. However, if a smartphone becomes infected with malware which enables the unauthorized

[24] Self-erase refers to a function that will delete system data when a password is entered more than the prescribed number of times.

operation of the device, the infected device may possibly be used as a platform for facilitating activities such as DDoS (distributed denial-of-service) attacks, or spreading malware infections into PCs, just as would be the case when a PC becomes infected with the same type of malware. In addition, while the use of the Wi-Fi tethering function [25] on smartphones is becoming popular, there is a risk that improper connection settings on a smartphone could allow other unknown devices that are nearby to connect to that smartphone, and the smartphone may then be used as a platform for committing a wide range of cyber crimes.

(6) Issues arising from changes in business models (A, B, i, W)

It needs to be recognized that, since OS providers and mobile device manufacturers offer global model products, it is very difficult for Japan alone to request of these companies that they implement information security measures.

[25] Using the tethering function, a smartphone can be used as an access point for a wireless LAN, thereby allowing PCs, game devices, and other such devices that have wireless LAN capability to connect to the Internet through a network, etc. of a mobile service provider.

Chapter 3　Information Security Measures Implemented by Business Operators and the Government

In the present chapter, measures will be proposed with regard to each of the issues that face smartphones which were outlined in Section 2 of Chapter 2 above, namely, measures which should be implemented as well as measures that should be seriously considered by business operators and the government.

It should be noted that the information security measures for PCs connected to the Internet as we know them today were not created in a single step; rather, it has taken more than 10 years for these measures to be developed and established. By the same token, a reasonable amount of time will likely be needed for information security measures for smartphones to mature from a technical point of view, and to be adequately accepted by users. In keeping with the foregoing, the discussions that follow in the sections presented hereunder will include those information security measures that will likely be difficult for some operators of device to put into practice promptly, due to various limitations imposed on them by business models, smartphone specifications, etc.

Section 1　Basic Concept for Considering Information Security Measures

(1) Significance of cooperation

Not only the information security measures for smartphones, but information security measures in general require cooperation among firms, research organizations, and government administration, such as the sharing of information regarding information security incidents.

It is a fact that it is difficult to work out information security measures that can be applied uniformly across the board, as mobile phone operators, mobile device manufacturers, and others differ from one another with regard to the way their OSes are customized, their opinions on information security measures, their means for implementing these measures, as well as their proprietary technologies and device specifications. Nonetheless, for the purpose of promptly strengthening information security measures, it is important to facilitate the sharing of information among trade associations, with regard to the enhancement of the information security level for smartphones.

In addition, when new smartphone models are being rushed to the market, they may go on sale even though there are still serious information security issues to be resolved. This kind of situation must not occur, as they can distort the sound development of the smartphone related industry. In view of the above, it is important for all business operators involved to implement the proper information security measures.

(2) Significance of raising user awareness

A great advantage of smartphones is the fact that users are given freedom, to a certain degree, to customize software programs and device functions in accordance with their own needs. On the other hand, there are some cases where, due to this very advantage, the security measures implemented by mobile phone operators alone cannot ensure the safety of smartphones. Therefore, it is important that users themselves gain the necessary knowledge, and undertake the proper actions on their own to ensure information security.

Therefore, it is crucial for business operators and the government to, in addition to taking the initiative to work out the proper information security measures, raise the awareness of smartphone users towards the importance of these information security measures, educate these users on specific methods, for applying these measures, and at the same time, create an environment which can make it easy for users to take the proper information security measures. Promotion of both the measures to be implemented by operators and those to be implemented on the part of users is definitely important and should be promoted in unison, just like the wheels of a car.

(3) Ensuring convenience

It is necessary to keep always in mind that the measures and efforts implemented domestically, and guidelines and other voluntary regulations established by trade associations, do not cause deterioration in the domestic industry’s ties to the global market, the convenience of smartphones, or the competitiveness of domestic business operators.

In addition, this final report is intended to underpin the sound development of the smartphone-related industry, and, as stated in the “Preface” at the beginning of the report, it is important to focus on what types of information security measures should be worked out, while ensuring the convenience of smartphones. In order to ensure that smartphone users will recognize and accept these information security measures, it is also important, therefore, to pay careful attention to the performance of OSes, battery consumption, and other matters, in order to make sure that the convenience of smartphones will not diminish.

(4) Variations in information security measures among OSes, etc.

Since design concepts and business models differ among smartphone OSes (i.e. Android, Blackberry, iOS, and Windows Phone), it is appropriate to work out measures that are suit for the characteristics of each OS.

Section 2 Measures to be implemented by Business Operators to Address the Issues under Consideration

In the present section as well as the next section, specific measures will be proposed which will address each of the issues that have been raised in Section 2 of Chapter 2 above (refer to Figure 9 on the next page). The measures proposed in the present section are to be implemented by mobile phone operators, mobile device manufacturers, and information security providers, unless it is otherwise mentioned that any of these measures is intended for OS providers, or application distribution site operators. In addition, a list has been prepared as per Appendix 1, which summarizes the measures that are proposed in the present section.

(1) Measures relating to OSes

a. Solutions for vulnerabilities in OSes, and the release of security patches (A, W)

Vulnerabilities in the OSes are fixed through OS version upgrades, as well as security patches that are released by OS providers. Therefore, it is crucial that smartphone users apply these upgrades and patches to their devices as quickly as possible.

To address this issue, mobile device manufacturers must continue to make an effort to set priorities for solving various vulnerabilities in accordance with their details, strengthen their cooperation with mobile phone operators, and take other actions as necessary so that they can notify users accordingly, and provide FOTA (Firmware Over-the Air) [26]. In doing so, mobile device manufacturers must pay careful attention so that OS version upgrades, or security patches, are not released in an incomplete form or manner, which could result in a decline in the level of information security in each OS.

b. Detection and sharing of information relating to vulnerabilities in the OSes (A, B, i, W)

As an effective preemptive move against vulnerabilities in OSes, the business operators concerned should, within the framework of trade associations, work together to gain a grasp of both the detail information of vulnerabilities and the damage suffered by users arising from those vulnerabilities, and consider appropriate countermeasures to be implemented. However, in order to prevent the said information on vulnerabilities from being misused, careful consideration must be taken when determining the range of information sharing. In addition, the above efforts should be linked to the existing framework for sharing information

[26] FOTA (Firmware Over-the-Air) refers to the procedure for updating an operating system, etc. for smartphones via wireless communication.

on vulnerabilities in software programs.

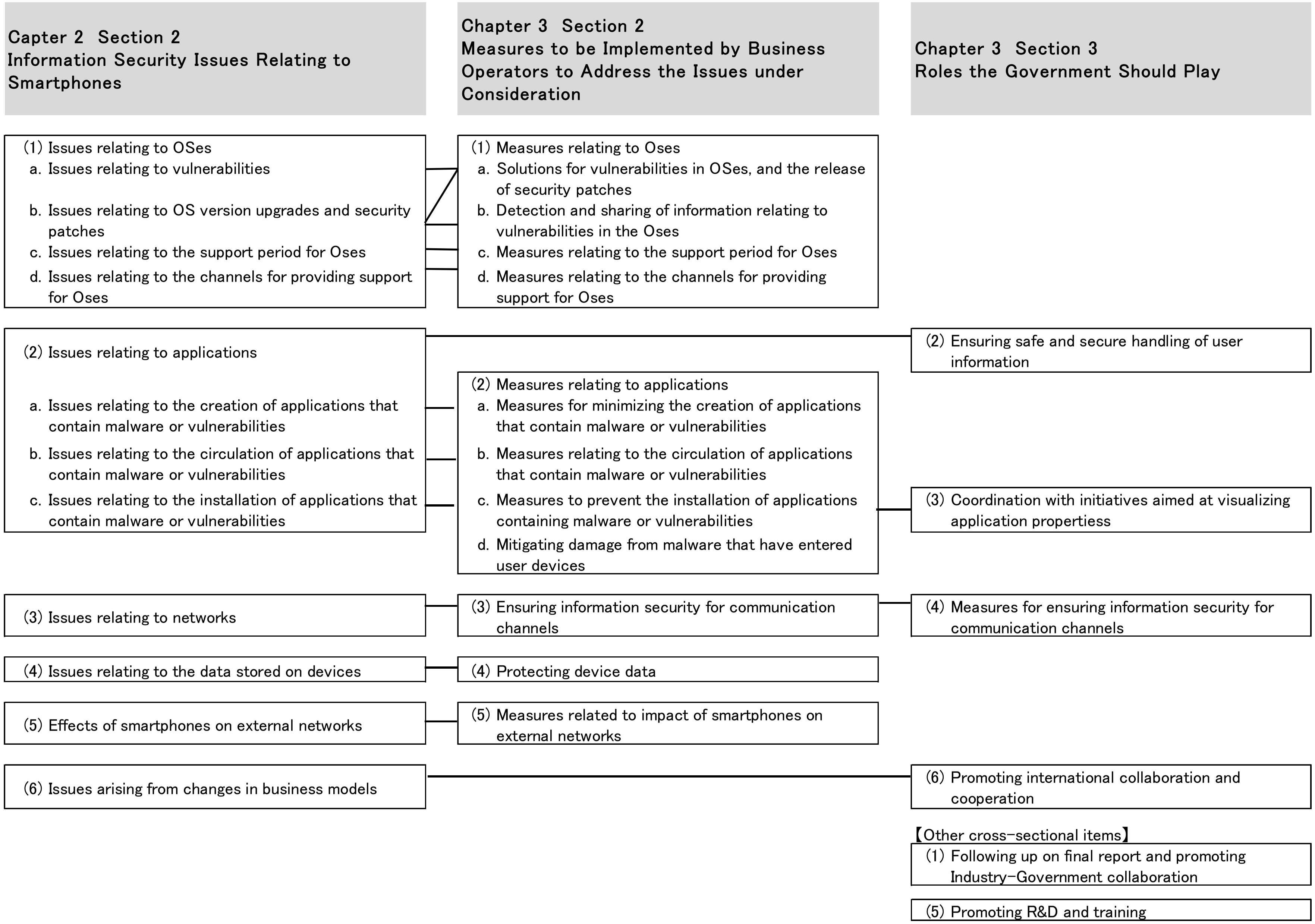
Furthermore, it is important to develop detection tools that can enable the early detection of vulnerabilities.

c. Measures relating to the support period for OSes (A, B, i, W)

To lower the risk that smartphone users may continue to use OSes after the support period for these systems has ended, it would be advisable that the OS providers publicly make an announcement before they end the support for their respective OSes.

d. Measures relating to the channels for providing support for OSes (A, B)

To address issues such as the inability of smartphone users to receive support for an OS after they have ended their contracts with mobile phone operators, it is necessary for these operators to clearly explain these issues to users at the time of contract expiry.



Capter 2 Section 2
Information Security Issues Relating to Smartphones

(1) Issues relating to OSes
a. Issues relating to vulnerabilities
b. Issues relating to OS version upgrades and security patches
c. Issues relating to the support period for Oses
d. Issues relating to the channels for providing support for Oses

(2) Issues relating to applications
a. Issues relating to the creation of applications that contain malware or vulnerabilities
b. Issues relating to the circulation of applications that contain malware or vulnerabilities
c. Issues relating to the installation of applications that contain malware or vulnerabilities

(3) Issues relating to networks

(4) Issues relating to the data stored on devices

(5) Effects of smartphones on external networks

(6) Issues arising from changes in business models

Chapter 3 Section 2
Measures to be Implemented by Business Operators to Address the Issues under Consideration

(1) Measures relating to Oses
a. Solutions for vulnerabilities in OSes, and the release of security patches
b. Detection and sharing of information relating to vulnerabilities in the Oses
c. Measures relating to the support period for Oses
d. Measures relating to the channels for providing support for Oses

(2) Measures relating to applications
a. Measures for minimizing the creation of applications that contain malware or vulnerabilities
b. Measures relating to the circulation of applications that contain malware or vulnerabilities
c. Measures to prevent the installation of applications containing malware or vulnerabilities
d. Mitigating damage from malware that have entered user devices

(3) Ensuring information security for communication channels

(4) Protecting device data

(5) Measures related to impact of smartphones on external networks

Chapter 3 Section 3
Roles the Government Should Play

(2) Ensuring safe and secure handling of user information

(3) Coordination with initiatives aimed at visualizing application propertiess

(4) Measures for ensuring information security for communication channels

(6) Promoting international collaboration and cooperation

【Other cross-sectional items】
(1) Following up on final report and promoting Industry-Government collaboration

(5) Promoting R&D and training

Figure 9 Issues and Recommended Measures

(2) Measures relating to applications

a. Measures for minimizing the creation of applications that contain malware or vulnerabilities (A, B, i, W)

As an effective way of coping with the issue of the creation of applications that contain malware or vulnerabilities due to a lack of expertise and knowledge on the part of developers, it is important to provide training and education to developers as necessary with regard to secure programming techniques, as well as technical knowledge relating to modules [27]. Since the demographics of developers consists of various tiers that range from individuals to engineers of corporations, it is important to carry out specific training and education measures that can cater to as many of these tiers of developers as possible.

The JSSEC (Japan Smartphone Security Association) prepares and releases secure programming guides which include code samples. In order to enable a broad range of developers from the various tiers to learn specific techniques and programs, it is recommended that these types of up-to-date guides be posted and/or made available on the JSSEC's website, through seminars and technical publications, and other forms of media which developers are likely to come across. In addition, it is advisable that, due to the fact newer versions of OSes, SDKs (software development kits) [28], and modules will be released continually, the contents of the guides and code samples be reviewed and revised as necessary on an ongoing basis.

Furthermore, it is recommended that the operators of application distribution sites and mobile device manufacturers provide the necessary information for the purpose of ensuring an adequate level of information security, through the release of programming guides and development tools released through appropriate websites, the hosting of seminars designed for developers, and other such measures. It should be also noted that at present the demand for smartphone application developers in the market is growing, and there has been a spurt in staff training activities among corporations employing programmers, and in self-organized seminars held by various developer communities [29]Therefore, it is recommended also that, using the opportunities like the above, the proper measures be implemented to provide education and training for developers to help enhance their knowledge of improving the level of information security.

[27] Module refers to a program that serves as an individual component used to bring about the realization of a group of functions.

[28] SDK (software development kit) refers to a set of tools that is used for the development of software programs.

[29] Developer communities include the Japan Android Group, and others.

b. Measures relating to the circulation of applications that contain malware or vulnerabilities (A, B, i, W)

Actions have been taken on the application distribution sites that are operated by OS providers and mobile phone operators to remove those applications containing malware or vulnerabilities (refer to Table 3 and Table 4). At the present time, there are no standardized criteria, either within or outside of Japan, for the adequacy of applications posted on application distribution sites. Therefore, the operator of each application distribution site runs the site in accordance with its own policy for making various applications available.

The operators of application distribution sites should pay attention to the expectations of their users who are seeking to download safe applications, and must make every effort to continue or improve their operation of these sites. In addition, it is preferable that each application distribution site disclose to users the site's operation policy as well as the posting policy of applications thereon, so that users will be able to determine the reliability and credibility of the site.

Furthermore, in the future, the operators of various application distribution sites would be advised to work with one another from a user standpoint to standardize, to the greatest extent possible, and the minimum criteria for the posting of applications on their respective sites.

Table 3: Application Distribution Sites Operated by OS Providers

Application Distribution Sites			Application							
					Posting policies					
					Availability to the public		Upon posting	After Posting		
Operator	Company Name	Type	Device platform	Install base	Users	Developers	Verification of policy violation	Detection of policy violation	Measures taken when policy violation is discovered
Google	Google Play	Application distribution	Android	450,000 + March 2012	Yes	Yes	Once posted, applications are verified by: (1) Checking whether the developer distributed malware, etc. in the past; (2) Performing static analysis to detect known malware; (3) Running the application and analyzing its operation.	Applications are vetted based on automated application scanning as well as reporting by developers and users.	Warnings are sent to developers or applications are removed from the distribution site depending on the type of application or policy violation.
Research In Motion	App World	Application distribution	BlackBerry	approx.60,000 March 2012	No	Yes (English)	Applications are reviewed prior to posting (via undisclosed review process).	Applications are vetted based on reports from users, etc.	Same as above
Apple	App Store	Application distribution	iPhone*1 iPad*1	approx.585,000 (at the end of February, 2012)	No	No*2	Applications are reviewed prior to posting (via undisclosed review process).	Applications are manually checked on a routine basis and upon reports from users.	Same as above
Microsoft	Market-place	Application distribution	Windows Phone*1	approx.64,000 + March 2012	No	Yes	Applications are reviewed manually before posting to see if they meet the requirements that have been made public. If they fail to meet the requirements, the developer will be notified in writing of the reason(s) for rejection along with how they were tested.	Applications are vetted based on reports from developers, etc.	Same as above

*1. Applications cannot be installed via other application distribution sites.

*2. Policies are published but require a developer account (with a fee) to view.

(Secretariat data)

Table 4: Application Distribution Sites Operated by Mobile phone operators

Application Distribution Sites			Applications						
					Publishing policies				
Operator	Company Name	Type	Device platform	Install base	Availability to the public		Upon posting	After posting	
					Users	Developers	Verification of policy violation	Detection of policy violation	Measures taken when policy violation is discovered
NTT Docomo	d Market	Portal to applications	NTT Docomo Android	approx. 1,000 March 2012	No	No	Applications are manually run and visually tested prior to posting.	Applications are manually checked on a routine basis and upon reports from users.	Applications are removed from the distribution site.
	d Menu	Portal to application distribution sites	NTT Docomo Android	approx. 4,800 sites (March 2012)	No	Yes	Once the app distribution site operator consents to the positng policy, its written proposal is reviewed.	Applications are manually checked on a routine basis and tested via Docomo Anshin virus scans as well as upon reports from users.	Warnings are sent to developers or applications are removed from the distribution site depending on the type of application or policy violation.
KDDI	au Market	Application distribution	KDDI Android	approx. 7,500 (April 2012)	No	Yes	Applications are verified by: (1) Automated function analysis; (2) Running the app manually and analyzing its operating log; (3) Visually verifying whether explanations or confirmations given to users are sufficient enough to prevent possible infringement of the privacy policy or unauthorized charges.	(A) Reported by users (B) Step (1) described on the left will be performed for all applications listed when analysis patterns are updated, and the logs collected before publication (as described in steps (2) and (3) on the left) will be reevaluated.	If the app is found to pose a big risk, it will be removed from the list once its developer is notified, and users will be notified as necessary (This is yet to occur). If the risk is small, the developer will be asked to make necessary corrections and update the app.
Softbank Mobile	@Appli	Portal to applications	Softbank Mobile Android	approx. 2,000 (April 2012)	No	No*	Consent of the application developer to the posting policy is obtained.	Applications are manually checked on a routine basis and upon reports from users.	Applications are removed from the distribution site.

* The policy is available on the web page used to sign up for a developer account, but only individual developers signing up for an account are notified of the web page URL. (The URL can be accessed by anybody.)

(Secretariat data)

C. Measures to prevent the installation of applications containing malware or vulnerabilities

(i) Anti-malware software [A, B]

Anti-malware software is effective to a certain degree in preventing applications containing malware from being installed. Therefore, efforts should be made to improve the functions of anti-malware software and to promote increased use of such software.

As a solution to the structural limitations of anti-malware software, developing devices that authorize anti-malware software to privileged access to the OS is currently under review. Some point out, however, that authorizing privileged access involves changing the OS's information security model and hence will generate new threats if the anti-malware software contains vulnerabilities. Future efforts must be made with careful considerations in light of the above-mentioned concerns.

As an alternative solution, some mobile operators prefer to develop an enhanced security kernel and combine it with conventional anti-malware software to achieve a level of security that is equivalent to anti-malware software with privileged access.

(ii) Mobile device management (MDM) [A, B, i, W]

Applying enterprise mobile device management (MDM[30]) solutions to personal mobile devices might be one answer to the problem that does not rely on the use of anti-malware software. MDM software provides advantages for companies that use smartphones in their business operations. It gives their system administrators integrated control of mobile devices used at work[31], including the ability to configure devices to meet their company's information security policy, manage software versions, restrict applications to be installed, and more. These companies use MDM solutions to prevent malware from being installed on their employees' smartphones. Such smartphone management solutions based on a unified policy are still scarcely available to general mobile device users. If they become more widely available, these solutions will enable individual smartphone users to ensure a high level of information security.

That's why we must examine MDM solutions for individual mobile device users. The road ahead leading to these solutions, designed for general

[30] Mobile device management (MDM) provides organizations with unified control over the smartphones used by their employees at work and enables them to enforce their information security policy. MDM enables system administrators to remotely monitor system operations of smartphones used in various locations, configure devices to limit the use of certain functions in order to ensure information security, etc.

[31] Either company-owned or personally owned devices used at work (BYOD).

consumers who use various types of mobile devices, is fraught with obstacles. One such obstacle is that MDM solution providers must always keep their products up to date in order to support the latest OS.

(iii) Visualization framework for application properties [A]

Android applications are available through many third-party marketplaces and websites other than the official Google Play site and installed onto smartphones. In addition to the measures taken by application distribution sites described in section B above, further consideration is necessary to build a framework that will enable users to identify application properties, including whether an application contains malware, how user information is handled, whether communications made by an application are encrypted, etc., so that information on such properties can be made available to the public.

It is also necessary to consider developing tools for analyzing and visualizing application properties.

D. Mitigating damage from malware that have entered user devices

It is important to examine measures for mitigating damage in the event of an information security breach based on the premise that no security measure is perfect.

(i) Dynamic access control by OSes [A, B, i, W]

When installing an application, if the user allows it an excessive access to OS resources, the sandbox model may become ineffective. If the application installed by the user contains any malware or vulnerability, he/she may be exposed to the risk of data leakage or access to his/her device. It is for this reason that the GPS and wireless LAN on/off function is equipped in smartphone devices. If users can change their OS settings so that they can more flexibly switch on and off each application's access to their address book data and other data stored in their device as well as the calling function, SD card, etc., they can mitigate damage that can arise from installing an application containing malware or other vulnerabilities.

Since it is difficult or inefficient for mobile device manufacturers to implement these measures, OS providers should consider incorporating them into their OS. In doing so, OS providers should take careful note of applications that are designed to access data or device.

(ii) Kernel security measures [A]

Information security measures for the OS kernel designed to enhance OS safety include minimizing authority in case of application takeover, minimizing OS functions (e.g. deleting unnecessary commands, etc.) in case administrative rights are taken over, detecting alterations and freezing functions in case system files are rewritten.

Two or more of these measures can be combined to enhance the robustness of the OS and mitigate damage in case one of the measures fails.

(3) Ensuring information security for communication channels [A, B, i, W]

Wireless LAN access point providers[32] should promote widespread use of wireless LAN access points that feature the specifications of WPA[33] and WPA2[34] with an eye to increasing the information security level of public wireless LAN services. They should also promote use of SSL[35] and VPN[36] to enhance information security.

Mobile device manufacturers can incorporate into their products a system that will enable a smartphone to identify the network it is connecting to and change the protection level depending on the reliability of the network. They should also continue to equip their products with a mechanism that will alert users and ask for their approval before they connect to an unprotected wireless LAN without knowing it.

(4) Protecting device data [A, B, i, W]

Users should always protect their mobile device by password in the event of loss or theft. The remote erase and self-destruct capabilities are also considered other ways to protect data stored in a mobile device if it's lost or stolen. We must note that the remote erase feature can be used only when the power to the device is turned on and it is connected to a network. Business operators should point this out to users when making them aware about information security, which will be detailed in Chapter 4.

[32] These include mobile phone operators if wireless LAN access points are set up for data offloading.

[33] WPA (Wi-Fi Protected Access) is a security protocol that improves on the original wireless security protocol, WEP (Wired Equivalent Privacy). It uses a more sophisticated data encryption method known as Temporal Key Integrity Protocol (TKIP) to cover the vulnerabilities of WEP. WPA also provides user authentication. Authentication methods include IEEE 802.1X, which involves the use of an authentication server, and Pre-Shared Key (PSK). WEP is not recommended for use today.

[34] WPA2 is a wireless LAN security protocol that features a stronger encryption method (CCMP; Counter-mode CBC-MAC Protocol) than WPA.

[35] SSL (Secure Socket Layer) is a protocol for securely transmitting information via the Internet by encrypting data. It is widely used for on-line shopping, web mail and other services that handle personal and/or confidential information.

[36] A VPN (Virtual Private Network) is an encrypted communication channel over a public network such as the Internet, which provides a network connection that is as secure as a dedicated network.

In order to prevent data leakage, mobile devices should incorporate a mechanism for encrypting data stored on a mobile device or an SD card so that the data will be unreadable should it be leaked.

(5) Measures related to impact of smartphones on external networks [A, B, i, W]

As described in Chapter 4, mobile phone operators should consider drawing on security awareness promotional activities to notify users of the risk of their smartphone being abused and utilized as a springboard for cyber-attacks.

Users should take necessary measures to prevent other devices from also being infected with malware just like they protect their own mobile devices. When using a smartphone for Wi-Fi tethering, users should employ the same kind of strong encryption method as used for wireless LAN routers, manage passwords appropriately, and take other precautions.

Section 3 Roles the Government Should Play

This section looks at the roles the government should play in solving the issues addressed in Section 2 of Chapter 2 for which solutions were not presented in the former Section.

(1) Following up on final report and promoting Industry-Government collaboration

The government should take the initiative to implement the types of awareness-raising measures described in Chapter 4 while relevant business operators should work with one another to implement those measures. The government should also encourage relevant business operators to take technological measures and work together to come up with solutions to the problems at hand.

The government should also use the venues provided by business organizations to share as much information as possible on the technological measures and initiatives aimed at raising public awareness with the private sector. The Secretariat should then examine the initiatives of both sectors on a semiannual basis and make its findings available to the public.

It is also necessary to look at how the government can assist business operators when their initiatives alone are not expected to deliver sufficient results over the long run.

(2) Ensuring safe and secure handling of user information

In January 2012, 'the Working Group on the User Information Sent through Smartphones under 'the Ministry of Internal Affairs and Communications' Study Group on Consumer Issues with ICT Services' started looking into how smartphone user information is handled as well as challenges to ensuring safe and secure handling of user information with an eye to delivering more user-friendly services. The Working Group published an interim report of their findings in April 2012 and will continue to examine the characteristics and classifications of user information as well as appropriate ways for business operators to obtain, manage and use that information.[37] The Working Group will use its findings to implement the exact measures needed.

(3) Coordination with initiatives aimed at visualizing application properties

The previous section discussed application distribution site operators' policies

[37] Specifically, the Working Group will look into how various business operators and other parties involved in smartphone services should handle user information and what kind of measures they should take in light of complying with privacy-related laws and regulations, protecting personal information, and responding to user concerns.

and initiatives related to posting applications as well as service providers' initiatives geared toward visualizing application properties needed to solve issues related to application installations. The government should not only engage in thorough research and investigations but also work with the private sector to implement measures that will dovetail with operators’ initiatives.

(4) Measures for ensuring information security for communication channels

Public wireless LANs have been made available by various service providers and their use is expected to increase for various purposes, including data offloading, business and community revitalization, emergency management, and more. The Study Group for Wireless LAN Business was established under the Ministry of Internal Affairs and Communications (MIC) in March 2012 to examine the current use of wireless LANs. The Study Group looks into issues as well as measures concerning the safe and secure use and promotion of wireless LANs. It also examines information security measures and ways to raise user awareness.

It is important that the MIC continue the research undertaken by the Study Group for Wireless LAN Business and take necessary action based on its findings. In light of changes in technological trends as well as increasing use of wireless LANs via smartphones and the use of smartphones for Wi-Fi tethering, the MIC should also work on revising its guidelines for “The Guide for Safe Use of Wireless LAN” by incorporating the Study Group's activities and findings.

(5) Promoting R&D and training

Smartphones are expected to face increasingly advanced and complex security threats. That's why the government should take the initiative to promote research and development of technologies needed to protect smartphone users. In order to appropriately address new threats, the government should also continue to examine ways to enhance human resources development with a focus on advanced information security skills on a medium- and long-term basis. That includes implementing training programs for smartphone-related business operators, information security service providers, and research organizations, etc.

(6) Promoting international collaboration and cooperation

Since business models for smartphone OSes and devices are not confined to a single country or region, there are a number of global smartphone models with universal specs that are available in the Japanese market. This means that smartphones throughout the globe share the same information security threats regardless of where they are used. Also, because smartphone applications and services are provided across national and regional boundaries, some of the information security problems associated with these services cannot be solved solely by efforts made in Japan.

Sharing information and opinions about specific threats, issues and countermeasures with other countries is essential, and such discussions should take place within an international framework. Rather than merely sharing knowledge of information security, it is crucially important that cooperation takes place within an international framework to solve known issues. Japan should address security threats and issues as a way to gain an influential voice in the global community, and make ongoing efforts to share information and opinions about countermeasures and solutions while gaining the support of nations across the world. Japan should leverage the functions of international standardization organizations to compile best practices of smartphone security measures based on their findings and the information it gets from overseas. It should also focus on international standards for protecting smartphone users depending on the situation.

The government should focus on not only on domestic initiatives but also on its role in the international arena and keep the lines of communication open for international coordination and information sharing through international conferences and bilateral talks.[38]

[38] Japan brought up security issues at the November 2011 Japan-ASEAN Information Security Policy Meeting. Opinion exchanges on smartphone security were initiated between Japan and the U.S. at an intergovernmental meeting held in January 2012.

Chapter 4 Publicity to Raise Awareness on Smartphone Information Security for General Users

Better awareness among users is also required to solve specific issues mentioned in Chapter 2 on information security of smartphones. To that end, we need to develop a good approach on 'what' to be educated to the users as well as 'how' to communicate with them. From that point, we will present the contents of such publicity under Section 1, and methodologies under Section 2.

Section 1 Contents of the Publicity for Awareness Improvement

As smartphones have certain level of flexibility to customize the software or function of the handset depending on the purpose of the users, ensuring safety just through the measures by service providers could become a challenge sometimes. Therefore it is necessary for users themselves to obtain relevant literacy to take proper measures on information security.

Although various organizations started offering publicity campaigns today, one should consider following matters, for example, to urgently improve the awareness across all users as part of the whole society and let each of them take measures against information security.

[Matters requiring awareness promotion/publicity]

(1) Nature of the smartphones

Smartphones have advanced information processing functions on top of the functionality of conventional mobile handsets, and rich customization options depending on the purpose of users. It is therefore important to take special care on information security measures for users themselves instead of just relying on the ones provided by the service operators, which has been the case for conventional mobile phones.

(2) Matters where users are encouraged to take measures

a. Updating the smartphone OS or applications could also solve vulnerability issue, in addition to modify/enhance the functions. Leaving vulnerability will increase the risk of malware infection and information leakage etc. Any relevant and available software patch or updated version should be installed without delay.

b. It is recommended for Android users to install anti-malware software to prevent the installation of any malware-inclusive applications, by mistake. It is also effective to utilize the screening services by mobile phone operators on information security for communications.

c. Malware-inclusive applications may be detected on application distribution sites without preliminary or sufficient screening. It is therefore recommended to use application distribution sites where certain level of safety examination is conducted by OS providers, mobile phone operators etc., when users get any applications. Upon installation, it is important to understand the contents about the function and subscriber information which is used by the application.

(3) Matters to promote the awareness among users

a. Users are required to recognize that the OS information security could be compromised through an attempt to remove limitations set by the OS provider by the target attack of the OS vulnerability ("Jailbreak") etc.

b. Wireless LAN may not have a mechanism for encryption or authentication, and not warrant the safe communications. It is therefore necessary to understand that any communications via Wireless LAN could be exposed to outside parties.

c. One should recognize the existence of ON/OFF function for the use of GPS in the configuration of devices. Turning OFF the use of GPS will ensure confidentiality of GPS information of the user against social networking services (SNS) or other applications, but also have a potential issue of not properly activating MDM for remote wipe etc. As a conclusion, it is necessary to correctly understand that above factors should be carefully considered when selecting any services or functions.

4. Other

As part of information security measures for the use of overall mobile handsets both smartphones and conventional cell phones, it is also recommended to take comprehensive approach for preventing any abuse by third parties upon loss/theft (such as handset lock, remote wipe, etc.), data backup, use of privacy filter etc., in addition to the measures mentioned in (1) through (3).

Regarding the protections from crank calls or spam mails, it is useful to implement the same countermeasures as the ones for conventional mobile phones[39].

Above matters may not apply to certain types of OS or devices. It is therefore desirable to identify the features of each of them and match the best solutions by

[39] For the information about web sites of mobile phone operators or countermeasures against spam mails, visit the site of Anti-Spam Consultation Center of Japan Data Communications Association (http://www.dekyo.or.jp/soudan/index.html) and other relevant sites as reference.

target audience or actual occasions before implementing awareness-raising publicity.

Based on that, the Interim Report has reflected the situation where smartphones are well penetrated among users in various age groups and has taken fundamental policy to focus on the specific/easy-to-understand tips for the compilation of the Appendix 2 - 'Three Recommended Actions for Smartphone Information Security'[40]- as the Study Group, citing minimum requirement for users on such measures. The Interim Report concluded that it is necessary to start publicity for users in a timely manner through cooperation among relevant parties.

Then, 'Smartphone Privacy Guide' has been compiled based on the discussions on minimum information required for users to protect their privacy as well as necessary countermeasures at the above mentioned 'Working Group on the User Information Sent through Smartphones'. In addition, update and revision is expected for the user guidelines 'For safe usage of wireless LANs' which is cited in Section 3 of Chapter 2.

From now on, it is necessary to promote clear and more effective publicity for the users through the cross-utilization of these outputs, that is, 'Three Recommended Actions for Smartphone Information Security' compiled by this Study Group, 'Smartphone Privacy Guide', and 'The Guide for Safe Use of Wireless LAN'.

[40] For the convenience of users' understanding, the word 'anti-malware software' in the 'Three Recommended Actions for Smartphone Information Security' is rephrased as 'anti-virus software' which is more commonly accepted by general public.

Section 2 Methodologies for Promoting Awareness

In order to promote users' awareness, effective implementation is important through mutual collaboration among the government, smartphone related business operators (mobile phone operators, mobile device manufacturers, application distribution site operators etc.) and service provider groups consisting of smartphone related companies, while leveraging their existing initiatives.

Listed below are necessary courses for each stakeholder, common issues across entities, and methodologies for follow-ups.

(1) Initiatives taken by mobile phone operators

Mobile phone operators have been involved in publicities for raising users' awareness on smartphone information security and countermeasures through the explanations of important steps upon contract, or distribution of relevant information through their web sites or their application distribution sites. Their publicities mainly focus on recommendations for using various information security services they provide under the partnership with information security provider etc.

Meanwhile, 'Study Group on Consumer Issues with ICT Services' under Ministry of Internal Affairs and Communications (MIC) has compiled a 'Proposal to Maintain and Improve Interests of Telecommunication Service End Users' (December 21, 2011). The proposal pointed out that the existence of the users who just believe smartphones are as safe as conventional mobile phones is partially attributable to insufficient explanations through advertisement or information disclosures, by mobile phone operators.

Based on that, following initiatives are considered to be useful, if taken by mobile phone operators.

a. Easy-to-understand explanations on the importance of information security measures

For the explanation upon contract, it is recommended to improve the way of communication, for example, to present the information not only about the possible malware infection as part of the exemption clause, but also educating the users to properly understand the threat on information security and necessity of countermeasures,.

b. Documentation of basic information security measures

The summary of basic information security measures to be implemented by the users should be added as part of handset user manuals through the cooperation with mobile device manufacturers or should be compiled as a start-up manual for beginners.

c. Request support from distributors.

They should ensure that users can get explanations on information security regardless of sales channels for the purchase of the product, by asking support for distributors.

(2) Initiatives for application distribution site operators

Currently, the biggest risk for smartphone information security is the installation of harmful applications. Therefore, below mentioned initiatives should be considered on the application distribution sites.

a. Posting advices on information security

Post information security related topics and create banners on the top page etc., for the users to easily find the information.

b. Information disclosure on web site operation policy etc.

As presented in Chapter 3, operators themselves should make effort to continue/improve their initiatives for eliminating any applications containing malware or vulnerability from their own sites. They should also make effort to disclose their web site operation policy and application posting policy for general users in easy manner. It is expected that this will create opportunities for users to assess the sites by accessing to the information on the operation policy of application distribution sites, and enrich their understanding on the importance of information security.

(3) Initiatives by the government

'Information Security 2011' (adopted at the Information Security Policy Council in July 2011) states, as the MIC and other relevant Ministries/Agencies' mission, that 'technical issues accompanying the widespread use of smartphones will be made known to the users … with differences from conventional mobile phones and PCs taken into consideration.'.

Regarding the 'Three Recommended Actions for Smartphone Information Security' and other contents compiled as part of the Interim Report of this Study Group, MIC has already implemented publicities for raising users' awareness through the government publicity activities, relevant web sites, or brochures etc.[41]. It

[41] Below are the major initiatives by the government for promoting users' awareness since the compilation of the Interim Report in December last year.

*Introduction of 'Three Recommended Actions for Smartphone Information Security' as part of the government Internet TV program with the topic of information security (Since February 2012) is important to accelerate the efforts even further, by utilizing media such as newspapers, magazines, and TV.

*Special articles about the features and safe use of smartphones in MIC's PR magazine (February and April in 2012)

*Expanding the importance of information security measures of smartphones by utilizing 'Three Recommended Actions for Smartphone Information Security' across the nationwide seminars/symposiums, mainly in the Information Security Month (since January 2012)

*Posting 'Three Recommended Actions for Smartphone Information Security' on the MIC's 'web site on Information Security for Citizens' (Since January 2012)

(4) Other General Matters

Educational material on smartphone information security is growing. But public awareness requires an environment in which users who want information on information security have ready access to it. At the same time, there also needs to be a means of calling attention to information that heightens awareness of information security among users who receive information on information security but have no interest in such information.

With respect to the former, government, businesses, and media outlets have become publicizing information, but efforts continue to be needed to provide accurate information on the status and risks of services.

With respect to the latter, as with other safe uses of ICT, it is considered important to provide information to the following groups: 1) school-age adolescents who are still developing ICT literacy, 2) adults in their early twenties who are beginning their lives as economically independent, autonomous consumers, and 3) senior citizens with little experience and knowledge using ICT.

Regarding the first group, seminars and study materials for building ICT lietarcy are already provided to schools and other educational organizations and PTA groups by private organizations, government, and mobile phone operators.[42] An effective approach would be to include smartphone information security measures as part of this content.

Regarding the second and third groups, it is important to strengthen coordination with consumer groups, which have deep experience dealing with actual consumer inquiries. With the young generation, an effective approach would be to learn from past examples while delivering information via media that are frequently used by young people (e.g. internet). Additionally, it is generally the case that many people, regardless of age, discuss their ICT usage with knowledgeable people around them. In local communities, another important initiative would be to foster human resources able to support the people around them with information.[43]

(5) Follow-Up with Concerned Parties

In the future, the targets, volume, and quality of smartphone information security information will continue to grow. Accordingly, it is recognized that periodic summary and review of such information and activities is an effective approach to ensuring the effectiveness of these initiatives. Through periodic publication of information on technological countermeasures and user awareness measures

[42] For instance, e-Net Caravan (MIC/MEXT), regional symposiums by the Anshin Nettozukuri Initiative, Internet Security Class (METI), Mobile Phone Security Class (NTT Docomo), KDDI Mobile Phone Class (KDDI), "Think About Your Mobile: Lesson Programs in Information Morals" (Softbank Mobile), etc.

[43] SPREAD (Security Promotion Realizing sEcurity meAsures Distribution), a council to promote security, is an example of one organization engaged in such activities.

taken by concerned parties, it can be expected that their public awareness initiatives will be more effective and sustainable.

Chapter 5 Information Security When Using Smartphones to Access the Cloud

This chapter looks at the relationship between smartphones and cloud services from two perspectives. It examines risks, issues, and countermeasures regarding the protection of cloud data when using smartphones to access the cloud (Sections 2-4), as well as methods of using the cloud as one facet of smartphone data security (Section 5).

Section 1 Affinity between Smartphones and Cloud Services

The use of cloud services has grown in tandem with the rapid popularization of smartphones. In addition to hosting services used by corporations to outsource their data resources, cloud services that offer technology for virtualization and utilization of advanced resources has emerged, as well as cloud services for individual consumers ("personal cloud"). As this suggests, the market continues to grow.[44]

Although smartphones have less storage capacity as devices than PCs, they make it possible for users on the go to access the internet by through various channels. As a result, there is a strong tendency to use data that is stored in the cloud (figure 10). At present, there is a growing trend toward accessing the cloud from smartphones using web applications.

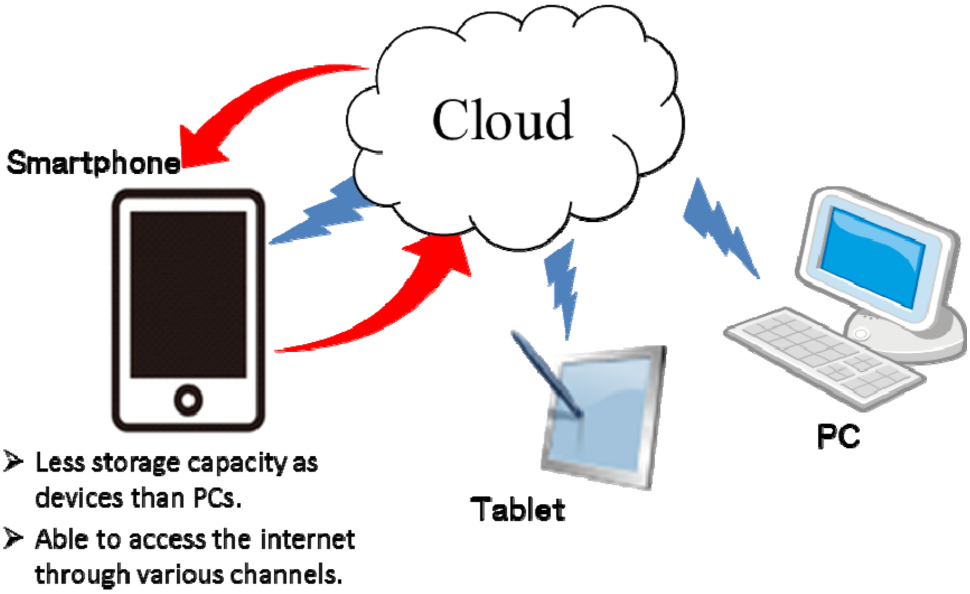

Cloud
Smartphone
PC
Tablet
➢ Less storage capacity as devices than PCs.
➢ Able to access the internet through various channels.

Figure 10 High affinity between smartphones and cloud services

[44] According to an October 2011 survey by ICT Research & Consulting (http://www.ictr.co.jp/topics_20111004.html), the number of personal cloud users in Japan at the end of 2010 was 14.72 million. The company also finds that the total number of users in 2011 grew by 33% to 19.65 million, and forecasts that the number of users will grow to 56.01 million by 2015, or 3.8 times the number in 2010.

Section 2 Risks When Accessing the Cloud via Smartphone

The risks, issues, and countermeasures regarding cloud service information security have been discussed in numerous venues.[45] From the perspective of corporate users, putting corporate-managed data resources under the management of an outside cloud service entails risks, including loss of governance (e.g. when security cannot be verified because a cloud operator's system configuration may be a black box), compliance violations (e.g. when a cloud service operator cannot be adequately supervised), sudden service termination, incomplete data removal when a service is terminated, or data stored at sites overseas.

From the perspective of individual users, as the level of information security depends on each cloud operator, the principal risk is that information in data stored in the cloud might be leaked or loss when, for instance, a cloud operator has not taken adequate security measures. There is also the risk that data stored in the cloud cannot be accessed when the network or servers are down. Additional factors that increase the risk of using the cloud, especially from smartphones, include:

(1) Storage of user information

In comparison with cloud services for business use or PCs, data that is stored in the cloud via smartphone includes a wide range of user information.

(2) Links between data stored via various devices

One of the benefits of using cloud services is the central access that users have to data stored via PC or various other devices. At the same time, in comparison to a PC, there is greater risk of a smartphone being lost or stolen; if a lost device were used to gain unauthorized access to a person's data in the cloud, all of that person's information could potentially get leaked, including data stored using their PC or other device.

Section 3 Issues Regarding Smartphone Use of Cloud Services

This section touches on the threats in the previous section while surveying anticipated future issues regarding smartphone use of cloud services.

(1) Unconscious use of cloud services

Some smartphone applications have interfaces that utilize the cloud in a way that

[45] In Japan, guidelines have been drafted by MIC, METI, ASPIC (ASP-SaaS-Cloud Consortium), IPA (Information-technology Promotion Agency), and others, and guidelines from NIST and ENISA (European Network and Information Security Agency) are often consulted. Discussion has also been advanced by ITU and other international associations.

leaves users unaware they are doing so; it is conceivable, therefore, that users may store data in the cloud unconsciously. In such cases, even users who are generally aware of the risks of leaked or damaging information are not given the option of not storing their highly confidential information in the cloud, making it difficult to make such a decision.

(2) Applications that use the cloud without adequate information security measures

With the growing market for cloud services, there are now services that provide varying levels of pricing, service quality, and information security. When a cloud lacks adequate security measures, there is a risk of leaked or damaging information. For that reason, a cloud operator's level of security is important; yet at present, it is often difficult for users, application distribution site operators, or even an application's developer to know the security level of the cloud operator used by the application.

(3) Protection of cloud data

Effective countermeasures to cloud operator information leaks include not only technological measures--for instance, vulnerability testing of the cloud server and web applications that run on it, logging of unauthorized access to the cloud server, and data encryption--but also compliance measures on the part of the cloud operator.

In the case of vulnerabilities in web applications, it is also necessary to have measures for parties that borrow the cloud server from the cloud operator to develop web applications; this is why measures that only take the cloud operator into consideration are insufficient.

With respect to the encryption of data stored in the cloud, which technology has already been implemented, there are many cases in which encrypted data must be decrypted in the cloud for data processing, which means cloud operators of such services will have access to the contents of the data.

(4) Authentication when using cloud services

Authentication methods for access to the cloud might use smartphone device authentication or, for greater convenience, might cache authentication data (e.g. user IDs and passwords) on the smartphone device. From the perspective of user convenience, none of these methods should be simply rejected. At the same time, however, if a device is lost, stolen, or infected with a malicious bot and comes under the control of another party that can easily get past authentication to access the cloud, then the smartphone might potentially be misused by that party as a means of accessing the cloud or impersonating its user.

Section 4 Countermeasures When Accessing the Cloud via Smartphone

This section presents countermeasures for issues identified in the previous section.

(1) Measures to prevent unconscious use of cloud services

An effective means of enabling smartphone users to avoid storing data in the cloud unconsciously is to show an application's features regarding the application's use, or non-use, of the cloud at the time the application is chosen on the application distribution sites.

(2) Measures to address applications that use the cloud without adequate information security measures

At present, there are no common standards for third-party evaluation of cloud operator security. Rather, due to the rapid pace of development of these services, parties to the agreement are left to examine the operator's terms of service and make decisions for themselves.

In order for an application to avoid use of a cloud with inadequate information security measures, the foremost important thing is for the application's developer to select a cloud operator with highly secure services when designing the application. Next, to further increase security for users, the application distribution site operator should not only collect reported information from the application developer regarding the cloud which the application uses, but also combine it with information regarding cloud operator security distributed by cloud-related industry groups. Doing so is an effective means of enabling users to make an overall judgment of an application's security, including its use of the cloud.

Finally, as part of the efforts by business groups discussed in Chapter 3 regarding the transparency of application features, if exactly what data each application sends to the cloud is made clear, then by combining that information with information on the cloud that the application uses, along with information on the security of the cloud operator, it becomes possible to make an overall evaluation of the application.

(3) Measures to protect cloud data

With respect to web application vulnerabilities, if an application's reviewers likewise review and indicate the security of web applications used by the application, this would provide users with useful information. Unfortunately though, as others have noted, there are practical challenges to adding such a review of web applications and the cloud to the evaluation of an application given that the criteria and cost of evaluating just the application still raise numerous issues. This is why it is best to consider it within the overall context of the efforts discussed in Chapter 3 regarding the transparency of application features.

To overcome the issue of cloud operators gaining access to data because encryptions are often decrypted in the cloud, element technology exists that makes it possible to process some cloud data without decrypting it. The application of such element technology would do away with the decryption process, making it possible to eliminate the risk of information being leaked from decrypted data. However, because there are limits on the operations and speed that such element technology can perform, it cannot be said that it provides a ready countermeasure for accessing the cloud using a smartphone. In the future, it is important that encryption-related element technology make further advances and that technology be developed to support its application.

(4) Authentication when using cloud services

To avoid unauthorized use by third parties when a smartphone uses device authentication or caches authentication data, it is necessary for users to have greater awareness and take preventive measures in the event their device is stolen or lost (e.g. locking the device, etc.). It is also important to consider implementing two-factor authentication, as well as authentication methods specifically for smartphones that would enable secure access.

Section 5 Using the Cloud to Maintain Smartphone Information Security

This section considers smartphone information security from a different perspective than the previous section by considering ways that the cloud itself can be used as one facet of smartphone information security.

(1) Storing data in the cloud

From the perspective of reducing the risk of leaked information when a smartphone device has been lost or stolen, one measure sometimes taken is the ability to delete data using a remote data-deletion feature or the like, though it requires regular backups on one's data.

Others have also noted that the risk of data being leaked or lost can be reduced by deliberately storing all data in the cloud, rather than on the device itself or an internal SD card.

In the latter case, however, there are additional issues--from anxiety about utilizing the cloud without an awareness of where the data is stored, to service interruptions in areas with poor communication infrastructure, increased bandwidth demands as a result of increased data traffic, and the risk of data being leaked from the cloud--that make it important to compare and weigh each option before choosing one or the other. When using such cloud-based storage services, it is also important for users to make decisions based on their own assessment of a cloud's security based on the cloud-operator agreement, and to consider the nature of their data to decide what data to store in the cloud.

(2) Smartphone devices as thin clients

Current smartphones normally run their OSes and applications on the device. In the future, however, services are envisioned that will provide functions comparable to the OS and applications with utilizing the function of PaaS and SaaS and run them in the cloud. With the device used as a means of displaying the results from the cloud, the risk of data being leaked from the device will be drastically reduced.

Under such a service model, OS and application updates, as well as security patches, will be implemented by the cloud service operator, making it possible for users to use an OS that ensures the latest in information security.

By the same token, such a service model inevitably raises issues of cloud use, making it necessary to examine the effectiveness and issues of adopting such a method.

Lastly, because the use of the cloud for smartphone information security purposes has only just begun, there is the potential for various complications to arise in the future. That being the case, not only should ongoing efforts be made to properly understand data collection and its risks and issues, but effective use of collaborations between government, industry, and academia, as well as international entities, should also be made to investigate strategic measures.

Chapter 6 "Smartphone Information Security Action Plan"

This chapter builds on the countermeasures presented in previous chapters to offer an action plan of priority items that should currently be implemented. Moreover, the flexibility to review the current action plan as needed should be incorporated into the plan by building on the conditions of follow-up under (6).

(1) Review of trade association countermeasures

Within the framework of information security-related trade associations, a collaborative initiative between business operators should be launched within the year 2011 to understand OS vulnerabilities and review strategic countermeasures.

(2) Research and development from the perspective of user protection technology

Within the year 2011, the National Institute of Information and Communications Technology should leverage its general research and development efforts in the area of information security, including encryption technology and mobile environments, to undertake research and development on smartphone information security regarding methods of securely storing smartphone user information in the cloud as well as information security countermeasures, and methods of evaluating information security, with respect to data and device access by smartphone applications.

(3) Creating a framework for transparency in application properties

Within the fiscal year 2011, the Ministry of Internal Affairs and Communications will undertake necessary field research and offer findings on creating a trade association framework for presenting users with easily understandable information on application properties, such as whether or not they include malware, what methods of collecting user information they use, and whether or not they encrypt data over communication channels when transmitting data externally. MIC will also support widespread adoption of the trade association-structured framework.

(4) Promoting international collaboration and cooperation

MIC will coordinate with NISC and related ministries and agencies to promote continued exchanges of information and opinion on threats, issues, and countermeasures through international and bilateral meetings, and to foster international cooperation considering the possibilities of creating international standards with respect to user protections.

(5) Raising overall public awareness among smartphone users

To provide users comprehensively with necessary information on smartphone information security as well as on measures pertaining to user information, MIC will swiftly initiate a "Promotion Program for Safe and Secure Use of Smartphones" to promote sustained cooperation between concerned businesses, trade associations, and others. It will also undertake reviews of the program's content as necessary as the initiative progresses and circumstances evolve.

(6) Periodic follow-up to this final report

With respect to the technological measures and user education outlined in this final report, the Secretariat will survey the initiatives undertaken by concerned businesses, government, and others and publish the results of its findings approximately once every six months. Because the smartphone environment is evolving daily, it will concurrently also coordinate with industry, academia, and government to collect and share information to ensure the ongoing investigation of countermeasures.

Postscript

This Study Group extracted and sorted information security issues when using smartphones and accessing the cloud via smartphones since October 2011 and discussed measures for solving the issues for business operators and the government and put together a final report using the results.

In order to follow up the final report with regard to technical measures and user awareness hereafter, the Secretariat will research relevant business operators' and the government's efforts once every six months and publish the results. The follow-ups will encourage business operators to enforce full measures and provide an opportunity to inspect their efforts.

We hope this final report will be utilized for information security measures of relevant business operators and application developers and provide thorough awareness to users so that the sound development of smartphones and the cloud will be achieved.

Reference

"Study Group on Information Security Issues of Smartphone and Cloud Computing" Member list

(Titles omitted and in Japanese alphabetical order)

Hiroyasu ASAMI	Managing Director of Smart Communication Services Department, NTT DOCOMO, INC.
Yoshiaki UCHIDA	Executive Director General Manager, Operations Division, KDDI CORPORATION
Masami OHBATAKE	Executive Officer, Group General Manager Communication Systems Group, Sharp Corporation
Hisamichi OKAMURA	Visiting Professor, National Institute of Informatics Attorney
Mamoru SAITO	Manager, Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, Internet Initiative Japan Inc.
Kazue SAKO	Innovation Producer, Central Research Laboratories, NEC Corporation
Tetsuo SHIOZAKI	Chief Architect, Cloud Business Support Unit, Fujitsu Limited
Hidemune SUGAHARA	Senior Vice President, Applications and Content, NTT Communications Corporation
Shuji SENOO	Senior Director of Solutions Operations, Security & Smart ID Solution Division, Hitachi, Ltd..
Masaki TAKEUCHI	Head of Software Tokyo Development, Sony Ericsson Mobile Communications, Japan Inc. [up to 6th meeting]
Hisashi TAMAI	Head of Product Software, Software Tokyo Development, Sony Mobile Communications, Japan Inc. [from 7th meeting]
Hironobu TAMBA	Division Head, Product & Service Division, SOFTBANK MOBILE Corp.
Koji NAKAO	Distinguished Researcher, Network Security Research Institute, National Institute of Information and Communications Technology
Itsuro NISHIMOTO	Director and CTO, LAC Co., Ltd.
Eiji HAGIWARA	Managing Director, Member of the Board, Panasonic Mobile Communications Co., Ltd.
Nobuo MIWA	Advisor of Chief Information Officer, Ministry of Internal Affairs and Communications
Suguru YAMAGUCHI	Professor, Nara Institute of Science and Technology [Chairman]

(Observer)

Reiko KONDO	Counselor for International Strategy, National Information Security Center (NISC), Cabinet Secretariat [from 3rd meeting]
Junichi EGUCHI	Director, Office of IT Security Policy, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry [from 6th meeting]
Masahiro UEMURA	Director, Office of IT Security Policy, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry [from 7th meeting]
Hisashi SEKINE	Director, Digital Consumer Electronics Strategy Office, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry [from 8th meeting]
Yasushi SUMITANI	Director, Digital Consumer Electronics Strategy Office, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry [from 9th meeting]

(Secretariat)

Kenji SATO	Director, ICT Security Office, Information and Communications Bureau, Ministry of Internal Affairs and Communications
Junji NAKATANI	Deputy Director, ICT Security Office, Information and Communications Bureau, Ministry of Internal Affairs and Communications
Tomoko MAKINO	Assistant Director, ICT Security Office, Information and Communications Bureau, Ministry of Internal Affairs and Communications
Kensaku KAGECHI	Researcher, ICT Security Office, Information and Communications Bureau, Ministry of Internal Affairs and Communications

Discussion Overview

1st Meeting (October 19, 2011)

- Outlined current status of information security measures relating to smartphones taken by each company
- Identified issues relating to information security of smartphones

2nd Meeting (November 4, 2011)

- A hearing of activities of Japan Smartphone Security Forum (JSSEC)
- Outlined discussion issues relating to information security of smartphones
- Discussed user awareness measures regarding information security measures for smartphone users

3rd Meeting (November 29, 2011)

- Main examples of inquiries relating to smartphone information security received by the Consumer Affairs Center
- Outlined discussion issues relating to information security of smartphones
- Discussion on an essential part of an interim report (draft)

4th Meeting (December 19, 2011)

- Compiled and discussed the interim report (draft)

5th Meeting (February 1, 2012)

- Checked statuses of measures taken by business operators
- Identified issues and measures including use and utilization of the cloud computing

6th Meeting (March 9, 2012)

- A hearing of opnions from OS providers
- Outlined issues and measures for the final report

7th Meeting (April 3, 2012)

- Discussion on public comment plan of the final report

8th Meeting (April 26, 2012)

- Compiled and discussed the public comment plan of the final report

9th Meeting (June 29, 2012)

- Compiled the final report

Smartphone Information Security List for Business Operators

In the Appendix 1, business operators' measures presented in Section 2 of Chapter 3 are listed and current possible main organizations to implement these measures are shown. The main organizations are not limited to this list and measures should be taken flexibly as situations change. Furthermore, business owners may be categorized into multiple main organizations depending on their business categories.

Countermeasure items	Mobile Phone Operators	Mobile device manufacturers	Business Groups	Application Distribution Site Operators	OS Provider	Information security services	Content of Countermeasures
(1) Measures relating to OSes							
A. Solutions for vulnerabilities in OSes, and the release of security patches [A, W]	Yes	Yes					- Apply security patches published by OS providers to user terminals as soon as possible.
B. Detection and sharing of information relating to vulnerabilities in the OSes [A, B, i, W]			Yes		Yes		Identify OS vulnerability information and damage situation caused by the vulnerability with cooperation and discuss countermeasures. However, pay attention to an extent of sharing the information.
		Yes	Yes		Yes	Yes	Develop inspection tool to detect vulnerabilities in early stage.
C. Measures relating to the support period for OSes [A, B, i, W]					Yes		Make an announcement when terminating support.
D Measures relating to the channels for providing support for OSes [A, B, W]	Yes						Remind users that they cannot receive OS support after canceling a contract with mobile phone operators.

Appendix 1

Countermeasure items	Mobile Phone Operators	mobile device manufacturers	Business Groups	Application Distribution Site Operators	OS Provider	Information security services	Content of Countermeasures
(2) Measures relating to applications							
A. Measures for minimizing the creation of applications that contain malware or vulnerabilities [A, B, i, W]			Yes		Yes		Continuously inspect and review contents of a secure programming guide and sample code and publish a latest guide on media that attracts developers' attention.
		Yes		Yes	Yes		Provide information through website and seminars for developers from the viewpoint of securing information security.
B. Measures relating to the circulation of applications that contain malware or vulnerabilities [A, B, i, W]				Yes			Continue and improve measures for removing applications that include malware and vulnerabilities.
				Yes			Provide information regarding website operation policy and application posting policy to users.
				Yes			Standardize minimum standards of application posting policy.
C. Measures to Prevent the Installation of Applications Containing Malware or Vulnerabilities							
(i) Anti-malware Software [A, B]	Yes	Yes				Yes	Install anti-malware software and improve functions.
		Yes				Yes	Develop a device that grants anti-malware software for privileged access to the OS. However, careful considerations are required.
		Yes					Enhance information security measures for the OS kernel when developing devices and use them with conventional anti-malware software.
(ii) Mobile Device Management (MDM) [A, B, i, W]	Yes				Yes	Yes	Use mobile device management such as configuring devices, managing software versions, and limiting installations of applications comprehensively.
(iii) Visualization Framework for Application Properties [A]			Yes				Build a framework that enables users to identify application properties such as existence of malware, how user information is handled, and whether communications made by an application are encrypted.
			Yes	Yes		Yes	Develop an application analysis tool.

Countermeasure items	Mobile Phone Operators	Mobile device manufacturers	Business Groups	Application Distribution Site Operators	OS Provider	Information security services	Content of Countermeasures
D. Mitigating Damage from Malware that Have Entered User Devices							
(i) Dynamic Access Control for OSes [A, B, i, W]					Yes		A function that flexibly enables or disables accesses to address book data and data that is stored in devices as well as the calling function and SD card, etc. in the OS settings.
(ii) Kernel Security Measures [A]		Yes					Minimization of authentication provided to applications, minimization of OS functions (removal of unnecessary commands, etc.), detection of alterations, and freezing functions.
(3)Ensuring Information Security for Communication Channels [A, B, i, W]	Yes						Promote access points of wireless LAN that uses highly secure encryption technology and authentication method.
		Yes					Install a mechanism that enables smartphones to identify the network that devices are connected to and changes the protection level depending on the reliability of the network to devices.
		Yes			Yes		A mechanism that will alert users and ask for their approval when connecting to a wireless LAN.
(4) Protecting Device Data [A, B, i, W]	Yes	Yes	Yes	Yes		Yes	Explain users regarding preventative measures in the event of loss or theft of their devices when business operators educate users.
		Yes					Install a mechanism that encrypts data inside devices and SD cards and protects encrypted data from being read when it is leaked.
(5) Measures Related to Impact of Smartphones on External Networks [A, B, i, W]	Yes	Yes	Yes	Yes		Yes	Explain users about the risk that their smartphones might be abused as a springboard of cyber-attacks when business operators educate the users.

Appendix 2

Three Recommended Actions for Smartphone Information Security

(Minimum information security measures to be taken by users)

Smartphones are handy mobile phones that can add various functions by installing applications freely. On the other hand, due to this very advantage, there exist some dangerous applications. It is necessary that users take information security measures by themselves.

First, it is important to take measures similar to conventional mobile phones, such as the measures for preventing any abuse by third parties in the event of loss or theft. Furthermore, the following three preventative measures are important when using a smartphone.

1 Update the OS

Smartphones require OS updates. Using older OS will increase a risk of virus infection. Install updates when you receive a notification of updates.

2 Check whether your smartphone needs anti-virus software

Applications with virus have been discovered. Mobile operators and other related operators provide anti-virus software for each smartphone model. Consult with these operators for using anti-virus software.

3 Download applications with caution

There have been cases where applications containing virus are found at application distribution websites that do not fully screen applications. Use application distribution websites where OS providers and mobile phone operators conduct safety examination. Pay attention to functions and terms of use when installing applications.