

# **Security Guideline for using Smartphones and Tablets**

**- Advantages for work style innovation -**

**[Version 1]**

**December 1, 2011**

**Japan Smartphone Security Forum (JSSEC)  
Smartphone Utilization Committee Guideline Working Group**

■Drafted by

Smartphone Utilization Committee Guideline Working Group Task force

Leader	Ayako Matsushita	(Alps System Integration Co., Ltd.)
Members	Hiroaki Aihara	(Netmarks Inc.)
	Natsuki Asai	(ITC Networks Corporation)
	Shinichiro Kataoka	(Toppan Printing Co., Ltd.)
	Yuji Kitamura	(Cybertrust Japan Co., Ltd.)
	Etsuo Goto	(Toyota Motor Corporation)
	Ryohei Takahashi	(NTT Communications Corporation)
	Toshio Nishihara	(Cisco Systems G.K.)
	Toshio Makino	(NextGen, Inc.)
Shogo Matsumoto	(Infosec Corporation)	

(Listed in the order of the Japanese syllabary.)

■Editor

Mitsuhiko Maruyama (Deloitte Tohmatsu Risk Services Co., Ltd.)

■Published by

Japan Smartphone Security Forum (JSSEC)  
Keiichiro Kyoma, Director, Smartphone Utilization Committee (Hitachi Systems, Ltd.)

- ※ Neither JSSEC nor the editors extend any sort of guarantee, warranty, liability and/or compensation arising from direct, indirect or consequential damages in using any or the whole part of the Guideline. The Guideline may be used at your own risks.
- ※ The product and service names in the Guideline are the trademarks or registered trademarks of their respective companies.
- ※ In your reference to the Guideline for internal company documents etc., observe the Copyright laws. Specify the sources in such references.
- ※ The English version of this data is for use in Japan. Priority is given to the Japanese version.
- ※ In this document, "Smartphones" represents the general description of Smartphone.

# Table of contents

<b>1. Introduction</b>	<b>3</b>
1.1. Guideline Usage	3
1.2. Objectives of the Guideline	3
1.3. Target Readers of the Guideline	3
1.4. Scope of the Guideline	3
1.5. Structure of the Guideline	4
<b>2. Advantages in Using and Utilizing Smartphones</b>	<b>5</b>
2.1. Aims and Reasons for using Smartphones	5
2.2. Examples for the Utilization and its Effects	5
2.3. Circumstances Surrounding Smartphones	5
<b>3. Mechanism and Overview of Smartphone</b>	<b>7</b>
3.1. Characteristics of Devices and Types of OS	7
3.2. Applications and Procurement	7
3.3. Communication styles and Networks	8
3.4. Differences from Existing PC Security	8
<b>4. Characteristics and Considerations of Smartphones</b>	<b>9</b>
4.1. Characteristics	9
4.2. Threats and Countermeasures from the Characteristic Perspectives	9
4.3. Future considerations	10
<b>5. Threats and Countermeasures from Use Case Perspectives</b>	<b>11</b>
5.1. Phone address book Usage	11
5.2. Phone Usage	11
5.3. E-Mail Usage	12
5.4. Schedule Usage	12
5.5. Browser Usage	13
5.6. Connect with Network	14
5.7. Corporate Network Usage	14
5.8. SaaS/ASP services subscribed by an organization Usage	15
5.9. Application Usage	16
5.10. Device functionalities Usage	17
5.10.1. Camera Usage	17
5.10.2. Microphone Usage	17
5.10.3. Location Information Usage	18
5.10.4. NFC Usage	18
5.10.5. 1seg, a terrestrial TV broadcasting programs on mobile phones Usage	19
5.10.6. Bluetooth Usage	19
5.10.7. Infrared Communications Usage	19
5.11. Media Data Usage	20
5.12. Backup/Synchronize	20
5.13. 【Reference】 Internet Storage Service Usage	20
5.14. 【Reference】 SNS Usage	21
<b>6. Consideration on Lifecycles</b>	<b>22</b>

6.1.	Plan.....	22
6.1.1.	Set Out an Internal Rule .....	22
6.1.2.	Set out a User Manual .....	22
6.1.3.	Prepare a Support System .....	22
6.2.	Introducing Smartphones .....	22
6.2.1.	Start-using Procedures.....	22
6.2.2.	Procure or Place Attachments.....	23
6.2.3.	Acquire User Account .....	23
6.2.4.	Initial Setting of a Device .....	23
6.2.5.	Activate a Device Lock Functionality .....	23
6.2.6.	Acquiring E-Mail Accounts .....	23
6.2.7.	Introduce an Application.....	23
6.2.8.	Trainings Implementation .....	23
6.2.9.	Distribute Devices .....	24
6.3.	Operation.....	24
6.3.1.	Acquire and Monitor Device Information.....	24
6.3.2.	Control Device Functionalities.....	24
6.3.3.	Manage OS versions .....	24
6.4.	Discarding .....	24
<b>7.</b>	<b>Conclusion.....</b>	<b>25</b>
7.1.	Balance between the Purposes of Use and Security.....	25
7.2.	Security Policy of an Organization and Decision Making.....	25
7.3.	Necessity for Continuous Data Acquisition.....	25
<b>8.</b>	<b>Glossary .....</b>	<b>26</b>
<b>Appendix A</b>	<b>.....</b>	<b>27</b>
A-1	Check Sheet for Countermeasures per Characteristics .....	27
A-2	Check Sheet for Countermeasures per Case Usage.....	27
A-3	Example of Items Described in a Procedure.....	31
A-4	An Example for Items to be Listed on Pledge .....	32
A-4-1	Corporate Owned Version .....	32
A-4-2	BYOD Version.....	33

# 1. Introduction

## 1.1. Guideline Usage

Smartphones are mobile devices that equip advanced information processing functionalities in addition to the services offered by conventional mobile phones. In addition to voice communications, rich communication functionalities for example, data communications and wireless LAN (Hereinafter "Wi-Fi") are supported. There are also mobile devices called tablets which support almost equal functionalities as smartphones but have larger screen sizes.

In this Guideline, we define "smartphones" to cover both smartphones and tablets.

The Guideline is version 1.0 as of December 1st 2011, and is subject to further changes.

## 1.2. Objectives of the Guideline

Presently, the number of businesses that actively utilize IT for work style innovations is increasing. Smartphones trigger an attention as key IT devices in the initiative.

Even in businesses where organizational initiatives utilizing IT for work style innovations have not been promoted, the individual users have already started using smartphones in various business situations.

Smartphones however are still technically in a developing stage, the information is not readily available for companies that plan to introduce them for their business uses, and there are number of issues that require to be resolved before using them in full-scale for business.

The Guideline is intended mainly to identify the security threats and countermeasures that businesses and organizations need to observe in using smartphones as an essential element to help improve the labor productivity and innovate the work styles in Japan, and to contribute to facilitate the environment for securely and safely using smart phones at the workplace.

## 1.3. Target Readers of the Guideline

The Guideline is mainly targeting the following readers.

- (1) The managers and planning persons who are responsible for introducing smartphones to their companies or organizations.
- (2) The managers and individuals who are responsible for setting out security policies for introducing smartphones to their companies or organizations.
- (3) The managers and planning persons who are responsible for the work style innovations at their companies or the organization.

## 1.4. Scope of the Guideline

The scope of the Guideline is defined in terms of the ownership and the utilization purposes of smartphones.

The scope is not only limited to the business usage of the smartphones owned and supplied by companies but also to the business users bring their own smartphones (BYOD :Bring Your Own Device) and the multi-purpose users for business and private.

In the information security sphere, the classifications in order of importance is now becoming commonly used, but a threat analysis of the smartphone characteristics was applied in this Guideline for a better understanding of usage cases.

Table 1 The Scope of the Guideline

Purpose \ Ownership	For business use only	For business and private use	For private use only
Company owned	○	○	Out of Scope
Privately owned	Out of Scope	○ (BYOD)	Out of Scope

□ "Out of Scope" items are not handled in the Guideline.

## **1.5. Structure of the Guideline**

In Chapters 2, 3 and 4 that constitute the first half of the Guideline, the advantages, functionality, and characteristics of smartphones are described for your better understanding of the smartphone features.

In Chapters 5 and 6 that constitute the latter half of the Guideline, the security issues of smartphones are described in terms of "usage scenarios" and "device life cycles" to alert the managers of the threats and their countermeasures.

"Threats and Countermeasures" of each Chapter focus on differences between smartphones and PCs and encompass issues irrespective of occurrence frequencies, with multilateral possibilities in mind. It does not mean therefore that all of the described measures need to be addressed, but with the awareness of those threats, the measures may rather be selectively used in accordance with the purposes of actual smartphone uses. In the Table, corporate owned cases and privately owned cases are commonly described. The lines stipulated as "BYOD" however are specific to the cases for smartphones that are privately owned.

The Appendix is the summary of the threats and countermeasures in the Chapter 4 and 5. "The check sheet for countermeasures per property/usage scenario" can be used for studying required security measures. "The example of the items described in procedure manuals" and "the example of items described in pledge (Corporate owned version and BYOD version)" can be used in producing a procedure manual and/or pledge, as may be necessary.

## 2. Advantages in Using and Utilizing Smartphones

In this chapter, the advantages in using and utilizing smartphones are presented.

Smartphones in comparison to other devices have the outstanding features as communication tools for example superior portability, always-on power and always-on connection. They also have higher scalability in their functionalities and are easy to be personalized, with the additions of applications by users at their preferences.

### 2.1. Aims and Reasons for using Smartphones

Smartphones are now more frequently used in viewing websites, e-mails and schedules when outside offices. Such usage scenarios can also be achieved by note book PCs that are connected with the network. In consideration of the convenience and the agility however, smartphones yields overwhelming advantages.

Therefore, increasing number of organizations have been trying to use smartphones for achieving various objectives for work style innovations for example, "active communications", "faster decision making", "cost reduction" and, "productivity improvement", and other factors for example, "business continuity" and "customer satisfaction improvement" etc.

### 2.2. Examples for the Utilization and its Effects

The examples for typical work style innovations are shown below:

#### □ Activate communications and streamline businesses

In addition to the more timely communications that could be achieved if e-mails can be responded easily at outside of offices or during waiting time, also big improvements would be expected in our business efficiencies by using idle time. Thereby, the time that is required in responding e-mails after returning to the office would be substantially reduced. If we could reduce the time at offices by 1 hour per day for example, about 20 hours (Supposing for 20 business days) will be saved per person per month. With 500 employees for example, business efficiencies 10,000 hours (1,250 business days) will be achieved.

#### □ Faster decision making

Corporate managers, who stay out of their offices for a business trip etc., have piled up tasks for decision making for their organizations and for their daily issues. With the use of smartphones, important subjects could be naturally checked with the voice and e-mail functions, but moreover, corporate decision making would become expedited and those managers' time for the duty would be reduced if they connect with corporate networks securely "at anytime and anywhere" and may electronically provide necessary approvals.

#### □ Reduce cost and enhance business efficiency in achieving "the paperless office"

The aim at cost reduction and business efficiency with a paperless office is an ongoing trend.

At businesses or other organizations, hardcopies tend to be produced for instruction manuals and brochures. When those copies need to be revised frequently, a large burden is imposed to the organizations, in terms of the workload and cost. People need to carry hardcopies to distribute, and rush to search applicable copies in need. These issues can be substantially resolved digitizing paper documents and using smartphones and tablets for viewing and searching media.

#### □ Efficient transfer when going out for a visit

In order to enhance the convenience in going out for a visit, use of maps and location information should be useful and effective. There is no need to search destinations and print out information beforehand.

### 2.3. Circumstances Surrounding Smartphones

Smartphones attracted attention as the tools to meet the following social needs:

#### □ Deal with natural disasters and support work-at-home

There is a trend in organizations trying to seek for business continuity during a natural disaster, to assume social responsibilities for example, reducing power consumption, and to promote work-at-home. The smartphones are expected to work as an effective tool in innovating a work style and improving the balance between the business and private lives of employees.

#### □ Affinity with Cloud services

Since Cloud services help reduce idle IT assets in organizations thereby letting them off the balance-sheet, efficient

business management can be achieved, while providing the environment to reach necessary IT resources "at anywhere at any time". In order to fully exploit the Cloud services, smartphone uses in combination with them are growing.

□ Utilize privately owned smartphones

The ownership style of smartphones themselves has changed remarkably. Organizations have now started authorizing users of privately owned smartphones to use their phones at work (BYOD). Various reasons behind this can be assumed for example reducing and streamlining expenses, dealing with emergencies and alleviating cost burdens for owning 2 phones, etc. The new trend can be considered as noteworthy.

The environments surrounding organizations in response to the globalization and the increasing intelligence in the society impose volatility and uncertainty. The utilization of smartphones will likely enable the work styles of individuals to be flexible, new ideas to be created, reliability and human relations to be deepened, and individual capabilities to be enhanced, thereby enhancing organizational competitiveness and productivity.

Let's now see how such benefits can be lead to work style innovations.

“Let`s Go Beyond with Smartphones ! ”



### 3. Mechanism and Overview of Smartphone

In this Chapter, the mechanisms and the overview of smartphones are described.

#### 3.1. Characteristics of Devices and Types of OS

The hardware of smartphones is different from conventional mobile phones and PCs. Smartphone screens (LCD) are larger than conventional phones and support a software keyboard, making them thinner and lighter than PCs.

There are many different types of smartphones with various OSs, and users need to make a best choice out of them. The following is a list of the main OSs and characteristics of smartphones in the Japanese market;

Table2 OS and Characteristics

Types of OSs	OS supplier	Characteristics
iOS (iPhone/iPad)	Apple Inc.	Vertically integrated across the OS, devices and application markets. Operated only on iPhone and iPad. Easy to apply latest versions.
Android	Google Inc.	Horizontally specialized across the OS, devices and application markets. Rich choices of devices available. Open source based OS. Each device vendor customizes the OS for their own device. Even for an identical OS version Android is not the same, it depends on the device also.
BlackBerry OS	Research In Motion Limited (Hereinafter RIM)	Basically vertically integrated for the OS, device and application markets. High security functionalities are supported by BES and BIS servers. Operated only BlackBerry. QWERTY key is supported in the major models.
Windows Phone 7	Microsoft Corporation (Hereinafter MS)	Horizontally specialized for the OS and devices. Devices selectable. Designed to be collaborative with the existing Microsoft assets. Support the management functionalities for example METRO UI and Exchange etc.

#### 3.2. Applications and Procurement

Unlike existing phones, smartphones require to activate an application even for a call. In that respect, all smartphone functionalities for example call, e-mail and schedule are considered as applications.

There are the applications that are pre-loaded before device shipments and there are applications that are downloaded from the markets by users.

The markets are offered by OS suppliers, communication telecom carriers and/or device vendors. The applications that are downloaded from the markets may not have been screened, and therefore the security risks for important data leakage exist. A caution is required upon downloading the applications, in such a way as checking the reliability of a market and an application. (Refer to "Application Usage" in the Section 5.9.)

Furthermore, since smartphones are always connected with networks, they can access the markets at anytime anywhere, smartphones enable us to obtain applications far easier than PCs do.

Companies or other organizations may distribute their own applications, and in such cases, the developer can have the control on how to distribute them. In this case however, a careful attention needs to be paid in order not to infringe the intellectual property rights of third parties.

Table 3 Markets and Characteristics

Suppliers	Markets	Market characteristics
iPhone/iPad	"App Store"	Register the third-party applications that Apple screen. For distribution and use of the applications, need to sign an agreement with Apple and received their certificates. Distribute and charge via App Store.
Android	①Google "Android market" ②Telecom carrier operated market	①Google does not screen the applications. The utilizations are at users' discretion. ②Telecom carriers etc. Register applications depending on their own criteria. Each has a distribution and billing model.
BlackBerry	"App World"	Register the third party applications screened by RIM. Distribute and charge via App World.
Windows Phone	"Marketplace"	Register the third party applications screened by Microsoft. Distribute and charge via Marketplace.

### 3.3. Communication styles and Networks

Smartphones can use voice communications and data communications (Packet communications). For network access, either mobile networks or Wi-Fi etc. can be used. Their bandwidths and supported areas differ respectively.

To connect with Internet via mobile networks using the Wi-Fi router functionalities of smartphones is called tethering. Since tethering result in creating more outlets as their access points to Internet from organizations, the use requires caution.

Table 4 Line types and Connection methods

Network	Characteristics	Available connection destinations
Mobile networks	<ul style="list-style-type: none"> <li>• Voice and data communications supported.</li> <li>• Wider coverage areas.</li> <li>• Slower in speed than Wi-Fi.</li> <li>• The connection authentications are handled by telecom carriers.</li> </ul>	<ul style="list-style-type: none"> <li>• Base stations (Data and voice) for telecom carriers.</li> </ul>
Wi-Fi	<ul style="list-style-type: none"> <li>• Data communications only.</li> <li>• Limited area coverage.</li> <li>• Faster in speed than mobile networks.</li> <li>• The connection authentications are proprietary. (Either by individuals or by service providers)</li> </ul>	<ul style="list-style-type: none"> <li>• Public Wi-Fi. (Hotels and hot spots etc.)</li> <li>• Wi-Fi router.</li> <li>• Home Wi-Fi.</li> <li>• Corporate networks. (Wi-Fi)</li> <li>• Tethering. (Use other smartphones)</li> </ul>

Threats and countermeasures need to be studied on the basis of understanding in the differences in ①"access to corporate networks" and ②"access to contracted SaaS/ASP".

In addition to the above usages, short range communications for example "Bluetooth Usage" and "Infrared Communications Usage" require to study its threats and countermeasures. Refer to the each item in the chapter 5, for further details.

### 3.4. Differences from Existing PC Security

Smartphones are still at an early stage, and the standardizations for their functionalities and security implementations by the OS vendors, the device vendors and the telecom carriers have made little progress.

In terms of the management and control for business uses, smartphones are still premature in some aspects, and with the limited measures to imposed across the board, those issues will need to be taken into considerations in use. Furthermore, there are frequent version updates that result in mixture of old and new devices to create further complexity in management.

Since PCs are much more standardized, it is hard to impose the security system of PCs to smartphones, and therefore various countermeasures need to be combined from the perspectives of a device itself, a network access, a system and service access, data storage, and management aspects, etc.

## 4. Characteristics and Considerations of Smartphones

In this Chapter, the threats unique to the nature of smartphones are described.

### 4.1. Characteristics

Smartphones include rich functionalities as communication tools. Furthermore, there are also various additional functionalities to support them. They contain the following characteristics:

Table 5 List of the characteristics of smartphones

Characteristics	Conventional mobile phones	Smartphones	PCs
Portability	⊙	⊙	△
Network connectivity	○	⊙	△
Convenience	○	⊙	○
Functionality and processing power	△	○	⊙
Expandability	×	○	⊙
Flexibility and personalization	×	⊙	⊙

### 4.2. Threats and Countermeasures from the Characteristic Perspectives

As listed on table 5, smartphones have superior portability. That makes us think about possible thefts and losses. Not only devices but also the SIM cards may be taken away.

In addition, they may break by falling to the ground or into the water. Smartphones are often used in public places, and the display information may be accidentally viewed.

Meanwhile for improved network connectivity, always-on connection is supported, for easier access to external services. The possible leakage of data when phones are lost could include not only the internal data in the lost devices but also the data stored at external services.

Furthermore, the convenience of saving passwords etc. could pose a risk for information leakage.

Users can download applications on their smartphones. Since unreliable markets may contain applications to include malware, make sure to select reliable markets.

Table 6 Threats and Countermeasures (Characteristics of smartphones)

Threats	Descriptions (Risks)	Countermeasures or requirements
Theft or loss of devices	<ul style="list-style-type: none"> <li>The stored data on device lost.</li> <li>Data leakage may include as far as external services.</li> </ul>	<ul style="list-style-type: none"> <li>Set a lock on device.</li> <li>Force to delete data when failing lock release.</li> <li>Encrypt the data domain of devices.</li> <li>Disable the saving function for user ID and password.</li> <li>Periodically back-up the data.</li> </ul>
SIM card theft	<ul style="list-style-type: none"> <li>Phone numbers and phone ID numbers etc. may be misused.</li> </ul>	<ul style="list-style-type: none"> <li>Call a telecom carrier to suspend the use.</li> </ul>
Damage by dropping or submersion	<ul style="list-style-type: none"> <li>Data losses.</li> </ul>	<ul style="list-style-type: none"> <li>Periodically back-up the data on phones.</li> <li>Wear a strap etc. to prevent falling</li> <li>Use water-proof and shock-resistant devices</li> </ul>
Peeping	<ul style="list-style-type: none"> <li>The data may be leaked.</li> </ul>	<ul style="list-style-type: none"> <li>Place a peeping screen protector etc.</li> </ul>
False recognition	<ul style="list-style-type: none"> <li>Operation mistakes can be more derived from the reaction ranges and speeds of touch panels.</li> </ul>	<ul style="list-style-type: none"> <li>Give users a heads-up on careful operations (Many of the panels use the capacitance system, and are more susceptible to static electricity.</li> </ul>
Vulnerability	<ul style="list-style-type: none"> <li>Many types of devices with various OSs. Difficult to put a patch.</li> </ul>	<ul style="list-style-type: none"> <li>Reduce or unify the types and OSs of devices.</li> </ul>
Unreliable markets	<ul style="list-style-type: none"> <li>Infected by malware due to an inadvertent access authorization upon installing an application.</li> <li>An application to become malware. (An initial access authorization enables automatic approvals on onward upgrade installations.)</li> </ul>	<ul style="list-style-type: none"> <li>Obtain applications from reliable markets.</li> <li>Prevent an inadvertent access authorization upon installing applications.</li> <li>Obtain the latest information on applications. (Illegal behaviors, unintended behaviors, reliable information etc.) (Refer to "Application Usage" in the Section 5.9)</li> </ul>
Modifications by user	<ul style="list-style-type: none"> <li>Infected by malware after OS modification. (Rooting, Jailbreak)</li> </ul>	<ul style="list-style-type: none"> <li>Prohibit modification.</li> </ul>

### 4.3. Future considerations

Devices and OSs will continue to be upgraded to higher functionality enhancing use capability.

For example, a smartphone user with an additional subscription may use Cloud storage service for automatic data synchronization from a smartphone to the Cloud. It is really an appealing service, but the user of the service without understanding its nature may cause private information leakages, illicit accesses and security threats.

Furthermore, damages may become larger due to the higher and larger data exchange rates of network, and battery charging from a PC via a USB cable may cause illicit information leakage.

More convenience will promote further business efficiencies, while continuous study on the countermeasures would be required.

## 5. Threats and Countermeasures from Use Case Perspectives

In this Chapter, the threats and countermeasures are described from the perspectives of smartphone users. Smartphones itself is hereinafter called Device.

In case of smartphones, all functionalities including voice calls are executed by applications.

When we look at the threats from use cases, an identification of data saving areas is important. Therefore in the use cases of the Guideline, "mail" (data saved to a Device) and "browser" (mainly accessing external data) in which data saving area can be easily identified, and "applications" of which data saving area cannot be easily identified, are separately described.

### 5.1. Phone address book Usage


The phone address books of smartphones have the functionalities to work as interfaces for phones, e-mails, SNS and instant messages, as well as to record use histories.

In order to offer such functionalities, they contain not only names and phone numbers but also various other personal data for example multiple e-mail addresses and SNS accounts etc.

A phone address book data saving area can be freely selected from a Device, an external memory medium and an external service. External services offer shared basis plans as well.

The saving areas are hard to be found by users, and saving data to unintended areas or automatic synchronizations with external services may cause data leakage. Therefore, the behaviors of applications need to be checked to provide an alert, and appropriate control and management for saving areas and synchronization settings are required.

Table 7 Threats and Countermeasures (Phone address book Usage)

Threats	Descriptions (Risks)	Countermeasures or requirements
Incorrect operations. Lack of knowledge.	<ul style="list-style-type: none"> <li>• Saving data to unintended areas causing data leakage.</li> <li>• The data on Devices may be synchronized with a certain Cloud.</li> </ul>	<ul style="list-style-type: none"> <li>• Produce a procedure manual. (Refer to the Appendix.)</li> <li>• Check the behaviors of an application. (e.g. data saving area, data publication scope etc.)</li> <li>• Appoint a dedicated data saving area for business.</li> <li>• Prevent users from selecting a saving area.</li> </ul>
Mixture with private data 【BYOD】 	<ul style="list-style-type: none"> <li>• With the mixture of business data and private data, countermeasures against leakages get complex, since the private data becomes subject to forced deletion upon leakage.</li> <li>• Difficult to delete data upon completion of business uses.</li> </ul>	<ul style="list-style-type: none"> <li>• Let users sign a pledge. (Refer to the Appendix)</li> <li>• Sort out data. (Separate saving areas for private and business)</li> <li>• Upon user's departure from a company or end of use, let users certify that they have deleted data.</li> </ul>

### 5.2. Phone Usage

There are 3 major communication channels as a phone; "calls using telecom carrier's voice channel", "VoIP based calls using telecom carrier's data communication channel" and "VoIP based calls using Wi-Fi".

Smartphones can also be used for house phones.

Using smartphones as house phones is an effective mean for cost reduction, smooth communications anywhere, and efficient office desk utilizations etc, but threats surrounding VoIP need to be aware of and appropriate measures should be taken. The following are the threats and countermeasures for the "VoIP based calls using Wi-Fi" case that requires the highest attention among the 3 channels.

In addition to the following Threats and Countermeasures, refer to "Corporate Network Usage" in Section 5.7.

Table 8 Threats and Countermeasures (Phone Usage)

Threats	Descriptions (Risks)	Countermeasures or requirements.
Wiretapping	<ul style="list-style-type: none"> <li>The communications over a phone are wiretapped and leaked to third parties.</li> </ul>	<ul style="list-style-type: none"> <li>When using VoIP, encrypt the communication channel.</li> </ul>
Illicit uses	<ul style="list-style-type: none"> <li>Phone numbers are illicitly scammed.(Zombie and information leakage.)</li> </ul>	<ul style="list-style-type: none"> <li>Correctly configure the equipment and services of IP PBX servers.</li> </ul>
Illicit access	<ul style="list-style-type: none"> <li>An IP PBX server becomes zombie and hacked.</li> </ul>	<ul style="list-style-type: none"> <li>Enhance the security of environments in adding passwords etc. to IP PBX servers.</li> <li>Authenticate a Device.</li> </ul>
Private uses	<ul style="list-style-type: none"> <li>Non-business phone use causes cost increase and productivity decrease.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> <li>Acquire communication histories.</li> </ul>

### 5.3. E-Mail Usage


Multiple mail accounts for smartphone mails can be used on one Device.

Since smartphones are always connected with the network of telecom carriers, a company is not able to access the e-mails that are directly transferred via the network of telecom carriers even after securely receiving the e-mails through VPN connection to a corporate network.

Furthermore, e-mails may include an attachment that is important for business transactions, and the attachment is normally downloaded to a Device. That requires us to take necessary measures to prevent information leakage.

In addition to the following threats and countermeasures, refer to "Corporate Network Usage" in the Section 5.7 or "SaaS/ASP services subscribed by an organization Usage".

Table 9 Threats and Countermeasures (E-mail Usage)

Threats	Descriptions (Risks)	Countermeasures or requirements
Illicit uses	<ul style="list-style-type: none"> <li>A text and attachment can be easily transferred, leading to information leakage.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> <li>Let users sign a pledge. (Refer to the Appendix)</li> <li>Use the mails for example web mails that do not leave data to Devices.</li> <li>Encrypt a text and attachment.</li> </ul>
Incorrect operations	<ul style="list-style-type: none"> <li>Data losses due to the deletion by incorrect operations.</li> <li>Information leakage due to erroneous transmission.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> <li>Let users sign a pledge. (Refer to the Appendix)</li> <li>Prohibit file attachments, and instead provide alternative means.</li> <li>Encrypt a text and attachment.</li> <li>Retain data in a server, and save the originals.</li> </ul>
Mixture with private date 【BYOD】 	<ul style="list-style-type: none"> <li>With the mixture of business data and private data, countermeasures against leakages get complex, since the private data becomes subject to forced deletion upon leakage.</li> <li>Difficult to delete data upon completion of business uses.</li> </ul>	<ul style="list-style-type: none"> <li>Let users sign a pledge. (Refer to the Appendix)</li> <li>Sort out data. (Use separate applications for private and business.)</li> <li>Upon user's departure from a company or end of use, let users certify that they have deleted data.</li> </ul>


### 5.4. Schedule Usage

Smartphones are easy to carry, to use as a datebook. The schedule function is often used. In addition to the schedule management of individuals, the schedule sharing function among an organization helps enhance the efficiencies of work.

Real-time views and updates of schedule on Cloud or on corporate networks can be possible, and furthermore some services offer managing private and official schedules in one calendar. In such case, depending on whether data is stored on the Device side or an external service side, threats and countermeasures differ.

In addition to the following threats and countermeasures, refer to "Corporate Network Usage" in the Section 5.7 or "SaaS/ASP services subscribed by an organization Usage" in the Section 5.8.

Table 10 Threats and Countermeasures (Schedule Usage)

Threats	Descriptions (Risks)	Countermeasures or requirements
Incorrect operations, Lack of knowledge	<ul style="list-style-type: none"> <li>When the range of scope for data publication is wrongly designated, unintended data is publicized. (Since there is a case where a local schedule is synchronized with the schedule on Cloud, it may impose a threat for automatically publicizing the schedule.)</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> <li>Check the behaviors of an application. (e.g. data saving area, data publication scope etc.)</li> <li>Designate a safe data storage area for business data.</li> <li>Prevent users from selecting a saving area.</li> </ul>
Private uses 【BYOD】 	<ul style="list-style-type: none"> <li>With the mixture of business data and private data, countermeasures against leakages get complex, since the private data becomes subject to forced deletion upon leakage.</li> <li>Difficult to delete data upon completion of business uses.</li> </ul>	<ul style="list-style-type: none"> <li>Let users sign a pledge. (Refer to the Appendix)</li> <li>Sort out data. (Separate applications and separate accounts etc. for private and business.)</li> <li>Upon user's departure from the company or end of use, let users certify that they have deleted data.</li> </ul>

## 5.5. Browser Usage

Smartphones unlike the conventional mobile phones support full browsers. Accessible sites have sharply increased, contributing to the benefit of business.

When employees use PCs, an access control and an access log acquisition can be made, in case of their accesses to non-business related sites or improper sites.

However in the case of smartphones, the network of telecom carriers are directly used, and therefore corporate IT administrators are not able to control accesses to non-business related sites and improper sites and acquire access logs. Under such circumstances, compliance with security policies and countermeasures against data leakage are essential.

Furthermore, a browser itself is an application, configurable functionalities for example whether or not cache deletion and password saving are possible, need to be checked in advance.

In addition the following threats and countermeasures, refer to "Corporate Network Usage" in the Section 5.7 or "SaaS/ASP services subscribed by an organization Usage" in the Section 5.8 as may be necessary.

Table 11 Threats and Countermeasures (Browser Usage)

Threats	Descriptions (Risks)	Countermeasures or requirements
Illicit uses	<ul style="list-style-type: none"> <li>Use maliciously using cache data.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> <li>Do not leave cache.</li> <li>Protect with web filtering.</li> </ul>
Wiretapping	<ul style="list-style-type: none"> <li>The content of the communication is wiretapped by the third party and information leaks.</li> </ul>	<ul style="list-style-type: none"> <li>Encrypt communications for corporate access.</li> </ul>
Malware	<ul style="list-style-type: none"> <li>A Device is hacked to lose control and information leaks.</li> <li>Possibility to become an offender.</li> </ul>	<ul style="list-style-type: none"> <li>Obtain applications from reliable markets.</li> </ul>
Private uses (improper contents).	<ul style="list-style-type: none"> <li>Non-business phone use causes cost increase and productivity decrease.</li> <li>Higher criminal chances.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> <li>Produce a corporate policy, and apply web filtering to limit.</li> <li>Acquire a view history. (In case of 【BYOD】 , the privacy of individuals may possibly be infringed.</li> <li>Sort out data. (For example account data and view history etc.). (Separate applications for private and business.)</li> </ul>
Phishing	<ul style="list-style-type: none"> <li>Due to the smaller display space, user may happen to access to phishing sites without recognizing illicit URLs.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> <li>Protect with Web filtering.</li> </ul>

## 5.6. Connect with Network

In order to use networks with smartphones, firstly access a target service via subscribed mobile networks or Wi-Fi. Depending on the routing and the services, threats and countermeasures need to be studied.

Some of the smartphone models support tethering. As the tethering has the characteristics as described in the "Communication styles and Networks" in the Section 3.3, the use is not recommended unless otherwise specifically required.

Mobile networks may not be used due to network failures or at outside coverage areas. In time for disasters, alternative connectivity for example Wi-Fi may need to be prepared.

The following are the threats and countermeasures at a gate of networks from smartphones.

Refer to "Corporate Network Usage" in the section 5.7, for the threats in using corporate Wi-Fi networks.

Table 12 Threats and Countermeasures (Connect with Network)

Network connected to	Threats	Descriptions (Risks)	Countermeasures or requirements
Wi-Fi router tethering (Router function)	Illicit access	<ul style="list-style-type: none"> <li>Illicitly used by third parties, and traffic increases.</li> </ul>	<ul style="list-style-type: none"> <li>Use the SSID that cannot be easily recognized an organization name and a model type.</li> <li>Use robust encryption methods as much as possible.</li> <li>Use complex passwords.</li> </ul>
	Illicit uses	<ul style="list-style-type: none"> <li>A direct connection with Internet from a corporate PC, causing information leakage.</li> </ul>	<ul style="list-style-type: none"> <li>Ban uses at corporate offices.</li> <li>Monitor to make sure that a tethering function is not activated.</li> </ul>
Public Wi-Fi	Wiretapping	<ul style="list-style-type: none"> <li>The information during the access is wiretapped, and leaked to third parties.</li> <li>Connected to a disguised access point, and passwords etc. are stolen.</li> </ul>	<ul style="list-style-type: none"> <li>Use reliable services. Do not use unidentified access points.</li> <li>Limit available access points.</li> </ul>
Mobile phone lines	Communication restrictions by telecom carriers	<ul style="list-style-type: none"> <li>Difficult to connect.</li> </ul>	<ul style="list-style-type: none"> <li>In time for possible communication restrictions by telecom carriers, prepare multiple means for connections.</li> </ul>
	Telecom carrier's connection line fault	<ul style="list-style-type: none"> <li>Unable to communicate.</li> </ul>	<ul style="list-style-type: none"> <li>Prepare Wi-Fi connectivity.</li> </ul>
	Illicit uses	<ul style="list-style-type: none"> <li>Non-business data communication use causes cost increase, and productivity decrease.</li> </ul>	<ul style="list-style-type: none"> <li>Let users sign a pledge. (Refer to the Appendix)</li> </ul>

## 5.7. Corporate Network Usage

In order to use corporate internal systems, we need to connect with corporate networks.

There are 3 ways as the access channels to corporate networks.

- Direct connection with corporate Wi-Fi networks
- Use mobile networks or public Wi-Fi and connect with VPN
- Use dedicated line services offered by telecom carriers

For each of the channels, countermeasures are required, and an authorizing party as well requires their measures.



Table 13 Threats and Countermeasures (Corporate Network Usage)

Access channels	Threats	Descriptions (Risks)	Countermeasures or requirements
Corporate Wi-Fi Network	Masquerade (User)	<ul style="list-style-type: none"> <li>An unauthorized user access to a corporate network.</li> </ul>	<ul style="list-style-type: none"> <li>Impose a user authentication. (In case of Wi-Fi, a Device authentication and a user authentication cannot be made concurrently, and therefore a prioritization depending on threats is required. In case of a user authentication only, an access from an authorized Device cannot be prevented.)</li> <li>Acquire an access log.</li> </ul>
	Masquerade (Device)	<ul style="list-style-type: none"> <li>An unauthorized Device is connected to a corporate network.</li> </ul>	<ul style="list-style-type: none"> <li>Impose a Device authentication. (In case of Wi-Fi, elimination of unauthorized Devices tends to be a major objective, and in such case the system side for access imposes a user authentication.)</li> <li>Acquire an access log.</li> </ul>
	Wiretapping	<ul style="list-style-type: none"> <li>The information during the access is wiretapped and leaked to third parties.</li> </ul>	<ul style="list-style-type: none"> <li>Encrypt communications.</li> <li>Use stronger encryptions.</li> <li>Protect important data. (Encryption, password etc.)</li> </ul>
	Illicit uses	<ul style="list-style-type: none"> <li>Non-business use via corporate networks.</li> </ul>	<ul style="list-style-type: none"> <li>Acquire an access log.</li> </ul>
	Illicit access	<ul style="list-style-type: none"> <li>Access to a corporate system without necessity or authorization, to take out data.</li> </ul>	<ul style="list-style-type: none"> <li>Limit accessible corporate systems. (Separate networks, SSID, access points etc.)</li> <li>Acquire an access log.</li> </ul>
VPN (Mobile networks or public Wi-Fi)	Masquerade (User)	<ul style="list-style-type: none"> <li>An unauthorized user accesses to a corporate network.</li> </ul>	<ul style="list-style-type: none"> <li>Impose a user authentication.</li> <li>Acquire an access log.</li> </ul>
	Masquerade (Device)	<ul style="list-style-type: none"> <li>An unauthorized Device is connected with a corporate network.</li> </ul>	<ul style="list-style-type: none"> <li>Impose a Device authentication.</li> <li>Acquire an access log.</li> </ul>
	Equipment trouble	<ul style="list-style-type: none"> <li>Due to a network equipment trouble, a service is down. Unable to precede a business operation.</li> </ul>	<ul style="list-style-type: none"> <li>Prepare redundancy.</li> <li>Secure alternative measures.</li> </ul>
	Attack vulnerability	<ul style="list-style-type: none"> <li>The vulnerability of network equipment is attacked for illicit access.</li> </ul>	<ul style="list-style-type: none"> <li>Upgrade equipment etc. to take measures against vulnerability.</li> <li>Acquire an access log.</li> </ul>
Telecom carrier closed network	Communication restriction by telecom carrier	<ul style="list-style-type: none"> <li>Unable to communicate or delay in communications due to telecom carrier's restrictions.</li> </ul>	<ul style="list-style-type: none"> <li>Have a diversity of telecom carriers to use.</li> <li>Prepare to be able to use other services for example public Wi-Fi.</li> </ul>
	Telecom carrier's subscription line trouble	<ul style="list-style-type: none"> <li>Unable to communicate due to telecom carrier's line trouble.</li> </ul>	

### 5.8. SaaS/ASP services subscribed by an organization Usage

Owing to the convenience of smartphones, SaaS/ASP is expected to be further used in organizations.

When using the SaaS/ASP services subscribed by an organization, we are provided with an access right for example an ID. When connected with Internet, we could access with any Devices including PCs, irrespective in or outside an office. With the higher convenience, the threats and measures need to be thoroughly studied.

In using SaaS/ASP services, it is necessary to be aware of SaaS/ASP service specific threats for example legal

restrictions and service troubles.

Table 14 Threats and Countermeasures (SaaS/ASP services subscribed by an organization Usage)

Access channel	Threat	Descriptions (Risks)	Countermeasures or requirements
Corporate Wi-Fi network, Mobile network, Wi-Fi Router etc.	Illicit use	<ul style="list-style-type: none"> <li>Access to organization subscribed SaaS/ASP services from outside of office, to cause external information leakage.</li> </ul>	<ul style="list-style-type: none"> <li>Acquire an access log on a service provider side.</li> <li>Impose a restriction on accessible networks, and acquire an access log internally.</li> </ul>
	Masquerade	<ul style="list-style-type: none"> <li>Services are used by an unauthorized user.</li> </ul>	<ul style="list-style-type: none"> <li>Collaborate with an internal authentication system.</li> <li>Check access logs.</li> </ul>

### 5.9. Application Usage


In downloading applications, we need to be aware that the reliability of applications depends on markets. (Refer to the "Applications and Procurement" in the Section 3.2)

Users may not be able to judge easily whether they should store an application externally or locally to their Devices, depending on applications. Investigate the behaviors of applications and take necessary measures. Access authorization to start an application can be valid for continued version upgrade installations. Careful attention is required in order to prevent users from causing unintended data leakage.

In case of using utilizing the applications that are independently developed by a company or an organization, separate measures in meeting the characteristics of the applications are required.

In addition to the following threats and countermeasures, refer to "Corporate Network Usage" in the Section 5.7 or "SaaS/ASP services subscribed by an organization Usage" in the Section 5.8.

Table 15 Threats and Countermeasures (Application Usage)

Threats	Descriptions (Risks)	Countermeasures or requirements
Incorrect operations Lack of knowledge	<ul style="list-style-type: none"> <li>As the result of selecting a wrong data saving area, information is accidentally publicized.</li> <li>Accidentally save data to an area, to cause information leakage.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> <li>Check the behaviors of an application (e.g. data saving area, data publication scope etc.)</li> <li>Appoint a dedicated data saving area for business.</li> <li>Prevent users from selecting a saving area.</li> </ul>
Wiretapping	<ul style="list-style-type: none"> <li>The content of the communication is wiretapped by the third party and information leaks.</li> </ul>	<ul style="list-style-type: none"> <li>Encrypt communications for corporate access.</li> </ul>
Malware	<ul style="list-style-type: none"> <li>Illicitly used by a malicious application.</li> </ul>	<ul style="list-style-type: none"> <li>Obtain applications from reliable markets.</li> <li>The application permitted in the organization is decided.</li> <li>Prevent an inadvertent access authorization upon installing applications.</li> <li>Obtain the latest information on applications. (Illegal behaviors, unintended behaviors, reliable information etc.)</li> </ul>
Private uses	<ul style="list-style-type: none"> <li>Private uses during business hinder business operations.</li> </ul>	<ul style="list-style-type: none"> <li>Limited uses during business.</li> </ul>
Private uses (improper contents)	<ul style="list-style-type: none"> <li>Non-business phone use causes cost increase and productivity decrease.</li> <li>Higher criminal chances.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> <li>Produce a corporate policy and use filters to limit.</li> <li>Acquire a use history.</li> </ul>
Mixture with private data 【BYOD】 	<ul style="list-style-type: none"> <li>With the mixture of business data and private data, countermeasures against leakages get complex, since the private data becomes subject to forced deletion upon leakage.</li> <li>Difficult to delete data upon completion of business uses.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> <li>Let users sign a pledge. (Refer to the Appendix)</li> <li>Sort out data. (In case of using an identical application for private and business.)</li> <li>Upon user's departure from a company or end of use, let users certify that they have deleted data.</li> </ul>

## 5.10. Device functionalities Usage

The "Device functionalities" herein mean the hardware functionalities equipped in devices.


Noteworthy functionalities among those in Devices are one for "an entrance for acquiring data" and "an exit for sending information". The functionality for "an exit for sending information" has been addressed so far in the "Data Communications" (From software point of views, "E-Mails", "Browsers" and "Applications" are also exits) therefore it is not covered in this report.

"Camera" and "Microphone" are typical "entrances for acquiring data". Such functionalities tend to increase further as new models are released.

### 5.10.1. Camera Usage

Many smartphones include a camera for still pictures and videos. Picture data can be easily transferrable. In order to prevent leakage of pictures, a key point is to stop unwanted picture shooting as much as possible.


Table 16 Threats and Countermeasures (Camera Usage)

Threats	Descriptions (Risks)	Countermeasures or requirements
Illicit use	<ul style="list-style-type: none"> <li>Use at and carry to prohibited areas violate the security rules of business partners etc. and cause illicit data leakage.</li> </ul>	<ul style="list-style-type: none"> <li>Paste a security seal etc. to avoid using.</li> <li>Disable camera functions.</li> </ul>
Incorrect operations Lack of knowledge	<ul style="list-style-type: none"> <li>As the result of selecting a wrong data saving area, information is accidentally publicized.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> </ul>
Incorrect operations	<ul style="list-style-type: none"> <li>Unintended camera activation causes unintended shooting.</li> </ul>	<ul style="list-style-type: none"> <li>Paste a security seal etc. to avoid using.</li> <li>Disable camera functions.</li> </ul>
Lack of knowledge	<ul style="list-style-type: none"> <li>With a use of functionalities too easily, unintended data are acquired. (Violate the portrait rights of others, or use a camera at prohibited areas.)</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> </ul>
Phishing	<ul style="list-style-type: none"> <li>The site connected using a bar-code reader may be a phishing site.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> </ul>
Malware	<ul style="list-style-type: none"> <li>With a malicious application, camera functionality is illicitly used.</li> </ul>	<ul style="list-style-type: none"> <li>Do not inadvertently authorize an access when installing an application.</li> <li>Disable camera functions.</li> </ul>
Picture data leak.	<ul style="list-style-type: none"> <li>Exif (Shooting data for example location information etc. and camera model type etc.) - the picture meta data of shooting with smartphones accidentally leak.</li> </ul>	<ul style="list-style-type: none"> <li>Suspend functionality of getting location information when shooting.</li> <li>When publicizing pictures to outside, delete Exif. (Data, properties and attributes.)</li> </ul>
Mixed with private data 【BYOD】 	<ul style="list-style-type: none"> <li>With the mixture of business data and private data, countermeasures against leakages get complex, since the private data becomes subject to forced deletion upon leakage.</li> <li>Difficult to delete data upon completion of business uses.</li> </ul>	<ul style="list-style-type: none"> <li>Let users sign a pledge. (Refer to the Appendix)</li> <li>Move business data to a dedicated storage area. (Quickly delete them from a Device.)</li> <li>Upon user's departure from a company or end of use, let users certify that they have deleted data.</li> </ul>

### 5.10.2. Microphone Usage

A microphone is embedded to a smartphone, to be used for call recordings and a voice recorder. Recorded data can be easily transmitted. In order to prevent leakage of recording, a key point is to stop unwanted recordings as much as possible.

Table 17 Threats and Countermeasures (Microphone Usage)

Threat	Descriptions (Risks)	Countermeasures or requirements
Lack of knowledge	<ul style="list-style-type: none"> <li>Use at and carry to prohibited areas violate the security rules of business partners etc. and cause illicit data leakage.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> </ul>
Incorrect operations Lack of knowledge	<ul style="list-style-type: none"> <li>As the result of selecting a wrong data saving area, information is accidentally publicized.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> </ul>
Malware	<ul style="list-style-type: none"> <li>With a malicious application, recording functionality is illicitly used.</li> </ul>	<ul style="list-style-type: none"> <li>Prevent an inadvertent access authorization upon installing applications.</li> </ul>
Mixture with private data 【BYOD】 	<ul style="list-style-type: none"> <li>With the mixture of business data and private data, countermeasures against leakages get complex, since the private data becomes subject to forced deletion upon leakage.</li> <li>Difficult to delete data upon completion of business uses.</li> </ul>	<ul style="list-style-type: none"> <li>Let users sign a pledge. (Refer to the Appendix)</li> <li>Move business data to a dedicated storage area. (Quickly delete them from a Device.)</li> <li>Upon user's departure from a company or end of use, let users certify that they have deleted data.</li> </ul>

### 5.10.3. Location Information Usage

Many of the smartphones have GPS functionalities, enabling us to find out where we are. The capability to identify where a user or a device is located is useful in knowing the safety of a person in emergency or in finding a lost Device.

Table 18 Threats and Countermeasures (Location Information Usage)

Threat	Descriptions (Risks)	Countermeasures or requirements
Incorrect operations Lack of knowledge	<ul style="list-style-type: none"> <li>With a use of functionalities too easily, unintended data are publicized.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> </ul>
Wiretapping	<ul style="list-style-type: none"> <li>Let others known our location accidentally.</li> </ul>	<ul style="list-style-type: none"> <li>Suspend a location information functionality if it's not necessary.</li> </ul>
Malware	<ul style="list-style-type: none"> <li>An application acquires the location information of a smartphone, and the information is illicitly used.</li> </ul>	<ul style="list-style-type: none"> <li>Do not inadvertently authorize an access when installing an application.</li> </ul>

### 5.10.4. NFC Usage

Some smartphones have a NFC\* functionality. Smartphones can be used as a device for an access control to offices and for payment.

\*NFC (Near Field Communication)

Table 19 Threats and Countermeasures (NFC Usage)

Threat	Descriptions (Risks)	Countermeasures or requirements
Skimming	<ul style="list-style-type: none"> <li>The data inside a Device are read out, leading to information leakage.</li> </ul>	<ul style="list-style-type: none"> <li>Use a lock function when not in use.</li> <li>Put a cover on a chip portion.</li> </ul>
Masquerade	<ul style="list-style-type: none"> <li>An illicitly acquired Device can easily be used to impersonate the owner, enabling illicit accesses to an office and payments.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (How to contact and handle, in case of a theft and a loss.)</li> <li>Activate a lock function.</li> </ul>

### 5.10.5. Iseg, a terrestrial TV broadcasting programs on mobile phones Usage

Some smartphones support a Iseg receiving functionality, capable of receiving TV programs and data broadcasting programs.

Table 20 Threats and Countermeasures (Iseg Usage)

Threat	Descriptions (Risk)	Countermeasures or requirements
Private uses	<ul style="list-style-type: none"> <li>Private uses during business hinder business operations.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (For example clarifying the scope of use and limiting use during business hours)</li> <li>Limited uses during business.</li> </ul>

### 5.10.6. Bluetooth Usage

Bluetooth is the standard to be used for relatively near range inter-equipment communications. (From several meters to several 10 meters) In between pre-configured (Pairing) equipment, connections can be easily established. Bluetooth is now being used for connections with headphones and PCs.

Table 21 Threats and Countermeasures (Bluetooth Usage)

Threats	Descriptions (Risks)	Countermeasures or requirements
Illicit access	<ul style="list-style-type: none"> <li>Illicitly connected with a Device, and the data there are read out.</li> </ul>	<ul style="list-style-type: none"> <li>Limit accessible equipment with a Device.</li> <li>Disable Bluetooth.</li> </ul>
Illicit use	<ul style="list-style-type: none"> <li>A user connects with a PC that is not authorized by an organization for connection, and sneaks the data on the Device out of the office.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> <li>Let users sign a pledge. (Refer to the Appendix)</li> <li>Limit accessible equipment with a Device.</li> <li>Disable Bluetooth.</li> </ul>
Malware	<ul style="list-style-type: none"> <li>Malware that can be infected via Bluetooth communication channels exists.</li> </ul>	<ul style="list-style-type: none"> <li>Limit accessible equipment with a Device.</li> <li>Disable Bluetooth.</li> </ul>
Automatic activation of Bluetooth	<ul style="list-style-type: none"> <li>A user accidentally activates Bluetooth to connect.</li> <li>Even after ending an application, Bluetooth itself continues to be active, causing other threats.</li> </ul>	<ul style="list-style-type: none"> <li>Check the applications to use Bluetooth.</li> </ul>

### 5.10.7. Infrared Communications Usage

Infrared communications have been used for conventional mobile phones, using the standard for conventional mobile phones using the standard for connectivity of equipment with short ranges .(e.g. small measurements) They can be used for some of smartphones.

They are used for transferring data relatively in a short time period, for example sending and receiving phone address books data.

Table 22 Threats and Countermeasures (Infrared Communications Usage)

Threats	Descriptions (Risk)	Countermeasures or requirements
Incorrect operations Lack of knowledge	<ul style="list-style-type: none"> <li>unintended data leakage.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> </ul>

### 5.11. Media Data Usage


A smartphone can also facilitate as large capacity USB storage.

With the functionality, a smartphone can become a transport media for other data, enabling leaks of high volumes data. The severity of losses could be deemed as equivalent to that of PCs.

Depending on a device and an application, data in a Device and an external memory medium for example a SD card can be encrypted, but in such case as well, the authentication of a device lock may be cracked to enable the data view. Therefore, a countermeasure in time for losses is essential.

We strongly recommend not using, in principle, smartphones as a data medium.

Table 23 Threats and Countermeasures (Media Data Usage)

Threat	Descriptions (Risks)	Countermeasures or requirements
Theft, loss and breakdown	<ul style="list-style-type: none"> <li>Data dissipation and information leakage occurs due to theft, loss and breakdown. (Due to higher portability than that of PC etc.)</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> <li>Prepare alternative means. (USB storage, and a storage service for businesses.)</li> <li>Encrypt the data domain of smartphones and external memory medium.</li> </ul>
Remove external medium	<ul style="list-style-type: none"> <li>In case inserted memory medium is inadvertently removed or is stolen, to cause leakage of the recorded data.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> <li>An organization lends external medium.</li> <li>Encrypt data.</li> <li>Paste a security seal.</li> </ul>
Mixed with private data 【BYOD】 	<ul style="list-style-type: none"> <li>With the mixture of business data and private data, countermeasures against leakages get complex, since the private data becomes subject to forced deletion upon leakage.</li> <li>Difficult to delete data upon completion of business uses.</li> </ul>	<ul style="list-style-type: none"> <li>Let users sign a pledge. (Refer to the Appendix)</li> <li>Prohibit use.</li> <li>Upon user's departure from a company or end of use, let users certify that they have deleted data.</li> </ul>


\*In addition to the above, it may serve as a medium for malware on PCs.

### 5.12. Backup/Synchronize

We can backup (Synchronize) data on a PC or to Cloud etc.

Thus, backup data must be subject to security control.

Table 24 Threats and Countermeasures (Backup/Synchronize)

Threats	Descriptions (Risks)	Countermeasures or requirements
Incorrect operations Lack of knowledge	<ul style="list-style-type: none"> <li>Without awareness on how to synchronize data and where to save data, data is accidentally overwritten or dissipated.</li> </ul>	<ul style="list-style-type: none"> <li>Produce a procedure manual. (Refer to the Appendix)</li> <li>Check the behaviors of an application. (Data saving area etc.)</li> <li>Use a backup tool.</li> </ul>
Coexistence of business data in backup data 【BYOD】 	<ul style="list-style-type: none"> <li>Backup data including business data may leak from a privately owned PC.</li> </ul>	<ul style="list-style-type: none"> <li>Let users sign a pledge. (Refer to the Appendix)</li> <li>Protect backup data in a private storage area. (For example privately owned PCs, Cloud and external memory media etc.)</li> <li>Apply encryptions in data backup. (Including privately held PCs.)</li> </ul>

### 5.13. 【Reference】 Internet Storage Service Usage

Internet storage services are becoming popular especially among individuals, due to their convenience of using identical data "at anywhere anytime" and "sharing with required persons".

An access control (Filtering) and usage monitoring can be possible for PCs but not for smartphones.

Furthermore since smartphones are always connected with the data communication lines of telecom carriers, a company is not able to grasp the data transmission that are directly transferred to Internet storage services via communication lines of telecom carriers even after securely receiving the data via a VPN connection with a corporate

network. Therefore, we would strongly recommend that the business uses other than organizationally nominated services be not used.

#### **5.14. 【Reference】 SNS Usage**

SNS and mini blog are becoming popular as communication tools especially among individual users. They fit the characteristics of smartphones as users can promptly inform their friends etc. of what they've seen and heard.

The number of companies using them as marketing and active communication tools is increasing.

However the threats of SNS for example a writing mindlessness, an incorrect data publication, a private use during office hours, and location discovery from the GPS data and the pictures of the phone are intensifying. It is recommended to set out a rule in an organization before using.

## 6. Consideration on Lifecycles

The discarding plan is called a lifecycle. In this Chapter, considerations for a lifecycle are described.

In order to securely use smartphones, we need to be aware of the differences between PCs, and study necessary security means in meeting the objectives of uses, while achieving low cost and steady means to avoid the risks with the expansion, optimization and operation of existing facilities.

The descriptions in this Chapter may also be used for warning in temporarily authorizing to use smartphones for emergencies for example natural disasters.

Additionally, we describe the important point of view about BYOD.

### 6.1. Plan

During the planning stage of smartphones introduction, the objectives for business uses need to be clarified and assumed use cases need to be identified. On the basis, you may refer to the "Threats and Countermeasures from use case perspectives" in the Chapter 5, and decide to accept with the risks in mind.

When authorizing BYOD, a prior agreement with a user regarding observing security policies is important for an operation. A pledge should be prepared at this stage.

#### 6.1.1. Set Out an Internal Rule

To set out an internal rule is necessary, irrespective of the types of ownership and the objectives of use. Please determine the scope of smartphone use, check the threats and countermeasures of use cases, and produce the rules and procedures for use. The procedures indicate the documents of compiled internal rules.

Regarding the rules for illicit uses and incident occurrences, pledge may need to be produced and/or updated to meet the requirements of smartphones.

Especially in view of the characteristics of smartphones, the rules to cope with thefts and losses need to be set out.

#### 6.1.2. Set out a User Manual

To set out a user manual is required for business uses irrespective of the types of ownership and the purposes of use. In drafting a user manual, smartphones specific technical terms for example "tap", "flick" and "pinch" need to be well explained. Settings and configurations depend on models.

An instruction manual should be drafted on the assumption that it will be viewed on smartphones.

In drafting a manual, a corporate owned case and a BYOD case should be taken into consideration.

#### 6.1.3. Prepare a Support System

To put a support system in place is required for business uses irrespective of the types of ownership and the purposes of use. Users presently do not have accurate and enough knowledge for smartphones. Before using smartphones, an appropriate support system should be well prepared. In addition, the study on how to reduce support burdens throughout the period from a planning stage to an implementation stage, with facilitating self-support tools for example simplified introduction procedures, instruction manuals and FAQ.

The countermeasures for thefts and losses outside business hours should be planned for in advance.

### 6.2. Introducing Smartphones

At time of introducing smartphones to an organization, an efficient implementation for example drafting a start-using procedure, buying attachments to Devices, configuring an initial setting, setting accounts, and registering the applications to use, etc. is required, in minimizing the burden of users.

In addition to such initial introduction of smartphones in large volumes, periodical small scale additions, or the replacement for losses or breakdowns need to be taken into consideration, and a lower work load and an error free implementation are the biggest challenges.

#### 6.2.1. Start-using Procedures

The procedures for Start-using can be different depending on the types of ownership and the purposes of use. Irrespective of the types of ownership however, they are required for business uses. For a Device control, it is recommended to produce a ledger to correlate a user and a device, etc.

In case of authorizing BYOD, setting out the terms and conditions for checking and acceptance applications, agreeing on a pledge, and showing terms of use are important.



### **6.2.2. Procure or Place Attachments**

The attachments that should be procured or placed for smartphones depend on the types of ownership and the purposes of use. We recommend using a measure to prevent falling, for a corporate owned phone. We recommend adopting countermeasures against peeping and illicit uses, irrespective the types of ownership and the purposes of use.

### **6.2.3. Acquire User Account**

The account acquisition methods for an initial setting depend on the types of ownership and the method of use. In case of BYOD, it is common for a user to have acquired an account, and therefore an organizational registration upon use may need to be considered. In case of acquiring an account for a corporate owned Device, an account naming guideline may better be produced in advance, for a smother operation and management.

### **6.2.4. Initial Setting of a Device**

The initial setting methods of Devices depend on the types of ownership and the purposes of use. In case of corporate owned smartphones, there are two possibilities; the initial setting of device is done by the company or done by the user's self services. In case of BYOD the latter situation takes precedence.

In setting a device initially, device settings and functionality restrictions should be in line with a security policy. Depending on OS differences, or version differences for an OS, device settings and functionality restrictions may have limitations. In addition, there is a case in which almost all of the settings can be automatically set, or a case in which some manual interventions are required in setting.

For some of OSs, device settings compliant with a security policy could be revised or deleted by a user. When organizational control is essential, separate measures should be required.

### **6.2.5. Activate a Device Lock Functionality**

Setting device lock functionality is necessary irrespective of the types of ownership and the purpose of use.

The names and the functionalities of the lock depend on devices and OSs. When using smartphones, make sure to activate lock functionality for example limiting number of error entries, in accordance with a security policy.

### **6.2.6. Acquiring E-Mail Accounts**

The methods to acquire an e-mail address depend on the type of ownership and the purposes of use. In case of BYOD, it is common for a user to have acquired e-mail addresses, and therefore an organizational registration upon use may need to be considered. In case of acquiring a mail address for a corporate owned Device, an e-mail address naming guideline may better be produced in advance, for smother operation and management.

### **6.2.7. Introduce an Application**

The methods for introducing applications depend of types of ownership and the purposes of use.

In case a user introduces security related applications on their own, an administrator needs to be able to be able to check the status of introducing application.

In case of BYOD, broad ranges of OSs and Devices are expected; we must make sure that the applications to be used are compatible with the target OSs and Devices.

### **6.2.8. Trainings Implementation**

Training is required irrespective of the types of ownership and the purposes of use. Presently, users do not have accurate and enough knowledge on smartphones. Therefore, the training for an introduction is quite important. Please periodically provide trainings in order to enhance user's security awareness, regarding the subjects of the characteristics of smartphones as described in the Guideline, the cautions for use cases and others.

### **6.2.9. Distribute Devices**

The distribution of devices relates only to a corporate owned case. For both of the cases of a device setting by a user, and kitting by corporate, managing the relationship between an asset and a user is important. Especially in case of kitting, personal data are registered to a device, and therefore the device must be delivered to a legitimate user.

## **6.3. Operation**

At an operation phase of smartphones, appropriate management must be imposed for safer use of smartphones at business. In order to achieve this objective, we may need to periodically monitor on whether a device is properly used, and is properly configured and restricted for minimizing expected risks. Procedures should be set out in advance, regarding the actions toward incidents for example losses and thefts, and the ways to apply updates in addressing the vulnerability of the OS.

### **6.3.1. Acquire and Monitor Device Information**

Acquiring and monitoring device information is required for business uses irrespective of the types of ownership and the purposes of use.

The information on the hardware of a smartphone, OS and applications to be used, applied Device settings and functionality restrictions, and whether or not the OS has been modified should be periodically acquired to monitor the status of a device. With a constant monitoring on the use status of smartphones, administrators can make sure that the smartphones are not illicitly used, and check the vulnerability of the OS.

Modifying the OS could become the biggest threat for the security of smartphones, and such modifications must be monitored and detected.

In order to acquire the location information of a Device in time for losses, we will need to obtain a prior agreement from a user to do so, since it may possibly infringe user privacy, and a cautious consideration should be taken in acquiring the data.

### **6.3.2. Control Device Functionalities**

The control of devices is required irrespective of the types of ownership and the purposes of use.

Administrators are always required to manage and control the safety at business uses, employing those measures as the functionality control of smartphones, and the remote locking and data deletion.

In order to control devices, a security policy for Devices must be drafted and implemented.

There are various differences in OSs and Devices, and it's hard to target all of them under control. We must be careful especially in case of BYOD.

Some of OSs use SMS for device controls, but in such case, the tablets that do not support SMS may not be controlled.

### **6.3.3. Manage OS versions**

Management of OS versions is required irrespective of the types of ownership and the purposes of use.

Especially when an upgrade to the OS version that includes the hot fix for vulnerability is available, this is a crucial issue. Due to the policies of device vendors or telecom carriers however, upgrades may not be used.

Thus, administrators shall require to know which version of OS is being used, and to understand reported threats, in order to impose technical and operational countermeasures, or to accept risks.

## **6.4. Discarding**

It is important to completely delete the business data in a device and in an external memory medium, various devices setting information, account information, and used applications.

The discarding includes "device return" due to breakdown, "device replace" due to buying a new one, and "device transfer as secondhand to others".

Any of these cases require deleting business data, device setting data, applications, and cache data including the authentication data for external services.

Especially upon completion of BYOD uses, the above actions need to be definitely taken.

## **7. Conclusion**

### **7.1. Balance between the Purposes of Use and Security**

The purposes of using smartphones vary depending on organizations. The most important factor is taking a balance between the purposes of use and security. Please scrutinize the security requirements in meeting your objectives, and selectively use and implement countermeasures that fit organizational needs.

Smartphones have superior characteristics as a communication tool. It supports the creativity and motivation of users, and contains the huge potentiality for business renovation. Studies to exercise the benefits of smartphone use, manage assets, and manage human resources need to be made.

The Guideline encompasses the threats. To meet all of the requirements as described may be difficult, and may not be recommended. You may need to understand the threats as described, analyze the severances, think about the purposes of use, and take necessary measures cautiously.

### **7.2. Security Policy of an Organization and Decision Making**

Criminals and accidents by an insider or an outsider alike may occur. When studying the security aspects of smartphones, usual security considerations for emergencies, significances, and the confidentiality of data must be well taken, and the set-out security measures need to be reviewed in line with a PDCA cycle, though there may be some exceptions due to the characteristics.

Furthermore, non-conventional know-how for example the feasibility study of the countermeasures, compatibility checking with existing security policies and necessary amendments, control and management that is different from PC's, and legal checking of overseas laws in using Cloud services is required. The time and budget required for the effort, and the literacy of users, and the scope to be able to support as an organization must be well studied.

### **7.3. Necessity for Continuous Data Acquisition**

As stated at the beginning, the security measures of smartphone are still on a developing stage, leaving some issues unaddressed at moment. A decision must be taken on whether to avoid an operation with an acceptance of the issues, to select a usage to exclude the issues, or not to use smartphones. In addition, the selection on whether to provide to an employee a corporate owned smartphone or to turn a privately owned one BYOD is worthwhile to study.

The environment surrounding smartphones is rapidly changing. Please study the characteristics as described in the Guideline, always acquire the latest information, and implement the most appropriate and valid security measures.

An intellectual productivity improvement is the need of the present time. Let's challenge for innovations, and utilize a smartphone as a good tool to enhance organizational power. We sincerely wish that the Guideline can be of help in decision making.

## 8. Glossary

Page first appeared	Chapter No first appeared	Term	Meaning
7	3.1	Software keyboard	The function to show a keyboard on a touch panel screen, and enter characters etc. with software processing.
7	3.2	Market	The selling sites of applications that user download. The popular markets include App Store of Apple inc. and Android Market of Google Inc.
8	3.3	Mobile network	3G network etc. that telecom carriers offer.
8	3.3	Public Wi-Fi	The Public wireless LAN services that can access to Internet from various types of equipment via public Wi-Fi access points.
9	4.2	SIM card	Abbreviation of "Subscriber Identity Module Card". The IC cards that are issued by each telecom carrier, and record the subscriber data of mobile phone numbers etc. and phone address books data.
9	4.2	Malware	Malicious software and program.
10	4.2	Access authorization	When installing an application, a user is shown the list of functionalities to be used, and is authorized to use. (Android OS calls it "Permission".)
10	4.2	Rooting, Jailbreak	Utilize vulnerability and obtain a root (Supervisor) authorization.
10	4.3	Cloud storage	The service to store data using Cloud.
12	5.2	IP PBX	Abbreviation of "Internet Protocol Private Branch eXchange". The hardware and software to realize a house phone network with IP phones.
15	5.7	User authentication	The processing to enter a user ID and passwords to identify the user that enters them.
15	5.7	Device authentication	The processing to identify a device using User ID data etc. assigned to a device.
17	5.10.1	Security seal	A seal to paste on the lens part of a camera, to restrict a camera use.
17	5.10.1	Exif	Abbreviation of "Exchangeable image file format". The data format to save the camera shooting data for example shooting date, a camera model, location data, as image data.
18	5.10.4	NFC	Abbreviation of "Near Field Communication". The communications in close proximity to enable non-contact communications.
20	5.11	Lock a Device	The functionality to lock devices with passwords and patterns. The functionalities and the names are different by device. There is an automatic lock function etc. that works when a terminal is not used for a certain period of time.
22	6.1.2	Tap	To lightly hit a touch panel screen with a finger, to operate.
22	6.1.2	Flick	Flick and trace a touch panel screen with a finger, from side to side and up and down, to operate.
22	6.1.2	Pinch	Use fingers on a touch panel to expand and shrink.
23	6.2.4	Kitting	To configure necessary settings of a Device by an administrator so that a user can readily use it.
24	6.3.2	SMS	Abbreviation of "Short Message Service". The service to send and receive short messages, with a telephone number as the address.
32	A-3 (5.5)	Short URL	Short URL to match the requirements of SNS etc. on their number of characters, in accessing to websites.

# Appendix A

## A-1 Check Sheet for Countermeasures per Characteristics

Level of recommendation: ■ Strongly recommended □ Recommended

Chapter number	Classification	Threats	Countermeasures or requirements	Level of recommendation
4.2	Threats from the view point of characteristics	Theft or loss of devices	-Set a lock on a Device. -Force to delete data when failing to unlock. -Encrypt the data area of a phone and external memory media. -Disable the saving function for user ID and password. -Periodically back-up data.	■ ■ □ □ □
		Theft of SIM card	- Contact a telecom carrier to suspend use.	■
		Damage by dropping or submersion	- Periodically back-up the data on phones. - Wear a strap etc. to prevent falling. - Use water-proof and shock-resistant devices.	□ □ □
		Peeping	-Place a peeping screen protector etc.	□
		False recognition	-Give users a heads-up on careful operations. (Many of the panels use the capacitance system, and are more susceptible to static electricity.)	□
		Vulnerability	-Reduce or unify the types and OSs of devices.	□
		Unreliable markets	-Obtain applications from reliable markets. - Do not inadvertently authorize an access when installing an application. -Obtain the latest information on applications. (Illegal behaviors, unintended behaviors, reliable information etc.) (Refer to "Application Usage" in the Section 5.9)	■ □ □
		Alterations by user	-Prohibit alteration.	■

## A-2 Check Sheet for Countermeasures per Case Usage

Level of recommendation: ■ Strongly recommended □ Recommended - Not applicable

Chapter number	Classification	Threats	Countermeasures or requirements	Level of recommendation
5.1	Phone address book Usage	Incorrect operation, Lack of knowledge	-Produce a procedure manual. (Refer to the Appendix) -Check the behaviors of an application. (e.g. data saving area, data publication scope etc.) -Appoint a dedicated data saving area for business. -Prevent users from selecting a saving area.	- □ □ □
		Mixed with private data <b>【BYOD】</b>	-Let users sign a pledge. (Refer to the Appendix) -Sort out data. (Separate saving areas for private and business.) -Upon user's departure from a company or end of use, let users certify that they have deleted data.	- □ ■
5.2	Phone Usage	Wiretapping	-In using VoIP, encrypt the communication channel.	□
		Illicit use	-Correctly configure the equipment and services of IP PBX servers.	□
		Illicit access	-Enhance the security of environments in adding passwords etc. to IP PBX servers. Authenticate a Device.	□
		Private uses	-Produce a procedure manual. (Refer to the Appendix) -Acquire communication histories.	- □
5.3	E-mail Usage	Illicit use	-Produce a procedure manual. (Refer to the Appendix) -Let users sign a pledge. (Refer to the Appendix) -Use the mails for example web mails that do not leave data to Devices. -Encrypt a main body and attachment.	- - □ □
		Incorrect operations	-Produce a procedure manual. (Refer to the Appendix) - Let users sign a pledge. (Refer to the Appendix) -Prohibit a file attachment, and instead provide alternative means. -Encrypt a main body and attachment. -Retain data in a server, and save the originals.	- - □ □ □
		Private mails are mixed <b>【BYOD】</b>	-Let users sign a pledge. (Refer to the Appendix) -Sort out data. (Use separate applications for private and business.) -Upon user's departure from a company or end of use, let users certify that they have deleted data.	- □ ■

5.4	Schedule Usage	Incorrect operations. Lack of knowledge	-Produce a procedure manual. (Refer to the Appendix) -Check the behaviors of an application. (e.g. data saving area, data publication scope etc.) -Nominate a dedicated data storage area for data. -Prevent users from selecting a saving area.	- <input type="checkbox"/>  <input type="checkbox"/> <input type="checkbox"/>
		Private uses 【BYOD】	-Let users sign a pledge. (Refer to the Appendix) -Sort our data. (Separate applications and separate accounts etc. for private and business.) -Upon user's departure from a company or end of use, let users certify that they have deleted data.	- <input type="checkbox"/> <input checked="" type="checkbox"/>
5.5	Browser Usage	Illicit use	-Produce a procedure manual. (Refer to the Appendix) -Do not leave cache. -Protect with Web filtering.	- <input type="checkbox"/> <input type="checkbox"/>
		Wiretapping	-Encrypt communications for corporate access.	<input checked="" type="checkbox"/>
		Malware	-Obtain applications from reliable markets.	<input type="checkbox"/>
		Private uses (improper contents)	-Produce a procedure manual. (Refer to the Appendix) -Produce a corporate policy, and apply WEB filtering to limit. -Acquire a view history. (In case of 【BYOD】 , the privacy of individuals may possibly be infringed.) -Sort out data. (For example account data and view history etc.) (Separate applications for private and business.)	- <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
		Phishing	-Produce a procedure manual. (Refer to the Appendix) -Protect with Web filtering.	- <input type="checkbox"/>
5.6	Connect with Network  Wi-Fi router tethering (router functionality)	Illicit access	-Use the SSID that cannot easily assume an organization name and a model type. -Use robust encryption methods as much as possible. -Use complex passwords.	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
		Illicit use	-Ban uses at corporate offices. - Monitor to make sure that a tethering function is not activated.	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Connect with Network  Public Wi-Fi	Wiretapping	-Use reliable services. Do not use unidentified access points. -Limit available access points.	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Connected with Network  Mobile network	Communication restriction by telecom carrier	-In time for possible communication restrictions by telecom carriers, prepare multiple means for connections.	<input type="checkbox"/>
		Telecom carrier's subscription line trouble	-Prepare Wi-Fi connectivity for off-road.	<input type="checkbox"/>
		Illicit use	-Let users sign a pledge. (Refer to the Appendix)	-
5.7	Corporate Network Usage  Corporate Wi-Fi Network	Masquerade (User)	-Impose a user authentication. (In case of Wi-Fi, a device authentication and a user authentication cannot be made concurrently, and therefore a prioritization depending on threats is required. In case of a user authentication only, an access from an authorized device cannot be prevented. ) -Acquire an access log.	<input checked="" type="checkbox"/> <input type="checkbox"/>
		Masquerade (Device)	-Impose a Device authentication. (In case of Wi-Fi, elimination of unauthorized Devices tends to be a major objective, and in such case the system side for access imposes a user authentication.) -Acquire an access log.	<input checked="" type="checkbox"/> <input type="checkbox"/>
		Wiretapping	-Encrypt communications. -Use stronger encryptions. -Protect important data. (Encryption, password etc.)	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
		Illicit use	-Acquire an access log.	<input type="checkbox"/>
		Illicit access	-Limit accessible corporate systems. (Separate networks, SSID, access points etc.) -Acquire an access log.	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Corporate Network Usage  VPN (Mobile network and public Wi-Fi)	Masquerade (user)	-Impose a user authentication. -Acquire an access log.	<input checked="" type="checkbox"/> <input type="checkbox"/>
		Masquerade (Device). Equipment trouble	-Impose a Device authentication. -Acquire an access log. -Prepare redundancy. -Secure alternative measures.	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

	etc.)	Attack vulnerability	-Upgrade equipment etc. to take measures against vulnerability. -Acquire an access log.	<input type="checkbox"/> <input type="checkbox"/>
	Corporate Network Usage	Communication restriction by telecom carrier	-Diversify telecom carriers to use. -Prepared to be able to use other services for example public Wi-Fi.	<input type="checkbox"/> <input type="checkbox"/>
	Telecom carrier's closed network	Telecom carrier's subscription line trouble		
5.8	SaaS/ASP services subscribed by an organization usage	Illicit use	-Acquire an access log on a service provider side. -Impose a restriction on accessible networks, and acquire an access log internally.	<input type="checkbox"/> <input type="checkbox"/>
	Corporate Wi-Fi network, Mobile network and public Wi-Fi router etc.	Masquerade	-Collaborate with an internal authentication system. -Check access logs.	<input type="checkbox"/> <input type="checkbox"/>
5.9	Application Usage	Unauthorized operation limited knowledge	-Produce a procedure manual. (Refer to the Appendix) -Check the behaviors of an application. (e.g. data saving area, data publication scope etc.) -Appoint a dedicated data saving area for business. -Prevent users from selecting a saving area.	- <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
		Wiretapping	-Encrypt communications for corporate access.	<input checked="" type="checkbox"/>
		Malware	-Obtain applications from reliable markets. -The application permitted in the organization is decided. -Do not inadvertently authorize an access when installing an application. -Obtain the latest information on applications. (Illegal behaviors, unintended behaviors, reliable information etc.)	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
		Private uses	-Limit uses during business.	<input type="checkbox"/>
		Private uses (improper contents)	-Produce a procedure manual. (Refer to the Appendix) -Set out a corporate policy, and restrict with filtering. -Acquire a use history.	- <input type="checkbox"/> <input type="checkbox"/>
		Mixed with private data 【BYOD】	-Produce a procedure manual. (Refer to the Appendix) -Let users sign a pledge. (Refer to the Appendix) -Sort out data. (In case of using an identical application for private and business.) -Upon user's departure from a company or end of use, let users certify that they have deleted data.	- - <input type="checkbox"/> <input checked="" type="checkbox"/>
5.10	Camera Usage	Illicit use	-Paste a security seal etc. to avoid using. -Disable camera functions.	<input type="checkbox"/> <input type="checkbox"/>
		Incorrect operations. Lack of knowledge	-Produce a procedure manual. (Refer to the Appendix)	-
		Incorrect operations	-Paste a security seal etc. to avoid using. -Deactivate camera function.	<input type="checkbox"/> <input type="checkbox"/>
		Lack of knowledge	-Produce a procedure manual. (Refer to the Appendix)	-
		Phishing		
		Malware	-Do not inadvertently authorize an access when installing an application. -Disable camera functions.	<input type="checkbox"/> <input type="checkbox"/>
		Picture data leak	-Suspend location information functionality when shooting. -When publicizing pictures to outside, delete Exif. (Data, properties and attributes.)	<input type="checkbox"/> <input type="checkbox"/>
		Mixed with private data 【BYOD】	-Let users sign a pledge. (Refer to the Appendix) -Move business data to a dedicated storage area. (Quickly delete them from a Device.) -Upon user's departure from a company or end of use, let users certify that they have deleted data.	- <input type="checkbox"/> <input checked="" type="checkbox"/>
	Microphone Usage	Lack of knowledge	-Produce a procedure manual. (Refer to the Appendix)	-
		Incorrect operations. Lack of knowledge		
		Malware	-Do not inadvertently authorize an access when installing an application.	<input type="checkbox"/>

		Mixed with private data <b>【BYOD】</b>	-Let users sign a pledge. (Refer to the Appendix) -Move business data to a dedicated storage area. (Quickly delete them from a device.) -Upon user's departure from a company or end of use, let users certify that they have deleted data.	- <input type="checkbox"/> <input checked="" type="checkbox"/>
	Location Information Usage	Incorrect operations Lack of knowledge	-Produce a procedure manual. (Refer to the Appendix)	-
		Fraud	-Suspend a location information functionality if not it's not necessary.	<input type="checkbox"/>
		Malware	-Do not inadvertently authorize an access when installing an application.	<input type="checkbox"/>
	NFC Usage	Skimming	-Use a lock function when not in use. -Put a cover on chip portion.	<input type="checkbox"/> <input type="checkbox"/>
		Masquerade	-Produce a procedure manual. (Refer to the Appendix) -Activate a lock function.	- <input type="checkbox"/>
	1seg, a terrestrial TV broadcasting programs on mobile phones Usage	Private uses	-Limited uses during business.	<input type="checkbox"/>
	Bluetooth Usage	Malware	-Limit accessible equipment with a Device. -Disable Bluetooth if it's not used.	<input type="checkbox"/> <input type="checkbox"/>
		Illicit access		
		Illicit use	-Produce a procedure manual. (Refer to the Appendix) -Limit accessible equipment with a Device. -Disable Bluetooth if it's not used.	- <input type="checkbox"/> <input type="checkbox"/>
		Automatic activation of Bluetooth	-Check the applications to use Bluetooth.	<input type="checkbox"/>
	Infrared Communications Usage	Incorrect operation, Lack of knowledge	-Produce a procedure manual. (Refer to the Appendix)	-
5.11	Media Data Usage	Theft, loss and breakdown(external storage)	-Produce a procedure manual. (Refer to the Appendix) -Prepare alternative means. (USB storage, and a storage service for businesses.) -Encrypt the data domain of smartphones and external memory media.	- <input type="checkbox"/> <input type="checkbox"/>
		Remove external storage	-Produce a procedure manual. (Refer to the Appendix) -An organization lends an external storage. -Encrypt data. -Paste a security seal.	- <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
		Mixed with private data <b>【BYOD】</b>	-Let users sign a pledge. (Refer to the Appendix) -Prohibit use. -Upon user's departure from a company or end of use, let users certify that they have deleted data.	- <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
5.12	Backup/Synchronize	Incorrect operation, Lack of knowledge	-Produce a procedure manual. (Refer to the Appendix) -Check the behaviors of an application. (Data saving area etc.) -Use a backup tool.	- <input type="checkbox"/> <input type="checkbox"/>
		Coexistence of business data in backup data <b>【BYOD】</b>	-Let users sign a pledge. (Refer to the Appendix) -Protect backup data in a private storage area. (For example privately owned PCs, Cloud and external memory media etc.) -Apply encryptions in data backup. (Including privately held PCs.)	- <input checked="" type="checkbox"/> <input type="checkbox"/>



### A-3 Example of Items Described in a Procedure

Chapter number	Use case	Important point
5.1	Phone address book Usage	-Select a data saving area (Device, Cloud or external media), safety. -Designate the scope for data publication, synchronization. - 【Additional items for BYOD】 , Data classifications. (Separate saving areas for private and business.)
5.2	Phone Usage	-heads-up for manners etc. for business hour uses.
5.3	E-mail Usage	-Comply with the rules regarding mail transfer prohibition, a file attachment and synchronization etc. -Warning against wrong transmission. (Check an address and whether with or without an attachment, before transmission.) -Warning in case of using an attachment. -Communications in case of wrong transmissions. - 【Additional items for BYOD】 Data classifications. (Use separate applications for private and business.)
5.4	Schedule Usage	-Designate the scope of data disclosure. -Encode data in order to prevent unauthorized people from deciphering easily. - 【Additional items for BYOD】 Data classifications. (Use separate applications, accounts and others for private and business.)
5.5	Browser Usage	-Disable the saving function for use ID and password. (Cache) -Warning of internet access. (An access to the sites that are not authorized by an organization.) -Check whether a URL is correct, and warning against an easy connection to a short URL. - 【Additional items for BYOD】 Data classifications. (Account data and view histories etc.) (Use separate applications and others for private and business.)
5.6	Connect with Network	-Restrict using tethering.
5.9	Application Usage	-Warning for downloading and installing. (Urging to use reliable markets etc.) -Warning for use. (Data saving areas, and the extent of the effect caused by a publication, etc.) -Specify the manners and rules for use. (Judging public order and morals.) - 【Additional items for BYOD】 Data classification. (In case of using a same application for private and business.)
5.10	Camera Usage	-Specify the scope of use. -Select a data saving area. (Device, Cloud or external media.) -Warning for portrait rights. -Check the URL that is shown after a barcode read connection. - 【Additional items for BYOD】 Move business data to a designated saving area. (Delete promptly from a Device.)
	Microphone Usage	-Specify the scope of use. -Select a data saving area. (Device, Cloud or external media.) -Warning for copyrights etc. - 【Additional items for BYOD】 Move business data to a designated saving area. (Delete promptly from a Device.)
	Location Information Usage	-Specify the scope of use. -Warning that location information may be disclosed externally. -Acquire location information in accordance with an organizational policy.
	NFC Usage	-How to contact and handle, in case of a theft and a loss. -Specify alternative measures in case of a breakdown. (For an office access, and a payment.)
	1seg, a terrestrial TV broadcasting programs on mobile phones Usage	-Specify the scope of use. (For a disaster.)
	Bluetooth Usage	-Specify the scope of use. -Warning for providing and receiving data. (Check whether a Bluetooth icon is shown on a home screen.)
	Infrared Communications Usage	-Specify the scope of use. -Warning for providing and receiving data.
5.11	Media Data Usage	-Specify whether to allow it or not. (Recommend to prohibit it.)
5.12	Backup/Synchronize	-The implementation methods for back-up, synchronization and restore. -Warning for a data saving area. (Use the areas for synchronization and back-up that are authorized by an organization.) - 【Additional items for BYOD】 Protect back-up data in a private saving area. (Privately held PCs, Cloud and external media, etc.)

## A-4 An Example for Items to be Listed on Pledge

### A-4-1 Corporate Owned Version

The Level of Recommendation: ■ Strongly recommended □ Recommended

Classification	Item	Descriptions (aim)	Notes in drafting pledge	Level of recommendation
Specify the purposes of use	Specify and clarify the purposes of use.	Specify the purposes and scope of smartphone use, and remind users to observe the rules that are set out by an organization.		■
Management	An approval by an individual regarding data acquisition by an organization. (In case of data acquisition and monitoring )	An agreement on data acquisitions for smartphone uses, in order to prevent illicit uses and malware damages.	Since a smartphone is always carried, careful drafting of an agreement is necessary in paying an attention to "a privacy infringement" in case of acquiring location information. Both of systematic data acquisitions and information checking by an administrator are included.	■
	An approval by an individual for an organizational control. (In case of imposing controls and OS updates)	An agreement by an individual for an organization to change settings, limit functionalities and delete data.	OS and application updates are controlled by an organization. Systematic controls, administrator's setting changes and an instruction to a user for settings are included.	■
	Protect back-up data.	An agreement to prohibit back-up to individual owned PCs, in order to protect confidential information.		□
Report	Report when certain events occur.	An agreement to report immediately on losses, thefts and whether there contain confidential data or personal data, in order to assess the effect of an incident.	Report in accordance with the rules set out by an organization. For example, "damaged", "breakdown", "fault", "theft" and "loss" etc.	■
Prohibited matters	Modification of a terminal, OS and an application.	An agreement not to modify, in order to prevent security threats.		■
	Violation of the terms of use for terminal vendors and telecom carriers.	An agreement not to use against the intent of suppliers.		□
	Install and use of applications that are not allowed by an organization.	An agreement not to install and use the applications that are not authorized, in order to prevent the intrusion of malware.	Set out the applications that can be installed and used (A white list), or the applications that cannot be installed and used (A black list).	□
	Private use	Agree not to use privately, in order to prevent a cost increase, business productivity drops and information leakage.		□
	Lend, assign and sale to third parties.	An agreement not to let others than the user to use.		□
	Intended or negligent information leakage.	Warning under the increasing use cases for carrying data and privately sending data. In case of information leakage, take actions in accordance with a company policy.	Specify to restrict writing company information etc., and to let users to pay an enough attention not to spread or leak data inadvertently.	□
Finish using	Return terminals.	An agreement to delete the data, and to return the terminal.	Handling of data back-up.	■
Violation of pledge	Penalty	Specify that the uses are subject to the penalties as set-out by an organization.		□

**A-4-2 BYOD Version**

The level of Recommendation: ■ Strongly recommended □ Recommended

Classification	Item	Descriptions (aim)	Warnings for drafting pledge	Level of recommendation
Representations and warranties	Ownership, name of subscriber.	Let a user warrant that the subscriber is the user himself or herself.	Specify the terms and conditions for an approval.	■
Specify the purposes of use	Clarify the purposes and scope for use.	Set out the rules for the purposes of smartphone use and the scope of use, and let users comply with those.		■
Management	An approval by a user for acquiring certain data of the person by an organization.	An agreement to acquire the data for smartphone use, in order to prevent illicit uses and malware damages.	Since a smartphone is always carried, careful drafting of an agreement is necessary in paying an attention to a privacy infringement in case of acquiring location information. Both of systematic data acquisitions and information checking by an administrator are included.	□
	An approval by an individual for an organizational control. (In case of imposing controls and OS updates)	An agreement by an individual for an organization to change settings, limit functionalities and delete data.	Present recommendable configurations on OS and an application. Specify how to address troubles.	□
	Protect back-up data.	In case that business data are stored in a smartphone, urge a strict management and control when backing-up data to a privately owned PC.		□
Reporting	Reporting when specific events occur.	An agreement to report immediately on losses, thefts and whether there contain confidential data or personal data, in order to assess the effect of an incident.	Report in accordance with the rules set out by an organization. For example, "breakdown", "theft", "loss", "repair", "model type change", "assignment", and "resale".	■
Prohibited matters	Modification of a terminal, OS and an application.	An agreement not to modify, in order to prevent security threats.		■
	Install and use of the applications that are prohibited by an organization to do so.	Prohibit to install and use the applications that are prohibited, in order to prevent the intrusion of malware etc.	Set out the applications that shall not be installed and used. (Blacklist)	□
	Lend to third parties.	An agreement not to let others than the user to use.		□
	Use other terminals than applied for an approval.	Prohibit the use of other terminals than declared to use for business.		■
	Intended or negligent information leakage.	Warning under the increasing use cases for carrying data and privately sending data. In case of information leakage, take actions in accordance with a company policy.	Specify to restrict writing company information etc., and to let users to pay an enough attention not to spread or leak data inadvertently.	□
Finish using	Delete business data and applications.	Let a user delete business data and applications, in order to prevent security threats.		■
Violation of pledge	Penalty	Specify that the uses are subject to the penalties as set-out by an organization.		□