Security Guidelines for Product Categories

- OPEN POS -

Ver. 1.0

CCDS security guidelines WG
POS SWG

Revision history

Version	Date	Description
Ver.1.0	June 8, 2016	Created a new edition

■Trademarks

・All company and product names mentioned in this book are company trademarks or trademarks registered.

■Further notices

・All information provided in this book is stated at the time of publication and may change without notice.

・Any copying or reprinting of the contents of this document without obtaining permission from CCDS is prohibited.

Table of contents

1 INTRODUCTION 4

1.1 Current status of and issues relating to POS security 5

1.2 Scope of the guidelines 6

1.3 Object of the guidelines 6

1.4 Abbreviations 6

2 SYSTEM CONFIGURATION AND OPERATIONAL MODEL 8

2.1 POS system configuration and characters 8

2.2 Operation of the POS system 12

3 SIGNIFICANT THREATS TO SECURITY 13

3.1 Criminal case in the past and considerable point of view 13

3.2 Limitations to existing security measures 14

3.2.1 Security measures against security breaches 14

3.2.2 Operational conditions in the security measures 15

3.2.3 The cost of security measures 15

3.2.4 Deflection of the viewpoint of security measures 16

4 SECURITY GUIDELINES 19

4.1 The premises that need to be made when considering security measures 20

4.2 Policies on security measures 22

4.3 Security concepts for credit transactions 27

5 THE DEVELOPMENT PHASE AND SECURITY MEASURES 29

5.1 Definitions of the phases in the life cycle 29

5.2 Action required during each phase 31
5.2.1 Initiation phase 31
5.2.2 Development phase 32
5.2.3 Deployment phase 33
5.2.4 Operation and maintenance phase 34
5.2.5 Disposal phase 34

5.3 Guidance of the security measures within each phase 35

6 CONCLUSION 37

REFERENCES 38

Figure 2-1 POS system layout and human interaction 8
Figure 2-2 Example of a POS system 12
Figure 3-1 Flowchart of information leakage using the malware skimming technique 14
Figure 3-2 Suggested security measures in the previous system 17
Figure 3-3 Pertinent issues for existing security measures 18
Figure 4-1 Critical data that must be protected 23
Figure 4-2 Critical data to be protected 24
Figure 5-1 Phases in the life cycle 29

Table 1-1 List of abbreviations 6
Table 2-1: A description of the components of the POS system 9
Table 2-2 Description of the characters 11
Table 3-1 Summary of the concepts of risk 13
Table 4-1 Corresponding part of this book that corresponds to “IoT Safety/Security Development Guidelines” 22
Table 5-1 Definition of the phases 29
Table 5-2 Security measures during the initiation phase 31
Table 5-3 Security measures during the development phase 32
Table 5-4 Security measures during the deployment phase 33
Table 5-5 Security measures during the operation and maintenance phase 34
Table 5-6 Security measures of the abolition phase 34
Table 5-7 The security measures of each phase 35

1 Introduction

To date, every product industry has formulated its own safety standards. Security standards relating to organizational administration (ISO27001) and product design security assessment and authentication (ISO15408) have already been formulated, while recent years have witnessed the formulation of standards targeting control systems for critical infrastructure (plants and facilities essential to social infrastructure) (IEC62443).

With the popularity of IoT, devices in widespread use are supporting a variety of networking features, increasing security concerns. That said, it is undeniable that security standards relevant to IoT products and services are not yet sufficiently in place.

In the U.S. and European nations, moves are underway to determine security standards by using industry-specific safety standards. However, while in Japan there are tangible security concerns that may lead to the establishment of security standards, there are few areas where practical discussions have yet led to action.

The Connected Consumer Device Security Council (CCDS) was established in response to this situation. The Council is committed to formulating security standards for common devices and launching an authentication program to confirm and verify compliance with these standards in order to reassure users of IoT products.

On August 5, 2015, the Information-technology Promotion Agency, Japan (IPA) launched the IoT Safety/Security Development Guidelines Review WG to initiate discussions on security at the national level. The CCDS has come together with the IPA-WG to establish a number of proposals concerning the results of the reviews of guidelines within the CCDS.

On March 24, 2017, the results of the reviews at the IPA-WG were compiled and released as “IoT Safety/Security Development Guidelines - Important Points to be understood by Software Developers toward the Smart-society [1]“. While the IPA’s development guidelines focus on the common subjects by comprehensive approach, the CCDS field-specific guidelines is developed for locating individual industry specific safety and security promotion of design or development process.

1.1 Current status of and issues relating to POS security

With any POS other than cash, such as credit card, electronic money and gift coupons, the coupon or the reward card are utilized, as with cash, in the storing of proceeds. While transactions involving credit cards and electronic money are protected by each company's internal security procedures, in most cases where an operator receives and stores payment directly in the form of cash or gift coupons, recent expansion of payment types has lead to an increasing possibility of deliberate fraud or of customers being accidentally short changed by the POS cashier.

There has been progress in recent years to automate the system via POS self-service automatic payment machines, but more needs to be done to improve the security of these machines, as they are vulnerable to conventional theft, and cyber crime, of which the latter is on the increase generally. In the United States, there have been many cases of information (credit card numbers etc.) being stolen through the use of physical media malware, which is surreptitiously installed in the POS control module. This malware is then operated locally or by remote control.

It is therefore clear that, as there has been an increase in cyber, physical and combined crimes related to POS systems, protecting sales information has become even more vital. However, while the spread of IoT technology in society means that the demand for security measures has increased, several issues are hindering effective security management, such as a lack of investment in store operations and POS systems, insufficient training, unavailability of staff, and employment of foreigners etc.

This form of information theft is becoming more common because of the increasing awareness of hacking techniques and the falling prices of the necessary equipment required to perform them. As methods of information theft are becoming more sophisticated, the number and seriousness of such crimes involving malware is increasing, particularly as the criminals are sometimes company insiders. This makes it essential to fully vet all insiders, such as developers, operators, maintenance personnel and clerks. This measure is unnecessary for traditional security points, which are only subject to external attack as there are no insiders with any malicious intent.

With respect to credit transactions, there are security standards required by the operator, such as the security measures applied by the international brands (VISA, MASTER, JCB, etc.) in the PCI (Payment Card Industry), and additional enhanced security measures (EMV standard) by the IC of the particular media type. However, a feature of our country is that there is little progress in improving the standards of POS because of the high costs

and operative skills required to apply the necessary measures for the individual requirements and business operations of each particular merchant.

Strengthening of credit transaction security is addressed by measures such as government-led initiatives, disconnecting sensitive information about credit and electronic money payments from the POS system, and by employing trustworthy operators. The following guidelines are intended to outline effective security measures against direct attack in terms of the POS operations previously mentioned.

1.2 Scope of the guidelines

These guidelines are intended to apply to the POS system, but only in terms of the POS terminal, the POS server and the components present therein. It does not apply to the external connection network supporting the POS that includes an external computer.

In addition, these guidelines are not intended as a recommended standard of data and protection requirements for the PCI (Payment Card Industry) and EMV (Europa Master Visa) as a replacement of any existing standard. Neither are these guidelines intended to cover the protection requirements with respect to magnetic track information, etc., as this is already covered by the PCI-DSS standard. For example, in the case of PCI-DSS (Payment Card Industry Data Security Standard), the standard is PAN (Primary Account Number: card number).

1.3 Object of the guidelines

These guidelines are intended to be a summary of the considerable design and development process involved during the implementation of the appropriate security measures used in devices that utilize IoT. The guidelines are for the benefit of:

1) The designers and developers of a device
2) The person in charge of the design development project
3) Managers responsible for the budget and appointment of the personnel of the device design project

1.4 Abbreviations

The abbreviations used in the Development Guidelines are as follows:

Table 1-1 List of abbreviations

Abbreviations	Term in full
CAT	Credit Authorization Terminal
CCDS	Connected Consumer Device Security Council
EFT	Electronic Fund Transfer
IEC	International Electrotechnical Commission
IoT	Internet of Things
IPA	Information-technology Promotion Agency
ISO	International Organization for Standardization
MICR	Magnetic Ink Character Reader
MSR	Magnetic Stripe Card
NIST	National Institute of Standards and Technology
OLE	Object Linking and Embedding
POS	Point of Sales
SWG	Sub Working Group
WG	Working Group

2 System Configuration and Operational Model

2.1 POS system configuration and characters

The POS system generally has two main functions: account keeping and storage of proceeds. The operator who keeps records is called a checker and the operator who collects proceeds is called a cashier. Both operations are often performed by one person, but a single POS terminal may be operated by two people at a busy food supermarket, if required.

In department stores, it has become standard practice to perform sales at front of desk, and store proceeds via a centralized cash register system kept off the shop floor. It is common for one person at the store to perform both operations.

The basic system configuration of the POS is shown in Fig. 2-1.

The PC-based control module of the POS operates the module controls of peripheral devices such as the display and scanner, POS keyboard, card reader, change machine, receipt printer and cash drawer.

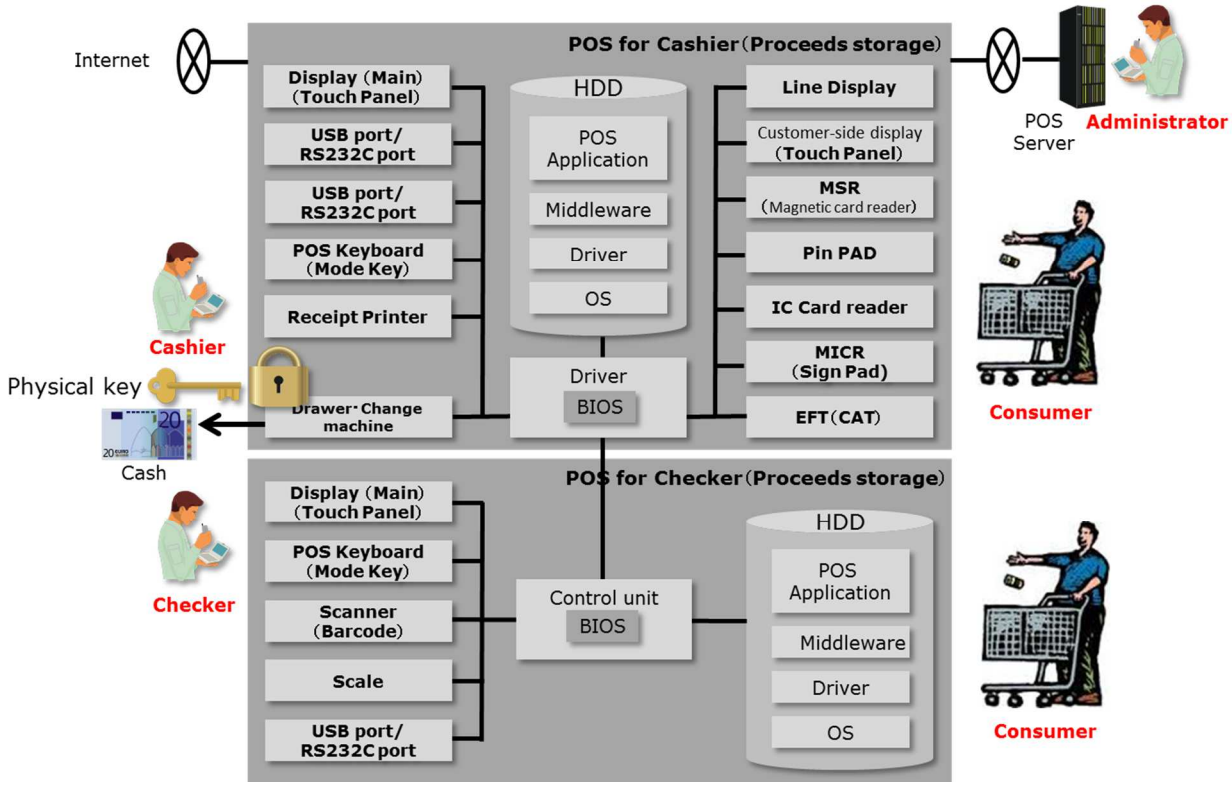

Figure 2-1 POS system layout and human interaction

A detailed description of the components of the POS system is shown in Table 2-1, and a detailed description of the characters is shown in Table 2-2.

Table 2-1: A description of the components of the POS system

No.	Component	Function
1	Control	Computer controlling devices such as MSR or Drawer in the POS and Windows are often equipped with an OS. A hard disk (HDD) is often part of the Control.
2	HDD (Hard Disk Drive)	A HDD is part of the control department. The OS, a driver, middleware applications and the software for maintenance are installed on the HDD.
3	BIOS	A system such as a boot device which provides control. Users can set a password to access the BIOS. This is required to prevent unauthorized access to the boot from boot media, such as a USB memory or a CD-ROM drive, other than the HDD.
4	Display	The display function allows the transaction menu and processing results to be displayed on the POS.
5	Customer-side Display	Displays customer relevant transaction menus and processing results on a display for customers. In addition, the function is also provided to perform verification by inputting age limit confirmation, etc., for the customer via the touch panel.
5	USB Port/ RS232C Port	The USB/RS232C port allows personal computers and peripherals to be connected via a USB / RS232C cable.
6	MSR (Magnetic Card Reader)	A general term for plastic devices that read magnetic stripe cards. MSRs are mainly used to read magnetic card information and make credit payments at the POS when the customer provides their card. There are also POS systems that include MSR.
7	Scanner（Barcode）	A device for reading a bar code which is mainly used to read product information at POS.
8	POS Keyboard	One of the input devices at POS. The POS keyboard works in the standard manner by transmitting character

		signals to the POS through typing. It is used for the overall operation of the POS.
9	Touch Panel	Another POS input device. The touch panel also transmits character signals to the POS by typing on the keys. As with the POS keyboard, the touch panel is used for the overall operation of the POS.
10	Mode Key	The name used for keys that switch the POS display. POS functions such as discounts are often the name of a mode key.
11	MICR（Sign Pad）	A magnetic ink character recognition device that recognizes input characters via a Sign Pad (LCD handwriting input device) when credit cards are used.
12	Scales	The device which weighs goods when appropriate and transmits the weight to the cash register/POS.
13	Pin PAD	The device that is used to enter a personal identification number when an IC credit card is used in a shop.
14	IC Card Reader	The card reader device with a built-in IC chip (integrated circuit) on which is recorded required information (data). This device is used at a POS to read a plurality of information such as the amount of prepaid electronic money remaining, credit information, point information and other customer information.If required, the IC card reader can be connected to the serial communication port.
15	Receipt Printer	A device used to print hard copies of a receipt showing the amounts of money in the registers.
16	EFT（CAT） ※Not covered by these guidelines.	EFT is a POS system for electronic payments that is used to withdraw money from an account by presenting a bank cash card at the checkout at a supermarket etc.CAT is a credit inquiry terminal which performs a credit check prior to payment. This involves confirming the validity of the card by contacting the credit card call center to ask for a credit check.
17	Drawer	An actual drawer that is usually located under the cash register and POS. It is used to hold cash, cash vouchers

		and complete non-electronic transactions.
18	Change Machine	The change machine, which dispenses the correct change during transactions as specified by the POS. It is also used to receive payments.
19	Line Display	The customer display, which is set on a height-adjustable telescopic pole to complement the shop environment. It can be set in four directions.

Table 2-2 Description of the characters

No	Character	Role
1	Checker	The operator at a two-person cash register, who is mainly in charge of recording products, and exists as part of a two, not a one-person system register.
2	Cashier	The operator at a two-person cash register who is mainly in charge of payment.
3	Manager (Person in Charge)	As a manager has more authority than other positions such as the cashier and checkers, he or she is able to use all POS functions.

2.2 Operation of the POS system

Figure 2-2 shows one possible POS system:.

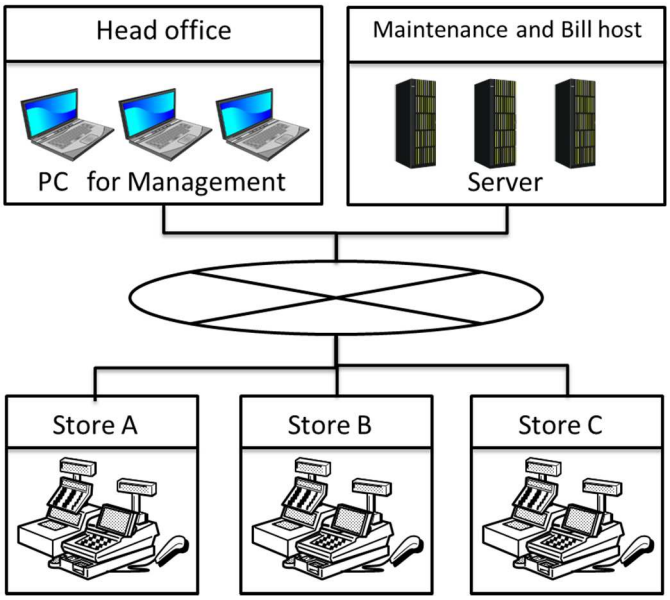

Figure 2-2 Example of a POS system

The purpose of a POS system within a store is to exchange product and credit information via a corporate intra-network or over the Internet.
Other functions, such as sales, customer and inventory control, are performed at a management station in the head office. Maintenance, both hardware and software, is also included in operational duties.

- Hardware maintenance
  Repair or replacement of POS terminals and peripheral device components by the manufacturer or factory.
- Software maintenance
  Technical assistance, development and inquiries in the event of failure from the developer.

POS terminal systems have to be introduced to a wide range of businesses, such as department stores, food supermarkets, grocery stores, fashion boutiques, restaurants and florists. Similarly, the customers that need to be introduced to POS systems also vary widely depending on the business content, installation locations, and the number of staff in the workplace.

3 Significant Threats to Security

3.1 Criminal case in the past and considerable point of view

Key Features of Common Breaches of SecuritySituations and operational failures that increase the risk of breaches of POS-security are listed below:

Table 3-1 Summary of the concepts of risk

No.	Security Breaches	Notes
1	Unauthorized Intrusion	Breaches of malicious intent are possible. These may involve the use of USB devices that are hard to trace.
2	Leak of information	The publishing of interface specifications on line that can lead to the development of engineered malware, generally suggests that the source has been company leaked information.
3	Operation Inadequacy	There is a risk of malware becoming installed on a POS system due to operational deficiencies that need to be targeted, such as overt USB ports.
4	Unauthorized modification	A risk of unauthorized remodeling can occur due to a regular device distributing in the circulation market.
5	Spread of the damage caused by IoT	As the network via ‘smart-society’ expands, it increases the chance of exposure to malware that has to be installed on the POS system physically at present. In that case, an existing risk is doubled.

Figure 3-1 is an example of a security breach using malware

In the above case, the product specifications, such as software, are uploaded to an internet site by someone considered to be a regular developer, and then downloaded by a malware developer to develop malware. This is then installed to a POS system with operational media deficiencies, such as allowing USB memory access by a local operator.

As with other installation methods, malware is usually downloaded/installed through malicious Web links and E-mail attachments that are opened by the end user when the POS is connected to an Internet or email enabled PC.

Another example of a technique is skimming by connecting an unauthorized device to a POS terminal system physically to obtain card data. This data, which is then leaked out via malware and skimming, is bought and sold by fraudsters to create forged credit-debit cards,

etc.

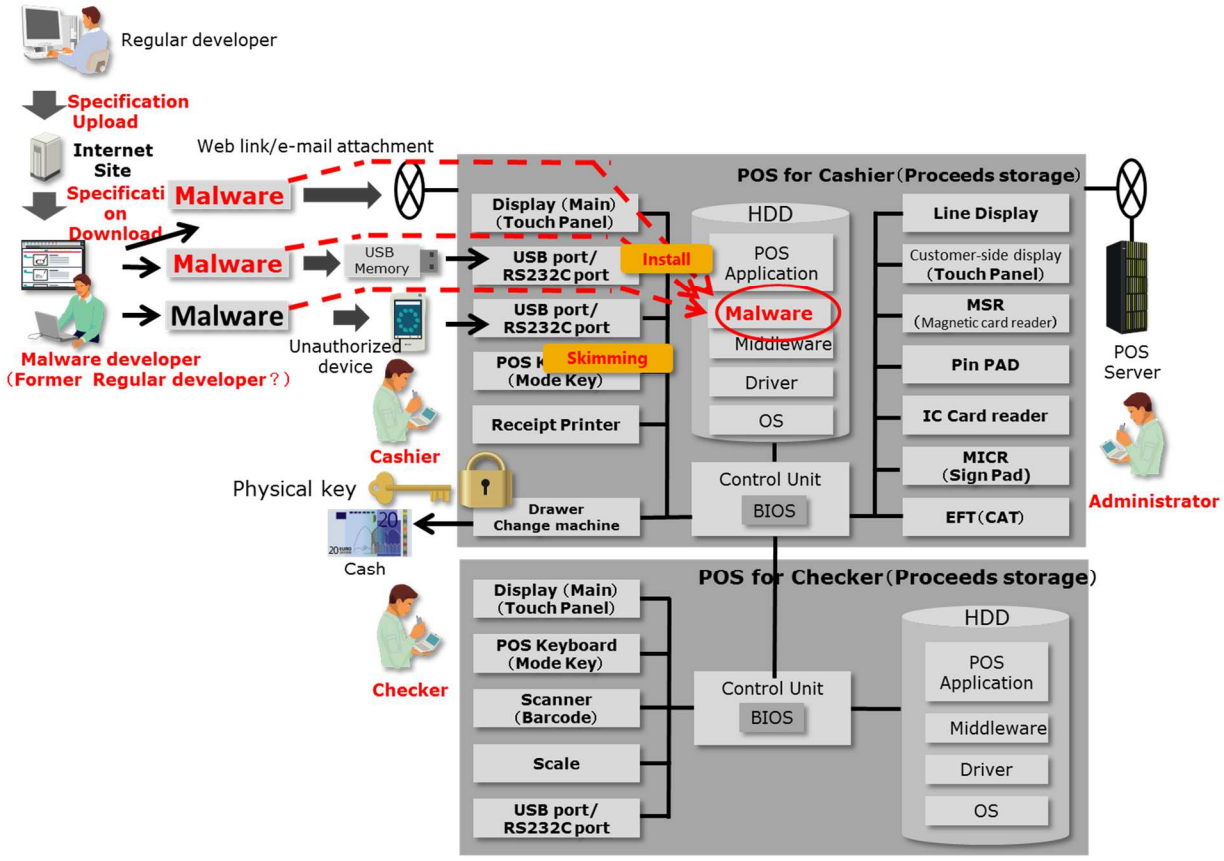

Figure 3-1 Flowchart of information leakage using the malware skimming technique (Overseas cases)

3.2 Limitations to existing security measures

As mentioned in the previous section, it is clear that there are many points that are not adequately addressed by existing security measures.

When considering counter measures against breaches of POS security, the problems caused by conventional thinking are explained as follows:

3.2.1 Security measures against security breaches

In the classic case of the security breach described in Section 3.1, the assumption is that the threat is only from external attacks. However, supposing that there can be no attacks from malicious insiders is unacceptable when using POS. As has been explained in the “Unauthorized Intrusion”, “Information leakage” and “Deficiencies in the Operation” sections, there is always the possibility of an insider being involved in system manipulation and fraud.

In terms of “Unauthorized Intrusion”, it is supposed that an insider is involved because an unauthorized device must have been physically connected to a POS system by USB etc.

In terms of “information leakage”, interface specifications must have been published on the Web by a developer.

In terms of “deficiencies in the operation”, the possibility that the criminal must have known the vulnerability of the POS that had been targeted must be considered.

It is therefore imperative that POS security measures be considered in terms of internal, as well as external attacks. For example, it needs to be understood that instances of “unauthorized intrusion” must involve an insider.

3.2.2 Operational conditions in the security measures

Due to the difficulties encountered nowadays when trying to hire suitable staff, it cannot be assumed that cashiers or POS operators will always be highly skilled and extremely honest. This means that it is extremely difficult to force staff to conform to complicated operational techniques and security measures through excessive management. In addition, the way that a POS is used varies according to factors such as the store and how busy it is, so the best ways to rectify failures in security measures vary from case to case. No matter how good security measures are, they will not be effective if they are not adapted to actual on-site operational conditions.

It is therefore necessary for security measures to be flexible if they are to be of practical use. There is also the problem of constraints placed on an operation serving to complicate effective implementation of POS security measures.

Since security measures should be considered under such circumstances, acceptable security measures in a store cannot be implemented by only conducting conventional threat analysis and by not considering all possible risks. Thus, new analysis methods that take into account all relevant threats and risks, as well as being suitable for the nature of the operation, are required.

3.2.3 The cost of security measures

Despite effective implementation of security measures often being expensive under difficult situations, such as those described in Section 3.2.1 and 3.2.2, allocated budgets are often limited. However, security is a necessary expense that needs to be considered in

the use and maintenance of POS.

When allocating security budgets, the subsequent enforcement and checking of measures also needs to be considered along with the initial cost of introducing the measures.

As shown in Figure 2-1, it is necessary to check and supervise the results of work performed with POS because the cashier, checker or manager may have malicious intent.

Although the verification and management of work should be reduced by security measures, it will never be reduced to nothing, so this also needs to be included in the costs and risks. In addition, it is also necessary to consider the turnaround time required for repairing and replacing service parts.

In order to effectively implement security features on a component of the system, it should be considered unacceptable for security overhauls of that component to have to take place in special locations, such as in “a secure room”. In other words, if advanced security features such as tamper-resistance are added to components, overhauling of the system cannot only take place in the secure room, as that may create a situation where repair parts are not readily available during maintenance and operation. It is therefore necessary to consider that it is undesirable to accept security that limits practical use in terms of time, as well as in cost.

3.2.4 Deflection of the viewpoint of security measures

Figure 3-2 relates to the case described in Section 3.1, and shows the contents of the security measures proposed by US-Cert (United States Computer Emergency Readiness Team).

The measures on the right side of the figure, and measures such as “access restriction to BIOS” and “boot prohibited from USB” under the right side of the figure, are all designed to protect the information on the hard disk drive.

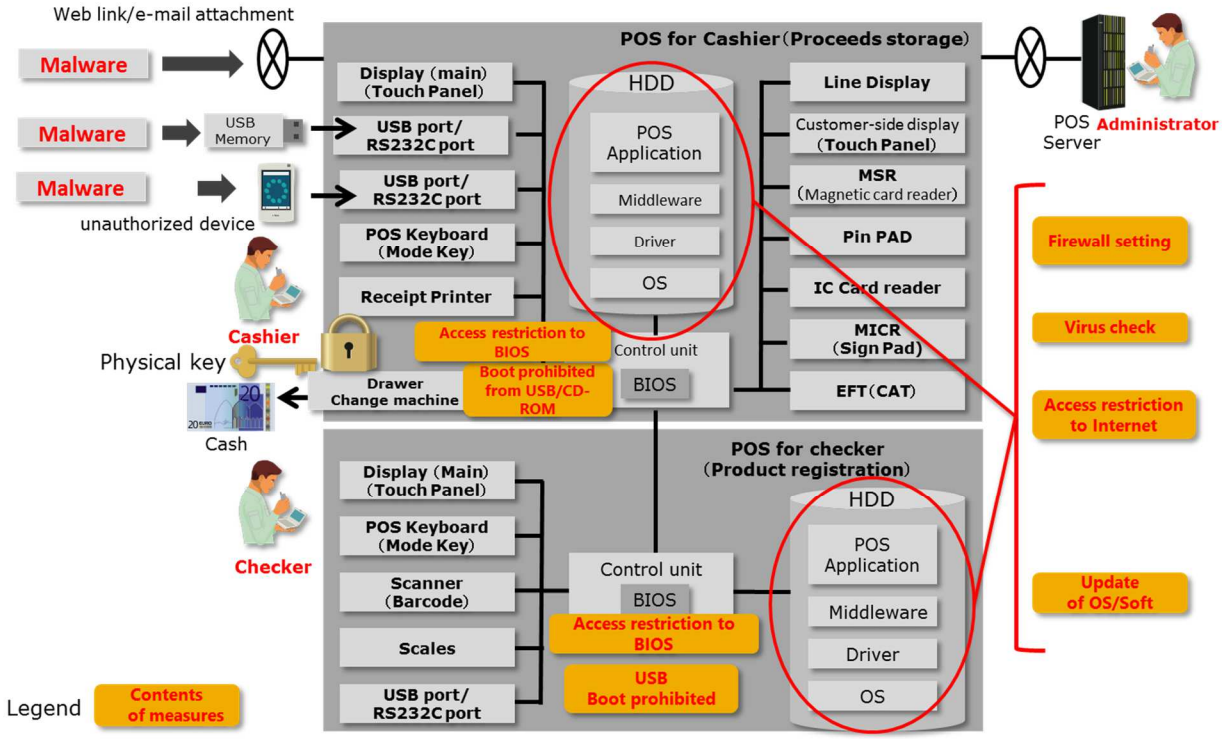

Figure 3-2 Suggested security measures in the previous system

The application should be updated frequently to reflect changes in the service contents of the store.

In the above situation, if any item to be managed is missing even one of the required security measures, the administrative burden may be increased due to an attack from a malicious individual. This would mean a loss in function in the overall management of the system.

Another issue to consider is that proposals for security measures cannot always be applied during certain times. For example, a suggested security measure could be a virus check. However, it may not be possible to implement virus check software of the resident type (virus Buster) due to the constraints of the CPU, memory requirements or the way an application is used in a particular working environment of a traditional POS system. Furthermore, although virus updates are freely available, updating virus systems means waiving downloading restrictions. Another problem is that it is difficult to monitor and prevent a worker committing an illegal act or doing something inappropriate by mistake.

The pertinent issues for existing proposals are summarized in Fig. 3-3.

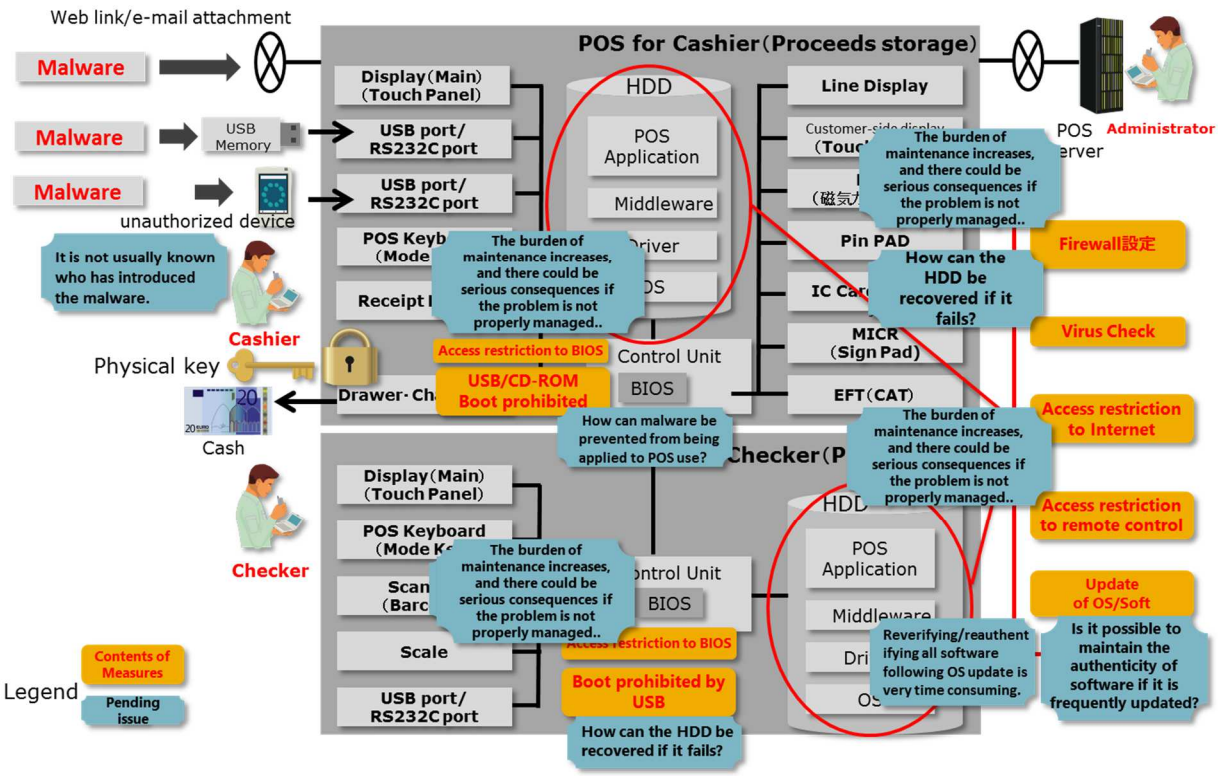

Figure 3-3 Pertinent issues for existing security measures

4 Security Guidelines

As described in Chapter 3, it is vital to consider the best security measures against risks such as information leaks and connection of an unauthorized device due to the constant threat of internal crime and the unknown level of sophistication of any attack on the system.

In terms of the ultimate goal being to protect the information assets in the HDD, which is the usual scenario, listed below are some of the main problems of ensuring effective security measures:

(a) Since there are usually a large number of items that need to be protected, managers may be unable to perform this task effectively. The problem is compounded if a system has a large number of terminals.
(b) OS and firmware are based on package software such as Microsoft Windows. While OS security patches or updated versions of the OS are released periodically, it is very difficult to update them for local use.
(c) Due to the difficulties of updating OS, software and firmware, the increased necessity for re-inspection and re-certification are often not considered.
(d) There may be inadequate protection against system failure and the inability to recover lost data.
(e) Proposed security measures may not be applicable for the system being used.

It can be seen that for measures to be effective, the operational realities, in terms of the actual purposes of the system, must be considered. The following guidelines list the premises that need to be made to ensure adequate security.

4.1 The premises that need to be made when considering security measures

❒ **Premise 1**: Developers, operators, users and maintenance personnel cannot be trusted (The ethical view that human nature is basically evil).

In the case described in Chapter 3, it is assumed that malware developers referred to specifications related to the POS system that must have been internally leaked. There is also the possibility that an insider might be involved because it is necessary for the unauthorized device or devices to be physically connected to the POS terminal system.

Therefore, it has to be assumed that system developers, users and operators are all untrustworthy when setting up security measures.

❒ **Premise 2**: The operators, users and maintenance personnel involved in POS operation are incompetent and immoral.

As described in Premise 1, it is necessary to presume that the connection of an unauthorized device to the POS terminal system by insiders was due to either an immoral or an incompetent act. In addition, it also needs to be assumed that the staff has not been properly trained, perhaps as a result of the current trend towards higher staff turnover. This means that it cannot be presumed that complicated security operations and procedures can be correctly assimilated by POS staff.

❒ **Premise 3**: Interface specifications have been published.

As described in Chapter 3, it is supposed that any malware introduced to a POS peripheral device via the connection of an unauthorized device to a POS terminal has utilized the interface specifications of the POS peripheral device that have been referred to online by the malware developer.

Interface specifications are standardized for international unification by an OPOS technology conference to allow open access, a variety of POS terminals, and development of POS production and applications. This means that interface specifications which can be integrated into a POS system easily, such as OLE for Retail POS, are freely available on the Web.

In addition, because these specifications may evolve at any time, and the standard specifications of the interfaces for all devices mostly used by POS have been determined,

it is extremely difficult to conceal specifications from malware developers as they have been published, distributed and are in general use.

❒ **Premise 4**: An illegally remodeled and unauthorized device may be connected to the system.

As described in Chapter 3, it is physically possible to connect an unauthorized device for the following reasons:

- There have been cases of stolen card information being obtained by connecting an unauthorized device to the POS system as part of the skimming process.
- It is physically possible to connect the unauthorized device because the POS terminal has a multi-purpose port (such as a USB or serial port).

Therefore, when considering security measures, it is necessary to assume that tampered or unauthorized devices may be connected.

❒ **Premise 5**: There are unacceptable operational constraints on the implementation of security measures.

As explained in Section 3, although a virus check may be proposed as a security countermeasure, it might not be able to be implemented due to limitations of the use of the POS. Therefore, when reflecting on operational constraints, it is necessary to accept the premise that there are security measures which cannot be applied.

4.2 Policies on security measures

Following the premises as described in the previous section, the policies for performing security measures are described below.

The measures are presented by comparing the 17 sections of the “IoT Safety/Security Development Guidelines” document, which was published by IPA in advance of this document.

Table 4-1 Corresponding part of this book that corresponds to “IoT Safety/Security Development Guidelines”

"Smart-society development guidelines"			Corresponding part of this document	
Major item		Guideline	Chapter No.	Overview
Policy	Making corporate efforts for the Safety/Security of the Smart-society	Guideline 1 Formulating the basic policies for Safety/Security	n/a	The formulation of the basic policies is not applicable in this book.
		Guideline 2 Reviewing systems and human resources for Safety/Security	n/a	The reviewal of the structure and human resources is not applicable in this book.
		Guideline 3 Preparing for internal frauds and mistakes	Guideline 5	It is described how to detect internal fraud or mistakes.
Analysis	Understanding the risks of the Smart-society	Guideline 4 Identifying the objects to be protected	Guideline 1	It is describe for prioritization of the information and assets to be protected, and selection of the objects to be protected.
		Guideline 5 Assuming the risks caused by connections	Guideline 1,5,8	Assuming the risks caused by connections, it is described for strengthening of traceability depending on prioritizing of the objects to be protected, and impact of unexpected at the time of connection.
		Guideline 6 Assuming the risks spread through connections	Guideline 1,2	Assuming the risks spread through connections, it is described for prioritization for the object to be protected and localization of the domain that is to be protected.
		Guideline 7 Understanding physical security risks	Guideline 8	Assuming the physical risks, it is described for strengthen the traceability for the device.
Design	Considering the designs to protect the objects to be protected	Guideline 8 Designing to enable both individual and total protection	Guideline 2～6	As an example of implementation, it is described for the scope of the measures, the level of the measures and measures examination.
		Guideline 9 Designing so as not to cause trouble in other connected entities	Guideline 5,7,8	As an example of implementation, it is described the abnormal detection and the study on countermeasure.
		Guideline 10 Ensuring consistency between the designs of safety and security	Guideline 6	It is described for securement of the flexibility and the ease of carrying out of management by implementing the security measures at the lower layer.
		Guideline 11 Designing to ensure Safety/Security even when connected to unspecified entities	Guideline 4	It is described for the study of the mechanism that does not fatal if specifications are published.
		Guideline 12 Verifying/validating the designs of safety and security	Guideline 6	Same as Guidelines 10
Maintenance	Considering the designs to ensure protection even after market release	Guideline 13 Implementing the functions to identify and record own status	Guideline 5,7	It is described for mechanism to detect the program which is being executed, identify and record own statusor functions, or maintain safety/security after the own status the passage of time with the introduction of traceability.
		Guideline 14 Implementing the functions to maintain Safety/Security even after the passage of time	(Same as above)	Same as Guidelines 13
Operation	Protecting with relevant parties	Guideline 15 Identifying IoT risks and providing information after market release	Guideline 8	It is described for strengthening of traceability that is required after market release. The transmission of information is not applicable in this book.
		Guideline 16 Informing relevant business operators of the procedures to be followed after market release	n/a	Thorough to the well-known to relevant business operators is not applicable in this book.
		Guideline 17 Making the risks caused by connections known to general users	n/a	Thorough to the well-known to general users is not applicable in this book.

❒ Policy 1: Prioritize the information and assets that need to be protected

It is inefficient to protect all information and assets equally, and the cost of doing so is also unnecessarily large.

On the other hand, the types of information that are targeted by criminals are limited.

It is therefore necessary to prioritize the targets that should be protected and determine what information and assets are critical.

In particular, since a previously occurring crime is likely to reoccur, it is sensible to use lessons learnt from previous attacks when deciding what information and assets should be protected.

Level	Target for the protection with existing standard ※ and frame	Target for the non-protection with existing standard ※ and frame
High	・PIN ・Magnetic card data	・Cash-receipt-and-disbursement command ・POS sales details data ・Point member number
Medium	・Card number (the log data including the card number is applicable)	・Card data (On the memory in the application)
Low	–	Log data not including the above

Figure 4-1 Critical data that must be protected

❒ Policy 2: To minimize or disconnect the domain that is to be protected

In terms of protecting against internal crime, the larger and the more complicated the domain, the greater the burden of the measures and maintenance required, and the more likely it is for omissions in protection to occur. Therefore, the domain to be protected should be as small and simple as possible. In terms of strength of measures, flexibility of operational and cost, a simple structure with a less frequently updated domain is overwhelmingly more beneficial than a complex structure with a frequently updated domain, even if the same date is being protected in both cases.

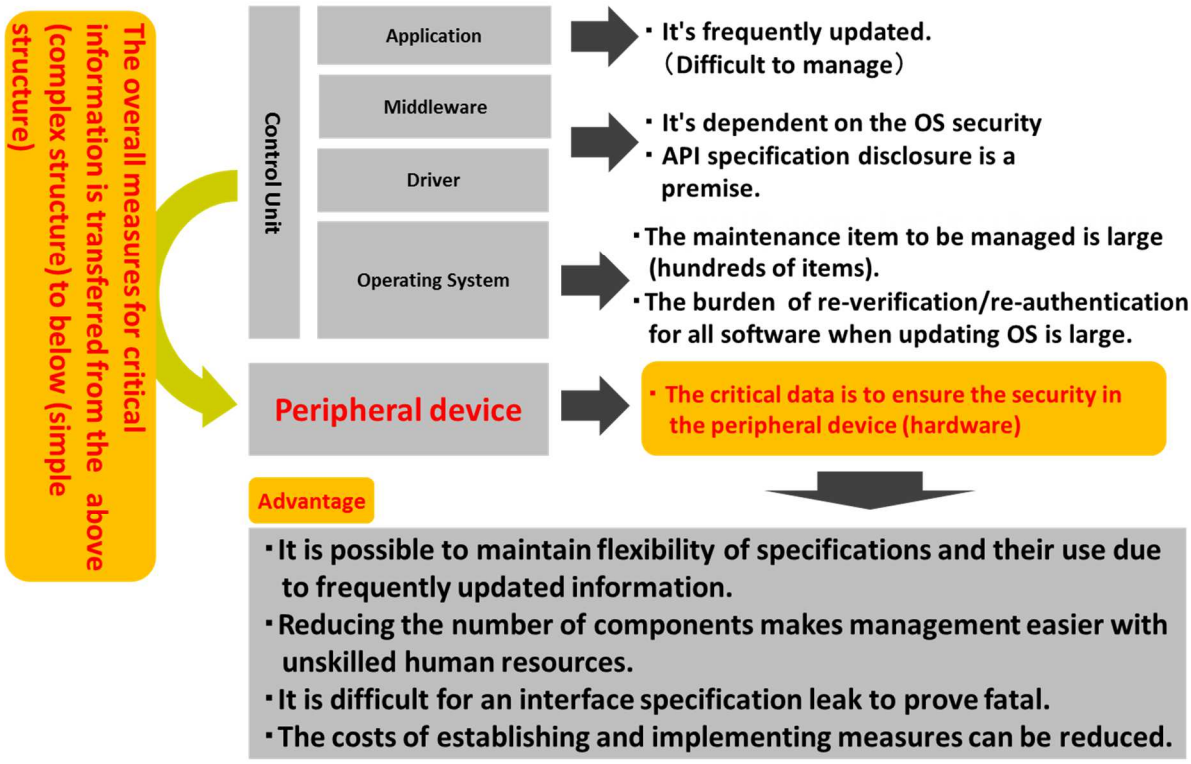

Figure 4-2 Critical data to be protected

❒ Policy 3: Change the amount of action taken according to how critical it is to protect the data.

In order to obtain the maximum effect with limited resources and budget, adjusting the amount of action taken in accordance with the importance of the data to be protected improves flexibility and reduces costs.

❒ Policy 4: To adopt a coding mechanism that does not fail if specifications are published.

As described in Premise 3 of Section 4.1, it can be extremely difficult to manage and conceal information if the standardized interface specification has been widely circulated, which is often the case. Thus, it should not be disastrous if specifications are published, and the most effective way to achieve this is to use modern encryption technology. With this technology, although the technology itself, its algorithms and the specifications may be well known and easily available by anyone, the data is protected by the complexity of the decryption calculations and careful management of the encryption key. If the interface specifications are encrypted, it can prevent an interface being taken over even if the specifications are published.

❒ Policy 5: To adopt a mechanism for replacing security measures that cannot be applied.

As mentioned in Premise 5 of Section 4.1, there may be measures that cannot be applied due to operational constraints. In such cases, alternatives to these measures need to be considered.

For example, if a virus check cannot be applied, it would be necessary to substitute the virus check with another mechanism of virus (malware) detection (Execution program monitoring) that is equally effective.

One alternative is to introduce a white list structure for detecting a program (Execution program monitoring) that is not permitted to run. This ensures comparable safety by blocking the activation of non-software registered on the white list.

In addition, if there is a deficiency in the registration process of the white list, due to the risk of the malware not being correctly registered on the list, the management man-hours for detection and verification are expected to be included as acceptable costs.

❒ Policy 6: To ensure flexibility of the existing specifications and operations as much as possible

Generally speaking, in a system designed to have a plurality of hierarchies, it is preferable for the lower layer to have versatility and a simple functional structure that allows security restrictions to be imposed at that level. This is because if a multitude of constraints have to be implemented in the upper layer, then there are excessive restrictions that have to be imposed to specifications and practical use, and flexibility is lost. In other words, it is much easier to implement security measures at the lower layers than at the upper ones.

❒ Policy 7: To keep the costs of implementing measures as low as possible

Security measures cannot be effective for the whole of society if the cost of implementing measures and operational maintenance is not low. This is achieved by clearly classifying the information and assets to be protected, minimizing the domain size to be protected as much possible, and realizing the protection at a lower level.

On the other hand, if all the security countermeasures are completed by a particular piece of software, or device, etc., this is disadvantageous not only in cost, but also in the ease of

an omission being made. Such an approach will also make it difficult to ensure the flexibility of specification and operation.

As described in the Premise 4 of Section 4.1, it is necessary to prevent tampered or unauthorized devices being connected. However, if the security measure is applied only to the regular device with a tamper-resistant mechanism, this will increase not only the cost of the POS terminal, but it will mean that it can only be repaired at a repair center with advanced security measures. As a result, not only the maintenance cost rises, but also its lead time becomes longer, and the flexibility of the use of the terminal becomes greatly diminished.

Therefore, a more effective method is considered to be the introduction of traceability in order to compensate for the security deficiencies of software and devices. Including the appropriate traceability function isn't a significant obstacle in terms of practical use and maintenance, and it also maintains flexibility.

The advent of the age of IoT is expected to be advantageous as a future effective security measure, since it can be expected that the infrastructure needed for traceability will be greater and the costs will be lower.

As a final point about traceability, not only the operational phase, but also the destruction phase should be considered.

❒ Policy 8: Strengthen the traceability.

When using POS, strengthening of traceability is required in the following three areas:

(1) Traceability of information properties for important devices

It is usually the case with POS operations related to the processing of returned-goods that once the receipts for the returned-goods are collected from a customer, and the processing of the returned-goods is performed after checking the past transactions, it is possible to complete return processing without a receipt on-site. This means that even if there have been no previous transactions, it is possible to remove money, coupons etc. via a bogus return processing operation.

Thus, a log of credit transactions and the processing of receipts and payments is maintained to ensure that payment processing is not accepted if there is no evidence of past transactions. This is done by detecting any tampering with a critical device, such as a card reader or a change machine, that internally processes critical physical assets and information.

(2) Traceability of important devices for maintenance

As described in Premise 4 of Section 4.1, the traceability of important devices to be managed needs to take into account the possibility of “an illegally remodeled and unauthorized device that may be connected to the system”.

This means that a mechanism to record, notify and inspect the removal of each device is required because leakage or loss of critical information and assets can be caused by connecting an unauthorized device.

(3) Traceability of maintenance work

The following possibilities must be considered in terms of the traceability of maintenance work.

1) The security may be compromised due to a mistake that occurs during key encryption, even if the task is completed with critical devices in the manner described in the above section “(1) Traceability of assets in critical devices”.
2) Loss or leakage of critical information initiates unnecessary maintenance work, such as a change machine becoming locked due to the physical key being lost by a person of malicious intent.

It is necessary to ensure traceability and verification in order to guarantee that maintenance tasks such as encryption key configuration and a regular change of the physical key in the encrypted communication are properly executed.

4.3 Security concepts for credit transactions

Security measures for credit information relating to credit transactions should implement measures on the basis of the “Action plan for the strengthening of security measures in credit card transactions, 2016” (H28.2.23 publication) of the “Credit Transaction Security Council”. These have been defined separately below:

(1) POS credit transactions must be separate from credit processing functions

To enable protection during credit processing, the following items are required as security information:

- Card information (magnetic/IC)
- Personal identification number (PIN)

Handling of this sensitive information should be separated from POS physically and functionally, as specified in the implementation plan.

(2) Non-retention of security information

The purpose of separating the payment procedures from the settlement procedures of the POS is to remove unnecessary card information being retained on the POS system. This is achieved by not recording the card information from the terminal dedicated to settlements.

(3) Dedicated security standards for credit transactions

Security standards for credit processing, as well as international and other certification standards have been established and defined by each international brand of credit card. These standards are in addition to the policies that are listed in (1) and (2), since the certification for international brands is required to be based on EMV and PCI standards.

5 The Development Phase and Security Measures

5.1 Definitions of the phases in the life cycle

The system development has a life cycle that continues until planning can be disposed with. It is important to consider security during every phase of development.

This chapter provides an overview of a typical system development life cycle (SDLC), and the action on security that takes place during each phase. More details can be found in the following publication: NIST SP800-64 “Security Considerations in the System Development Life Cycle”.

The system development life cycle can be roughly divided into the following five phases.

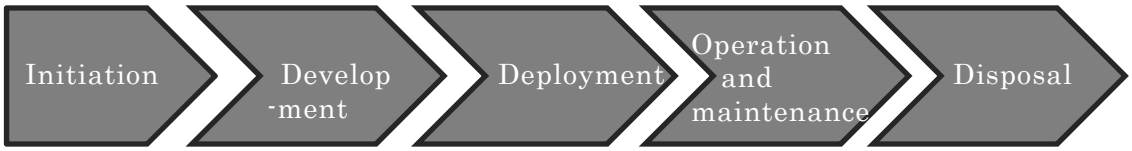

Figure 5-1 Phases in the life cycle

Table 5-1 Definition of the phases

Phase	Description
Initiation	During this phase, the system requirements are clarified and purposes are documented. Taking security into consideration is very important in the first phase of SDLC. Security activity in this phase includes the following: • Clarifying the outline of business requirements in terms of confidentiality, integrity and feasibility. •Classification of information and clarification of handling requirements such as transmission and preservation of personal information etc. • Clarification of the privacy requirements. Evaluating the security of the whole project from the start will lead to savings in cost and time by creating the appropriate risk management plan in the early stage of development and allowing concerned parties to be notified in advance.
Development	Design and development of the system takes place in this phase. The main security activities in this phase are as follows: • Performing a risk assessment study to obtain results that will supplement the baseline security measures.

	• Analyzing security requirements. • Performing functional and security testing. • Providing documentation for system and practical use approval. • Designing security architecture.
Deployment	During this phase, further development of the system takes place following an acceptance test. The main security activities in this phase are as follows: ・Adaptation of the security measures to the system's parameters. ・Planning and executing activities suitable for the system. During this phase, it is usual to conduct a test of adherence to security management policies. ・Complete authorization procedures for managers of the system.
Operation and maintenance	This phase represents standard operation of a system, which can be changed at any time by adding new hardware and software. The main security activities in this phase are as follows: ・Establishing the steps and procedures for safety operations and providing continuous monitoring of the security management measures for the system. ・Implementing reauthorization, if necessary.
Disposal	The final phase occurs if it is necessary to provide a controlled shutdown of a system, protect important information and transfer data to a new system. The main security activities in this phase are as follows: ・Purging media records ・Discarding the hardware and deleting the software

5.2 Action required during each phase

Below is a description of the security measures that need to be taken in each phase of the life cycle of system development outlined in the previous section.

Since the POS is the target of development, the word “system” in “system development” has been replaced with the word “product”.

5.2.1 Initiation phase

In the initiation phase of the life cycle of product development, the following security measures are required:

Table 5-2 Security measures during the initiation phase

No	Life cycle of product development
1	Formation of a security plan As the initiation phase is the first step of the product development cycle, it is vital to make a plan for security from the outset. The following procedures are normally carried out in a security plan. ・Determination of the important role security will play in product development, especially in terms of the information about the system security that will be disseminated to the staff. ・Establishing the basis of security requirements (laws, regulations and standards, etc.). ・Coming to an agreement with all of the main people concerned in the implications, considerations and requirements of the system’s security. ・Devising an overall security projection (draft level).
2	Classification of security level by the product type. Classification of the type of product to be developed to determine the security level required.
3	Evaluation of the possible impact of security issues on the business. Clarification of what the effects on the business might be if a security problem occurs with respect to the product.
4	Formation of a policy on personal information Consideration of whether or not to convey, store and create information related to personal information for the product targeted for development. If it is decided that the product targeted for development requires the use of personal information, appropriate protective measures and a security management plan must be carried out.

5	Implementation of the secure product development process The primary responsibility for security in the early stages lies with the development team. They have the greatest understanding of every detail of the product's features, and thus are best able to identify the security flaws in functionality and business logic. Utilization of this team is the key to planning the construction of the protective environment to the source code level and successful implementation of the team's plan can only be achieved by conveying what is expected of them.

5.2.2 Development phase

In the development phase of the life cycle of product development, the following security measures are required.

Table 5-3 Security measures during the development phase

No.	Life cycle of product development
1	**Risk assessment** The purpose of risk assessment is to evaluate the system's design, system and security requirements, as well as estimate the effect of these measures in reducing the risks assumed. The results of the evaluation normally show clearly whether the security countermeasures concerned will be enough, or if further consultation is required. To perform a successful evaluation, the participation of the relevant person (user, engineer, or system operators,etc.) who is familiar with each field of the system domain is required. Before the design specification is approved, a security risk evaluation should be put into effect. This indicates if subsequent revisions or additional measures should be included.
2	**Choice of security measures** The security measures adopted during the product development stage are a combination of measures common to this type of development process and the results of the above-mentioned risk evaluation.
3	**Security design** It is important for all parties to understand how security will be included in a product. Security is therefore incorporated into the product at the design stage.
4	**Development of security design and measures** Suitable security measures are designed and incorporated.
5	**Implementation of the developmental, functional and security testing**

	Tests must be conducted within the system, software, hardware, and communication channels to determine if there needs to be further developments or modifications. The purpose of the tests is to verify that the system meets functional and security requirements.

5.2.3 Deployment phase

The following security measures are required during the deployment phase of the life cycle of product development.

Table 5-4 Security measures during the deployment phase

No.	Life cycle of product development
1	**Integration of security measures within the environment or system in which probability has been carried out** In an operational site, products are integrated as a system. Integration testing and acceptance testing are carried out when the product has been delivered and deployed. Security measures are put into effect according to the vendor's directions, available guidance on security implementation and documented security specifications.
2	**Evaluation of product security** Evaluation is carried out to verify that the product meets functional and security requirements. Before an organization begins to use a product, security approval should be put into effect to estimate whether measures have been properly introduced, and how well they operate as intended.
3	**Approval of the information within the system** According to the results of the previous system evaluation, checks and approval determine whether security measures are achieving the level which had been previously agreed upon, or whether residual risks fall within the tolerance level.

5.2.4 Operation and maintenance phase

During the operation and maintenance phase of the life cycle of product development, the following security measures are required.

Table 5-5 Security measures during the operation and maintenance phase

NO	Life cycle of project development
1	**Implementation of configuration management** The management of the system's layout is very important in terms of maintenance, as it is necessary to confirm that the initial constitution of hardware, software and the firmware components related to the data within the system and product are working as intended, and change the current system and product if they are not.
2	**Implementation of ongoing monitoring** Monitoring of the effectiveness of security measures needs to be maintained continuously, even if there is an unavoidable change in the environment where a product is being managed.

5.2.5 Disposal phase

During the abolition phase of the life cycle of product development, the following security measures are required.

Table 5-6 Security measures of the abolition phase

No.	Life cycle of system development
1	**Erasure of media data** The organization ensures that all appliances/procedures function correctly by means of tracking, documenting and verifying media data erasure and other destructive procedures. Periodical tests are also performed on data erasing apparatus/procedures. Data erasure and destruction prior to discarding the digital media of the information system, or re-using it outside the organization, prevents unauthorized access and use of any of the information included in the media.
2	**Disposal of hardware/software** The software is disposed in accordance with the license, developer, or other contracts/regulations. In terms of hardware, destruction and disposal is required if classified information remains even after the media has been removed.

5.3 Guidance of the security measures within each phase

This section summarizes which action items for security guidelines are described in Chapter 4.

The life cycle of each system development shown in Table 5-7 corresponds to the numbers of the policies to be applied as listed in these POS guidelines.

Table 5-7 The security measures of each phase

Phase	No.	Life cycle of system development	POS policy							
			1	2	3	4	5	6	7	8
Initiation	1	Formation of a security plan	●							
	2	Classification of the product type	●							
	3	Evaluation of impacts on the business	●							
	4	Formation of a policy on personal information	●							
	5	Implementation of the secure product development process		●						
Development	1	Risk assessment	●							●
	2	Choice of security measures		●	●	●	●			
	3	Security design		●	●	●	●	●		
	4	Development of security design and measures			●	●	●	●		
	5	Implementation of developmental, functional and security testing			●	●	●	●		
Deployment	1	Integration of security measures for the established environment or system						●		
	2	Evaluation of product security						●		
	3	Approval of the						●		

		information within the system								
Maintenance and operation	1	Implementation of configuration management					●			●
	2	Implementation of ongoing monitoring					●		●	●
Disposal	1	Erasure of media data		●					●	●
	2	Disposal of hardware/ software		●					●	●

6 Conclusion

This book of security guidelines was published with the intention for application in the field of open POS.

However, it is believed that the guidelines can be applicable in other areas, such as action on security when threats are assumed to exist in other forms of life cycles.

It is hoped that the guidelines will be used widely to consider the security measures required in the development process of a variety of products. It is intended that further revisions of these guidelines will be produced based on feedback from inspection results and further insights that arise from the utilization of the security measures described in these guidelines.

References

[1] H. Takada, A. Goto and et al., "IoT Safety/Security Development Guidelines," Information-technology Promotion Agency, Japan (IPA), First Edition, 2016, http://www.ipa.go.jp/files/000053920.pdf.

[2] クレジット取引セキュリティ対策協議会, "クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画-2016-," 2016, http://www.j-credit.or.jp/download/160223a2_news.pdf.

[3] NIST, "Special Publication 800-64 Revision 2: Security Considerations in the System Development Life Cycle," National Institute of Standards and Technology (NIST), First Edition, 2008, http://csrc.nist.gov/publications/PubsSPs.html.

[4] US-CERT, "Alert (TA14-002A): Malware Targeting Point of Sale Systems," UNITED STATES COMPUTER EMERGENCY READINESS TEAM (US-CERT), First Edition, 2014, https://www.us-cert.gov/ncas/alerts/TA14-002A.