# Security Guidelines for Product Categories
# - Automated Teller Machines (ATMs) -

Ver. 1.0

CCDS Security guidelines WG
ATM 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

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 issues relating to ATM security

In recent years, global ATM industries have been suffering not only conventional physical attacks, such as card skimming or physical crash of ATM bodies, and cyber attacks, but also new types of ‘cyber-physical’ attacks using IT technologies. In addition, such attacks have been sophisticated and diversified in its modus operandi than ever. It is reported that some ‘cyber-physical’ attacks using malware that dispenses cash or steals important information such as card data from ATMs without physical damages to the ATMs in Europe and other developing countries.

On the other hand, the security standards for the accounting systems of financial institutions, including ATMs, have been developed based on the rules [10] [11] defined by the Center for Financial Industry Information Systems (FISC) , a public interest incorporated foundation, in Japan. As the FISC’s rules are general security rules, counter measure guidelines are required, considering recent cyber-physical attacks. That is, a new viewpoint is required on a direction of ATM security measures in a ‘cyber-physical’ attack era and these guidelines suggest a direction for ATM security measures.

As the background, even in countries where ‘cyber-physical’ attacks occurred, the systems, including ATMs, seem to have been operating conforming to their own standards similar to those of the FISC. However, such successful attacks suggest that the preventative measures based on their existing standards did not work.

In this document, we would like to provide new guidelines for ATM security to prevent such cyber-physical attacks and reinforce the rules of FISC. As discussed later, the success of malware attacks comes from the two factors. One is that malware was installed into poorly managed ATMs such that all ATM’s maintenance doors can be opened with a same physical key. Another is the situation that cyber-attack technologies can spread much more quickly than ever in the world because conventional PC technologies make it easy to develop malware for ATMs built on the conventional PC technologies.

Nowadays, implementation of “IoT of Safety/Security in the Smart-society“ is required, and it is necessary to release a new “Guidelines for design“ in accordance with the implementation. So the new guidelines should include the effective feedback from such cyber-physical attacks that it was difficult to understand when the existing specifications and standards for ATMs were introduced. It is also essential that the new guidelines should be harmonized with existing ATM operational rules and situations. Therefore, we edited these guidelines to take into account both the existing rules, situations and the future issues.

## 1.2 Scope of the guidelines

### 1.2.1 Basic coverage

There are several security guidelines and standards that cover the whole ATM system in the world (note 1). The aim of this document is not to deny these existing security guidelines and standards, but rather to provide better counter measures by providing “alternative and complementary measures based on the idea of ensuring multiple levels of defense.“

The scope of these guidelines is limited to “an ATM terminal and the components installed in the ATM terminal,“ and is not applicable to host systems, such as banking host computer. The core banking systems in Japan have been built along with a certain security in its long history. Host systems are unlikely to be a target for ‘cyber-physical’ attacks by criminals, since they are considerably more difficult to attack compared to a PC with a less refined level of security.
Instead, these guidelines focus upon security measures against ‘cyber-physical’ attacks where cyber criminals carry out unauthorized withdrawal or important information fraud by either installing malware into an ATM, or installing a malicious computer inside an ATM.

### 1.2.2 Exceptional coverage

These guidelines do not cover the host systems. On the other hand, if security measures are required for both ATMs and host systems at the same time, guideline, and then the host systems are the scope of the guidelines as exceptional cases (note 2). It is assumed that an ATM vender would present such security measures to their customers (e.g. financial institutes) as alternatives, and that their customers would decide whether they introduce and deploy the measures or not according to their own security policies.

## 1.3 Scope of the readers

This document provides a detailed description of the appropriate security measures and operations for an ATM throughout its lifecycle, namely its design, development, installation, maintenance, and discard. Therefore, we assume these guidelines are useful for the following people.

[1] ATM vendor's designers who design devices, and staffs in charge of an ATM development project management,

[2] Business Operators who perform ATM system integration with devices purchased from ATM vendors,

[3] Employees of financial institutions and service providers who are in charge of the planning, development and operation of the entire system including ATM.

## 1.4 Abbreviations

The abbreviations used in these guidelines are as follows:

**Table 1-1 List of abbreviations**

| Abbreviation | Name |
|---|---|
| ATM | Automated Teller Machine |
| BIOS | Basic Input/Output System |
| CCDS | Connected Consumer Device Security Council |
| CEN | Comité Européen de Normalisation<br>(European Committee for Standardization) |
| EMV | Europay MasterCard Visa |
| HDD | Hard Disk Drive |
| IEC | International Electrotechnical Commission |
| IoT | Internet of Things |
| IPA | Information-technology Promotion Agency |
| ISO | International Organization for Standardization |
| NIST | National Institute of Standards and Technology |
| OS | Operating System |
| PCI | Payment Card Industry |
| PIN PAD | Personal Identification Number Pad |
| QR | Quick Response |
| SDLC | Systems Development Life Cycle |
| SMS | Short Message Service |
| SWG | Sub Working Group |
| UL | Underwriters Laboratories |

| | |
|---|---|
| USB | Universal Serial Bus |
| WG | Working Group |
| XFS | eXtensions for Financial Services |

# 2 Sample Model of an ATM Operational System

## 2.1 Example of an ATM system configuration and related perso nnel

As shown in Figure 2-1, there are some staffs physically accessing the inside of ATMs in ATM operations. That is, cash replenishment and collection conducted by financial institution’s staffs or employees of a Cash In Transit company entrusted by the financial institute, maintenance works for ATMs conducted by employees of a maintenance company. Roles of these staffs may change according to the financial institute’s operational form.

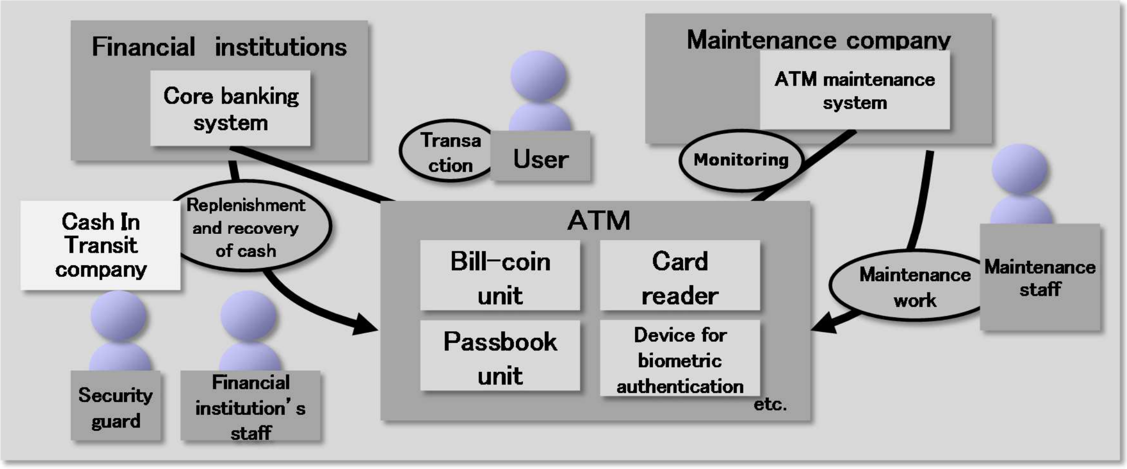

Figure 2-1 ATM operations and related service staffs

Table 2-1 shows a detailed description of the related staffs accessing the inside of ATMs in ATM operation.

**Table 2-1 Details of the related personnel accessing the inside of ATMs**

| No. | Character | Roles |
|---|---|---|
| 1 | Financial institution’s staff | ● Responsible for access control of physical keys to open an ATM maintenance door and physical keys to open the safe door in an ATM.<br>● Responsible for opening the maintenance door and the safe door of an ATM for the replenishment / collection of cash and for maintenance works.<br>● Support maintenance staffs by opening the safe door in an ATM and by keeping the cash cassettes in the |

| | | |
|---|---|---|
| | | banknote-processing unit installed in the safe aside from the banknote-processing unit during the maintenance works of the banknote-processing unit. |
| 2 | Cash In Transit (CIT) company's security guard | Security guards may replenish and collect cash in ATMs in accordance with the directions of a financial institution. (i.e. outsourced staffs)<br>● They may deliver cash with cash cassettes or with cash bags between ATM locations and a financial institution's cash center. In the case of cash bags, they may load cash from the bags into the cash cassettes and may collect cash from the cassettes into the bags at each ATM location.<br>● They may carry physical keys managed by a staff of a financial institution to access the inside of ATMs at ATM sites located apart from branch offices. |
| 3 | Maintenance company's maintenance staff | Maintenance staffs maintain inside an ATM.<br>- Maintenance staff does maintenance work, including fault recovery and repair, after a financial institution's staff or a CIT company's security guard opens the maintenance door and the safe door of the ATM. |

Figure 2-2 shows an example of an ATM system configuration. There is the control unit in the ATM system like PC, and its control unit is connected with peripheral devices via interface such as USB. There is BIOS in the control unit, and,. Device drivers, middleware and applications and etc. are installed in HDD connected with the control unit. Although not shown in this figure, there are journals of ATM transaction history and log files of software in HDD.

The peripheral devices include display for showing an operational guidance to the user, PIN pad or touch screen for inputting user's PIN, amounts of ATM transaction and some information, banknote-processing unit for dispensing and depositing banknotes, card reader for reading some information on a smart card or magnetic stripe card, and optical drive for reading installation media containing software for ATM system updating. Although not shown in this figure, the peripheral devices also include a receipt printer to print out an ATM transaction result on a slip or a passbook printer to print out the transaction result on a passbook. The banknote-processing unit includes cash cassettes for replenishment/collection of banknotes and is installed in a sturdy safe. The control unit is subsequently connected to another host system, such as core banking system (i.e. host computer), and to the maintenance computer system through the network.

A whole ATM is protected by a housing case that meets some certain criteria for physical protection, and there is also a maintenance door to access the inside of an ATM with a physical key.

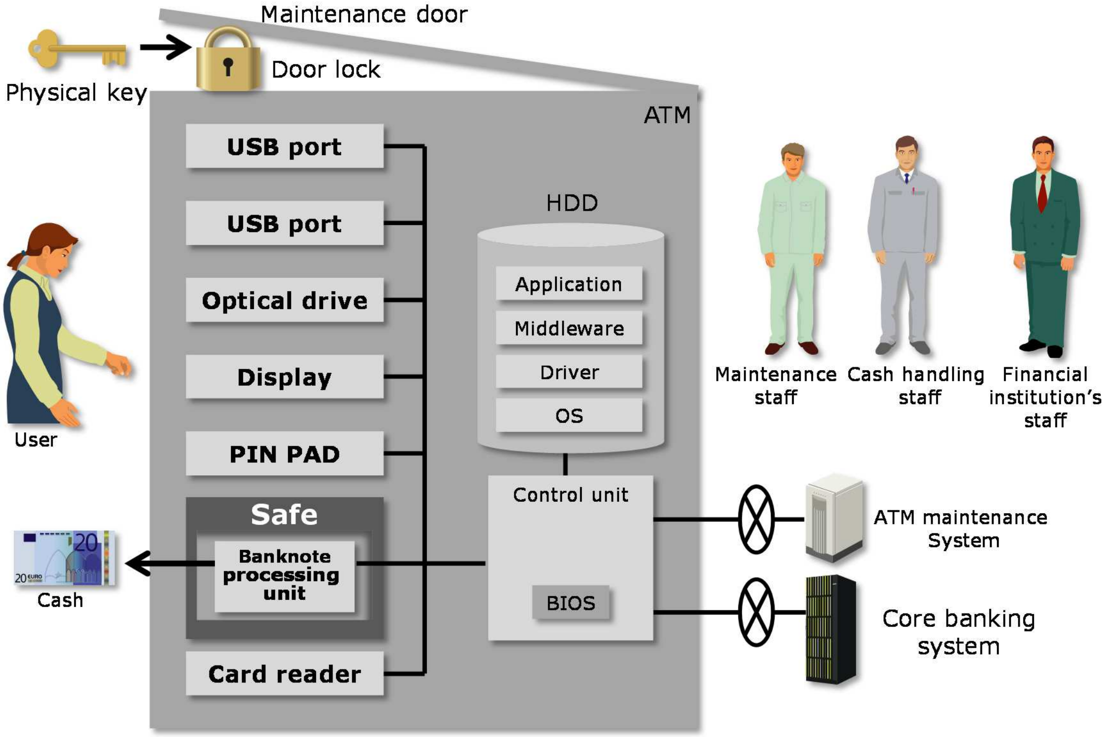

**Figure 2-2 Example of the of an ATM system configuration**

Table 2-2 shows a detailed description of the main components of an ATM system.

**Table 2-2 Main components of an ATM system**

| No. | Component | Function |
|---|---|---|
| 1 | Control Unit | Control unit is a computer, which controls peripheral devices (e.g. card reader, banknote-processing unit). Windows® (note 3) is often adopted as the OS. |
| 2 | HDD | A device connected to the control unit, which stores software such as an OS, device drivers, middleware, applications and maintenance software. |
| 3 | BIOS | BIOS controls boot devices. |
| 4 | USB Port | A USB memory is connected to install software or to collect log data, or a USB keyboard is connected for maintenance works. |
| 5 | Optical Drive | It is used to install software into the ATM and to download transaction history or log data to an optical media. |
| 6 | Display | A device used to display instructions during the transaction, as well as the processing results. Some display equips a touch screen function. |

| | | |
|---|---|---|
| 7 | PIN pad | A device to input the PIN and a transaction amount. Instead of PIN pad, ATMs in Japan are equipped with a touch screen as a PIN entry keyboard and a various menu selection method in general. |
| 8 | Banknote-Processing Unit | A device that dispenses and deposits banknotes and that verifies the authenticity of submitted banknotes and counts banknotes.<br>The device is equipped with multi-denomination cash cassettes storing banknotes. |
| 9 | Safe | Safe protects banknotes and a banknote-processing unit from vandalism and theft. The safe door may be opened with a physical key different from a physical key to open the maintenance door. |
| 10 | Card Reader | A device that reads a bank card or a credit card inserted into the ATM. The device handles a magnetic stripe card and/or a smart card. |
| 11 | Maintenance door | A door to access the inside of the ATM to replenish/collect banknotes or to perform maintenance works. |
| 12 | Physical key | A physical key to open the maintenance door. |
| 13 | Core banking system | Host computer(s) handles the account-based transactions with ATMs. In general, this system literally does not connect to the Internet directly. |
| 14 | Monitoring and maintenance system | Computer system that monitors whether the ATM is working or not. Sometimes this system distributes software and other applications to ATMs. |

## 2.2 Operation of the ATM system

### 2.2.1 Operation during transactions

When an ATM is powered on, the ATM starts an initializing process and consequently establishes a connection to the core banking system and the monitoring and maintenance system automatically. After these sequences, a user is able to make a transaction on the ATM.

An ATM supports various transactions, including deposits, withdrawals and money transfers. For example, in a case of a withdrawal transaction, a user inserts his or her bank card into the card reader after the selection of transaction menu via the touch screen, and the card reader obtains card information. Then the user enters the PIN for identity verification via a PIN pad or a touch screen and the amount to withdraw. The transactional information is sent to the core banking system (i.e. host computer) for the withdrawal processing. The host system's processes are executed based on information such as PIN, card information, and the amount of withdrawal. If the host system approves the process, it sends the approved result to the ATM. Then the ATM sends cash dispensing command to the banknote-processing unit to dispense the banknotes to the user, and completes the overall transaction.

### 2.2.2 Operations of replenishment/collection of banknotes and maintenance works

A maintenance staff or a financial institution's staff opens the maintenance door of an ATM with a physical key for maintenance works or cash handling operations. Additionally, it is necessary to open the safe door for replenishment / collection of banknotes in the cash cassettes. A financial institution's staff accompanies the security guard visiting an ATM site to open the safe door of an ATM, or two or more security guards visit an ATM site to open the safe door of an ATM. The same rule can be applied to open the safe's door for maintenance works of the banknote-processing unit, maintenance staffs.

As mentioned above, it is a standard practice to operate and manage works strictly based on the operating regulations of each financial institution in cases that humans are involved with the works.

# 3 Assumed Threats to the ATM Security

## 3.1 Examples of recent cyber-physical attacks and points to be considered

In this section, we would like to introduce two case studies of unauthorized cash dispensing attacks that have occurred overseas. The first case study shows unauthorized cash dispensing using malware installed in an ATM, and the second case study shows unauthorized cash dispensing by using a small malicious computer, known as 'black box,' installed in the middle of the cable connecting the banknote-processing unit with the control part in an ATM.

[Case study 1: Unauthorized cash dispensing using malware]

Figure 3-1 shows a possible composition of unauthorized ATM cash dispensing case based on opened cases such as news (note 4). The steps of this unauthorized ATM cash dispensing case are assumed to be the following.

(1) Cyber criminals (hackers) develop malware. Recent ATM applications and the APIs of ATM vendors are frequently developed based on the global standard API (note 5). In addition, the ATM vendors' API specifications were leaked due to poor management. The leaked API specifications may have fostered the development of malware (note 6).

(2) The criminal on site succeeds to get a physical key or to duplicate it at a poorly managed ATM site, and then opens the maintenance door with the physical key, and accesses the USB port / the optical drive to installs malware by the USB memory or CDROM in the ATM.

(3) After malware is booted, the criminal on site sends a QR code or a scramble code shown on the display to a remote mastermind (server) using a mobile phone or SMS services.

(4) The mastermind recognizes the message from the criminal on site and replies an authorization code via a mobile phone or SMS. The criminal on site inputs the received authentication code to malware via the PIN pad and then authorized cash dispensing becomes possible.

(5) The criminal on site can get banknotes by sending unauthorized cash dispensing commands to the banknote-processing unit.

(6) The above-mentioned QR code or scramble code includes information on the amount

of banknotes stored in the safe so that the mastermind can check whether the criminal on site does not cheat the banknote amount dispensed from the ATM.

(7) In some cases, communication between the mastermind (server) and the criminal on site may be performed through a SMS mail of a mobile phone connected to the USB port of an ATM.

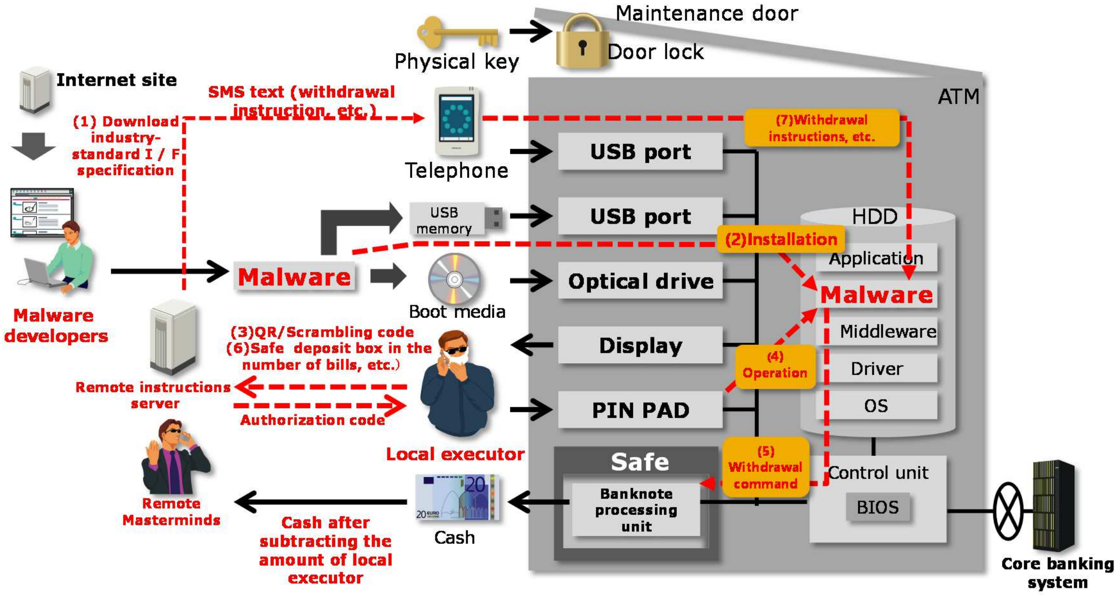

**Figure 3-1 Composition of unauthorized cash dispensing using malware (overseas case)**

[Case study 2: Unauthorized cash dispensing through a malicious small computer called ‘black box’]

Figure 3-2 shows a possible composition of unauthorized ATM cash dispensing case using malicious small computer called ‘black box’ (note 7). The steps of this unauthorized ATM cash dispensing case are assumed to be the following.

(1) The criminals obtain ATM devices for maintenance works, which are available in a black market, often from internet auctions. They analyze the architecture of the hardware, develop a malicious small computer system (black box) and a USB board to cheat the control unit so that the control unit does not detect an abnormal state of the banknote-processing unit.

(2) The criminal on site gets a physical key or to duplicate it at a poorly managed ATM site and then opens the maintenance door with the physical key to set the malicious small computer, the USB board and a mobile phone to the USB port.

(3) The malicious small computer hijacks the communication between the control unit and the banknote-handling unit. The malicious small computer can send unauthorized cash dispensing commands in accordance with the mastermind's (server) instructions via the mobile phone without any authorized transaction.

(4) The criminal on site waits for cash dispensing instructions sent from the mastermind (server) and receives the cash dispensed from the ATM.

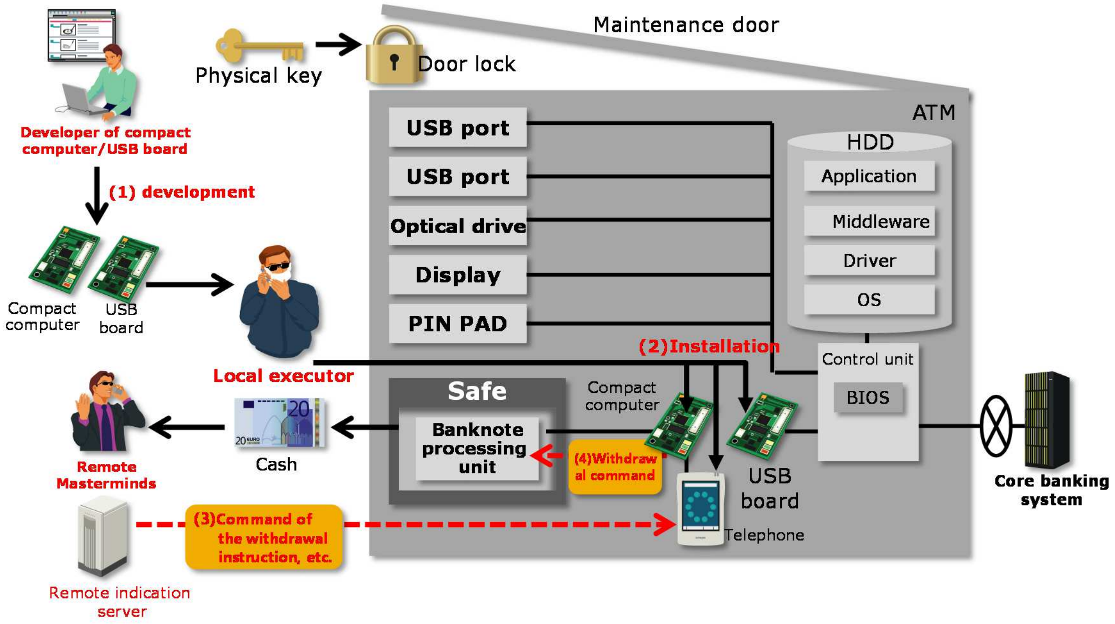

**Figure 3-2 Illustration of unauthorized cash dispensing with a malicious small computer (overseas case)**

In response to the incidents described above, enforcement organizations have instructed to banks and various preventative measures have been open to public on internet (note 8) (note 9).

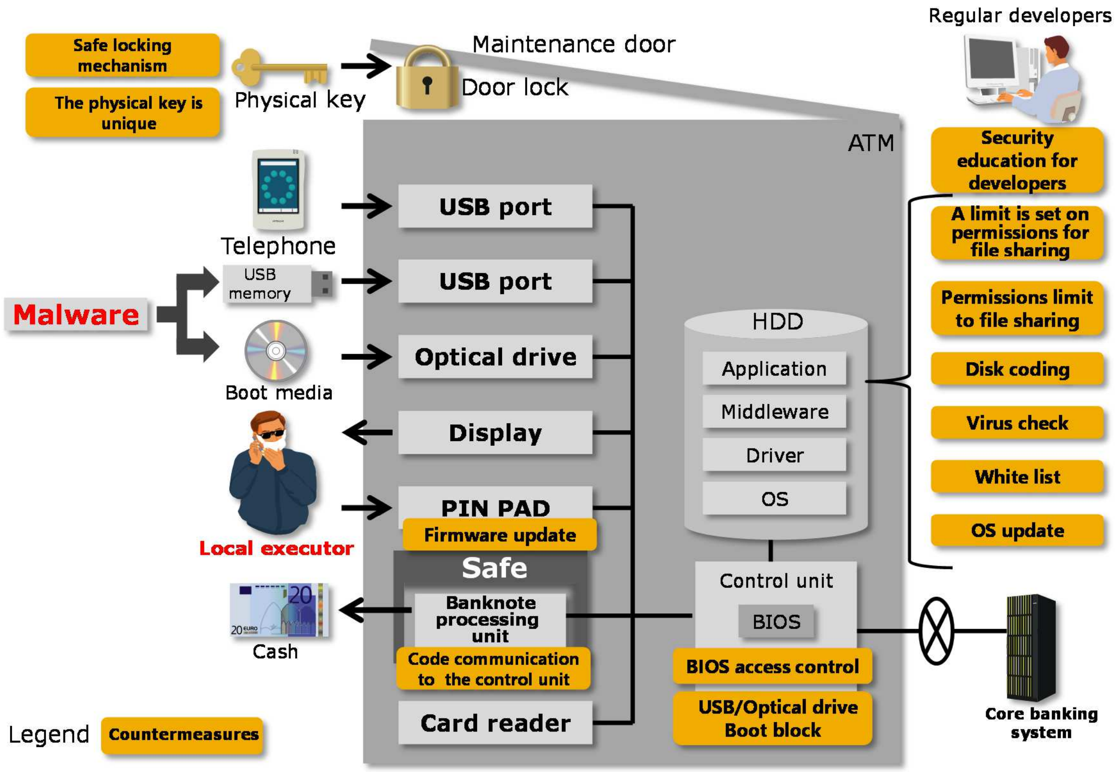

**Figure 3-3 An example of various preventative measures**

In short, the current situations suggest what should be feedback points. The cases described above that have occurred in other countries and not all of them are applied to Japan. However, they may need some attention in the future.

**Table 3-1 Feedback points from the incidents**

| No. | Classification | Feedback points |
|---|---|---|
| 1 | Widespread of damage by generalization and progress of information technology | Prevalence of information technologies make development of criminal methods easy and have assisted growing cyber-physical attacks, and the attack's technologies are still developing. More sophisticated modus operandi may occur.<br>Although a physical medium inserted into an ATM causes malware infection currently, there is no reason why the future progress of IoT might not bring malware intruded into ATMs through a network. |
| 2 | Intrusion route | There may be a malicious person who will insert a medium containing malware such as a USB memory or CD-ROM into a USB port or the medium drive in an ATM.<br>It is necessary to deploy an omnidirectional defense that may prevent the exploit of intrusion even by internal staffs. |
| 3 | Inadequate management | Malicious person can easily install malware into ATMs under the following conditions:<br>- Hardware : A physical key to open the maintenance door of an ATM is the same among all ATMs, and/or poor access control of the physical keys.<br>- Software : If the privileged account name of the system and/or the password is the same for all ATMs, rebooting an ATM from the any file system is allowed. There are other lapses in security, such as USB ports automatically connected with any media, absence of software for detecting malware. |
| 4 | Information leakage and distribution of unofficial maintenance parts | Analyzing the information disclosed improperly or the unauthorized spare parts distributed in black markets, cyber criminals might have developed malware and black box. It is required to consider security measures on the premise that information necessary for logical attacks has already been leaked. |

## 3.2 Concerns based on the feedback points

Further considering the feedback points described in section 3.2, concerns of the existing security guidelines are listed up to develop new security guidelines described in the following chapter.

❒ Concerns 1: The costs of enhancing security become relatively expensive

(1) Operating costs after introducing measures:
Assume that there is a malicious person among staffs operating ATMs, the cost of taking measures to devices as well as the costs for management to audit and check the work of the staffs seems relatively expensive.

(2) Education and training costs for human resources:
The re-education and re-training of staffs involved in an ATM system is one of essential requirements to strengthen security measures.

(3) High costs due to variations of ATM operational rules:
There are different ATM operation rules for each financial institution. Therefore, even if some financial institutions may accept the proposals for new enhanced security measures in the maintenance work, other financial institutions may not accept them because they are not consistent with the existing operational rules. Such a situation would lead to the need to customize the security enhancements for each financial institution and fall into a vicious spiral of a cost increase.

(4) Business opportunity loss due to ATM shut-down for upgrade:
For example, the part disassembly and upgrading operation at a secure room environment is required to have high anti-tamper by upgrading a ATM part, which may result in suspension of timely distribution of alternative parts. In this case, suspension of the ATM operation is not acceptable because it results in a business opportunity loss.

(5) High costs to respond to each evolving modus operandi:
Various preventative security measures in Figure 3-3 strongly focus on the protection of the information assets that exist on the hard disk drive. If responding to each evolving modus operandi arises, it increases costs into the future.

[4] The information assets on the hard disk drive include applications, middleware, device drivers, OS and so forth, which are complicated and multi-layered structure. It is inferred that more than 1,000 items (files) should be tightly controlled as security measures.

[5] ATM applications are frequently updated in accordance with new services provided and customization requested by the financial institution, and such updates are not for security objectives. However, it is still necessary to review all the information assets on the HDD from the security viewpoints in each updating time.

[6] The HDD is one of the most physically breakable devices, and requires frequent maintenance and replacement. Therefore, it is necessary to reset individual security settings in each maintenance works. Furthermore, protecting the control unit including the HDD with a tamper-proof box as a security measure results in repairing it frequently in a secure room. It may bring unacceptable loss of business opportunities due to long suspension in ATM operations described above.

(6) Various testing operations by OS updates are extremely difficult in terms of a cost and a performance:
In general, the OS supplier does not guarantee that the third-party software (i.e. ATM application, middleware) will work properly on a particular system when they provide an irregular update to overcome the vulnerabilities of OS. OS updates in its latter half of the life cycle, it is not guaranteed that performance will not deteriorate especially for old hardware resources. Therefore, the practical solution may end up with updating OS and renewal of obsolete hardware to ATMs at a same time.

Considering these situations, it is important to balance measures against threats and risks found through analysis and costs for the measures from the viewpoints of cost constraints.

❒ Concerns 2: Depending on human resource will fail

(1) It is difficult to tightly control any works at ATM sites. It is assumed that it is difficult to detect and verify malicious behavior of staffs and inappropriate works by mistake due

to limitation of the cost and the labor time.

(2) There is no guarantee that retired designers will not misuse their knowledge.

Many companies ensure that the designers are fully aware of the ethics during their tenure through the company's education, and impose various contractual obligations on the designer when he/she leaves the company.

However, it is not possible to make the development vendor responsible for the subsequent behavior of the designer.

(3) Threats of internally committed cyber-physical attacks

Considering the “intrusion route“, “poor management“, “information leak“ and “distribution of non-genuine spare parts“ described in Section 3.1, the possibility that a person or persons inside the financial institution was or were involved in the malicious operation and cyber-physical attacks cannot be excluded. It is not reasonable to expect all the members of an organization, including operation, maintenance, and developments of ATMs, behave completely morally in global business environment.

The three main types of human security breaches are:

[7] Intrusion route

As it is necessary to open the maintenance door of an ATM with a physical key to access the inside of the ATM, there is always the possibility that either operators, maintenance personnel or CIT company's staffs have deliberately provided cyber criminals with the physical key. The physical key has fallen accidentally into the hands of cyber criminals due to poor management of the physical key.

[8] Poor management

It is pointed that a possibility of informing cyber criminals of poorly managed ATMs (note 10).

[9] Information leak

There is a possibility that malware is developed based on the interface specifications leaked by the authorized designers (note 4).

A review of these concerns demonstrates that there are various difficulties in ATM operational management below when enforcing security measures.

(a) A large number of protecting items make management difficult, especially managing a large number of terminals. Cost increase in repeating tests and acquiring a certification by updates of OS, software and firmware are not taken into account.

(b) Security measures for a vulnerable state of an ATM are not sufficiently taken into account during fault recovery or maintenance work.

(c) There is no guarantee that all the retired designers behave ethically.

# 4 Guidelines for Security Measures

Following the assumptions described in the previous chapter, we would like to show guidelines to provide an adequate security measures.

The “IoT Safety/Security Development Guidelines - Important Points to be understood by Software Developers toward the Smart-society -“ issued by IPA contains 17 guidelines. 12 guidelines are extracted from 17 guidelines to explain its relation with this document and the “IoT Safety/Security Development Guidelines. We do not discuss remaining five guidelines because the ATM industry already knows and have a practice on them. However, it is necessary to review an existing framework or system to come through the IoT era.

**Table 4-1 Relationship between the development guidelines of “IoT Safety/Security Development Guidelines“ and ATM security guidelines**

| IoT Safety/Security Development Guidelines | | | Corresponding part of this document |
|---|---|---|---|
| Major item | | Guidelines | |
| Policy | Making corporate efforts for the Safety/Security of the Smart-society | Guideline 1 Formulating the basic policies for Safety/Security | n/a (*) |
| | | Guideline 2 Reviewing systems and human resources for Safety/ Security | ATM-Guideline 2 |
| | | Guideline 3 Preparing for internal frauds and mistakes | ATM-Guideline 3 |
| Analysis | Understanding the risks of the Smart-society | Guideline 4 Identifying the objects to be protected | ATM-Guideline 4 |
| | | Guideline 5 Assuming the risks caused by connections | ATM-Guideline 5 |
| | | Guideline 6 Assuming the risks spread through connections | n/a (*) |
| | | Guideline 7 Understanding physical risks | ATM-Guideline 7 |
| Design | Considering the designs to protect the objects to be protected | Guideline 8 Designing to enable both individual and total protection | ATM-Guideline 8 |
| | | Guideline 9 Designing so as not to cause trouble in other connected entities | n/a (*) |
| | | Guideline 10 Ensuring consistency of the design to achieve a safe and secure | n/a (*) |
| | | Guideline 11 Designing to ensure Safety/Security even when connected with the unspecified partner. | ATM-Guideline 11 |
| | | Guideline 12 Verifying/validating the designs of safety and security | ATM-Guideline 12 |

| | | | |
|---|---|---|---|
| Maintenance | Considering the designs to ensure protection even after market release | Guideline 13 Implementing the functions to identify and record own status | ATM-Guideline 13 |
| | | Guideline 14 Implementing the functions to maintain Safety/Security with the passage of time | ATM-Guideline 14 |
| Operation | Protecting with relevant parties | Guideline 15 Identifying IoT risks and providing information after delivery | ATM-Guideline 15 |
| | | Guideline 16 Informing relevant companies of the procedures to be followed after delivery | ATM-Guideline 16 |
| | | Guideline 17 Informing general users of the risks caused by connections | n/a (*) |

(*) n/a : These sections have not been covered because the systems and mechanisms have been recognized as being well-known in the ATM industry.

[ATM-Guideline 2] Reviewing organizational structure and human resources for Safety/Security

(1) **Establishing organizational structure and environments for discussing the Safety/Security issues of the Smart-society in an integrated manner.**

New types of ‘cyber-physical’ attacks, such as the use of malware to enable the unauthorized cash withdrawal from ATMs, have been increasing in overseas countries. The government agencies, industry associations and companies of several countries have subsequently issued information about these cyber criminals, along with security guidelines and example measures to counter them. In order to avoid these situations in future Japan, it is required to ensure the activity of sharing information on existing measures and cyber-physical attack cases in a timely manner within the company as well as reinforce its product security,

(2) **Securing and training / human resources (developers and maintenance staff) for that purpose.**

In order to counter ‘cyber-physical’ attacks, security measures based on a new point of view are required. It is therefore necessary to continue to develop new countermeasure technologies, while ensuring human resources, including designers and their training.

[ATM-Guideline 3] Preparing for internal fraud and mistakes

(1) **Recognizing the possible existence of internal fraud that can be a threat to the**

**Safety/Security of the Smart-society and discussing the counter measures.**

There have been many cases that malicious actions have occurred by exploiting the access granted to the inside of equipment for the operation and maintenance of the ATM. In the cases of overseas cyber-physical attacks, the skills of the staff, as well as their morale are not so sufficient that there may be a potential threat of a malicious activity that attacks ATMs in the situations of poor management of ATMs. Therefore, it is necessary to make an additional management effort such as monitoring and managing staff's behavior, ATMs and spare parts for maintenance.

However, it is important to avoid deteriorating the efficient ATM operation and maintenance due to excessive strengthening such monitoring and management. As the assets targeted by internal fraud and cyber –physical criminals are limited, it is possible to achieve effective maintenance, deterrence and operational efficiency using these guidelines for ATM security.

(2) **Discussing the measures to prevent mistakes by relevant parties and to protect Safety/Security even for mistakes.**

We should assume that staffs may make mistakes in their operations because we cannot expect their high skills and morale. We also should assume that staffs do not conform to necessary procedures by various reasons. Therefore, measures preventing a fetal error are required in case of a mistake or not complying with the procedure. (Multiple defenses utilized in a legacy information processing system).

For example, we should consider a good practice to prevent unauthorized cash withdrawals by an additional protecting mechanism implemented in the peripheral devices of an ATM even though there are security holes in the control unit.

Generally, the more complicated tasks and managed items an operation has, the more mistakes occur. In order to strengthen security, it is necessary to make efforts to reduce managed items, to simplify the work procedure, or to automate the work procedure by a system rejecting an incorrect operation.

[ATM-Guideline 4] Identifying objects to protect

(1) **Identifying the intrinsic functions or information in Smart-society to protect with the points of Safety/Security view.**

As the cyber-physical criminals target limited assets in ATMs, it becomes easier to ensure effective security and business efficiency if the order of information and asset in terms of their value are prioritized. For example, the cash dispensing command, card numbers, PIN are important assets to be protected. Furthermore, the existing Payment Card Industry (PCI) standards as described in [2], [3] and [4] define card numbers and PINs as information assets to be protected.

[ATM-Guideline 5] Assuming the risks caused by connections

(1) **Assuming the risks caused by connections for devices and systems of closed networks, provided that they can be used as IoT components.**

In general, ATMs are connected with the dedicated network of a financial institution and are isolated from the external network.
However, in the overseas cases, unauthorized cash dispensing from ATMs occurred by malware installed into the ATMs or by a small malicious computer, which can connect with an external network, embedded into the inside of the ATMs. As an ATM may be connected with an open network terminal such as a cell phone in an ATM transaction in near future, security measures protecting the control unit of an ATM are required.

(2) **Assuming the risks during maintenance and risks due to the malicious use of maintenance tools.**

Since accessing the inside of an ATM is required during certain ATM operations and maintenance works, risks to attack an ATM during these operations and works should be assumed:

■ **Malicious acts by maintenance staffs (Malware installation, etc.)**

It is necessary to take measures for the control unit of an ATM against the risks that malware may be installed into the control unit during accessing the inside of an ATM. Anti-virus software and OS hardening are the examples of the measures. . Since these measures may affect the whole ATM system operations, it is necessary to obtain the consent of the financial institution or the system integrator well before their implementation. Furthermore, it is effective to employ multi-layered defenses by peripheral devices in case that attacks bypass these measures for the control unit. In cases that measures for ATMs do not work well to prevent such attacks, deterring such attacks by monitoring or auditing works and the assets in ATMs is effective.

(a) Traceability of assets in important devices

If a small malicious computer (black box) is directly connected with the banknote-processing unit and sends unauthorized cash dispensing commands for unauthorized withdrawals, the control unit cannot record the log data of the unauthorized withdrawals. In preparation for such attacks, if the banknote-processing unit records all cash dispensing commands as log data inside, it is easier to detect the attacks by comparing the log data stored in the banknote-processing unit with the log data for withdrawal transactions stored in the control unit.

(b) Traceability of important maintenance devices

It is effective to have mechanism tracing embedment of unauthorized maintenance parts or preventing unauthorized maintenance parts from being embedded, considering risks embedding important maintenance parts that are modified wrongfully, such as backdoor.

(c) Traceability of maintenance works

It is desirable to monitor malicious acts in ATM operations and maintenance works by any means possible. Although one method is to use surveillance cameras monitoring the malicious acts, it is very time consuming to verify the recorded video data. So a more efficient way for monitoring and auditing is more desirable.

■ **Unauthorized use of I/F for maintenance by a third person (starting up non-disclosed maintenance mode and acquiring physical keys to open ATM maintenance doors)**

In overseas cases, the attackers took advantage of poor management of physical keys to open ATM maintenance doors. Therefore, appropriate management of physical I/F and logical I/F is required. For example, measures such as a unique physical key for each ATM, one-time password to start maintenance works, and pre-authentication to access an important maintenance function.

[ATM-Guideline 7] Recognizing physical security risks

(1) **Assuming the risks of unauthorized operations of stolen or lost devices, and physical attacks at locations where no administrator is present.**

Since the ATM operations and maintenance works accompany a physical access to the inside of an ATM, it is necessary to consider the risks incurred during maintenance works as indicated in ATM-Guideline 5. Furthermore, maintenance companies should consider the risks of physical theft of ATMs or maintenance parts from the warehouse. Regarding these measures, the guidelines described in ATM-guideline 5 are effective.

(2) **Assuming the risks of information retrieval, software alternation, and resale of secondhand or disposed devices.**

Although there are rules to erase information remaining on an ATM after the end of its operating life, it is necessary to consider the risks due to violation of the rules from the overseas cases that the attackers took advantage of poor management of ATMs. Referring the overseas cases that a malicious small computer is installed into an ATM to communicate with other device in the ATM, it is necessary to consider the risk that cyber –physical attacks are committed by installing wrongfully altered maintenance parts into ATMs, which are developed with disposed devices or used devices, though there are not any definite evidences. The guidelines described in ATM-Guideline 5 are effective for the implementation of appropriate measures.

[ATM-Guideline 8] Designing to protect both individual and total IoT components

(1) **Discussing counter measures for each individual IoT components against the risks via external interfaces, internally contained risks, and physical interaction risks.**

■ **Measures against risks via the external interface**

Referring the overseas cases that malware takes over the de facto standard API to execute unauthorized cash dispensing, it is necessary to protect the de facto standard API from malware by any measures without modifying the API. As examples of counter measures, there are measures for the control unit such as anti-virus software based on whitelisting software and hardening the OS.

To protect external I/F of important peripheral devices such as a banknote-processing unit, it is effective to verify the authenticity of message data with encryption technology. As for measures ensuring security in the I/F for maintenance, the guidelines described in ATM-Guideline 5 are effective.

■ **Measures to be taken against internally contained risks**

Since a protecting mechanism has already been provided for ATMs, we do not discuss it in this document.

- **Measures to be taken against physical interaction　risks**

  As there is a physical access to the inside of an ATM during certain ATM operations and maintenance works, the measures indicated in ATM- Guideline 5 are effective.

- **Each security measures should be taken according to importance of the objects to be protected**

  The targeted assets in an ATM are limited in existing cyber-physical attacks and malicious acts. There are cash dispensing commands, card numbers and PIN as important assets to protect. Therefore, multi-layered defenses in peripheral devices are effective to protect important assets in preparation for block of measures in the control unit, in addition to measures for the control units. With regard to the concept of taking each security measures in accordance with the importance of the objects to be protected, PCI standards in the credit card payment system are useful as reference (See PCI standards [2] [3] [4]). For example, security countermeasures such as an access control or audit to an ATM are required while card numbers exist as a plain text on the memory of ATM.

  On the other hand, an inputted PIN is encrypted in a PIN pad and an only encrypted PIN is allowed to exist outside of the PIN pad. Thus security standards are defined so that the measure level varies according to the possible impact at the time of data leak.

(2) **If the individual IoT components cannot handle some risks, measures in total IoT components, consisting of each IoT components, are required.**

If a security measure for the control unit and a security measure for each important peripheral device do not work well, it is possible to implement further measures by utilizing and unifying information held in the important peripheral devices and the control unit. For example, while the control unit stores transaction records, usually called an electronic journal, the banknote-processing unit also logs cash dispensing and depositing. Then these logs make it possible to compare whether the withdrawn amounts in the banknote-processing unit and the control units are the same. It is also possible similar verification by comparing information held in peripheral devices.

[ATM-Guideline 11] Designing to ensure Safety/Security even when connected to unspecified entities

(1) **Discussing the designs to enable IoT components to determine the connection methods according to the entities to be connected to and conditions of the connections.**

If an encrypted communication between components in an ATM, such as between the control unit and the banknote-processing unit, is effective as a security measure, an administrative privilege, such as a privileged mode, is required for the encryption settings. For example, when the maintenance staff is going to replace the existing control unit with a new one as the maintenance operation, a privilege mode is required to set a new encryption key for the encrypted communication between the new control unit and the existing banknote-handling unit.

Otherwise, an unauthorized staff could set an encryption key for the encrypted communication between the unauthorized staff's private PC and the banknote-processing unit without any permission, and could dispense cash from the ATM without authorization.

A privileged mode is required to suspend or delete the encrypted communication function after the function is implemented into the control unit or peripheral device as a security measure. It is also useful as a defense against any attacks to disable the encrypted communication function.

[ATM-Guideline 12] Evaluating/validating the designs of safety and security

(1) **Considering the unique risks of the IoT, where many devices connect to the network, evaluate and validate the Safety/Security design of devices and systems.**

Mechanisms to design and evaluate products to ensure the user safety and mechanisms to design and evaluate security products, such as a biometric authentication device and a banknote validator, have already established in an ATM design. So the sufficient mechanisms to validate and evaluate the design of the safety and security have already been established. On the other hand, attacks on security are constantly evolving, and a new modus operandi is emerging one after another largely in overseas. We should assume that it may be difficult to cope with such emerging attacks from the existing viewpoints. Therefore, it is necessary to constantly review and improve the existing mechanisms of validation and evaluation of the design.

[ATM-Guideline 13] Implementing the functions to identify and record its own status

(1) **Discussing the functions to identify and record the component's own status and the status of communications with other devices.**

The control unit and peripheral devices in an ATM are equipped with the function to save the unit/device status and the processing results as a log for maintenance purposes. As described in Guideline 8, it is possible to implement further security measures by comprehensively utilizing these log data.

(2) **Discussing the functions to disallow unauthorized deletion/manipulation of records.**

An access control setting and encryption to the log data stored in an ATM are approved by financial institutes. Furthermore, the log data should be stored in an ATM at least for the minimal time, and there is a way for access control to the log data, and a way to send the log data to the server or other parties both on a regular basis and on an irregular basis.

[Guideline 14] Implementing the functions to maintain Safety/Security even after the passage of time

(1) **Discussing the functions, such as update, to maintain Safety/Security against increased risks with the passage of time.**

Generally, ATMs are operated under a service agreement for maintenance between a financial institute and either the ATM vendors or system integrators. Therefore, there are functions to maintain safety and security of ATMs such as updates, and a service delivery scheme. As attacking parties' technologies are developing rapidly, it seems that necessity to update encryption technologies for ATMs will be high.

Once an encryption technology is introduced to ATMs, a new maintenance work is required for encryption keys management such as keys updating, and functions and a mechanism to securely conduct the key management are also required. Specific guidelines and methods for the key management are omitted in this document as they are described in the documents of the international standards and the industry standards. Furthermore, as the encryption key management may affect the entire ATM system, it is necessary to consider beforehand what effects such as a new agreement on maintenance might be.

[Guideline 15] Identifying IoT risks and providing information after the delivery

(1) **Collecting/analyzing latest information on defects, vulnerabilities, accidents, and incidents at all times.**

(2) **Providing risk information within the company, to relevant business operators, and on information provision sites as necessary.**

The public institutions, industry organizations and security companies disclose latest information on defects, vulnerabilities, accidents and incidents. It is necessary to share the information within the company and relevant business operators, and to utilize appropriately the information to product design. In addition, it is required to provide the customers with such information at appropriate timing, and furthermore it is preferable to provide them with solutions against these issues.

[Guideline 16] Informing what should be followed after the delivery

(1) **Informing what should be followed to the staff and external business operators directly involved in deployment, operation, maintenance, and disposal of the ATM.**

As sale and purchase, operations, and maintenance works are conducted on contracts basis regarding ATMs, there is a mechanism to deliver what should be followed on implementation, operation, maintenance, and disposal of ATMs to staffs in charge and external business operators. However, in light of overseas cases leaving poor management of ATMs, further improvement and ingenuity of the mechanisms are required, and it is necessary to make continual efforts to improve the mechanisms.

# 5 The Development Phase and Security Measures

There are two types of products in the world. One type ‘managed product’ is a product that the operations manager watch over carefully and the other type ‘unmanaged product’, such as consumer products, has no the operations managers. When taking into consideration overseas cases of unauthorized cash withdrawal from poorly managed ATMs, it is appropriate to regard ATMs as both “unmanaged product“ and “managed product“ though an ATM is generally a strictly “managed product“. When regarding an ATM as a managed product, this chapter describes how to apply the guidelines described in the previous chapter. NIST SP800-64 “Security Considerations in the System Development Life Cycle (SDLC)“ is covered as a development life cycle for a managed product. We would like to outline the definition of each phase within the life cycle in Section 5.1, and detailed descriptions of each phase in Section 5.2. Then the security guidelines are assigned to each phase in Section 5.3.

## 5.1 Definitions of the phases in the life cycle

System development follows a life cycle from the initiation to the disposal. A typical system development life cycle includes the following five phases.

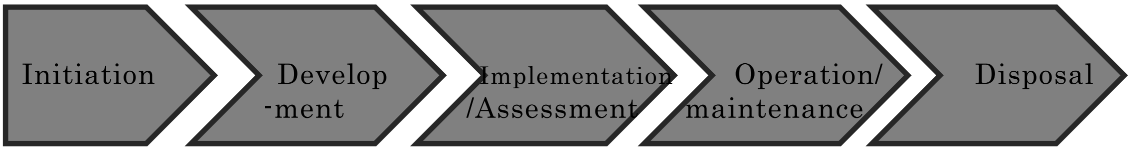

**Figure 5-1 Phases of the life cycle (SDLC model)**

**Table 5-1 Definitions of each phase**

| Phase | Description |
|---|---|
| Initiation | During this phase, the need for a system is expressed and the purpose of the system is documented. Security considerations are keys to diligent and early integration. Key security activities for this phase include:<br>・ Initial delineation of business requirements in terms of confidentiality, integrity, and availability<br>・Determination of information categorization and identification of known |

| | |
|---|---|
| | special handling requirements to transmit, store, or create information such as personally identifiable information<br>·Determination of any privacy requirements<br>Early planning and awareness will result in cost and timesaving through proper risk management planning. Security discussions should be performed as part of (not separately from) the development project. |
| Development | During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed. Key security activities for this phase include:<br>·Conduct the risk assessment and use the results to supplement the baseline security controls<br>·Analyze security requirements<br>·Perform functional and security testing<br>·Prepare initial documents for system certification and accreditation<br>·Design security architecture |
| Implementation /Assessment | After system acceptance testing, the system is installed or fielded. Key security activities for this phase include:<br>·Integrate the information system into its environment<br>·Plan and conduct system certification activities in synchronization with testing of security controls<br>·Complete system accreditation activities |
| Operation and maintenance | During this phase, the system performs its work. The system is almost always modified by the addition of hardware and software and by numerous other events. Key security activities for this phase include:<br>·Conduct an operational readiness review<br>·Manage the configuration of the system<br>· Institute processes and procedures for assured operations and continuous monitoring of the information system's security controls<br>·Perform reauthorization as required |
| Disposal | During this phase, the system performs its work. The system is almost always modified by the addition of hardware and software and by numerous other events. Key security activities for this phase include:<br>·Build and Execute a Disposal/Transition Plan<br>·Archive of critical information<br>·Sanitization of media<br>·Disposal of hardware and software |

## 5.2 Detailed descriptions of each phase

The security activities during each phase of the life cycle in system development outlined in the previous section are described in detail.

Since the development target is an ATM, the term “system“ is read as the word “products.“ Same security activities are omitted because there are the similar activities in the existing ATM development life cycles.

### Initiation phase

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

**Table 5-2 Security activities during the initiation phase**

| No. | Description of security activities |
|---|---|
| 1 | **Initiate Security Planning**<br>The following early involvement will enable the developers to plan security requirements and associated constraints into the project. Security planning should begin in the initiation phase by:<br>· Identifying key security roles for the system development<br>· Identifying sources of security requirements, such as relevant laws, regulations, and standards<br>· Ensuring all key stakeholders have a common understanding, including security implications, considerations, and requirements<br>· Outlining initial thoughts on key security milestones including time frames or development triggers that signal a security step is approaching |
| 2 | **Categorize the product**<br>Security categorization provides a vital step towards integrating security into the ATM business and information technology management functions and establishes the foundation for security standardization among information systems. Security categorization starts with the identification of what information supports which the financial institute’s lines of business. |
| 3 | **Assess Business Impact**<br>An assessment of product impact on the financial institute’s lines of business correlates specific product components with the critical business services that are provided. That information is then used to characterize the business and mission consequences of a disruption to the product’s components. |
| 4 | **Assess Privacy Impact**<br>When developing a new system, it is important to directly consider if the system will transmit, store, or create information that may be considered privacy information. This typically is identified during the security |

|  |  |
|---|---|
|  | categorization process when identifying information types.<br>Once identified as a product under development that will likely handle privacy information, the product owner should work towards identifying and implementing proper safeguards and security controls, including processes to address privacy information incident handling and reporting requirements. |
| 5 | **Ensure Use of Secure Product Development Processes**<br>Primary responsibility for application security, during early phases, lies in the hands of the development team who has the most in-depth understanding of the detailed workings of the application and ability to identify security defects in functional behavior and business process logic. It is important that their role not be assumed or diminished. Communicating and providing expectations is key to planning and enabling an environment that protects down to the code level. |

## Development phase

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

**Table 5-3 Security activities during the development phase**

| No. | Description of security activities |
|---|---|
| 1 | **Assess Risk to Product**<br>The purpose of a risk assessment is to evaluate current knowledge of the product’s design, stated requirements, and minimal security requirements derived from the security categorization process to determine their effectiveness to mitigate anticipated risks. Results should show that specified security controls provide appropriate protections or highlight areas where further planning is needed. To be successful, participation is needed from people who are knowledgeable in the disciplines within the system domain (e.g., users, technology experts, operations experts).<br>The security risk assessment should be conducted before the approval of design specifications as it may result in additional specifications or provide further justification for specifications. |
| 2 | **Select and Document Security Controls**<br>The selection of security controls consists of three activities: the selection of baseline security controls (including common security controls); the application of security control tailoring guidance to adjust the initial security control baseline; and the supplementation of the tailored baseline with additional controls based on an assessment of risk and local conditions. An organization-wide view is essential in the security control selection process to ensure that adequate risk mitigation is achieved for all mission/business processes and the information systems and organizational infrastructure supporting those processes. |
| 3 | **Design Security Architecture** |

| | |
|---|---|
| | At the product level, security should be architected and then engineered into the design of the product. This may be accomplished by zoning or clustering functions/services either together or distributed for either redundancy or additional layers of protection. |
| 4 | **Engineer in Security and Develop Controls**<br>During this stage, security controls are implemented and become part of the product rather than applied at completion. Applying security controls in development should be considered carefully and planned logically. |
| 5 | **Conduct Testing (Developmental, Functional and Security)**<br>Products being developed or undergoing software, hardware, and/or communication modification(s) must be tested and evaluated prior to being implemented. The objective of the test and evaluation process is to validate that the developed product complies with the functional and security requirements. |

## Implementation / Assessment phase

During the implementation / assessment phase of the product development life cycle, the following security activities are required.

**Table 5-4 Security activities during the implementation / assessment phase**

| No. | Description of security activities |
|---|---|
| 1 | **Integrate Security into Established Environments or Products**<br>Integration and acceptance testing occur after product delivery and installation. Security control settings are enabled in accordance with manufacturers' instructions, available security implementation guidance, and documented security specification. |
| 2 | **Assess product security**<br>Products being developed or undergoing software, hardware, and/or communication modification(s) must be formally assessed prior to being granted formal accreditation. The objective of the security assessment process is to validate that the product complies with the functional and security requirements and will operate within an acceptable level of residual security risk. |
| 3 | **Authorize the product**<br>This authorization (also known as security accreditation), granted by a senior financial institute's official, is based on the verified effectiveness of security controls to some agreed-upon level of assurance and an identified residual risk to financial institute's assets or operations (including mission, function, image, or reputation). |

## Operation and maintenance phase

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

**Table 5-5 Security activities during the operation and maintenance phase**

| No. | Description of security activities |
|---|---|
| 1 | **Perform Configuration Management and Control**<br>Configuration management and control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the product and subsequently for controlling and maintaining an accurate inventory of any changes to the product (Note). |
| 2 | **Conduct Continuous Monitoring**<br>A well-designed and well-managed continuous monitoring process can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status information to appropriate organizational officials. |

Note: If the ATM vendors provide security functions based on their individual guidelines for operation and maintenance phase, financial institutions, maintenance companies, and cash in transit companies should perform the operation and maintenance utilizing the ATM vendor’s individual security functions.

## Disposal phase

During the disposal phase of the product development life cycle, the following security activities are required.

**Table 5-6 Security activities of the disposal phase**

| No. | Description of security activities |
|---|---|
| 1 | **Sanitize Media**<br>The organization sanitizes product digital media using approved equipment, techniques, and procedures. The organization tracks, documents, and verifies media sanitization and destruction actions and periodically tests sanitization equipment/procedures to ensure correct performance. The organization sanitizes or destroys product digital media before its disposal or release for reuse outside the organization, to prevent unauthorized individuals from gaining access to and using the information contained on the media. |
| 2 | **Dispose of hardware and software**<br>Hardware and software can be sold, given away, or discarded as provided |

| | |
|---|---|
| | by applicable law or regulation. The disposal of software should comply with license or other agreements with the developer and with the financial institute’s regulations. There is rarely a need to destroy hardware except for some storage media that contains sensitive information and that cannot be sanitized without destruction. |

## 5.3 Action on security measures required for each phase

This section summarizes the action items in each product development life cycle concerning with the ATM security guidelines. Table 5-7 shows the correspondence between the security activities in each phase of the product development life cycle and the numbers of ATM security guidelines described in chapter 4. The mark ‘√‘ indicates the guideline that should be considered in each security activity in the product development life cycle. The description of the security activities without ‘√’ have been omitted because the systems and mechanisms in ATM systems have been well-known in the ATM industry.

**Table 5-7 Security guidelines corresponding to each security activity in each phase**

| Phase | No. | Description of activities in each phase | ATM security guidelines | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 11 | 12 | 13 | 14 | 16 |
| Initiation | 1 | Initiate Security Planning | √ | | | | | | | | | | | |
| | 2 | Categorize the product | | | √ | | | | | | | | | |
| | 3 | Assess Business Impact | | | | | | | | | | | | |
| | 4 | Assess Privacy Impact | | | √ | | | | | | | | | |
| | 5 | Ensure Use of Secure Product Development Processes | √ | | | | | | | | | | | |
| Develop-ment | 1 | Assess Risk to Product | √ | √ | √ | √ | √ | √ | | | | | | |
| | 2 | Select and Document | | √ | | | √ | √ | √ | √ | | √ | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Security Controls | | | | | | | | | | | | |
| | 3 | Design Security Architecture | | | | | | | √ | | | √ | √ | |
| | 4 | Engineer in Security and Develop Controls | | | | | | | √ | | | √ | √ | |
| | 5 | Conduct Testing | | | | | | | | | √ | | | |
| Implementation/ Assessment | 1 | Integrate Security into Established Environments or Products | | | | | | | | | | | | √ |
| | 2 | Assess product security | | | | | | | | | | | | |
| | 3 | Authorize the product | | | | | | | | | | | | |
| Operation and Maintenance | 1 | Perform Configuration Management and Control | | | | √ | | √ | | | | | | |
| | 2 | Conduct Continuous Monitoring | | | | √ | | √ | | | | | | |
| Disposal | 1 | Sanitize Media | | | | | | | | | | | | √ |
| | 2 | Dispose of hardware and software | | | | | | | | | | | | √ |

## Summary

Although this document was developed as security guidelines for the ATM sector, the contents such as assumed threats and security activities within the product development life cycle are applicable to other sectors.

We hope that many developers use these guidelines widely when considering security measures required in the product development processes.

# Endnotes

(Note 1) Examples of ATM-related guidelines issued by the central banks, governments, or industry associations:

- References [1]
- References [4]
- References [8]
- References [9]
- References [10]
- References [11]

This document does not cover the protection requirements with respect to data and equipment on these ATM-related guidelines already covered by the PCI standards. In this security guidelines, we do not discuss, for example security requirements with card information such as primary account number, magnetic track information, which are already covered by the PCI DSS standards. The same applies for the EMV standard [5].

(Note 2) For example, because this measure is effective for ATM security, this document recommends not only the encryption of data inside the ATM but also a decryption of data at the host computer.

(Note 3) Windows are registered trademarks or trademarks of the US Microsoft Corporation in the United States and other countries.

(Note 4) For example, you can find following cases published in the WEB.

- ATM API documentation for NCR Corp’s ATM is affordable on Baidu.

https://www.f-secure.com/weblog/archives/00002751.html

- PLANNING TO ROB A WINDOWS ATM? DITCH THE SLEDGEHAMMER AND BRING A USB STICK

http://www.theregister.co.uk/2014/01/06/atm_malware_stick_up/

- TEXTING ATMS FOR CASH SHOWS CYBERCRIMINALS’ INCREASING SOPHISTICATION

http://www.symantec.com/connect/blogs/texting-atms-cash-shows-cybercriminals-increasing-sophistication

(Note 5) APPLICATION PROGRAMMING INTERFACES

Includes EXTENSIONS FOR FINANCIAL SERVICES (XFS) MIDDLEWARE as a representative of this interface

(Note 6) ATM API documentation for NCR Corp’s ATM is affordable on Baidu.

https://www.f-secure.com/weblog/archives/00002751.html

(Note 7) THIEVES ‘JACKPOT’ ATMS IN NEW ‘BLACK BOX’ ATTACK

http://www.theage.com.au/it-pro/security-it/thieves-jackpot-atms-in-new-black-box-attack-20150107-12k0el.html

(Note 8) For example, the following cases are included:

- References [9]
- TEXTING ATMS FOR CASH SHOWS CYBERCRIMINALS’ INCREASING SOPHISTICATION

http://www.symantec.com/connect/blogs/texting-atms-cash-shows-cybercriminals-increasing-sophistication

- Backdoor.Ploutus.B Technical Notes

https://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2013-102523-2331-99&tabid=2

(Note 9) Guidelines and recommendation statements issued by parties who have encountered serious incidents

- References [9]

(Note 10) ATM JACKPOT WITH MALWARE (From: TIMES OF INDIA)

# 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] PCI SSC, "Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures Version 3.2", PCI SSC (Payment Card Industry Security Standards Council), April 2016.

[3] PCI SSC, "Payment Card Industry (PCI) Payment Application Data Security Standard Requirements and Security Assessment Procedures Version 3.2," PCI SSC (Payment Card Industry Security Standards Council), May 2016.

[4] PCI SSC, "Information Supplement: PCI PTS ATM Security Guidelines," PCI SSC (Payment Card Industry Security Standards Council), January 2013.

[5] EMVCo
https://www.emvco.com/

[6] 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

[7] NIST, "Special Publication 800-64 Revision 2: システム開発ライフサイクルにおけるセキュリティの考慮事項," National Institute of Standards and Technology (NIST), First Edition, 2008, https://www.ipa.go.jp/files/000025343.pdf

[8] MAS, "Technology Risk Management Guidelines," Monetary Authority of Singapore (MOS), June 2013, http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf.

[9] EUROPOL, "GUIDANCE AND RECOMMENDATIONS REGARDING LOGICAL ATTACKS ON ATMS, Mitigating the risk, setting up lines of defence

Identifying and responding to logical attacks," EUROPEAN LAW ENFORCEMENT AGENCY (EUROPOL), https://www.ncr.com/sites/default/files/brochures/EuroPol_Guidance-Recommendations-ATM-logical-attacks.pdf.

[10] FISC, "金融機関等コンピュータシステムの安全対策基準・解説書(第 8 版)," The Center for Financial Industry Information Systems (FISC), March 2011, https://www.fisc.or.jp/publication/disp_target_detail.php?pid=225

[11] FISC, "金融機関等コンピュータシステムの安全対策基準・解説書(第 8 版追補改訂)," The Center for Financial Industry Information Systems (FISC), June 2015, https://www.fisc.or.jp/publication/disp_target_detail.php?pid=316