Security Guidelines for Product Categories

- Automated Teller Machines (ATMs) -

Security Measures Review Practice Guide

- Analyzing Crime Incidents and Formulating Countermeasures -

Ver. 1.00

CCDS Security Guidelines WG
ATM SWG

Revision History

Version	Date of Revision	Description
Ver.1.0	2017/05/29	New edition

CONTENTS

1 Introduction

Criminal groups possibly lurking behind ATM cyber physical crime incidents are presumed to be developing malware and associated hardware while being exposed to the risks of being apprehended. The rate of return on risk should be of concern to the criminal groups. While a successful attack technique works well, attackers are possibly inclined to stick to the same technique, changing target countries and financial institutions. There are actually numerous variants of malwarederived from the same origin to attack ATMs.

In adopting ATM security measures, one should think that crimes actually happened in the past can accordingly be regarded as more risky than threats that are identified through general analyses. You should prioritize security measures intended to defend against them. This guide, the practice part of the Security Guidelines for Product Categories: Automated Teller Machines (ATMs) [1] cites typical techniques used in crime incidents that occurred in the past. This guide accordingly introduces analysis procedures and concepts of what security measures to take, for implementing defense in depth to prevent these techniques. The analysis approach in this guide is to decompose a crime technique into several crime steps and explains what and how should be protected from defense in depth point of view at each individual crime step. These analysis procedures can be applied to those crime techniques yet to beexploited.

It is important to consider characteristics unique to ATMs in analyzing defense in depth. Some systems such as electric power systems and rail transport systems are securely managed by administrators; other systems which are comprised of consumer devices such as smart home gateways and other smart home appliances are not. ATMs should essentially be viewed as a securely managed system because they are managed by financial institutions, trustworthy entities, together with dependable cash-in-transit (CIT) companies and maintenance contractors under legitimate contracts.

The ATM crime incidents committed in countries other than JAPAN, however, suggest the aspects of an uncontrolled system with poorly managed ATMs being targeted by attackers. There are accordingly two options in considering security measures for ATMs: one is to protect assets by enforcing stringent management in operation, the other is to protect them by using some mechanisms (e.g. encryption) similar to ones used in consumer devices regarding ATMs as unmanaged devices.

Each option has its own advantages and disadvantages. A financial institution will need to consider possible impacts of a security measure on existing ATM operations. This is why there is no simple way to tell which is the better option. This guide, therefore, provides clues to making decisions on whether to use a scheme of management or that of a system such as cryptographic technologies. What should deserve foremost consideration in this guide is the size of control workload. Security guidelines have already been released by a number of nations and public institutions, whether publicly or nonpublicly. None of these releases of guidelines, however, mentions the size of operational control workload possibly increased after recommending/mandating the security measures are implemented.

For example, criminals often illicitly withdrew money from ATMs by installing malware after opening the ATM maintenance doors with physical keys. Against such crime incidents, "Guidance and recommendations regarding logical attacks on ATMs" [2] , released by European Union Agency for Law Enforcement Cooperation (EUROPOL), recommends the following countermeasures: changing the physical locks of ATM maintenance doors with unique ones, demanding rigid personal authentication on those gaining access to the ATM maintenance doors and setting a unique password to log in as an OS administrator to each ATM.

The emergence of these guidelines has been motivated by concerns over a lack of proper management practices: a maintenance doors of every ATM could be opened with a single physical key, or the same OS administrator password was used for every ATM, which easily enabled criminals to install malware in the cases outlined above. Existing guidelines recommend a lot of stringent management in a bid to make up for such a lack of proper management. Financial institutions are forced to introduce excessive control workload, which might rather increase security risks because of possible incomplete management practices or possible default of due administrative tasks.

In certain countries, some ATMs are located in sites so far (e.g. half a day's distance) from their maintenance contractor. If a unique lock is used for the maintenance door to an ATM, for example, the ATM would be inaccessible for maintenance when the maintenance personnel failed to bring the correct physical key with them. As a result, the maintenance contractor would be accused by the financial institution because they could not perform a specified maintenance. In addition, the extended period of ATM inavailability would cause inconvenience to ATM users. Their ATM services being social infrastructures, financial institutions have obligations to provide consistent services to the society. This is one reason why security is not a foremost priority for financial institutions.

To ensure that the maintenance personnel will bring the correct key with them, additional aspects of management would be needed. Overdependence on management could result in a negative spiral of cyclic management hassles. If the introduction of a security measure is expected to have a major impact on the control workload, a security mechanism (e.g.

encryption) would be another option. Assume, for example, a crime technique that installs Personal Identification Number (PIN)-stealing malware in an ATM. One countermeasure against this threat, for example, might be equiping the ATM with a device, called "encrypting PIN pad," to encrypt a PIN within the device, instead of strictly restricting those having access to the ATM to prevent malware from being installed in the ATM.

Since all PINs output from an encrypting PIN pad are encrypted, it would be extremely difficult to abuse them even if they could be stolen by means of malware installed inside the ATM. Encrypting PIN pads, a security mechanism, thus help avoid critical consequences when ATMs cannot be placed under stringent access control, which would consequently lightened financial institutions' management burdens without sacrificing ATM user convenience.

In this way, if a security mechanism (e.g. encryption) is in place, it might lighten management burdens, reducing the chances of the maintenance personnel being unable to fix ATM failures because of the wrong physical key they carried. The result would be operational stability of ATMs. Because financial institutions need to make decisions on whether to depend on management or security mechanism (e.g. encryption) in exploring the security measures to implement, criteria in making such decisions are also included in this practice guide.

2 Security Measure Formulation Procedures

Table 2-1 outlines the procedural steps to formulate security measures for ATMs. Steps (1) to (4) are the ones where to analyze crime incidents and list proposed measures from a perspective of defense in depth. Steps (5) to (7) are the ones where to give a comparative review to the proposed measures thus listed. Step (8) is the one where to apply the proposed measures to crime incidents yet to be committed.

In (1), protected assets are listed first and their priorities are defined. Next, in (2), typical crime incidents targeting protected assets are collected. This is because typical crime techniques taken in the past are believed most likely risky. Criminals are thought to have a tendency to stick to a successful crime technique while making minor changes to it. In (3), the crime technique taken in each individual crime incident collected is broken down into attack steps. In (4), proposed measures for defending against the individual attack steps are listed with defense in depth taken into consideration.

In (5) to (7), the effectiveness of each individual measure is evaluated from a viewpoint of the control workload. Even though a financial institution introduces a security measure, if it involves an excessive control workload on the institution, inadequate perfection of management, it could result in incomplete management practice, omission or default to detract the usefulness of the security measure. Hence, the control workload needs to be analyzed to assess the practical usefulness of security measures in operation and to find out in which attack step they should prove most useful as defense. In step (5), the operations that may be impacted by the introduction of the proposed measures are listed to estimate the control workload arising from the affected operations. In step (6), risk values required for comparison purposes are derived from the estimates of the control workload with risk rating methodologies. In the last step, (7), the proposed measures are compared in terms of their practical usefulness on the basis of their risk values estimated in (6) to find out in which attack step they should be taken to prove most effective.

In step (8), analyses done in steps (1) to (7) are applied to crimes yet to be committed to estimate effective measures.

A detailed description of the step procedures by classification follows.

Table 2-1 Security Measure Formulation Procedures

Section	Classification	Item	Security Measure Formulation Procedure
2.1	Analyze crime incidents and list proposed measures	(1)	List protected assets
		(2)	Collect typical crime incidents targeting the protected assets
		(3)	Break down the crime incidents into attack steps
		(4)	List measures to defend against attack steps (with defense in depth taken into consideration)
2.2	Analyze the impact of security measures upon operations	(5)	Analyze the possible impact of the listed security measures upon existing operations (from a viewpoint of operational control workload).
2.3	Evaluate proposed measures to select adequate measures	(6)	Estimate the practical usefulness of the proposed measures with their impact upon existing operations taken into consideration.
		(7)	Compare and select proposed measures with their practical usefulness taken into consideration.
2.4	Extend application to crimes yet to be committed	(8)	Estimate effective measures through analyses in (1) to (7) above and extend their application to crimes yet to be committed.

2.1 Analyze Crime Incidents and List Proposed measures

This section describes the four steps, (1) to (4), given in Table 2-1 Security Measure Formulation Procedures.

(1) List assets to be protected

Table 2-2 lists the protected assets along with their levels of importance. The level of importance of an asset is determined from the magnitude of the impact attacks on that asset may have upon banking transactions and the size of profit the malicious group may gain. According to standards, such as PCI DSS or PCI PTS POI formulated and released by the PCI Security Standards Council, PINs and magnetic card track data have the highest level of importance followed by card numbers (primary account numbers).

On the other hand, among all assets that are not protected under existing standards, those linked to cash have a high degree of importance. For example, a cash dispensing command that gets cash out of a bill handling module is an information asset often targeted by malicious groups for its close linkage to cash. Although no cases have been reported as yet, there could be an attack in which the results of loading bills into an ATM and counting the amounts of deposits in deposit transactions are disguised to pile them up in a fraudulent account.

There have been no reports of the practice of such attacks so far, because criminals have to add attack steps in which unauthorized deposit amounts are built up in a given account in fraudulent deposit transactions before the criminals can withdraw cash from the account in normal withdrawal transactions. However, once countermeasures against fraudulent withdrawal attacks prevail, attackers could target deposit transactions.

Table 2-2 Examples of Protected Assets Listed

Importance	Asset Protected under Existing Standards or Frameworks	Asset Not Protected under Existing Standards or Frameworks
High	- PINs - Magnetic card track data	- Cash (bills, coins) - Withdrawal command - Deposit/withdrawal slot shutter open command

		- Deposit counting data - Deposit (remittance) destination account number
Medium	- Card numbers (including log data that contains card numbers)	- Card data (on memory in ATM applications) - Card media
Low	-	Log data, etc. that does not contain the above

* Payment Card Industry standard, etc.

It is necessary, therefore, to raise the priorities of those assets that can be easily targeted by attackers and that have a major impact on banking transactions.

(2) Collect typical crime incidents targeting protected assets

As explained in 1, “Introduction,” because ATMs are considered prone to the risk of iterations of past crime practices, typical practices of past crime incidents that target the “protected assets” extracted in Step (1) will be collected to aid in the formulation of security measures. Crime incidents that target the protected assets are listed in Table 2-3.

Table 2-3 Typical Crime Incidents Targeting Protected Assets

#	Import-ance	Category	Protected Asset	Crime Incident
1	High	PIN	PINs	PINs, if not encrypted, might be stolen by malware or the like.
2	Medium	Card holder data	Card holder data (memory in ATM applications)	Malware could steal Primary Account Numbers from the RAM of an ATM control unit. Malware intruding into the ATM control unit would be distributed from the software distribution server as authorized software, so that whitelist-based anti-malware protection may not work.
3	High	Cash (bills)	Cash dispensing command	a) Fraudulent withdrawals assisted by malware that is physically intruded via media. b) Fraudulent withdrawals assisted by malware that is intruded from the

				financial institution’s intranet.

(3) Break down crime incidents into attack steps

The typical practices of crimes collected in Step (2) are broken down into individual attack steps to build defense in depth against the crimes. Figure 2-1 shows the composition of a fraudulent withdrawal assisted by malware (physical intrusion), and Table 2-4 describes an example of breaking down crime incidents into attack steps.

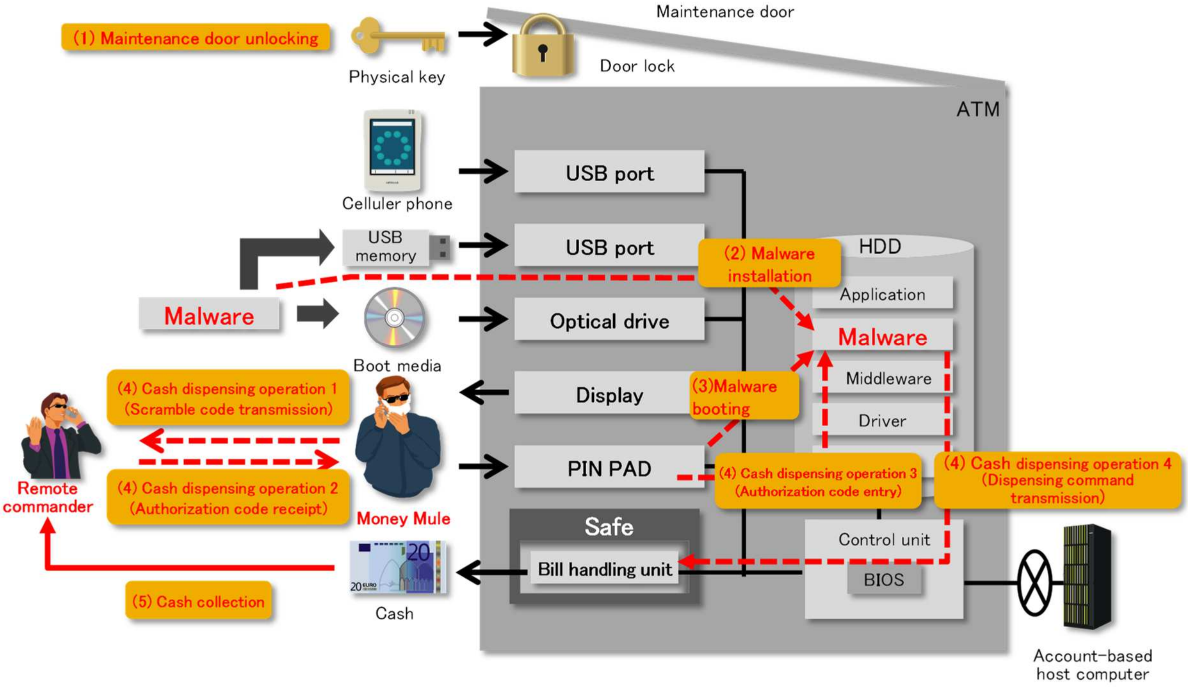

(1) Maintenance door unlocking
Physical key
Maintenance door
Door lock
ATM
Celluler phone
USB port
USB memory
USB port
(2) Malware installation
HDD
Application
Malware
Optical drive
Malware
Boot media
Middleware
Driver
(4) Cash dispensing operation 1 (Scramble code transmission)
Display
(3)Malware booting
Remote commander
(4) Cash dispensing operation 2 (Authorization code receipt)
Money Mule
PIN PAD
(4) Cash dispensing operation 3 (Authorization code entry)
(4) Cash dispensing operation 4 (Dispensing command transmission)
Safe
Bill handling unit
Control unit
BIOS
(5) Cash collection
Cash
Account-based host computer

Figure 2-1 Outline of a Fraudulent Withdrawal Assisted by Malware (Physical Intrusion)

Table 2-4 Attack Steps of a Fraudulent Withdrawal Assisted by Malware (Physical Intrusion)

#	Attack Step	Attack Description
(1)	Maintenance door unlocking	A criminal preliminarily gets (or duplicate) a physical key at a poorly controlled ATM operation site, and unlocks the maintenance door with the physical key.
(2)	Malware installation	Installs malware in the ATM control unit with a USB memory device, CD-ROM or any other media.
(3)	Malware activation	Operates the PIN pad to activate the installed malware. Even if whitelist-based anti-malware software is installed,it might be disabled by directly manipulating the ATM hard drive.
(4)	Withdrawal operation	Conducts withdrawal operations to let the malware issue a cash dispensing commands to the bill handling unit, with the result of bills

		being dispensed from the ATM. Detailed steps: The on-site criminal transmits a QR code or a scramble code appearing in the ATM screen to a remote commander (server) using a cellular phone, SMS mail or the like (1). The on-site criminal receives an authorization code on its cellular phone in reply (2) and enters it into the malware using the PIN pad on the ATM (3). This allows the malware to send cash dispensing commands to the bill handling unit and dispense bills (4).
(5)	Recovery of bills	The on-site criminal collects the bills dispenseed from the ATM.

(4) List measures to protect against attack steps (with defense in depth taken into consideration)

Once typical crime incidents are broken down into attack steps, the next step is to list measures to protect against the individual steps. Table 2-5 describes the individual attack steps of a fraudulent withdrawal case assisted by malware, with various action requirements outlined in “Guidance and recommendations regarding logical attacks on ATMs” [2] released by EUROPOL applied to them, with defense in depth in mind. In the table, boldface underscored in red identifies a requirement that possibly involves extensive control workload with the introduction of a measure. The table classifies those measures that frequently require manual logging, visual work checks and verifications or password management as “control workload-intensive measures” and other measures as “control workload-saving measures.”

Table 2-5 List of Measures to Protect against attack steps of a Fraudulent Withdrawal Assisted by Malware

	(1) Maintenance door unlocking	(2) Malware install	(3) Malware activation	(4) Withdrawal transaction
First round Physical access	**(1) Personal identification** **(2) Maintenance door key management** **(3) Surveillance monitoring**			
Second round Offline defense		**(4) BIOS password management** (5) Hard disk encryption (*1)		
Third round Online defense		**(6) OS hardening** (7) Anti-malware based on “whitelisting” (8) USB protection	**(6) OS hardening** (7) Anti-malware	

			based on “whitelisting”	
Fourth round Additional measures		**(11) Fraud monitoring** **(12) ATM monitoring** **(13) Segregation of duties**	**(11) Fraud monitoring** **(12) ATM monitoring**	**(14) Cash refilling cycles**

* Boldface underscored in red identifies a requirement that possibly involves much control workload with the introduction of a measure.

*1 If measures involve the use of passwords for encryption key management, they are classified as control workload-intensive measures.

2.2 Analyze the Impact of Security Measures upon ATM operations

This section describes Step (5) in Table 2-1.

(5) Analyze the possible impact of the listed security measures upon existing transactions

The implementation of security measures required for defense in depth could impact existing operations more or less, and/or create new management jobs. Too much impact on existing operations or burden on control work might impede thorough perfection of the management practices associated with security measures, adversely affecting their practical usefulness. Boldface underscored in red in Table 2-5 designates an action item that possibly impacts operational control workload, so that its practical usefulness is of concern. The following estimations are important to evaluate the effective strength of a security measure. One is what kinds of management items are involved in the implementation of the security measure; the other is how much associated control workload is involved in the implementation.

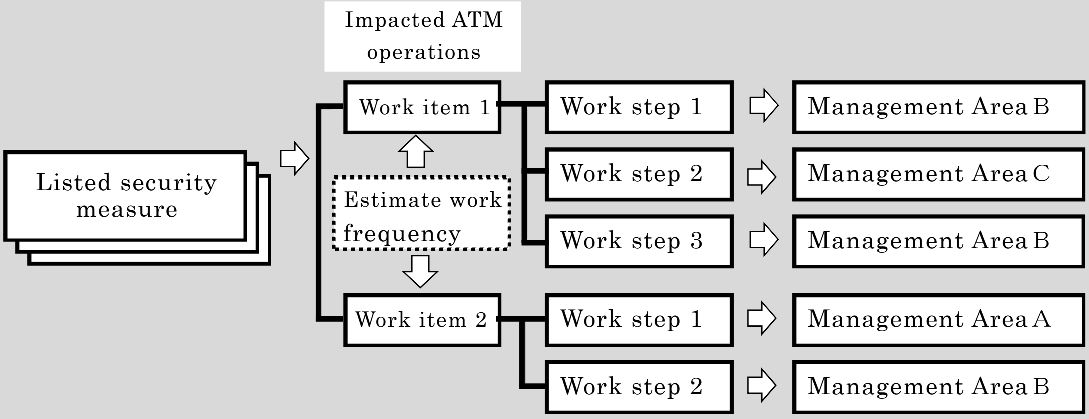
Figure 2-2 shows the procedures for analyzing the possible impact of the listed security measures upon existing operations. These procedures are organized into two analysis steps, which are further divided into six and three substeps, respectively, as outlined below.

(Analysis Step I) Analyze the possible impact of the listed security measures upon existing operations

I-(1) Identify the work items relevant to the ATM operations impacted by the implementation of the listed security measures and assume work frequencies per year.

I-(2) Break down each work item identified into a sequence of work steps.

I-(3) Define management areas relevant to ATM operations and apply a work step to each. A management area is a concept defined in this document to ease the task of estimating control work. Physical boundaries can be used to define management areas, such as work inside maintenance doors, work inside safe doors and work inside banking offices.



I-(4) Suppose the “ideal form of management” looming from the implementation of individual security measures by a management area.

I-(5) Identify new control work that is needed to achieve the “ideal form of management.”

I-(6) In addition to I-(5) above, identify control work that occurs routinely to meet the requirements, regardless of the work items occurring or not.

(Analysis Step II) Analyze the control workload of each of the listed security measures

II-(1) In each work step, estimate the control workload and accumulate them by work item. Estimate the control control workload that occurs routinely as well.

II-(2) Calculate the product of the control control workload accumulated by work item by the frequency of each work item in Ⅰ-(1). Add the workload of routinely occurring control work to the product. Then, accumulate the sums across all work items.

II-(3) Repeat II-(1) and II-(2) for each measure listed. When a listed security measure invokes a totally new work item, also repeat II-(1) and II-(2) for the new work item.

Figure 2-2 Procedures for Analyzing the Possible Impact of the Listed Security Measures upon Existing Transactions

2.2.1 (Analysis Step) Analyze the possible impact of the listed security measures

I-(1) Identify work items relevant to the ATM operations impacted by the implementation of the listed security measures and assume work frequencies per year.

To begin with, find out what existing operations will be impacted by the implementation of the security measures listed and identity such existing operations as work items. In order for a newly implemented security measure to work successfully, some kind of control work is required. For example, consider introducing a setting that disables AUTORUN to prevent malware from being installed in the ATM control unit through a USB memory device plugged into its USB port. In this case, a new management task, such as monitoring the workers' behavior to ensure keep that AUTORUN is disabled, would be needed as a work item. It would also be necessary to estimate the frequency with which that work item is carried out per year. Table 2-6 lists typical items of work relevant to ATM operations.

Table 2-6 Work Items Relevant to ATM Operations and Examples of Work Required

Work Item	Work Description
a) CIT work	A CIT company's employees or a bank's clerks collect extra cash from an ATM or replenish an ATM with wanting cash. Because the cash stored in an ATM is guarded by means of physical protection, such as a safe door, CIT work involves not only unlocking the ATM maintenance door but also unlocking the means of physical protection, such as a safe door. Financial institutions usually do not permit accessing cash alone at an ATM. They require more than one person in this case. In cash cassette installation and collection work, cash in an ATM may be exchanged using cash cassettes or may be replenished and collected without using cash cassettes. Recycling ATMs are in common service in Japan. Frequencies of CIT works vary depending on the financial institution or the branch office, because they depend on the balance between the amount of cash deposited and that of cash withdrawn. CIT works are the most frequently conducted among works gaining access to the inside of an ATM. Frequencies of CIT works are usually agreed upon between a financial institution and its CIT company to some extent, and the average frequency needs to be heard from the financial institution.
b) Periodic cleaning work	The inside of an ATM is cleaned periodically to remove dust that is accumulated inside as bills move. The dust could lead to troubles, such as bill jams. Because cleaning is carried out in the bill handling unit as well, the cleaning work arises to unlock the means of physical protection such as a safe door, as well as the ATM maintenance door. When accessing to the bill handling unit, it is normally carried out by a team of two or more workers to ensure security. Frequencies of cleaning works depend on how often the ATMs are used,

	how many bills are stored in the ATMs and what are the conditions of the bills like. To estimate work frequencies, therefore, it is necessary to verify the work records by checking with the financial institution concerned.
c) Software update work	With ATMs, software update work arises to improve ATM services. The work covers updating application, changing configuration, and renewing ad content in the ATMs and so on. The work of updating software involves developing updates at the software development site and testing them at a financial institution's test site, in addition to installing them in ATMs. Moreover, the work includes transporting the media containing software between these sites and transporting install media from media stock sites to the location of each ATM. If software is distributed from a software distribution server to individual ATMs through a network, control works are needed to prevent information leakage as the software is transported from the test site to the software distribution server site or transmitted through the network. Frequencies of the work vary from one financial institution to another. To find out how many updates are expected a year and to estimate the work frequencies, therefore, it is necessary to check with the financial institution concerned.
d) Fault recovery work	If a problem, such as a jam, occurs while bills are moving in an ATM service, fault recovery work is required. If a problem occurs outside the safe, or outside the bill handling unit, maintenance personnel would come to the site to fix it; that is, a clerk or security transporter opens the ATM maintenance door with a physical key to allow maintenance personnel to fix the problem. If a problem occurs within the bill handling unit, it involves access to the cash to fix it. Hence, access control by a team of two or more workers is required. Japan has fewer occurrences of ATM failures than other nations, but they could still happen and there is no deciding the frequencies with which to carry out recover work beforehand. It is necessary, therefore, to verify the work records by checking with the financial institutions concerned and then estimate expectations for the work frequencies under reasonable assumptions.
e) Supplies replenishment and parts replacement work	Work involving access to the inside of the ATM arises as supplies, such as operation slip print forms and passbook printer inks, are replenished and expendable parts, such as rubber rollers and belts, are replaced. Because the work of replacing rubber rollers, belts and other parts required for conveying bills sometimes requires access to cash stored inside, two or more workers working in a team, as in the case of CIT work, would be required as an access control practice. Frequencies with which the work needs to be carried out for ATMs depend on how often the ATMs are used, how many bills are conveyed and what their conditions are like. To estimate work frequencies, therefore, it is necessary to verify the work records by checking with the financial institution concerned.

I-(2) Break down each work item identified into a sequence of work steps.

After the work items that are impacted by the implementation of the listed security measures have been identified, break down each work item into a sequence of work steps and then identify the control work required for each of these work steps. Because the introduction of new security requirements could impact existing control work as well, the identification of control work required for the work steps helps size up their impact. Since financial institutions conduct operations that involve access to cash and other important assets, they are assumed to have certain management rules in place under which to ensure security in the implementation of the individual tasks procedures. These procedures also need to be broken down into work steps and the control work per step identified.

I-(3) Define management areas for ATM operations and apply a work step to each.

This document introduces the concept “management area” to ease the work of estimating the requirements for the control workload for introducing security measures. A management area consists of a group of work steps to make the control workload easier to estimate. Figure 2-3 shows an example of using physical boundaries as management areas to classify the control workload involved in the individual work steps. In this example, management areas are grouped into six: (m1) management at other sites, (m2) banking office outside in-transit management, (m3) banking office inside management, (m4) ATM maintenance door inside management, (m5) safe door inside management and (m6) monitoring center inside management. The work of moving from a site remote from the banking office in question to gain physical access to the inside (safe) of an ATM installed in that banking office, for example, would involve moving to that other site remote from the banking office, then from that site to the banking office, and moving for access within the banking office, inside the ATM maintenance door and inside the ATM safe door in this order. When the work is done, move and access will occur in reverse order. Different levels of control work by management area would be required at the same time. If surveillance cameras are available for capturing internal views of ATM booths, monitoring work at the monitoring center needs to be added as a management area.

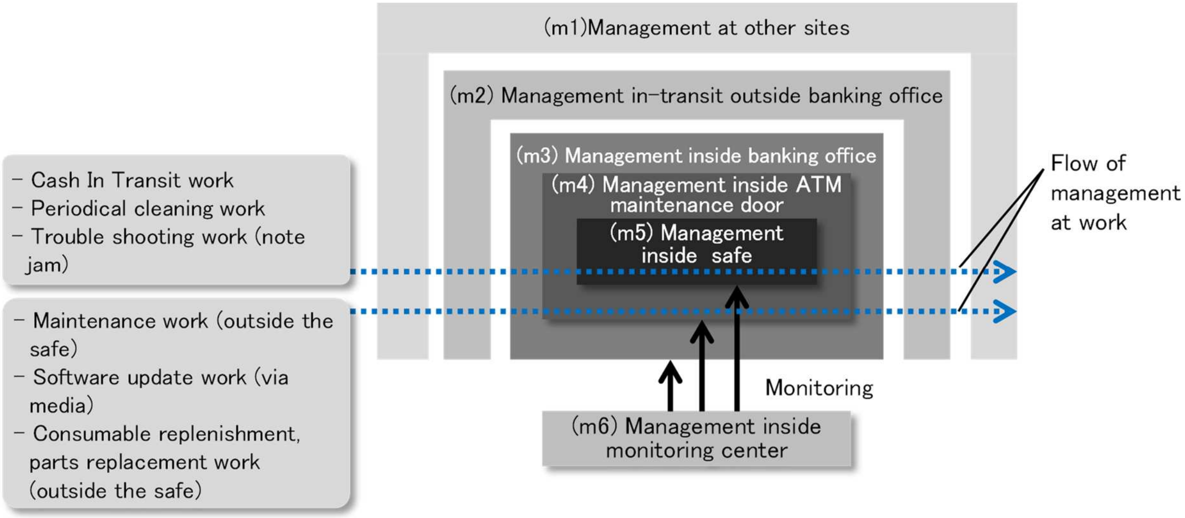

(m1)Management at other sites
(m2) Management in-transit outside banking office
(m3) Management inside banking office
(m4) Management inside ATM maintenance door
(m5) Management inside safe
Flow of management at work
Monitoring
(m6) Management inside monitoring center
– Cash In Transit work
– Periodical cleaning work
– Trouble shooting work (note jam)
– Maintenance work (outside the safe)
– Software update work (via media)
– Consumable replenishment, parts replacement work (outside the safe)

Figure 2-3 Typical Classifications of Management Areas Associated with ATM Operations

Figure 2-4 takes CIT work as an example, breaks it down into work steps, identifies the control work required per work step, defines management areas and assigns control work per work to a management area. Financial institutions usually require workers gaining access to cash stored in an ATM safe to unlock the safe door in a team or two or more. If the work does not require more than unlocking the maintenance door, only one worker might suffice to complete the task. This leaves room, however, for differences in the management level. For this reason, a management area may be set on each physical boundary to make control work easier to group and comprehend when such control work involves physical access. Individual work steps vary from one banking instruction to another in the system and working rules. Hearing from the financial institutions concerned is required to gain a precise insight into the work steps.

Further, assume that two new security measures are introduced, for example, disabling the ATM booting from media and disabling AUTORUN. These two tasks are considered identical in terms of control work because both require opening ATM maintenance doors. For this reason, both can fall into (m4) ATM management door inside management and thus can be estimated by management area to simplify the complexities of estimation work.

There is not only a single method to classify management areas. Any method of classification will do if it eases the work of estimating the administrative workload associated with the introduction of a security measure. Because cyber physical attacks at ATMs cause fraudulent dispensing cash from ATMs without opening the safe doors physically, this Guide focuses on control work analyses other than “(m5) safe door inside management.”

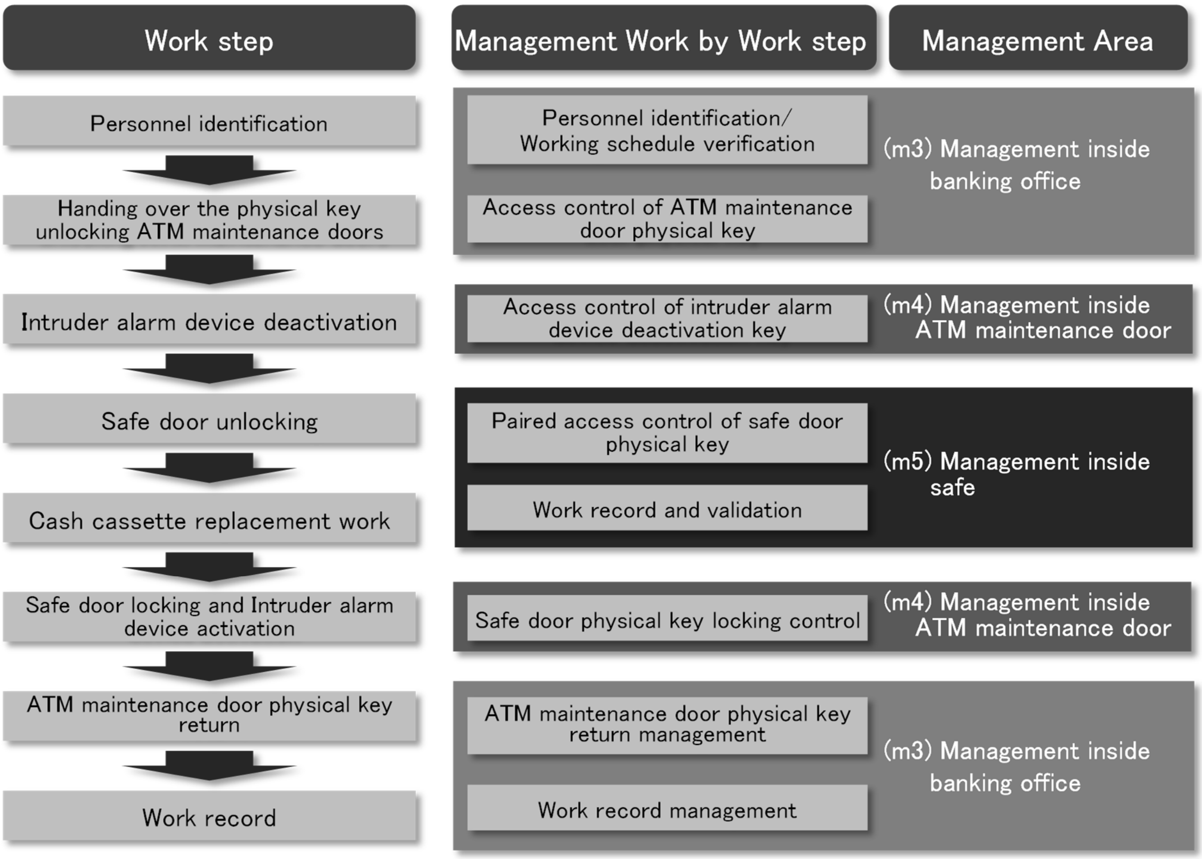

Work step
Management Work by Work step
Management Area
Personnel identification
Handing over the physical key unlocking ATM maintenance doors
Intruder alarm device deactivation
Safe door unlocking
Cash cassette replacement work
Safe door locking and Intruder alarm device activation
ATM maintenance door physical key return
Work record
Personnel identification/ Working schedule verification
Access control of ATM maintenance door physical key
(m3) Management inside banking office
Access control of intruder alarm device deactivation key
(m4) Management inside ATM maintenance door
Paired access control of safe door physical key
Work record and validation
(m5) Management inside safe
Safe door physical key locking control
(m4) Management inside ATM maintenance door
ATM maintenance door physical key return management
Work record management
(m3) Management inside banking office

Figure 2-4 Example of Breaking Down Cash In Transit Work into Work Steps and Classifying Management Areas

I-(4) Suppose the ideal form of management looming from the implementation of measures by management area.

I-(5) Identify additional management tasks needed to achieve ideal form of management.

For example, if a unique lock is introduced for a maintenance door security, it should be placed under proper access control of each key to ensure that it successfully works as a security measure. To keep ATM maintenance doors from being opened by malicious individuals exploiting a lack of proper maintenance practice, it would be necessary to take certain measures, such as enforcing strict personal identification for workers using ID cards or introducing unique lock for maintenance doors.

Appropriate control work is often needed to ensure that the security measures thus listed will work effectively. Conversely speaking, whatever measures implemented will fail to demonstrate their practical usefulness unless they are properly managed. The need arises, therefore, to identify the management tasks necessary to realize the ideal form of management to maximize the security effects of the listed security measures.

Table 2-7 describes how the management tasks needed to achieve the ideal form of management can be applied to management areas upon occurrence of work events targeting an ATM. If a physical key to an ATM maintenance door is to be brought out, it should be placed under rigid management at its checkout, usage and return. Further, if an ATM installed at an unstaffed office is to be serviced, the management of a physical key in transit to the branch (for example, a measure to keep the key from being duplicated by malicious staff) would be needed in addition. The ideal form of management in this example might include, for example, two staffs moving in a pair to check each other's behavior.

Table 2-7 Examples of Ideal Form of Management Tasks When Work Events Occur

#	Management Area	Assumed Scene	Management Tasks Required for Ideal Form of Management
1	(m2) Banking office outside in-transit management	When released	- Management while transporting media (management by two staffs working in pairs, etc.)
2		When servicing	- Management while transporting media and passwords (management by two staffs working in pairs, etc.)
3	(m3) Banking office inside management	When servicing	- Key checkout/return management, proper usage management - For branches, in-transit management (management by two staffs working in pairs, etc.)
4	(m4) ATM maintenance door inside management	When servicing	- Work-in-process fraud monitoring (management by two staffs working in pairs, etc.)
5	(m6) Monitoring center inside management	Periodic checking	- Check booth surveillance camera images periodically for problems.

I-(6) In addition to I-(5) above, identify the routinely occurring management tasks needed to meet individual requirements, regardless of whether work items occur or not.

Even for the case where an actual work does not occur as to listed security measures, it still is necessary to identify routinely occurring control work from the moment of their implementation and explore tasks needed to achieve the ideal form of management. Table

2-8 exemplifies ideal form of management tasks to routinely occurring control work by management area.

Physical keys used to unlock ATM maintenance doors need to be placed under access control not only when maintenance works are conducted accompanying accessing inside ATMs but also 24/7 even while maintenance work does not occur. The physical keys should be managed constantly so that malicious people do not pick up the keys without permission and so that malicious people make an impression of the keys to duplicate them. Even though unique locks are introduced as a security measure, if their keys are poorly managed, there will be no defending against malicious attacks. Accordingly, all management tasks that are liable to attack risks should be listed completely to preclude management flaws.

Table 2-8 Examples of Ideal Form of Management Tasks to Routinely Occurring Control work

#	Management Area	Assumed Scene	Management Tasks Required for Ideal Form of Management
1	(m3) Banking office inside management	Constantly (24hX365 days)	- Access control at physical key storage places (biometric authentication, etc.)
2	(m1) Management at other sites	Constantly during development (24h X 365 days)	- Access control or maintenance management for a development or evaluation environment
3		Constantly (24h X 365 days)	- Medium and password access control (biometric authentication, etc.) - For remote distribution, server or network security management (access control biometric authentication, etc.)
4	(m6) Monitoring center inside management	Constantly (24h X 365 days)	- Check for ATM malfunctions or unexpected shutdowns constantly. - Check booth surveillance camera video data periodically for problems.

2.2.2 (Analysis Step II) Analyze the Control Workload of the Listed

Security Measures

When the impact analyses of the administrative works are completed for the listed security measures, the next step is to estimate how much workload each administrative work will produce concretely. Human psychological aspects of the administrative works should be taken into account in this estimation. If the control works are intolerably high for staffs, they could omit or neglect some of necessary procedures, which could eventually lead to managerial vulnerabilities. Hence, the detailed load of management works involved is estimated in further depth. This step is broken into three analysis substeps as described below.

II-(1) Estimate the workload of the control work in each work step and accumulate the estimates by work item. In addition, estimate the workload of routinely occurring control work.

Estimate how much workload will be required per service for a work item on the basis of the analysis results gained in step II-(1). For example, a control work that physical keys to the ATM maintenance doors are lent to a maintenance person will involve the following: personal identification and recording in a management ledger when lending the keys, and the same when returning the keys. Even though no maintenance work occurs, access control to the physical keys is required 24/7 to keep them from unauthorized accesses by malicious individuals. Such control works could occur routinely. What kinds of management ways should be assumed are to be determined in consultation with the financial institution concerned.

Table 2-9 Examples of Estimates of Assumed Control Workload by Management Area

#	Management Area	Assumed Scene	Management Tasks Required for Ideal Form of Management	Assumed Control Workload
1	(m2) banking office outside in-transit management	When servicing	- Management while transporting media and passwords (management by two staffs working in pairs, etc.)	Labor unit cost x 2 workers x travel time / occurrence / banking office
2	(m3) Banking office inside management	When servicing	- Key checkout/return management, proper usage management	Key checkout/return procedure hours / occurrence / banking office
3			- For branches, in-transit management (management by two staffs working in pairs, etc.)	Labor unit cost x 2 staffs x travel hours / occurrence / banking office

4	(m4) ATM maintenance door inside management	When servicing	- Work-in-process fraud monitoring (management by two workers working in pairs, etc.)	Labor unit cost x 2 staffs x work hours / occurrence / ATM
5	(m6) Monitoring center inside management	Periodic checking	- Check booth surveillance camera images periodically for problems.	Video verification work hours / occurrence / week / office

One example of the management might be using a surveillance camera to constantly capture those gaining access to the physical keys. In this case, the names and times recorded in the management ledger can be verified against the images of the individuals and times captured on the surveillance camera. Once per week of video-recorded data might be played back at fast speed to verify in one hour, for example. In this way, it is necessary to estimate how much control workload will be needed so that listed measures work effectively under relevant assumptions. Table 2-9 exemplifies calculations to estimate the workload required for the ideal control work by management area. The estimation requires the number of staffs involved, their working time per occurrence, the number of banking offices and so on.

II-(2) Calculate the product of the workload of the control work accumulated by work item by the frequency of each work item in Ⅰ-(1). Add the workload of routinely occurring control work to the product. Then, accumulate the sums across all work items.

Multiply the control workload required for a work item occurring as estimated in II-(1) by the frequency estimated in I-(1) to estimate how much control workload will occur per year. Add estimates of the control workload that occurs routinely, regardless of whether work items occur or not, to the product. Because the control workload also varies depending on the number of ATMs installed, that of banking offices,and/or that of development sites, it needs to be proportionalized according to these kinds of factors. Assuming that CIT work occurs at a frequency of once a week, for example, it should occur 52 times a year. Assuming that the ad content in ATMs is renewed every season, then the software update work occurs four times a year. Regarding periodically occurring control work, if it is required, for example, to capture internal views of ATM booths with surveillance cameras and to verify the video data once each week, it should occur 52 times a year.

In this way, if the product of each work item by its frequency is calculated and then accumulated across all work items, then the annual control workload can be estimated for one measure listed.

II-(3) Carry out II-(1) and II-(2) above for each security measure listed. Even though a listed measure gives rise to a totally new work item, perform Analysis Steps I and II as well.

If two or more measures have been listed, the work outlined in II-(1) and II-(2) needs to be carried out for each measure. In practice, the requirements for control workload for each listed security measure are collectively estimated in groups, such as management areas. For example, if a listed security measure involves the work of setting a BIOS password and that of setting an OS administrator password, control work necessary to prevent these passwords from being stolen or abused will be required at the same time. Two workers must always work in a pair to check each other if setting at least either a BIOS password or a OS administrator password is introduced.

Thus, control work would become necessary if any requirement is involved in the work to be carried out inside maintenance doors, rather than separate control work will become required for each security measure to be implemented.

It follows, therefore, that, the job of estimating the control workload requirements can be conducted easier by grouping each of the listed security measures with a particular management area.

Table 2-10 outlines how each measure can be applied to a management area, without breaking the measure into work steps, to gain a preliminary estimate of the extent of its impact. As explained above, boldface underscored in red designates a requirement that possibly involves high operational control workload in the implementation of a measure. It roughly suggests which management area includes less control workload.

If a control work is newly introduced, additional control works should be considered. For example, if biometric authentication is introduced for access control of physical keys to ATM maintenance doors, the additional control work is verifying the biometric authentication logs or visually verifying the status of access to physical keys constantly captured by surveillance cameras. For these additional control works, Analysis of Steps I and II must be carried out as well.

Table 2-10 Examples of Management Areas Relevant to Measures (EUROPOL Requirements

#	Attack Step	Measure (EUROPOL Requirement)	Management Area
1	(1) Maintenance door unlocking	**(1) Personal identification** **(2) Maintenance door key management** **(3) Surveillance camera**	(m3) Banking office inside management
2	(2) Malware install	**(4) BIOS password protection** (5) Hard disk encryption (including password and encryption key management)	(m1) Management at other sites (m2) banking office outside in-transit management (m3) Banking office inside management (m4) ATM maintenance door inside management
3		**(6) OS hardening** (7) Whitelist (8) USB device defense **(11) Software behavior monitoring**	(m4) ATM maintenance door inside management
4		**(12) ATM equipment monitoring (unexpected reboot)**	(m6) Monitoring center inside management
5		**(13) Division of duties**	(m3) Banking office inside management
6	(3) Malware activation	**(6) OS hardening** (7) Whitelist **(11) Software behavior monitoring**	(m4) ATM maintenance door inside management
7		**(12) ATM equipment monitoring**	(m6) Monitoring center inside management
8	(4) Withdrawal transaction	**(14) Cash replenishment amount/interval optimization**	(m5) Safe door inside management

2.3 Evaluate Proposed Measures Comparatively

This section describes Steps (6) to (7) in Table 2-1.

(6) Estimate the practical effectiveness of the proposed measures with their impact upon existing operations.

Estimate how the security risks will vary before and after the implementation of the listed security measures, using a risk assessment formula. A number of risk assessment methods are available. Table 2-11 lists some typical risk assessment methods. The CVSS method is the most commonly used, whereby risk values are assessed from viewpoints of the impact of attacks and the ease of exploit.The CCDS prototype method is a simplified version of the CVSS method. The EDC method is a method estimating risk values with combination of an event tree and a defense tree. Risk values are estimated based on an event-driven of attacks, whereby an event whether an attack succeds or fails determines the subsequent attack steps or defense steps.

The ALE (annualized loss expectancy) method estimates a risk value in terms of an annualized loss amount. The annualized loss expectancy is calculated as the product of the single loss expectancy and the annualized rate of occurrence. The more an implemented security measure involves control workload, the more it would be prone to human mistakes or negligence, which might be exploited by attackers. Therefore, the control workload can be substituted for the annualized rate of occurrence with an appropriate equation. For example, human work errors are said to have an occurrence probability of 1% or so. If 1% of the 1% leaves solid blocks of exploitation time available for attackers, one 10,000th of the control workload (time) can be viewed as a time open to attacks. This estimate is just an example and appropriate risk assessment. Suitable risk values should be assessed based on an insight into the actual operating conditions of the financial institution.

OWASP (Open Web Application Security Project) is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. The OWASP Risk Rating Methodology (OWASP method) is a risk rating methodology developed by the OWASP. It is characterized by financial damages and reputation damages, being included in the risk factors. Overall likelihood and overall impact are evaluated on the basis of their average values of many factors. So each factor does not significantly impact the overall values.

Discussions above have reviewed the substantive effects of the listed security measures with risk assessment methods. The substantive effects of the measure can be compared in terms of the size of control workload involved as well. Too high control workload could incur omissions at work or defaults in the worst case, detracting the practical effectiveness of the measures. The lower the control workload is, the less risk the measure has and the more securely it works.

Table 2-11 Examples of Risk Assessment Methods

Assessment Method	Equation
CVSS method	Base score = RoundUp1 (min [(impact＋Ease of exploit), 10]) impact = 1 - (1 - C) * (1 - I) * (1 - A) ease of exploit = 8.22 * AV * AC * PR * UI C: Confidentiality Impact, I: Integrity Impact, A: Availability Impact AV: Attack Vector, AC: Attack Complexity, PR: Privileges Required, UI: User Interaction
CCDS Prototype method	Risk score = (Exploitability subscore + Impact subscore) * Attacker's motivation Difficulty = 4 ranks (multiple conditions, single condition, one or more conditions, no need for conditions) impact = 4 ranks (minor, medium, serious, destructive)
EDC method	EDC: Event tree and Defense tree combined method Total risk value = Add up risk values by time-series event Risk value by time-series event = Attack failure probability at that time-series event * Impact of damages incurred up to the time-series event before the last
ALE method	Annualized loss expectancy (ALE) = Single loss expectancy (SLE) * Annualized rate of occurrence (ARO) = Asset value (AV) * Exposure factor (EF) * Annualized rate of occurrence (ARO) single loss expectancy (SLE) = Asset value (AV) * Exposure factor (EF) SLE: Single Loss Expectancy ARO: Annualized Rate of Occurrence

OWASP method	Risk = Likelihood * Impact
	Likelihood = Threat agent + Vulnerability
	Impact = Technical Impact + Business Impact

(7) Compare and select proposed measures with their practical effectiveness.

Now the control workload or a risk value of each security measure has been calculated, those values can be compared to identify in which attack steps the measures should be implemented with maximum performance. As a control workload corresponds to a risk values, a method to compare the control workloads, instead of the risk values, is used in the following.

Table 2-12 Measures Associated with Management Areas (EUROPOL Requirements)

Attack Step	Management Area	Measure (EUROPOL Requirement)
(1) Maintenance door unlocking	(m3) Management inside banking office	**(1) Personal identification** **(2) Maintenance door key management** **(3) Surveillance camera**
(2) Malware installation	(m1) Management at other sites	**(4) BIOS password protection** (5) Hard disk encryption (including password and encryption key management)
	(m2) Management in-transit outside banking office	**(4) BIOS password protection** (5) Hard disk encryption (including password and encryption key management)
	(m3) Management inside banking office	**(4) BIOS password protection** (5) Hard disk encryption (including password and encryption key management) **(13) Division of duties**
	(m4) Management inside ATM maintenance door	**(4) BIOS password protection** (5) Hard disk encryption (including password and encryption key management) **(6) OS hardening** (7) Whitelist (8) USB device defense **(11) Software behavior monitoring**
	(m6) Management inside monitoring center	**(12) ATM equipment monitoring (unexpected reboot)**

(3) Malware activation	(m4) Management inside ATM maintenance door	**(6) OS hardening** (7) Whitelist based anti-malware software **(11) Software behavior monitoring**
	(m6) Management inside monitoring center	**(12) ATM equipment monitoring**
(4) Withdrawal operation	(m5) Management inside safe door	**(14) Cash replenishment amount/interval optimization**

While Table 2-10 summarized which management area each measure (the Guidelines requirements) is associated with, Table 2-12 summarized which measures each management area is associated with. Since annual control workloads have already been estimated by management area, it possible to identify and prioritize the attack steps to defend most efficiently and most effectively by comparing the control workloads. In Table 2-12, once the defense against “(3) malware activation” is failed, “(14) cash replenishment amount/interval optimization” is the only measure left to prevent “(4) withdrawal transaction.” This measure requires checking cash balances from time to time as a monitoring activity. If one were to seriously prevent fraudulent withdrawals at this stage, one would have to check cash balances every hour, for example. This would be too unrealistic to make the Guidelines requirements truly effective. Accordingly, a comparative assessment with the control workloads required should make it possible to formulate appropriate security measures within limited resources and budgets.

2.4 Extending Application to Crimes Yet to be Committed

This section focuses on Step (8) in Table 2-1.

(8) Extend application of measures to potential crimes through analyses above

Even for potential crimes, it is possible to break a crime down to attack steps and to estimate control workloads of security measures against an attack step in accordance with the procedural steps (1) to (7) above. In detail;

(1) identify protected assets,

(2) refer similar crime incidents,

(3) break down the crime into attack steps assumed with the similar incidents,

(4) list the measure candidates to defend the each attack step from a view point of defense in depth,

(5) analyze the possible impact of the measures upon the existing operations (operational control workload),

(6) estimate the practical effectiveness of the measures with their impact on the existing operations,

(7) select the most relevant measures by comparing the measures from a standpoint of their practical effectiveness and select the attack steps that can be most effectively defended against.

Regarding (2) (3), what is important is to think what kinds of attacks criminals are up to next, to maximize the effects of selected security measures. Just as the statement “The size of returns for risks should be of concern to the criminals as well” in Chapter 1 says. Supposing existing attacks to get some assets are completely failed, consider what assets with the second priority criminals would try to get. Then think of what attack methods criminals would prefer from a perspective of the criminal’s inventments, attack workloads, and risks of detection or apprehension. Namely, it is important to imagine what criminals would attack and how from a criminals’ standpoint. In this way, the framework presented here should make it possible to design specific security measures and to estimate the practical effectiveness of the measures even for potential crimes.

3 Conclusion

This document provides guidelines for the consideration of ATM security measures; which is better to protect assets by enforcing stringent management in operation or by mechanisms such as cryptography as well as consumer devices.

The vast amount of control workloads is required to make existing measures work effectively in some cases. Neverthaless, none of the existing security guidelines have expressly pointed out it. For this reason, ineffective measures have been introduced into financial institutions without regard to the situations. This document suggests one approach to evaluate the effectiveness of measures quantitatively by numerically estimating control workloads accompanying a measure to cope with such issues.

Although this document is developed as security guidelines relating to ATM operations, it might be applicable to other kinds of products as well: assumed threats, security measures in the life cycle of a product. Vendors are encouraged to make positive use of this guidelines volume in exploring security measures in their product development process.

APPENDIX RISK RATING FORMULA

Appendix 1 CVSS (Common Vulnerability Scoring System) v3 Method [3]

CVSS (Common Vulnerability Scoring System) is an open and generalized method of vulnerability assessment for information systems. It offers a vendor-independent common tool of assessment. CVSS employs three kinds of metrics to designate the severity of vulnerabilities: (1) base metrics, (2) temporal metrics and (3) environmental metrics. Each of these three kinds of metrics is expressed in a range of values from 0.0 (low) to 10.0 (high).

In the course of its upgrading from v2 to v3, CVSS has been modified to feature:

(1) use of a technique for assessment by component;

(2) introduction of an assessment item called “scope” to allow for an expanding scope of impact from vulnerabilities;

(3) segmentation of base metrics; and

(4) changes to the approach to environmental metrics.

For more information, see References.

1.1 Base Metrics

Base metrics is a standard under which to assess the characteristics of vulnerabilities. It assesses the impact upon three security characteristics required of an information system, that is, confidentiality impact, integrity impact and availability impact, from a perspective of being attackable from network to calculate a CVSS base score. With base metrics, the rating result is fixed and does not change with the lapse of time or differences in the user environment. It is assessed by vendors, organizations that publicize vulnerabilities and the like to represent the severity unique to vulnerabilities. CVSS base scores (base scores) are expressed in equations as follows:

(1) Impact

Before-adjustment impact = 1-(1-C) * (1-I) * (1-A) …Eq. (1)

Impact (Scope Unchanged) = 6.42 * Before-adjustment impact …Eq. (2)

Impact (Scope Changed) = 7.52 * (Before-adjustment impact - 0.029)

-3.25 * (Before-adjustment impact - 0.02)^{15} …Eq. (3)

(2) Exploitability

Ease of exploit = 8.22 * AV * AC * PR * UI …Eq. (4)

(3) Base score

If the impact is zero or less, base score = 0 …Eq. (5)

If the impact is larger than 0,

Scope Unchanged: Base score = Round up (min [(Impact + Exploitability), 10]) (First decimal place rounded up) …Eq. (6)

Scope Changed: Base score = Round up (min [(1.08 * (Impact + Exploitability)), 10]) (First decimal place rounded up) …Eq. (7)

Definitions of C, I, A, AV, AC, PR and UI are found in Table a1-1 and Table a1-2.

Table a1-1 Metrics Required for Calculating Impacts

Assessment Item	Metric Value	Description	Value
Confidentiality Impact (C)	High (H)	Confidential information or sensitive system files could be referenced to deliver an extensive impact.	**0.56**
	Low (L)	Problems, such as information leakage or avoidance of access restrictions, could arise but their impact is restricted.	**0.22**
	No (N)	No confidentiality impact.	**0.00**
Integrity Impact (I)	High (H)	Confidential information or sensitive system files could be modified to deliver an extensive impact.	**0.56**
	Low (L)	Information can be modified, except for confidential information and sensitive system files, so that the possible impact is limited.	**0.22**
	No (N)	No integrity impact.	**0.00**
Availability Impact (A)	High (H)	Resources (such as network bandwidths, processor processing and disk spaces) may be completely exhausted or shut down.	**0.56**
	Low (L)	Resources could be temporarily exhausted or operations could be delayed or interrupted.	**0.22**
	No (N)	No availability impact.	**0.00**

Table a1-2 Metrics Required for Calculating the Ease of Exploit

Assessment Item	Metric Value	Description	Value
Attack Vector (AV)	Network (N)	The target component is remotely attackable via a network, e.g., attacks launched from the Internet.	**0.85**
	Adjacent (A)	The target component needs to be attacked from an adjacent network, for example, via a local IP subnet, Bluetooth or IEEE 802.11.	**0.62**
	Local (L)	The target component needs to be attacked from a local environment, e.g., launching attacks with a local access privilege or by loading fraudulent files into a word-processing application is required.	**0.55**
	Physical (P)	The target component needs to be attacked from a physical access environment, e.g., launching attacks launched via IEEE 1394 or a USB device is required.	**0.20**
Attack Complexity (AC)	Low (L)	The target component is attackable at all times without needing special attack conditions.	**0.77**
	High (H)	There are attack conditions dependent on other than attackers. For example, any one of the conditions outlined below might apply in some case. Attackers need to collect information about the objects they are about to attack, such as configuration information, sequence numbers and common keys, beforehand. Attackers also need to define the environmental conditions under which their attacks can succeed, such as contention and heap spray success conditions.Attackers require an environment to launch intermediary attacks.	**0.44**
Privileges Required (PR)	None (N)	No special privileges are required.	**0.85 (0.68)***
	Low (L)	Basic privileges regarding components will suffice, such as the right of access to non-confidential information.	**0.62 (0.50)***
	High (H)	An equivalent of the administrator privileges for components is required, such as those gaining access to confidential information.	**0.27**
User Interaction (UI)	None (N)	Vulnerabilities could be exploited without users doing anything.	**0.85**
	Required (R)	User actions, such as clicking a link, viewing files or making configuration changes, are required.	**0.62**
Scope (S)	Unchanged (U)	The scope of impact is restricted to the authorization scope to which a vulnerable component is attributed.	**-**
	Changed (C)	The scope of impact could expand beyond the authorization scope to which a vulnerable component is attributed. Examples include cross-site scripting and vulnerabilities that could be exploited by reflector attackers.	**-**

(*) Value for “scope change.”

1.2 Temporal Metrics

Temporal metrics is a standard under which to assess the present severity of vulnerabilities. It assesses such severity from a standpoint of whether exploit codes appear or not or whether action information is available or not to work out a CVSS temporal score. The rating result based on temporal metrics varies with the lapse of time according to the status of approach to vulnerabilities. It is assessed by vendors, organizations that publicize vulnerabilities and the like to represent the present status of vulnerabilities. CVSS temporal scores (base scores) can be expressed in an equation as follows:

Temporal score = Round up (Base score * E * RL * RC) …Eq. (8)

(First decimal place rounded up)

E, RL and RC are defined in Table a1-3.

Table a1-3 Metrics Required for Calculating Temporal Scores

Assessment Item	Metric Value	Description	Value
Exploit Code Maturity (E)	Not Defined (X)	This item is not rated.	**1.00**
	High (H)	An exploit code is available under any circumstances. Attackable without needing an exploit code.	**1.00**
	Functional (F)	An exploit code exists and is usable in most situations	**0.97**
	Proof-of-Concept (POC)	A proof of concept exists. An imperfect exploit code exists.	**0.94**
	Unproven (U)	A proof of concept or exploit code is not available. Attack techniques exist only theoretically.	**0.91**
Remediation Level (RL)	Not Defined (X)	This item will not influence the score.	**1.00**
	Unavailable (U)	No remedies are available. Remedies cannot be applied.	**1.00**
	Workaround (W)	Unofficial remedies are available from other than product developers.	**0.97**
	Temporary Fix (T)	Workarounds are available from product developers.	**0.96**
	Official Fix (O)	An official measure is available from the product developer.	**0.95**
Report Confidence (RC)	Not Defined (X)	This item will not influence the score.	**1.00**
	Confirmed (C)	Vulnerability information has been confirmed by the product developer. Vulnerabilities have been confirmed at the source code level. Vulnerability information has been broadly confirmed from a proof of concept, exploit code or the like.	**1.00**

	Reasonable (R)	Multiple sources of unofficial information have been released by security vendors, survey groups or the like. Vulnerabilities have not been confirmed at the source code level. Vulnerabilities have not yet been fully determined or verified.	**0.96**
	Unknown (U)	Only unconfirmed information exists. There are several conflicting items of information.	**0.92**

1.3 Environmental Metrics

Environmental metrics is a standard under which to assess the severity of final vulnerabilities, including the product user's usage environment. It assesses the severity of final vulnerabilities from a standpoint of the magnitude of secondary damages from attacks, the status of usage of the target product within an organization or the like to work out a CVSS environmental score. The rating result based on environmental metrics varies from every product user according to the threat assumed for the vulnerabilities. It is assessed by product users to determine how to respond to vulnerabilities. CVSS environmental scores are expressed in equations as:

(1) Modified impact

Modified Before-adjustment impact = min [(1 - (1 - MC * CR) * (1 – MI * IR)
* (1 - MA * AR)), 0.915] ...Eq. (9)

Modified Impact (no scope change) = 6.42 * Modified Before-adjustment impact ...Eq. (10)

Modified Impact (scope change) = 7.52 * (Modified Before-adjustment impact - 0.029)
- 3.25 * (Modified Before-adjustment impact
- 0.02)^{15} ...Eq. (11)

(2)Modified ease of exploit

Modified ease of exploit = 8.22 * MAV * MAC * MPR * MUI ...Eq. (12)

(3)Environmental score

If the modified impact is zero or less, environmental score = 0 ...Eq. (13)

If the modified impact is greater than 0, no scope change:

Modified base score = Round up (min [(Modified impact + Modified ease of exploit), 10])

Environmental score = Round up (Modified base score * E * RL * RC) ...Eq. (14)

(First decimal place rounded up)

scope change:

Modified base score = RoundUp1 (min [(1.08 * (Modified impact
+ Modified ease of exploit)), 10])

Environmental score = RoundUp1 (Modified base score * E * RL * RC) …Eq. (15)
(First decimal place rounded up)

Definitions of CR, IR and AR in Eq. (9) above are found in Table a1-4; those of MC, MI and MA in Table a1-5; MAV, MAC, MPR and MUI in EQ. (12) in Table a1-6; and E, RL and RC in Eq. (14) and (15) in Table a1-3.

Table a1-4 Target System Security Requirements (CR, IR and AR: Security Requirements)

Assessment Item	Metric Value	Description	Value
Confidentiality Requirement (CR)	Not Defined (X)	This item will not influence the score.	**1.0**
	High (H)	Loss of this item could leave a devastating impact.	**1.5**
	Medium (M)	Loss of this item could leave a serious impact.	**1.0**
	Low (L)	The impact would be limited if this item is lost.	**0.5**
Integrity Requirement (IR)	Not Defined (X)	This item will not influence the score.	**1.0**
	High (H)	Loss of this item could leave a devastating impact.	**1.5**
	Medium (M)	Loss of this item could leave a serious impact.	**1.0**
	Low (L)	The impact would be limited if this item is lost.	**0.5**
Availability Requirement (AR)	Not Defined (X)	This item will not influence the score.	**1.0**
	High (H)	Loss of this item could leave a devastating impact.	**1.5**
	Medium (M)	Loss of this item could leave a serious impact.	**1.0**
	Low (L)	The impact would be limited if this item is lost.	**0.5**

Table a1-5 Reassessing Base Metrics with Environmental Conditions Taken into Account (Modified Base Metrics) 1

Assessment Item	Metric Value	Description	Value
Modified Confidentiality Impact (MC: Modified Confidentiality)	Not Defined (X)	If “Not Defined” is selected, reference the rating result with base metrics.	-
	High (H)	Confidential information or sensitive system files could be referenced to deliver an extensive impact.	**0.56**
	Low (L)	Problems, such as information leakage or avoidance of access restrictions, could arise but their impact is restricted.	**0.22**
	None (N)	No confidentiality impact.	**0.00**
Modified Integrity Impact (MI: Modified Integrity)	Not Defined (X)	If “Not Defined” is selected, reference the rating result with base metrics.	-
	High (H)	Confidential information or sensitive system files could be modified to deliver an extensive impact.	**0.56**
	Low (L)	Information can be modified, except for confidential information and sensitive system files, so that the possible impact is limited.	**0.22**
	None (N)	No integrity impact.	**0.00**
Modified Availability Impact (MA: Modified Availability)	Not Defined (X)	If “Not Defined” is selected, reference the rating result with base metrics.	-
	High (H)	Resources (such as network bandwidths, processor processing and disk spaces) may be completely exhausted or shut down.	**0.56**
	Low (L)	Resources could be temporarily exhausted or operations could be delayed or interrupted.	**0.22**
	None (N)	No availability impact.	**0.00**

Table a1-6 Reassessing Base Metrics with Environmental Conditions Taken into Account (Modified Base Metrics) 2

Assessment Item	Metric Value	Description	Value
Attack Vector (MAV)	Not Defined (X)	If “Not Defined” is selected, reference the rating result with base metrics.	-
	Network (N)	The target component is remotely attackable via a network, e.g., attacks launched from the Internet.	**0.85**
	Adjacent (A)	The target component needs to be attacked from an adjacent network, for example, via a local IP subnet, Bluetooth or IEEE 802.11.	**0.62**

	Local (L)	The target component needs to be attacked from a local environment, e.g., launching attacks with a local access privilege or by loading fraudulent files into a word-processing application is required.	**0.55**
	Physical (P)	The target component needs to be attacked from a physical access environment, for example, via IEEE1394 or a USB device.	**0.20**
Modified Attack Complexity (MAC)	Not Defined (X)	If “Not Defined” is selected, reference the rating result with base metrics.	-
	Low (L)	The target component is attackable at all times without needing special attack conditions.	**0.77**
	High (H)	There are attack conditions dependent on other than attackers. For example, any one of the conditions outlined below might apply in some case. Attackers need to collect information about the objects they are about to attack, such as configuration information, sequence numbers and common keys, beforehand. Attackers also need to define the environmental conditions under which their attacks can succeed, such as contention and heap spray success conditions. Attackers require an environment to launch intermediary attacks.	**0.44**
Modified Privileges Required (MPR)	Not Defined (X)	If “Not Defined” is selected, reference the rating result with base metrics.	-
	None (N)	No special privileges are required.	**0.85 (0.68)***
	Low (L)	Basic privileges regarding components will suffice, such as the right of access to non-confidential information.	**0.62** **(0.50)***
	High (H)	An equivalent of the administrator privileges for components is required, such as those gaining access to confidential information.	**0.27**
Modified User Interaction (MUI)	Not Defined (X)	If “Not Defined” is selected, reference the rating result with base metrics.	-
	None (N)	Vulnerabilities could be exploited without users doing anything.	**0.85**
	Required (R)	User actions, such as clicking a link, viewing files or making configuration changes, are required.	**0.62**
Modified Scope (MS)	Not Defined (X)	If “Not Defined” is selected, reference the rating result with base metrics.	-
	Unchanged (U)	The scope of impact is restricted to the authorization scope to which a vulnerable component is attributed.	**-**
	Change (C)	The scope of impact could expand beyond the authorization scope to which a vulnerable component is attributed. Examples include cross-site scripting and vulnerabilities that could be exploited by reflector attackers.	**-**

1.4 Seriousness Classifications

CVSS assesses (1) base metrics, (2) temporal metrics and (3) environmental metrics in sequence to represent the severity of vulnerabilities in a range of values from 0.0 (low) to 10.0 (high). CVSS v3 classifies the values thus assessed into the following scores of severity rankings:

Table a1-7 Qualitative Severity Rating Scale

Rating	CVSS Score
Critical	9.0 - 10.0
High	7.0 - 8.9
Medium	4.0 - 6.9
Low	0.1 - 3.9
None	0.0

Appendix 2 Modified CCDS Method [4]

The modified CCDS method is a risk assessment formula that represents a version of the CVSS method simplified from the CCDS perspective. The method of calculating risk values is mathematically expressed in an equation as:

Risk value = (Difficulty + Impact) * Attacker's motivation…Eq. (16)

Difficulty, impact and attacker's motivation criteria are defined in Table a2-1 to Table a2-3, respectively. Ranks, which are associated with the risk values calculated by solving Eq. 1, are listed in Table a2-4. CCDS has empirically found that there are no major differences between the RISK values calculated by the CVSS method and those calculated by the modified CCDS method, suggesting the modified CCDS method offers a convenient tool of assessing risk values.

Table a2-1 Difficulty Criteria

Rank	Criteria	Value
S	Multiple conditions (such as authentication and special privileges) are required, and connectable (for an attack) only from a local environment.	**1**
A	A single condition (such as authentication or special privilege) is required, and connectable (for an attack) only from a local environment.	**3**
B	One or more conditions (such as authentication and special privileges) are required, or connectable (for an attack) only from a local environment.	**5**
C	No attack conditions are required and connectable (for an attack) from a wireless network.	**10**

Table a2-2 Impact Criteria

Rank	Criteria	Value
Minor	Attacks leave no impact upon users, or only produce a minor error indication, and leaking information does not help identify an individual.	**1**
Medium	Attacks put users at a disadvantage or leaking information helps identify an individual.	**3**
Serious	Attacks put users at a disadvantage and also produce incidental damages, or leaking information helps identify multiple individuals.	**5**
Destructive	Attacks produce fatal damages or incidental damages.	**10**

Table a2-3 Attacker's Motivation Criteria

Rank	Criteria	Value
Low	Attacks occur accidentally and the attackers have no intention.	**1**
Medium	Attackers have objectives, such as testing, pastime or self-display.	**1.25**
High	Attackers have a specific strong motive, such as gaining monetary benefits or threatening security.	**1.5**

Table a2-4 Risk Value Rank Criteria

Rank	Risk Value
Must	17 - 30 (maximum value)
High	12 - 16.9
Middle	8 - 11.9
Low	0 - 7.9

Appendix 3 Event Tree and Defense Tree Combined Method (EDC) Method [5]

The “Event Tree and Defense tree combined method” (EDC) method is a method that was presented by Ryohei Ishi and others at the JSSM (Japan Society of Security Management). Attackers attacking a system often do so by varying their methods to suit the time-series events, such as proceeding further attacks if an attack method succeeds or otherwise resorting alternative methods. In the circumstances, the EDC method has been developed as a method of listing and compiling the events that are executed in a time-series into an event tree and estimating risk values from the probability of occurrence of the individual time-series events and their impact while formulating measures to mitigate their occurrence and assessing their effectiveness. A summary description of the EDC method is given below.

(1) Extract time-series events and describe their impact

In implementing a fraudulent withdrawal assisted by malware, for example, it is necessary to (1) unlock the maintenance door, (2) install malware, (3) activate the malware and (4) conduct a withdrawal transaction (because the on-site perpetrator could use a cellular phone, not a card, to get a withdrawal permit on challenge/response authentication). These time-series events are extracted and compiled into an event tree and the impact of individual events occurring is also described. The impact should be properly set to reflect the amount of damages and impact upon operations/business.

(2) Calculate probabilities of occurrence by time-series events and describe countermeasures

Next, conduct a defense tree analysis with regard to each time-series event as a top event. A defense tree analysis is to list and link the events that could generate a top event, from the top downward, to generate a fault tree and thus to calculate the probability of occurrence of the top tree from the probability of occurrence of each individual event. This method also defines the effectiveness of measures taken to inhibit the occurrence of lower-level events by listing them and their effects (reduction rate) side by side.

(3) Calculate the total risk value

Determine the product of the probability of occurrence of each time-series event by the impact (event risk) before totaling the products to arrive at a total risk value. Figure a3-1 shows how to calculate total risks with reference a fraudulent withdrawal assisted by malware as an example.

Attack Time-Series Event	Initial Event (malware development)	(1) Maintenance door unlocking	(2) Malware installation	(3) Malware activation	(4) Withdrawal transaction	(5) Attack success
Attack success probability	P0 (=1)	P1	P2	P3	P4	P1 * P2 * P3 * P4
Attack failure probability	(1 - P0) (= 0)	1 - P1	1-P2	1-P3	1-P4	-
Magnitude of impact at attack failure at that time-series event (*)	-	M1	M2	M3	M4	M5
Risk value by time-series event	-	(1 - P1) * M1	P1 * (1 - P2) * M2	P1 * P2 * (1 - P3) * M3	P1 * P2 * P3 * (1 - P4) * M4	P1 * P2 * P3 * P4 * M5
Total risk value	(1 - P1) * M1 * P1 * (1 - P2) * M2 + P1 * P2 * (1 - P3) * M3 + P1 * P2 * P3 * (1 - P4) * M4 + P1 * P2 * P3 * P4 * M5					

Figure a3-1 Scheme of Risk Value Calculation by the EDC Method

Appendix 4 Annualized Loss Expectancy (ALE) Method [8] [9] [8] [9]

A method of risk quantitization, called “annualized loss expectancy (ALE),” exists. While other risk assessment methods come up with classifications, or something closer to qualitative assessments, rather than specific amounts of losses, the ALE method is characterized by its ability to represent risk values in terms of specific amounts of annualized loss expectancies.

Annualized loss expectancy (ALE) = single loss expectancy (SLE) * Annualized rate of occurrence (ARO) …Eq. (18)

SLE: Single Loss Expectancy, ARO: Annualized Rate of Occurrence

In this equation, the single loss expectancy (SLE) is the amount of loss expected to arise when an event occurs once and is calculated by solving asset value (AV) * exposure factor (EV). In addition to the virtual loss, the associated loss, primary response, cost of recurrence prevention and so on must be reviewed. The annualized rate of occurrence (ARO) is the number of occurrences of an event expected to occur a year.

Because the equation single loss expectancy (SLE) = asset value (AV) * exposure factor (EV) also holds true, the annualized loss expectancy may be rewritten as follows:

Annualized loss expectancy (ALE) = Asset value (AV) * Exposure factor (EV)
* Annualized rate of occurrence (ARO) …Eq. (19)

Appendix 5 The OWASP Risk Rating Methodology [10] [11]

OWASP is an open community committed to the goal of solving the issues of Web application security. The OWASP Risk Rating Methodology (OWASP method) is a technique for vulnerability assessment developed by the OWASP (Open Web Application Security Project). It is characterized by financial damages, such as those to money, and reputation damages, being included in risk factors. The method involves the use of so many factors that overall risks are evaluated on the basis of their average value. The values of the individual factors are not weighted and hardly impact overall performance. Risk values start from a standard model as represented by Eq. (20).

Risk = Likelihood * Impact …Eq. (20)

The risk values of likelihood and impact can be expressed in equations as:

Likelihood = {Threat Agent
+ Vulnerability} / 2 …Eq. (21)

Impact = {Technical Impact
+ Business Impact} / 2 …Eq. (22)

The threat agent, vulnerability, technical impact and business impact can be expressed in equations as:

Threat Agent = {Skill level + Motive
+ Opportunity + Size} / 4
…Eq. (23)

Vulnerability = {Ease of discovery
+ Ease of exploit
+ Awareness
+ Intrusion detection}
/ 4 …Eq. (24)

Technical Impact = {Loss of confidentiality
+ Loss of integrity
+ Loss of availability
+ Loss of accountability}
/ 4 …Eq. (25)

Business Impact = {Financial damage +
+ Reputation damage
+ Non-compliance
+ Privacy violation }
/ 4 …Eq. (26)

Items contained on the right hand of Eq. (23) to Eq. (26) are defined in Table a5-1 to Table a5-4, respectively.

Table a5-1 Threat Agent Factors

Threat Agent Factor	Rating Result	Value
Skill level	No technical skills	**1**
	Some technical skills	**3**
	Advanced computer user	**5**
	Network and programming skills	**6**
	Security penetration skills	**9**
Motive	Low or no reward	**1**
	Possible reward	**4**
	High reward	**9**
Opportunity	Full access or expensive resources required	**0**
	Special access or resources required	**4**
	Some access or resources required	**7**
	No access or resources required	**9**
Size	Developers, system administrators	**2**
	Intranet users	**4**
	Partners	**5**
	Authenticated users	**6**
	Anonymous Internet users	**9**

Table a5-2 Vulnerability Factors

Threat Agent Factor	Rating Result	Value
Ease of discovery	Practically impossible	**1**
	Difficult	**3**
	Easy	**7**
	Automated tools available	**9**
Ease of exploit	Theoretical	**1**
	Difficult	**3**
	Easy	**5**
	Automated tools available	**9**
Awareness	Unknown	**1**
	Hidden	**4**
	Obvious	**6**
	Public knowledge	**9**
Intrusion detection		**1**
	Logged and reviewed	**3**
	Logged without review	**8**
	Not logged	**9**

Table a5-3 Technical Impact Factors

Threat Agent Factor	Rating Result	Value
Loss of confidentiality	Minimal non-sensitive data disclosed	**2**
	Minimal critical data disclosed, extensive non-sensitive data disclosed	**4**
	Extensive critical data disclosed	**5**
	All data disclosed	**9**
Loss of integrity	Minimal slightly corrupt data	**1**
	Minimal seriously corrupt data	**3**
	Extensive slightly corrupt data	**5**
	Extensive seriously corrupt data	**7**
	All data totally corrupt	**9**
Loss of availability	Minimal secondary services interrupted	**1**
	Minimal primary services interrupted, extensive secondary services interrupted	**5**
	Extensive primary services interrupted	**7**
	All services completely lost	**9**
Loss of accountability	Fully traceable	**1**
	Possibly traceable	**7**
	Completely anonymous	**9**

Table a5-4 Business Impact Factors

Threat Agent Factor	Rating Result	Value
Financial damage (financial damage)	Less than the cost to fix the vulnerability	**1**
	Minor effect on annual profit	**3**
	Significant effect on annual profit	**7**
	Bankruptcy	**9**
Reputation damage	Minimal damage	**1**
	Loss of major accounts	**4**
	Loss of goodwill	**5**
	Brand damage	**9**
Non-compliance	Minor violation	**2**
	Clear violation	**5**
	High-profile violation	**7**
Privacy violation	One individual	**3**
	Hundreds of people	**5**
	Thousands of people	**7**
	Millions of people	**9**

The risk levels of likelihood and impact can be determined from the following table:

Table a5-5 Risk Levels

Risk (Risk value)	0<=Risk value<3	3<=Risk value<6	6<=Risk value<9	MAX: 9
Rank (level)	LOW	MEDIUM	HIGH	

Overall risk severities can be determined from the following table:

Table a5-6 Overall Risk Severities

Overall Risk Severities				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

REFERENCES

[1] Connected Consumer Device Security Council, “CCDS Security Guidelines by Product Category: Banking Terminals (ATM) Volume Ver.1.0,” June 8, 2016, https: //www.ccds.or.jp/public/document/other/guidelines/CCDS Security Guidelines by Product Category: Banking Terminals (ATM) Volume_Ver.1.0.pdf

[2] European law enforcement agency, "Guidance and recommendations regarding logical attacks on ATMs", June 11, 2015, https://www.ncr.com/sites/default/files/brochures/EuroPol_Guidance-Recommendations-ATM-logical-attacks.pdf

[3] Information-technology Promotion Agency Security Center, “Common Vulnerability Assessment System CVSS v3 Overview,” December 1, 2015, https: //www.ipa.go.jp/security/vuln/CVSSv3.html

[4] Connected Consumer Device Security Council, CCDS Security Guidelines by Product Category: Automotive On-Board Devices Ver.1.01,” June 8, 2016, https: //www.ccds.or.jp/public/document/other/guidelines/CCDS Security Guidelines by Product Category: Automotive On-Board Devices _Ver.1.01.pdf

[5] Ryohei Ishii, Ryoichi Sasaki, Tokyo Denki University, “Proposal of a Risk Assessment Method That Combines Event Trees and Defense Trees and Its Preliminary Application to Targeted Attacks,” JSSM(Japan Society of Security Management), 29th National Conference Research Reports

[6] Information-technology Promotion Agency, “Supplement to Survey Report: Quantitative Security Scale Measurement Guidelines,” 15 Information Economics No. 651, http: //www.ipa.go.jp/files/000013701.pdf

[7] Institute of Electronics, Information and Communication Engineers, Chapter 8, Information Security Management - Institute of Electronics, Information and Communication Engineers Knowledge Base, Group 3, Volume 7 Computer Network Security Chapter 8 (ver.1), June 14, 2010, http: //www.ieice-hbkb.org/files/03/03gun_07hen_08.pdf

[8] FIPS PUB 31. “FEDERAL INFORMATION. PROCESSING STANDARDS PUBLICATION", "Guidelines FOR AUTOMATIC DATA PROCESSING PHYSICAL SECURITY AND RISK MANAGEMENT.”, June 1974, https: //www.ncjrs.gov/pdffiles1/Digitization/68759NCJRS.pdf

[9] FIPS PUB 65, “FEDERAL INFORMATION. PROCESSING STANDARDS PUBLICATION", “Guidelines FOR AUTOMATIC DATA PROCESSING RISK ANALYSIS”, August 1975, http: //www.femto-second.com/Documents/FIPS65.pdf

[10] The OWASP Risk Rating Methodology, https: //www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

[11] The OWASP Risk Rating Template, https: //www.owasp.org/images/5/5b/OWASP_Risk_Rating_Template_Example.xlsx