February 26, 2014
the Center for Financial Industry Information Systems

Report of the Council of Experts on Countermeasures Against Cyber Attacks on Financial Institutions

Contents

Introduction

Recently, a large number of cases of damage due to cyber attacks have been reported, worldwide. In March 2013, some major financial institutions in South Korea suffered cyber attacks, which caused their computer systems to go down. Regarding Japanese financial institutions, to date there have been no confirmed cases of leakage of customer information or system shutdown due to cyber attack. However, if a cyber attack were to occur, it can be anticipated that customers as well as the payment and settlement systems of financial institutions would suffer serious adverse effects. And, although phishing fraud is targeted at the customers of financial institutions rather than the institutions themselves, the potential for damage remains as high as ever.

What concrete steps should be taken against cyber attacks is not necessarily clear given the limited expertise and human resources within financial institutions. To counter phishing fraud, both measures taken by customers of financial institutions, such as reinforcing the security systems of personal computers, and measures taken by the institutions themselves are necessary. Nevertheless, the parties concerned, including those at financial institutions, have not always adequately considered such measures. Therefore, members of academia, the financial industry (including financial institutions and vendors), and observers from government agencies came together to discuss a wide-ranging agenda in a Council of Experts on

Countermeasures Against Cyber Attacks on Financial Institutions (hereinafter “Council”). The Council was established in response to a directive from the director general of the Center for Financial Industry Information Systems (hereinafter “FISC”). This report summarizes the results of the discussions.

We would be delighted if this report can help to bolster preparedness among Japan’s financial institutions and related industries against cyber attacks, improving measures taken by relevant government agencies and industrial organizations, and raising awareness of the importance of security among concerned parties, including the customers of financial institutions. Meanwhile, we would like to ask the FISC to revise its guidelines (FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions; hereinafter “FISC Security Guidelines”) and to conduct practical reviews aimed at encouraging the whole financial industry to reinforce countermeasures against cyber attacks, in cooperation with the parties concerned and based on this report.

I This Council’s definition of cyber attacks

1 Definition

Given the focus of this Council on cyber attacks against financial institutions and their customers, this Council established the following definition. Cyber attacks are actions aimed at: stealing, falsifying, and/or damaging information by illegally breaking into the information systems or information communications networks of financial institutions or their customers via the Internet, electronic recording media, etc., and executing unauthorized programs,[1] making other attacks, or rendering the information systems or information communications systems dysfunctional by causing them to malfunction or go down.

2 Methods of and motives for cyber attacks

Methods of cyber attacks vary and the motive for an attack can range from a prank through expression of the perpetrator’s ideology to theft of information/money. Examples of actual methods observed to date and motives that can be assumed from those methods are listed in References “1. ⑥ Types of cyber attacks (list).” However, the possibility that attacks using new methods will occur in the future cannot be discounted.

II Risk of coming under cyber attack

1 Attacks on financial institutions

(1) Estimated damage due to a cyber attack

Although each financial institution takes security measures against cyber attacks to some extent, if an attack is successful in breaching those security measures, various kinds of damage can be inflicted

[1] Generic term for malicious software or codes developed with an intention to perform illegal and harmful operations. Such software and codes include, for example: worms, Trojan Horses, bots, and micro viruses affecting Word and Excel.

depending on the systems environment of the institution.

Specific examples of damage common to financial institutions include unauthorized leakage of personal and corporate customer information (such as transaction details and customer information), suspension of settlement operations/Internet services, and supply and presentation of incorrect information arising from phishing fraud and falsification of websites. In the event that an institution incurs damage due to a cyber attack or fails to appropriately respond to such an attack, its social standing could be degraded and its reputation might be severely harmed. In addition, specific damage depending on the business category of the financial institution can also be anticipated. Deposit-taking financial institutions could suffer such damage as illegal withdrawal/transfer of customers' funds. Securities companies could see shutdowns of their systems for selling and purchasing securities, illegal leakage of information, or transfers of deposit assets. Moreover, market manipulation by means of intentional market-making through illegal ordering practices could take place. Exchanges and settlement institutions could suffer from shutdowns of their sales or purchase systems and payment and settlement systems; falsification of sales/purchase amounts, contract conditions, and information on the transaction board; shutdowns or illegal falsification of information disclosure systems. At life insurance companies and non-life insurance companies, systems for receiving and placing market orders for institutional investors or paying insurance money or maturity refunds could be disrupted. Credit card companies could experience leakage of information and illegal use of credit card information stored in the servers of member retail outlets and shutdowns of credit card settlement systems.

(2) Risk of attacks on medium-sized and small financial institutions

Not only major financial institutions engaged in international activities but also medium-sized and small financial institutions may be equally at risk of coming under cyber attack. This Council discussed the possibility that medium-sized and small financial institutions, which might not necessarily have sufficient protective measures, could come under DDoS[2] attack, with the attackers going on to launch further attacks against other financial institutions by way of e-mail channels.

(3) Risk that shared system centers, etc. could come under attack

In recent years, there has been a trend, particularly among regional financial institutions, toward sharing of systems in an effort to reduce costs and speed up the provision of new services. Just under 70%[3] of the banks that are members of the Regional Banks Association of Japan and the Second Association of Regional Banks use a system shared with other financial institutions as their core banking systems. Similarly, a number of financial institutions use servers located in shared system centers for Internet and mobile banking. If a shared system center should come under attack, several financial institutions could be affected as a result of their dependence on such a shared system center for their operations. That said, given the economies of

[2] Attack aimed at bringing down a computer system by sending a malicious program to a number of computers and simultaneously sending a vast number of packets from those computers to the target computer system

[3] Refer to Section 1 "Bank," Chapter 1, Volume 3 of the 2014 edition of "Financial Information Systems White Paper" issued by FISC

scale, it may be possible for more effective measures against cyber attacks to be mounted and maintained through shared system centers than can be taken by individual financial institutions.

Financial institutions are constantly sending and receiving data to and from other institution for the purposes of funds transfer, online coordination of their respective ATMs, etc., in order to execute their payment and settlement operations. Various shared systems are used for these operations and, if any of those systems were to be attacked, there is a risk that the damage could spread to multiple financial institutions. There are also risks that the websites of industry groups could be falsified and that, through installation of unauthorized programs in such website, such programs could be disseminated in the system of a financial institution whose website is accessed by its customers.

(4) Financial institutions' awareness of risk

① Reason for insufficient awareness of the risk of cyber attacks at some institutions

In the Council, it was noted that quite a few financial institutions are not sufficiently aware of the risk of cyber attacks and that they seemed to believe that they could never become targets of such attacks. As background to this low awareness of risk, it should be remembered that there have been no confirmed cases of a Japanese financial institution directly coming under cyber attack and suffering damage, such as leakage of customer information or theft of deposits, and that institutions mistakenly believe that their systems are safe because they are built on mainframe architecture, as seen in the core banking systems, and their networks are in closed environments. In addition, as sharing or outsourcing of systems has advanced, as mentioned in the above paragraph, there are situations where the number of systems that financial institutions manage themselves is declining and, as systems become increasingly complex, financial institutions are now less prepared to consider security measures that embrace the whole environment. Another consideration is that personnel responsible for systems struggle to stay abreast of progress in security technologies. And, it would appear that some financial institutions do not place particularly high priority on preparedness to respond to cyber attacks. This is because they are already heavily burdened with pressing issues besides those concerning systems, such as corporate reconstruction in the wake of expiration of the Act Concerning Temporary Measures to Facilitate Financing for SMEs, etc. (so-called SME Financing Facilitation Act), and because, even in respect of systems-related matters, they assign higher priority to responding to overall reviews of systems risks. It was also noted that financial institutions may potentially wish to avoid strengthening their systems whenever possible due to increasing costs, and also because the managements of some financial institutions may not be well-versed in systems-related matters.

② Measures required to raise awareness of risks

Financial institutions need to be aware that, if their customers incur damage or efficient operation of their payment and settlement systems are impeded as a result of cyber attacks, and if their responses to such issues are inadequate, they will be held responsible for such damage or face significant business risks.

First, financial institutions, related industry groups, and concerned parties, including the Supervisory Agencies, need to reinforce training and awareness activities and human resources development according

to the roles and responsibilities assigned to each party. They need to adequately study how the costs of these activities should be covered. It is also considered necessary for concerned parties, which exchange data and files through electronic recording media, to mutually confirm their preparedness for cyber attacks, whenever possible, in order to raise each company's awareness. It is recommended that the Supervisory Agencies more effectively check financial institutions' countermeasures against cyber attacks through audits, inspections, and examinations. The FISC is also required, based on discussion in this Council, to provide more details regarding cyber attacks in its guidelines (FISC Security Guidelines, FISC Information System Audit Guidelines for Banking and Related Financial Institutions, Manual for the Development of Contingency Plans in Financial Institutions (Plans for Measures in the Event of Emergencies)). In the course of this process, it is desirable ① to prevent written descriptions becoming out-of-date because attack technologies are developing rapidly, ② to decide on the volume of information to be included in order to balance organization of the entire guidelines, and ③ to classify responses, according to their importance, into "required responses" and "desirable responses."

2 Attacks on customers of financial institutions

(1) Attacks on customers of a deposit-taking financial institution

Regardless of the scale and location of a deposit-taking financial institution that provides Internet services, its customers are at risk of becoming targets of phishing fraud or unauthorized program invasion.

(2) Attacks on customers other than those of a deposit-taking financial institution

The risk of phishing fraud against customers of a securities company is considered relatively low because illegal withdrawal of assets requires two stages of illegal actions.[4] However, those customers are considered to be at risk of incurring losses due to intentional market making by means of illegal online trading. Customers of a life insurance company may be at risk of being targeted by phishing fraud if the company provides a money transfer service using the Internet.[5] For customers of a credit card company, there is a possible risk of damage through abuse of card information (e.g. card numbers) stolen by means of phishing fraud or card counterfeiting.

III How to prepare against possible cyber attacks on financial institutions

1 General issues

(1) Importance of countermeasures on the premise of invasion

In recent years, there has been an increase in targeted attacks that are relatively hard to detect and defend against. Examples would include surreptitious theft of information over an extended period through

[4] The following two stages of illegal actions are entailed in illegally withdrawing money through phishing fraud. ① Illegally cancelling a contract on assets on deposit and causing the correspondent financial institution to deposit the converted money. ② Illegally accessing the account of the corresponding financial institution and transferring the money to a third party.

[5] Currently, non-life insurance companies do not provide money transfer services via the Internet.

use of an unauthorized program that pretends to be a normal program, to hack into the computer system of a targeted organization or individual via e-mail, CD-ROM, or USB memory stick.

Cyber attack methods have become increasingly sophisticated and it is difficult to completely defend against them. Therefore, it is necessary to clarify a defense policy by assessing risks of attacks and considering risks that could compromise ongoing operation of a system if it should come under attack or go down. It is also necessary to enhance technological measures, such as inbound, internal, and outbound measures, and incident responses and forensics[6] against the possibility that a system is attacked.

(2) Countermeasures referencing overseas cases

An effective approach us to reference examples of damage stemming from cyber attacks on financial institutions and countermeasures in other countries while paying attention to the differences in Japan's systems environment, etc. Some examples are introduced below.

a) Countermeasures taken in collaboration with outsourcing contractors

It was reported that a targeted attack in the U.S. in the spring of 2013 resulted in a financial institution's customer card data, which had been outsourced to a settlement contractor, being falsified and illegally leaked, and to counterfeit cards being created. As a consequence, a large amount of money was illegally withdrawn from the leaked account via ATMs around the world. In South Korea, several major financial institutions came under targeted attacks and incurred serious damage, including temporary suspension of their ATM services. It was reported that a patch file installed by the outsourcing company was the conduit through which the unauthorized program was released. As a result of such attacks, in the U.S. and South Korea a key focus for financial institutions is to check for vulnerability to attack via outsourced services and to work with outsourcing vendors to reinforce preparedness.

b) Countermeasures against DDoS attack

Major financial institutions in Europe and the U.S. are strengthening intelligence functions[7] to monitor for signs of attacks on the Internet in cooperation with special vendors. Some of these institutions are mitigating the potential impact of DDoS attacks on their systems by diverting transactions to vendor-hosted and managed environments which screen transactions and pass only valid transactions to the institutions' systems. This helps to avoid significant disruption to large numbers of valid transactions.

c) Countermeasures against illegal money transfer via Internet banking

Financial institutions in Europe and the U.S. are also facing challenges in terms of their ability to cope with illegal online money transfer triggered by phishing fraud, which frequently occurs among customers. Consequently, some major financial institutions monitor their customers' transactions. If a transaction is

[6] Digital forensics are: a series of scientific investigation methods or techniques designed to preserve and analyze electromagnetic evidence in the case of an incident response, legal dispute, or lawsuit, and to analyze and collect information on falsification of and damage to electronic records (definition by the Institute of Digital Forensics, NPO).

[7] This function mainly monitors for signs of instigation such as "Let's attack financial institution ○○ on month ○ day ○" and collects information on chatter about the target and method of an attack (including targeted attacks as well as DDoS attacks), and it may be used to search counterfeit websites pretending to be those of financial institutions.

found to be abnormal in terms of the amount and transfer destination compared with the regular behavior of the customer concerned, it will be suspended until it has been reconfirmed by the customer.

d) Countermeasures by joint response organization

There are overseas examples of joint response organizations[8] being created to reinforce the responsiveness of the whole financial industry (U.S. and South Korea FS-ISAC and European FI-ISAC) to cyber attacks. The activities of a joint response organization vary from simply sharing information to deep response, including joint network monitoring. In such joint response organizations, activities are conducted on the assumption that an attack could threaten the entire global financial system, no matter where the attack occurs.

e) Conducting joint training

It is difficult to completely prevent cyber attacks because the techniques and methods used by attackers are constantly evolving. Once an institution is attacked, the influence can spread in a chain reaction to the financial industry, the market, payment and settlement systems, and even to other industries. Therefore, in Europe and the U.S., industry bodies sponsor joint training sessions focused on countering cyber attacks in order to check information sharing and communication systems among financial institutions as well as those between institutions and Supervisory Agencies.

(3) Cost effectiveness analysis

Financial institutions need to make massive financial investments in measures to protect themselves against cyber attacks. However, they tend to hesitate on actually taking such measures because their cost effectiveness is difficult to quantify. The measures to be taken may differ from one institution to another depending on the scale of the institution and the degree to which it is concerned about the risk of cyber attacks. Assessing cost effectiveness is an important consideration for financial institutions because, as noted above, developing a system to counter cyber attacks will increase costs. Cost effectiveness of countermeasures against cyber attacks can be studied using such techniques as scenario-based analysis and risk quantification, taking into account the overall operational risk control environment. Currently, however, it may be difficult for financial institutions to decide if they have the necessary expertise in mathematical analytical techniques to assess the extent to which each countermeasure addresses the potential damage that could be inflicted by a cyber attack.

In the Council, one member proposed an approach that would involve analyzing[9] cost effectiveness based on a risk quantification technique. It is hoped that this approach will be studied in academic and working circles, going forward.

(4) Vulnerability diagnosis

[8] In fact, some organizations that have been set up do not qualify for the title “joint organization” because their activities are limited to sharing or exchanging information on cyber attacks through mailing lists for the whole financial industry.

[9] Refer to “Improvement of Multiple-risk Communicator MRC and Application to Countermeasures against Targeted Email Attacks” (Ryoichi Sasaki, professor, School of Science and Technology for Future Life, Tokyo Denki University), contributed to FISC organ magazine “Financial Information System, Winter 2014.”

To objectively assess the vulnerability of a financial institution to cyber attacks, a vulnerability diagnosis by a third party is considered to be an effective approach. However, there are problems with this approach: First, the cost is high; and second, views as to which items should be diagnosed and the depth of such diagnosis have not been resolved. Therefore, it is necessary to give further consideration to standardizing the format for vulnerability diagnosis and, indeed, to the feasibility of conducting vulnerability diagnosis in some financial institutions. Meanwhile, it should be noted that there is a risk that the results of diagnosis can vary depending on the range and level of services supplied. There is also a concern that if only a specific third party, such as a joint organization, is entrusted with the diagnostic process, the results may not be able to be compared with those obtained through the diagnostic services of other companies, which may make it difficult to obtain accurate and effective results.

(5) Preparedness for response to cyber attacks on key external affiliates

There are risks that a business partner of a financial institution with which the institution shares customer information, or an external vendor with which the institution entrusts its systems for operation and maintenance, could be subject to a cyber attack and, as a result, customer information is leaked or the institution is unable to conduct its operations. Moreover, unauthorized programs could make inroads through a partner, such as a settlement organization or a major customer, with which a financial institution systematically exchanges data. Therefore, a financial institution should check, as far as possible, its preparedness for responding to cyber attacks as necessary. To check the preparedness of vendors, such methods as on-site inspections and requests for submission of necessary documents may be used by expanding the existing framework of managing vendors.

Each financial institution needs to assess the range and depth of vendors, business partners, and companies with which it exchanges data, in accordance with the principle of importance, when checking their preparedness to respond to cyber attacks. However, there is little likelihood that effective checking can be ensured unless guidelines on responses to cyber attacks which can be applied to all parties concerned are established.

2 Specific issues

(1) Outline of countermeasures against cyber attacks[10]

Inbound, outbound, and internal measures:

① Inbound measures

Measures aimed at preventing and defending against externally originated attacks

② Outbound measures

Measures to prevent information being extracted by unauthorized programs that have penetrated systems, i.e., measures implemented on the assumption that an unauthorized program could break into a system

[10] For details, refer to "1. ⑦ List of countermeasures (inbound, outbound, internal)" in References.

③ Internal measures

Measures to protect data against being stolen, wiretapped, falsified, or damaged, or systems being rendered dysfunctional by cyber attacks. As with outbound measures, these measures are based on the assumption that an unauthorized program could break in; early detection of such penetration falls into this category.

It is difficult to enumerate general countermeasures to which priority should be given because environments differ from one financial institution to another. Therefore, it is desirable that each institution first assesses its vulnerability and takes responsibility for assigning priorities based on its own circumstances. As prerequisites for implementing measures for cyber attack surveillance and early detection of penetration, logs (including those for networks, applications, use of privileges associated with privileged IDs) should be obtained and preserved. Logs to be obtained should be selected by an institution, taking into consideration the characteristics and importance of each system, and should be retained, preferably for at least one year.[11] When gathering information on cyber attacks and responding to incidents, cooperating with security support organizations[12] and the police is an effective approach.

(2) Inbound and outbound measures

As methods used in cyber attacks have become increasingly sophisticated, it is difficult to completely block attacks by means of inbound measures alone. Therefore, multilayer defense that executes outbound measures and internal measures on the assumption that a system will be breached by cyber attacks is required. Recently introduced firewalls and software for preventing unauthorized access support both inbound and outbound measures. Increasingly, this makes it more difficult to discuss inbound and outbound measures as separate issues.

(3) Internal measures

a) Reinforcing management of privileged IDs and passwords

Reinforcing management of IDs and passwords using techniques such as entitlement segregation of privileged IDs and restriction on the number of holders of privileged IDs, and controlling the situations in which the privileges can be used are necessary (privileged owners include DBA[13]). As specific points to reinforce management, the following can be cited: ① Not allowing more than one person to use a privileged ID and ② Obtaining a trail (of both successful and failed attempts to use privileged IDs), monitoring the patterns of use of IDs, and tracing the trail afterward. It is desirable to closely examine the trail at appropriate intervals.

b) Separation of Internet and systems environments within financial institutions

Considering that there is a risk of coming under cyber attack when accessing the Internet, it is desirable to

[11] According to "2011 Report of Survey on Obtaining and Managing Logs of Information System at Government Agencies" published by the National Information Security Center (NISC), the previous targeted attack lasted for something under one year; therefore, logs recorded in the initial stage of the attack can be extracted with high probability if the logs are preserved for one year. Hence, the government recommends that its agencies preserve logs for at least one year.

[12] Information-technology Promotion Agency, Japan (IPA) and JPCERT Coordination Center

[13] Stands for DataBase Administrator. Administrator of a database who creates, maintains, operates, and deletes the database using a database management system

physically and completely separate the internal and external systems environments of an institution. But, separating those environments is impractical in many cases when the expense entailed in creating infrastructure, such as networks and terminals, and cost effectiveness, are taken into account. It is possible to strengthen blocking of unauthorized access from the Internet environment to a financial institution's internal systems by introducing measures for blocking,[14] such as virtual environments for external connections. However, even if blocking is bolstered in this way, it should be noted that its effectiveness may be impaired unless data exchanged between two environments through devices such as USB memory sticks is properly controlled.

(4) Regular monitoring

Introducing a mechanism that regularly monitors the traffic on a network and detects symptoms of an attack, as well as invasion, is effective for coping with targeted attacks and DDoS attacks. To counter falsification of website contents and embedding of illegal codes, introducing a constant monitoring mechanism[15] is effective.

However, it may be difficult for an individual financial institution to introduce such mechanisms on its own, given limitations on funding and human resources (skills and experience). Use of a joint monitoring service operated by an external vendor could be a solution if such a service were to become available, going forward. It may be possible for the financial industry in Japan to establish a joint organization to conduct monitoring activities and for financial institutions to use the services of such an organization.

(5) Preparedness for incident response

Since it is difficult to completely block invasion through cyber attacks, it is necessary to make preparations for responding to an incident on the assumption that an invasion will take place. Considering the potential for damage, it is hoped that procedures for responding to incidents are formulated with priorities clearly assigned. Formation of a CSIRT[16] is also desirable.

a) Formulating procedures

It is considered necessary to study in advance a response procedure for examining the possible scope of damage, identifying the cause (vulnerability), recovering from damage, and maintaining operations from the following perspectives:

① Partial shutdown of a system (e.g. authority, procedure for such event)
② Preservation of evidence for forensic purposes (e.g. obtaining and managing logs in advance, etc.)
③ External and public communication
④ Responses to and compensation of customers
⑤ Recovery of data and the system

[14] For details, refer to "1. ⑧ Outline of measures for separation and isolation of network environments" in References.
[15] For example, it is conceivable that there could be a solution that provides for constant monitoring of publicly accessible Web content and that, if falsification is detected, alerts the administrator and automatically implements a recovery process.
[16] Abbreviation of Computer Security Incident Response Team

The specifics of formulating such a procedure could include: i) using an existing procedural manual designed to enable responses to system failures and adding descriptions that specifically address responses to cyber attacks, or ii) preparing a new procedural manual taking into consideration the risks particular to cyber attacks. Since it is impossible to include all response patterns in a procedural manual, the basic principles[17] underpinning actions and processing should be described so that, even if a situation not described in the manual arises, responses can be flexibly implemented based on appropriate judgment according to the circumstances.

b) Priorities

When a system comes under cyber attack it can be expected that there will be a number of tasks[18] to be handled by the impacted institution. It is difficult to make general assumptions about what should be given top priority because that will depend on the particular circumstances. However, if customers have incurred damage, response[19] to such event and compensation such as temporary payment should be given high priority. In responding to an attack, it may be justifiable to decide to minimize damage and facilitate rapid recovery by fully or partially shutting down the core banking system in the case of a deposit-taking financial institution, or the contract system or settlement system of a securities firm, rather than giving top priority to maintenance of system operation.

c) Establishing CSIRTs

In the event that a system comes under cyber attack, several departments will be involved in analyzing the cause, making information public, responding to customers, and developing recurrence prevention measures. Consequently, coordination among relevant departments will be essential. Therefore, in a financial institution, ideally a CSIRT should be formed as a department or team that is responsible for coordination between the respective departments as well as managing external communications. The form of a CSIRT may vary. It does not have to exist in every case or to comprise regular members. And, neither should the name “CSIRT” be used. Even after a CSIRT has been formed, it does not have to handle all incidents; requesting external assistance through a CSIRT is another possibility. It will be appropriate for a financial institution to select the most suitable form or function for a CSIRT according to the scale and form of the institution.

(6) Forensics

In the event that a financial institution is subjected to a cyber attack, it will be important to conduct a forensic investigation in order to identify the route and method of invasion and to trace and establish the scale of the information leak so that accurate prevention measures can be taken. However, financial institutions may encounter the following problems when implementing forensic investigations.

First, the types of information that should be prepared are not standardized; for example the range of logs

[17] For example, the principle of informing departments of the institution or concerned parties, assembling personnel, including those from affiliates, setting up a command center, and delegating authority in the absence of the superior is conceivable.

[18] For example, events such as system shutdown and inquiries, and subsequent escalation and technical recovery can be cited.

[19] For example, damage scale, explanation of assumed risk, and responses to inquiries can be cited.

required for forensics and their preservation period are unclear, and day-to-day operations and experiences are insufficient for preserving evidence in the event of an incident. Therefore, it is desirable that concrete guidelines for financial institutions are proposed, going forward[20].

To analyze the collected evidence, specialized expertise and techniques are required. However, fostering and securing personnel for forensics is difficult to justify if restrictions on funds and human resources and the frequency of occurrence of incidents are taken into consideration. In many cases, therefore, there is no choice but to entrust these tasks to an external vendor; however, the challenge of cost remains.

If a service that supports shared use of forensics is supplied by external vendors or shared system centers in the future, financial institutions will be able to use such a service easily and at a low price. However, it is not clear that external vendors and shared system centers would be capable of responding in emergency situations where multiple financial institutions come under cyber attack at the same time. Therefore, it is necessary for financial institutions to seek and clearly understand explanations from external vendors and shared system centers as to the extent of the services that they offer.

(7) Training and drills

It is hoped that, in addition to the existing disaster prevention training and system fault response training, response training specific to cyber attacks will be conducted. This would raise officials' awareness of the risk of cyber attacks and the importance of confirming the effectiveness of institutions' preparations against potential cyber attacks, and prepare those officials in advance to be able to respond to incidents and various other technical matters. As a framework for such training, the following options can be suggested; training conducted jointly with concerned organizations, training conducted by an individual financial institution, or a combination of the two. Methods would include desktop training, drills for checking the communication process, and forensics training, among others.[21] In conducting such training, it is hoped that the framework of an existing training scenario for responding to disasters, such as earthquakes, system failures, and influenza, are expanded and used, so that the load on the financial institution and its employees does not become excessive. Note that existing types of training are introduced in "5. Joint training" in References.

(8) Other countermeasures

In addition to the aforementioned countermeasures, the following are considered desirable:

a) Enhancing countermeasures against DDoS attacks

---

[20] For recommended methods of collecting and managing logs, refer to a report on a survey regarding obtaining and managing the logs of information systems in government agencies, conducted by the National Information Security Center (NISC) (http://www.nisc.go.jp/inquiry/pdf/log_shutoku.pdf). For specific guidelines to preservation of evidence in the event of an accident, Guidelines on Evidence Preservation (3rd edition) is available from the Institute of Digital Forensics, NPO (http://www.digitalforensic.jp/eximgs/20130930gijutsu.pdf).

[21] For recommended methods of collecting and managing logs, refer to a report on a survey regarding obtaining and managing the logs of information systems in government agencies, conducted by the National Information Security Center (NISC). (http://www.nisc.go.jp/inquiry/pdf/log_shutoku.pdf). For specific guidelines on preserving evidence in the event of an incident, "Guidelines on Evidence Preservation – 3rd edition" is available from the Institute of Digital Forensics, NPO. (http://www.digitalforensic.jp/eximgs/20130930gijutsu.pdf)

DDoS attacks are difficult to predict in advance but financial institutions with a strong focus on Internet operations should take countermeasures against them. Introduction of a joint surveillance system for effective surveillance is seen as an alternative.

To improve the effectiveness of countermeasures against DDoS attacks, measures such as enlisting the support of telecommunications operators to help in coping with illegal traffic or control of the bandwidth[22], and introducing a mechanism to distribute the point of access[23] (use of a cloud mechanism), could be implemented.

b) Reinforcing verification of patch[24] installation and software updates

In light of examples of cyber attacks in other countries, it is desirable to make the following responses in order to prevent infection via maintenance contractors and vendors. First, it is necessary to reinforce detection of unauthorized programs before applying software patches and version updates supplied by a maintenance contractor or a vendor. It is desirable to obtain data with electronic signatures that can be used to validate that a supplied patch or updating data[25] is official.

When maintenance contractors or vendors are patching or updating software through remote maintenance, it is desirable to restrict the work of the maintenance contractor or vendor to block intrusion of illegal programs from their equipment, etc. However, it should be noted that prohibiting remote maintenance would cause outsourcing costs to rise and increase the workloads of employees required to monitor the onsite work. If remote maintenance is permitted to continue as an exceptional case, the requirements under which this should be permitted need further consideration. To protect a financial institution against infection via maintenance contractors or vendors, the institution should ideally verify to its own satisfaction that the external party is sufficiently prepared against cyber attacks.

3 Desirable responses for medium-sized and small financial institutions

Because all financial institutions, regardless of scale, are at risk of cyber attack, medium-sized and small institutions are also expected to prepare for responding to these attacks. Given constraints on management resources (including human resources) in such financial institutions, their only option is to prepare their response strategies in stages. And, it is not practical for each institution to take its own measures against cyber attacks by outlaying large sums of money.

In order for medium-sized and small financial institutions to ramp up their countermeasures, the following actions may be necessary:

---

[22] For responses to pressure and traffic volume by a specific customer for Internet or specific applications, refer to “Guidelines on Packet Shaping,” jointly published by four organizations related to electronic communication (formulated in May 2008 and revised in March 2012).

[23] Should one of the routes no longer be available due to a failure, etc., operations can continue if dual routes are used by automatically changing the communication route, thus providing network resilience to communication failures.

[24] Program with only differential information and used to correct a software defect or perform a small-scale update, aka a patch file, patch program, or update program, which replaces only the part that needs to be changed, as opposed to the whole application or program. A patch that improves safety in order to block attacks by an unauthorized program or cracking is specifically called a security patch.

[25] Program that updates software. Versions for updating and fixing bugs to correct defects are available.

a) Cost reduction through joint purchasing of assets and services or sharing of related business processing (joint outsourcing[26])
b) Use of the services of vendors that have appropriate countermeasures against cyber attacks and systems for managing security and customer information
c) Implementation of monitoring activities through setting up and joining a joint monitoring organization
d) Clarification and standardization of outsourcing criteria and management techniques for appropriate management of outsource vendors
e) Participation in seminars and training programs offered by industry groups and public organizations (including FISC) with a view to enhancing the expertise of officials in each financial institution, and requesting service-supplying vendors to supply information on preparedness against cyber attacks

A number of deposit-taking financial institutions and securities companies entrust operation of their core systems to shared systems centers in the belief that they should cooperate with each other in order to accurately and efficiently deal with various kinds of cyber attacks. However, it should be noted that, if the shared systems centers' countermeasures against cyber attacks are inadequate, there is a risk that stable operation of the core systems of all of the financial institutions entrusting the shared systems centers could be affected.

4 How to disclose and share information

It should be at each institution's discretion whether or not to disclose the fact that an attack has occurred in that company. The way in which this is communicated should, ideally, be similar to that used to communicate other operational risk incidents or scandals. Disclosing or sharing information with other financial institutions has the advantage of promoting proactive actions by the whole industry in Japan but this approach could give rise to secondary damage. Therefore, it is necessary to decide if it is appropriate to disclose or share information, taking into consideration the particular circumstances of specific cyber attacks.

To share awareness of the risk or promote a response to the risk in the financial industry, it is considered to be an effective approach to reinforce sharing of information on attacks and any resulting damage that has not been made public while ensuring, where possible, that the source of the information remains anonymous. In particular, damage due to an attack similar to a targeted attack against a specific institution may be avoided if the financial institution that detects the attack supplies information on the characteristics thereof to other financial institutions or an external expert organization. In addition, the intention and method of the attacker may be able to be clarified through collation of pieces of information from each financial institution or expert organization. Such sharing information across the industry can be particularly effective in countering targeted attacks.

Since the content of information to be shared and the procedure for sharing such information have been

[26] With a number of companies jointly outsourcing their operations, their systems will be operated by a shared system center, etc., at low cost and with high security.

identified through public- and private-sector information sharing systems (such as an information sharing system created by key infrastructure operators, including financial institutions, the government, information security-related organizations, etc., and J-CSIP), it is important to make effective use of those systems. Relationships and cooperation with existing information sharing frameworks within the industry, such as the CEPTOAR-Council C4TAP and J-CSIP, needs to be studied, together with the detailed items described in "5. Establishing a joint response organization," below.

5 Establishing a joint response organization

In terms of preparedness for responding to cyber attacks against financial institutions, not only sharing the costs of a cyber attack response solution but also establishing a joint response organization specific to the financial industry could be seen as options. The purpose of such an organization would be to: ① share information on risk events particular to the financial industry and reinforce countermeasures against them, and ② assist with and promote preparedness of medium-sized and small financial institutions to respond to cyber attacks. In this case, it would be appropriate to seek participation from corporations engaged in financial business, such as deposit-taking financial institutions, securities companies, and life insurance and non-life insurance companies, regardless of their business categories, together with related vendors, but to allow each corporation to decide whether or not it needs to participate in the organization.

Upon establishing a joint response organization, taking the various characteristics of and environments in the financial world into consideration, existing frameworks, such as the CEPTOAR-Council and J-CSIP,[27] could be expanded or a new organization and framework could be created to cooperate or share roles with the existing framework. Further working-level study is needed among the parties concerned regarding the organization, its structure, cost sharing, role sharing, specific functions, and services to be provided. Items that require further study include:

(1) Organization, structure, cost allocation

- Whether a new framework should be created or an existing framework should be enhanced
- General estimation of initial cost and operating cost, and approach to cost-sharing
- Human resources structure

(2) Functions of the joint response organization

- Information sharing on vulnerabilities, unauthorized programs, attacks (or warnings of attacks), details of damage including feedback of analysis results)
- Diagnosis of preparedness of individual financial institutions to respond to cyber attacks, and vulnerability diagnosis
- Monitoring attacks against individual financial institutions through analysis of their network communication logs (24 hours a day and 365 days a year)
- Forensics support in the event that an invasion or damage is suspected

[27] For existing domestic frameworks and councils related to response to cyber attacks, refer to "2. Activities by major Japanese public organizations and councils for improving security, including countermeasures against cyber attacks" in References.

- Education and training of relevant officials in individual financial institutions
- Planning for joint training and supplying infrastructure for training

(3) Role sharing

- Role sharing and cooperation with existing information sharing organizations and frameworks, such as CEPTOAR and J-CSIP

IV How to prepare against possible cyber attacks on customers of financial institutions

1 Security of Internet banking

(1) Improvement of security for customers

To improve security of Internet banking, measures must be taken not only by the financial institutions but also by their customers. Therefore, it is considered important for the financial institutions to appropriately encourage customers to take such measures. For this process, it is desirable that each business segment implements consistent and integrated measures.

For example, the following measures could be considered for improving IT literacy and raising security consciousness among customers. Since the scale of risk for financial transactions using the Internet varies by business segment, financial institutions other than deposit-taking financial institutions may be able to take simplified measures for the time being, taking into account the extent to which their services depend on Internet transactions.

a) Launching intensive campaigns for customers across the whole financial industry

It is considered to be an effective approach to launch a campaign similar to that for remittance fraud (FURIKOME “It’s me” fraud) with each industry group playing a central role and with the cooperation of Supervisory Agencies and the police. For Internet transactions, however, reliance on promotion through branch networks may not suffice, and measures such as posting promotional material on institutions’ websites and sending notifications by e-mail are necessary, given the characteristics of remote channels.

b) Explanation of risks to customers when they open new accounts and provision of details of personal computer environments

When a customer applies to open a new account, measures such as ensuring customer awareness of the risks associated with Internet transactions and the importance of countermeasures against these, and obtaining information about the customer’s personal computer environment, such as installation of software to prevent unauthorized programs being installed, should be considered. However, in order for these measures to be effectively implemented, it is desirable that the whole industry launches them in concert, where possible, as there are concerns that customers who prefer simple procedures and efficiency when opening accounts could defect to competitive financial institutions. In the case of a financial institution specializing solely in Internet banking without manned customer channels, not only the website but also telephone and mail communication may need to be used to explain risks to customers.

c) Explanation of risks to existing customers

While it should be noted that the burden on financial institutions of explaining risks to customers will increase, it is desirable to actively pursue this course from the perspective of improving the safety and security of all online financial transactions.

d) Systematic response measures

To ensure the security of online transactions, it is desirable to take measures step by step, using one or more of these systematic response measures: ① distribution or dissemination of computer software to reject unauthorized programs, ② installation on customers' personal computers of tools to check system environments (functions for checking the type and version of the OS, presence or absence of countermeasures against unauthorized programs, and application of patches) and measures to block transactions ③ employment of one-time passwords, ④ introduction of transaction authentication, and ⑤ mechanism to monitor transaction content and temporarily suspend a transaction if any suspicious characteristic or abnormality is detected.

(2) Response to customers without sufficient security measures

Going forward, the following strengthening countermeasure should be considered in light of the spread of the aforementioned security improvement measures among customers. If a customer does not pay heed to explanations of risks or respond to questions about his/her/its computer environment from a financial institution, if he/she/it does not implement the security measures requested by the financial institution, or if the financial institution learns that the customer's computer environment is vulnerable, it may be necessary for the financial institution to consider taking action, such as ① refusing to open a new Internet transaction account, or ② temporarily suspending the customer's ability to use online banking unless he/she agrees "to take full responsibility for any subsequent transactions." However, such a response could prove difficult in some cases for securities firms specializing in Internet transactions that do not have physical branch networks. Consequently, it is hoped that each company will respond according to its particular business conditions and circumstances.

2 Countermeasures for smartphones and tablet terminals

Smartphones and tablet terminals are increasingly being used in the financial industry because of the ease with which functions can be added by installing applets, and their portability. But, as with personal computers, these devices are at risk of invasion by unauthorized programs. Moreover, smartphone and tablet users may not even be aware that they are accessing suspect websites because simplified URLs are displayed in their browsers. Therefore, security measures that take these points into consideration are considered necessary.

In devising protection for smartphones and tablet terminals, studying measures from the perspective of application management is especially important. Examples of measures that could be taken by users of such devices include: updating applications to the newest versions and installing software to prevent unauthorized programs being installed, using recommended applications supplied by the user's financial

institution(s), and prohibiting automatic connection to wireless LAN access points, etc.

Meanwhile, it is hoped that financial institutions will also implement measures, such as supplying their customers with recommended applications, encouraging them to use such applications, and alerting their customers to the threat of illegal applications. Because some illegal applications that tout improved convenience (such as bringing together Internet banking accounts with different financial institutions) are in circulation, financial institutions should study information on such applications and reinforce information sharing among the institutions and concerned parties. To study security measures, referring to the various guidelines[28] published by the Japan Smartphone Security Association[29] on security measures for smartphones and information to be disseminated to the users may be useful.

[28] Security Guideline for using Smartphones and Tablets- Advantages for work style innovation" [Version1], etc.
[29] Japan Smartphone Security Association (http://www.jssec.org/activities/index.html)

References

Reference documents related to the Report of the Council of Experts on Countermeasures Against Cyber Attacks on Financial Institutions are listed below.

1. Statistical information
   ① Number of incidents reported (Japan)
   ② Number of targeted attacks (Japan)
   ③ Number of cases of website defacement (Japan)
   ④ Number of malware sites
   ⑤ Number of cases of phishing fraud (Japan, U.S., South Korea)
   ⑥ Types of cyber attacks (list)
   ⑦ List of countermeasures (inbound , outbound, internal)
   ⑧ Outline of measures for separation and isolation of network environments
   ⑨ Examples of recent major cybercrimes and attacks
2. Activities by major Japanese public organizations and councils for improving security, including countermeasures against cyber attacks
   - Information-technology Promotion Agency, Japan (IPA)
   - Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
   - Cyber Force
   - Integrated Security Measures Council
   - National Information Security Center (NISC)
   - Information Security Policy Council
   - Capability for Engineering of Protection Technical Operation Analysis and Response (CEPTOAR)
   - CEPTOAR-Council
   - Information Security Measures Promotion Conference
   - Cyber Intelligence Information Sharing Network
   - Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP)
   - Cyber Incident Mobile Assistant Team (CYMAT)
   - CEPTOAR-Councils Capability for Cyber Targeted Attack Protection (C4TAP)
3. Major information sharing systems in Japan
   ① CEPTOARs (Capability for Engineering of Protection Technical Operation Analysis and Response) in the financial field
   ② Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP)
   ③ Targeted attack information sharing system at CEPTOAR-Council (CEPTOAR-Councils Capability for Cyber Targeted Attack Protection [C4TAP])

4. Activities by major overseas public organizations and councils

① Financial Services Information Sharing and Analysis Center (FS-ISAC)

② South Korea financial ISAC

③ Europe

- European Network and Information Security Agency (ENISA)
- Europe: Financial Institutions-Information Sharing and Analysis Center (FI-ISAC)
- United Kingdom: Cyber Security Information Sharing Partnership (CISP)

④ Others

- Forum of Incident Response and Security Teams (FIRST)

5. Joint training programs

① Ministry of Economy, Trade and Industry

② Joint training program organized by Ministry of Internal Affairs and Communications

③ Joint training program organized by NISC

④ Joint training program organized by three markets

⑤ Training for switching over backup center for settlement system operators (Bank of Japan)

⑥ Cross-sector exercises CIIREX 2013

⑦ U.S. (Quantum Dawn 2)

⑧ United Kingdom (Waking Shark II)

6. Countermeasures by major Japanese banks against illegal money transfer

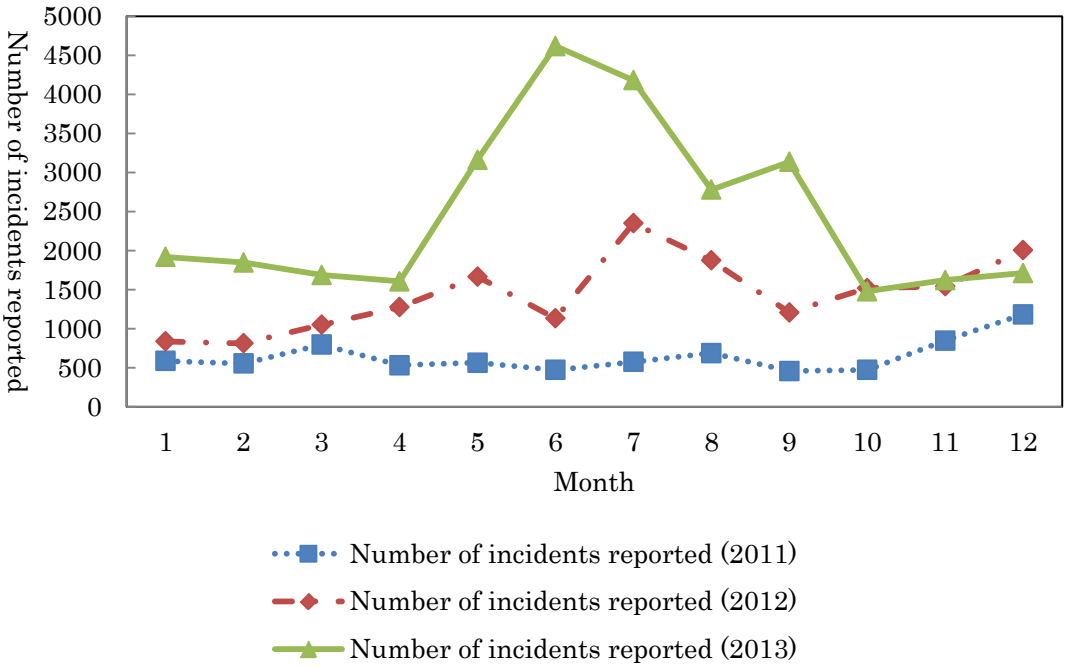
7. Activities by major overseas financial institutions, etc.

8. Record of the council held

Date and time of each council, agenda, list of members

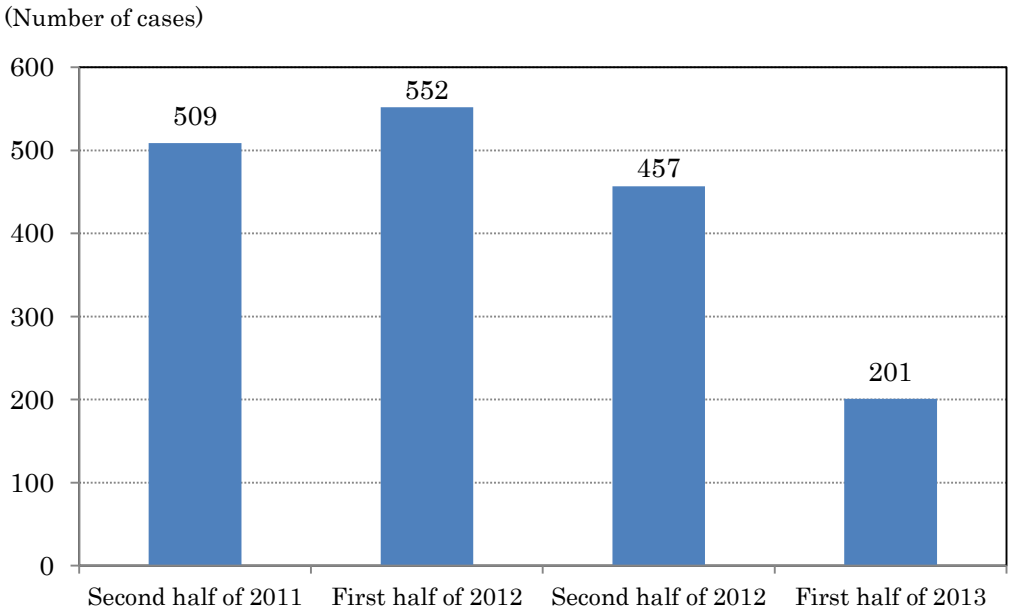
1 Statistical information

① Number of incidents reported (Japan)



Source: Report compiled based on incidents reported to JPCERT Coordination Center (JPCERT/CC) and made public on January 16, 2014 (https://www.jpcert.or.jp/ir/report.html)

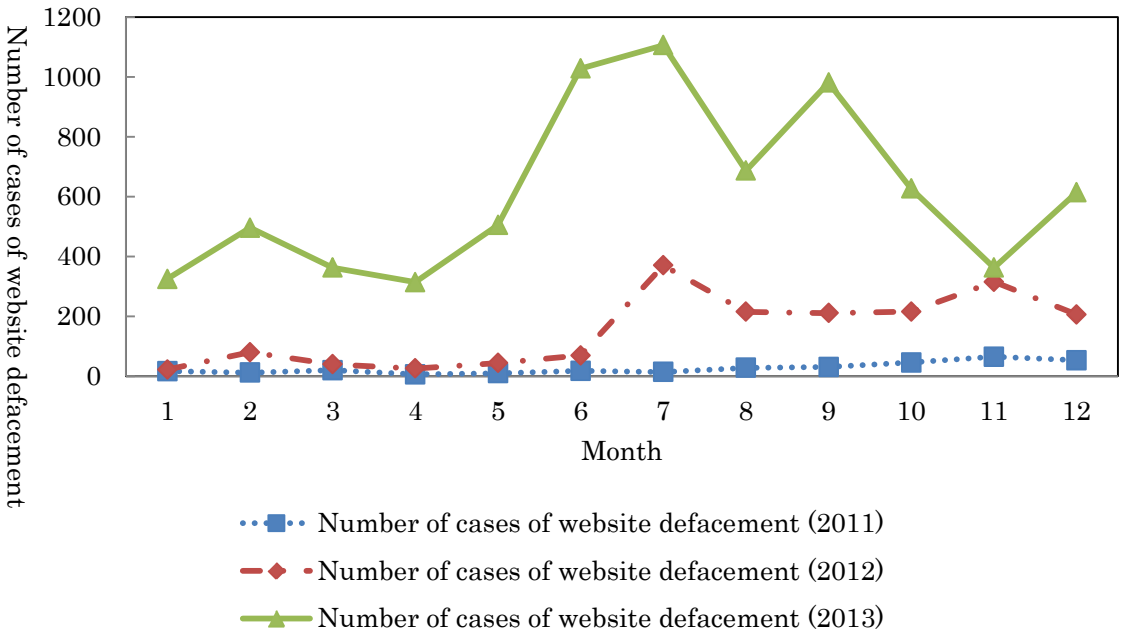
② Number of targeted attacks[30] (Japan)



Source: "Cyber Attacks in First Half of 2013," National Police Agency

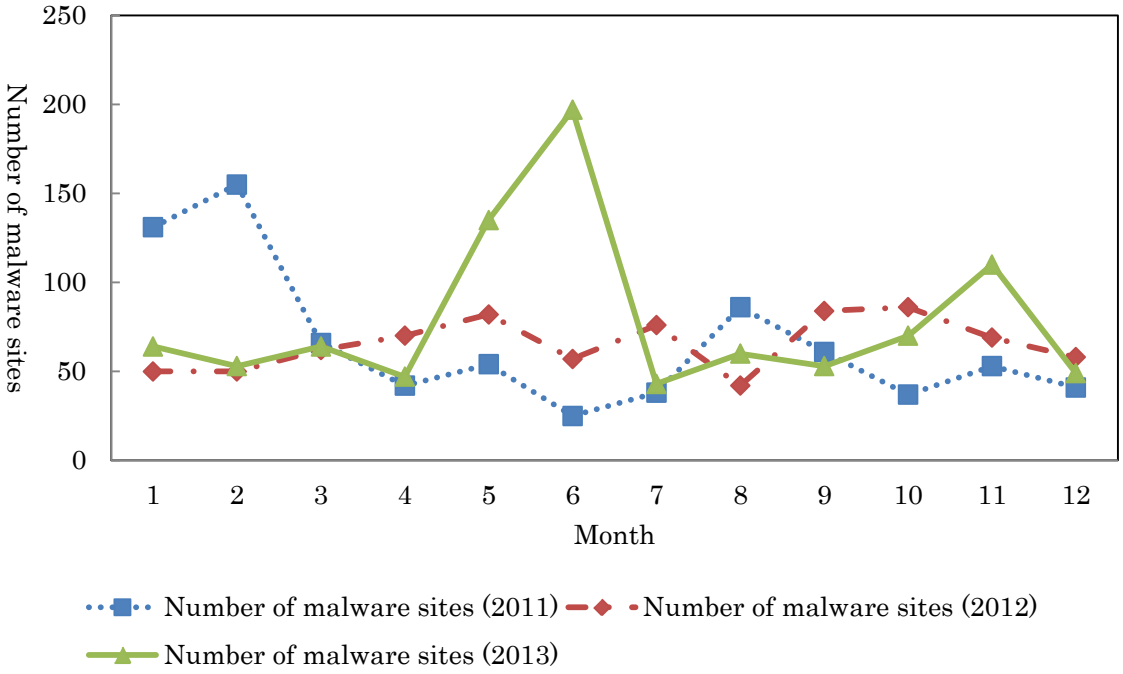
[30] Number of targeted mail attacks reported to the National Police Agency

③ Number of cases of website defacement (Japan)



Source: JPCERT/CC Incident Report

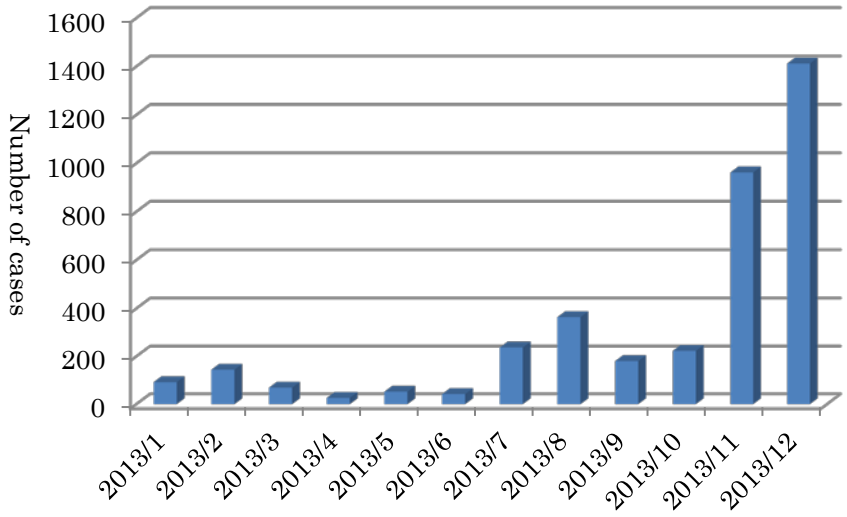
④ Number of malware sites



Source: JPCERT/CC Incident Report

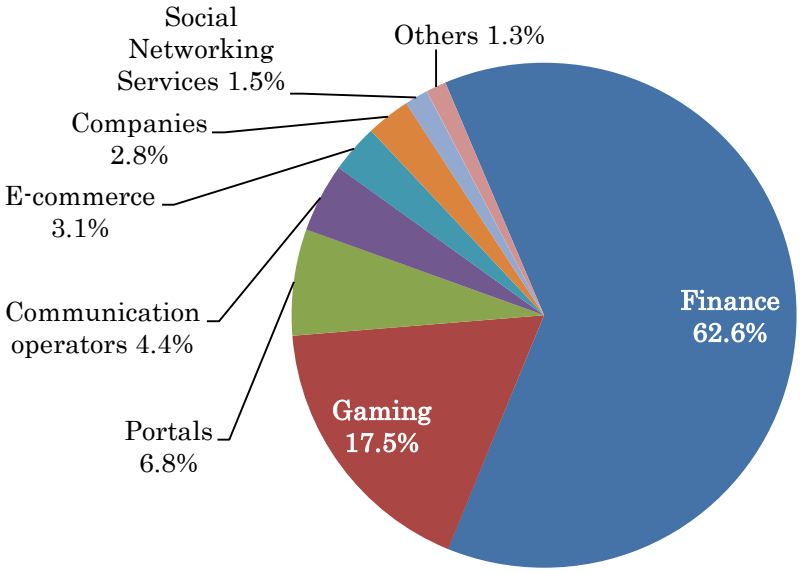
⑤ Number of cases of phishing fraud

a. Number of cases of phishing reported to the Council of Anti-Phishing Japan



Source: Council of Anti-Phishing Japan[31]

b. Percentage of phishing sites by brand type[32]

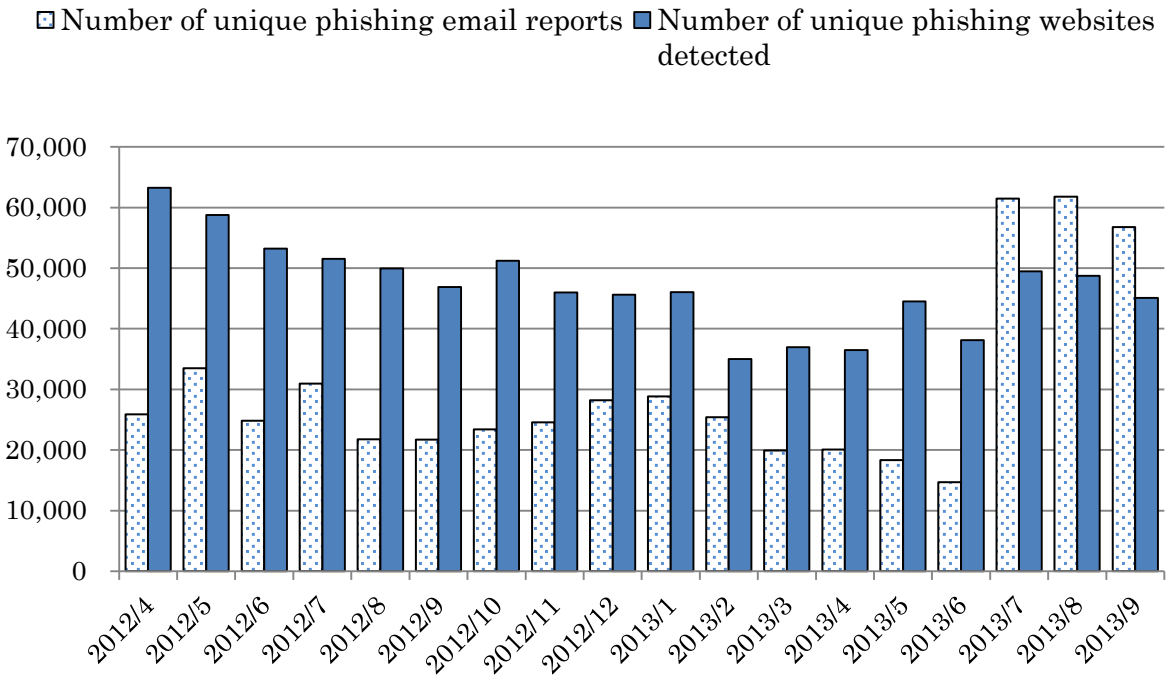


Source: JPCERT/CC Incident Report (October 1, 2013 to December 31, 2013)

[31] Organization established in April 2005 with a view to promotion of countermeasures against phishing, including information collection and provision, and alerts. Its objective is to reduce the number of cases of damage due to phishing fraud in Japan by collecting and providing information on cases and techniques of phishing fraud, which is inflicting serious damage, especially in the U.S. The secretariat is located in the JPCERT Coordination Center.

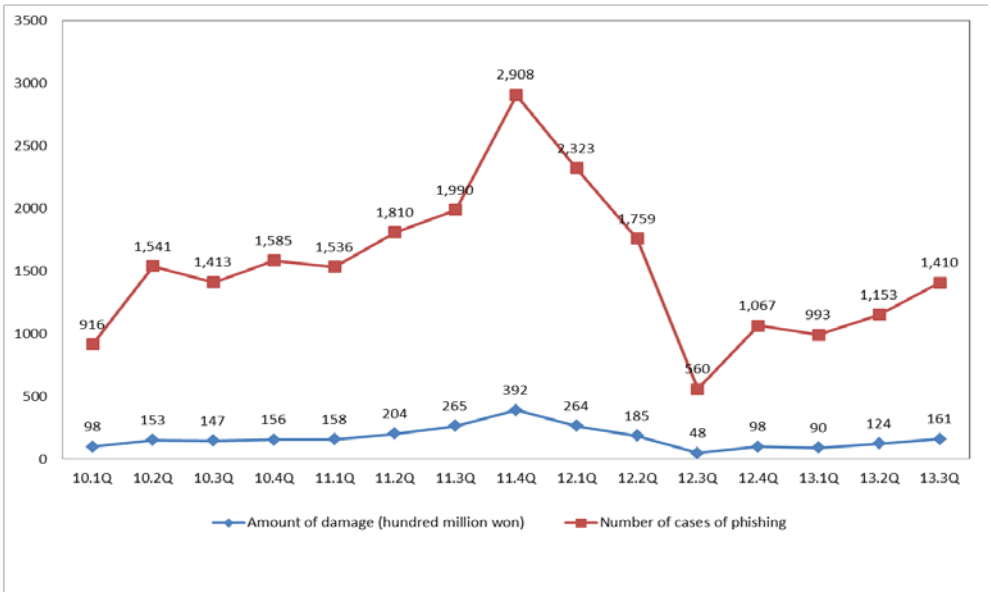
[32] Of the phishing sites reported to JPCERT/CC, those pretending to be sites of financial institutions account for 62.6%. By brand type, financial institutions are predominant in terms of both domestic and overseas brands.

c. Number of cases reported to the U.S. Anti-Phishing Working Group (APWG)[33]



Source: Council of Anti-Phishing Japan

d. Number of cases of phishing and amount of damage reported to Korea National Police Agency[34]



Source: Korean Financial Supervisory Service

[33] World's largest anti-phishing industry group headquartered in the U.S. Established in 2003 as an NPO (3,300 members from 1,800 organizations and companies). Major activities include log data collection on a global scale, provision of statistical information through these logs, and education.

[34] Number of cases of phishing and amount of damage reported to and calculated by the Korea National Police Agency (In South Korea, the Financial Supervisory Service, National Internet Development Agency of Korea, and Korea National Police Agency independently receive damage reports and gather information. The total number of cases of damage attributable to phishing is unknown.)

⑥ Types of cyber attacks (list)

Type of threat	Outline of threats and purposes of attack	Examples of attacks
Unauthorized access (attack)	- Investigation into Internet security vulnerabilities - Destruction and theft of information of an organization by illegally breaking in, suspending services	- Drive-by download (infection with illegal program) - SQL injection - Cross-site scripting - OS command injection - Break-in by evading authentication - Defacement of websites
Targeted attack	- Creation of backdoor, theft of information, falsification, destruction, hijacking computers or servers, suspending services (degrading functions)	- Targeted attack mail (infection with illegal program) - Watering hole attack (Note 1)
DoS attack	- Suspending services (degrading functions)	- DDoS attack (SYN flooding attack, (Note 2) UDP flooding attack (Note 3)) - DoS attack
Phishing	- Theft of customer information	- MITB (Man in the Browser) - Theft of account information using phishing site and phishing mail
Spoofing	- Illegal operation (illegal transactions)	- Spoofing by robbing account - List type attack (Note 4)
Wiretapping	- Account information leak, business information leak	- Wiretapping communication path

(Note 1) Cyber attack technique involving waiting for a specific customer to visit a site where customers frequently meet (watering hole) and infecting the target customer's system with a malicious program.

(Note 2) DoS attack technique that stops servers functioning by trying a large number of not-established TCP connections

(Note 3) Attack technique involving breaking a circuit by sending a large number of UDP packets, which are mainly used for real-time communication

(Note 4) Cyber attack technique whereby a third party who has obtained the IDs or passwords of others attempts unauthorized access to various websites using a list of IDs and passwords

Sources: Threats that can be anticipated as external cyber attacks were extracted from the threat list of Guidelines on Management for IT Security (GMITS[35]) and classified. Created by FISC based on hearings conducted by LAC Co., Ltd.

[35] Guidelines on Management for IT Security: Technical report ISO/IEC TR13335 of the International Standardization Organization (ISO). Describes the strategies an organization should adopt to protect security, need for security policies, items necessary for a security policy, and security techniques for companies

⑦ List of countermeasures (inbound, outbound, internal)

This table lists countermeasures (inbound, outbound, internal) against cyber attacks:

	Prevention	Detection and Defense
Inbound measures	- Using service packs to update OS to the newest version - Applying security patches for OS and general-purpose software - Updating pattern files of anti-malware software	- Firewall (Note 1) - Introduction of anti-malware device or software - Introduction of IDS/IPS (Note 2) and updating signature (Note 3) - Introduction of spam filter (Note 4) and Web filter (Note 5) and updating blacklist (Note 6)
Outbound measures	- Retrieving and periodically analyzing communication log and event log	- Introduction of IDS/IPS and updating signature - Next-generation firewall - Monitoring external connection (Note 7) - Integrated log analysis (Note 8)
Internal measures	- Appropriate management of IDs for OS and database, and management of passwords - Retrieving and periodically analyzing access logs, including error log - Applying minimum authority (Note 9) to users of system - Restricting start-up process - Encryption of files - Encryption of database	- Introduction of behavior detection type anti-malware device and software - Analyzing status of authority usage (Note 10) - Monitoring execution of specific commands (Note 11) - Policy-based monitoring of access to database (Note 12)

(Note 1) System that monitors communication at an external border to detect and block unauthorized access and thereby prevent any third party from breaking in via the Internet and peeping at, falsifying, or destroying data and programs

(Note 2) An intrusion detection system (IDS) monitors communication over a network to detect and report suspicious communication, such as for an illegal break-in or by a malicious program. An intrusion protection system (IPS) is a system for automatically blocking illegal communication that it has detected. These systems are used to block illegal intrusion from outside or monitor communication over a network.

(Note 3) Data defining the features of attacks and unauthorized accesses. By comparing transmitted or received traffic against this data, break-in and illegal communication to outside can be detected and blocked.

(Note 4) If spam mails are received in large numbers, the network may become overloaded and its resources may be wastefully consumed, impeding normal operation of the network. A spam mail filter is a measure for blocking incoming mails from a specific server or relay server that sends spam mails after identifying and registering the information on the server.

(Note 5) A web filter is a measure for blocking accesses based on a blacklist of the URLs or keywords of inappropriate websites.

(Note 6) The current mail system can identify the source server because the transmission route is recorded. A blacklist contains the IP addresses of servers that are known as transmission sources of spam mails and those that relay mails to hide the source of transmission. By registering a blacklist to the incoming mail server, incoming mails from such servers can be blocked.

(Note 7) Measure for detecting and blocking communication to suspect connection destinations. It detects and blocks communication to C&C servers (servers that communicate with computers hijacked by an illegal program from outside, and remotely control those computers by issuing commands from outside) using the IP addresses on a blacklist.

(Note 8) Centrally collecting and storing the logs of various systems distributed on a network and analyzing the correlation among those logs

(Note 9) Granting limited authority to system users. For example, a user account for backup does not need authority for installing software but authority is required for executing backup-related operations. Granting the minimum authority can minimize damage if the system is penetrated in using a certain user ID.

(Note 10) Controlling unintended exercise of a privileged ID. A log of exercising of a privileged ID should be monitored at appropriate intervals by retrieving logs of successful and failed access. In particular, some rules should be formulated for

a privileged ID whose password cannot be changed periodically due to its connection with important programs. Suggested rules include restricting use of the ID to within at limited time assigned by a batch, with access from a limited server or with access only to a set of specific operations. It is also recommended to have a function for detecting any irregular behavior. Incidentally, privileged IDs include the database administrator (DBA).

(Note 11) Monitoring specific commands that may be illegally executed in the course of the activity of malware, such as changing administrator authority

(Note 12) Monitoring SQL statements by registering regularly used SQL statements as a policy. If it detects suspect statements, (e.g. “SELECT*”-which could be used by an unauthorized program to steal information) its access to the database will be blocked.

Source: Created by FISC

⑧ Outline of measures for separation and isolation of network environments

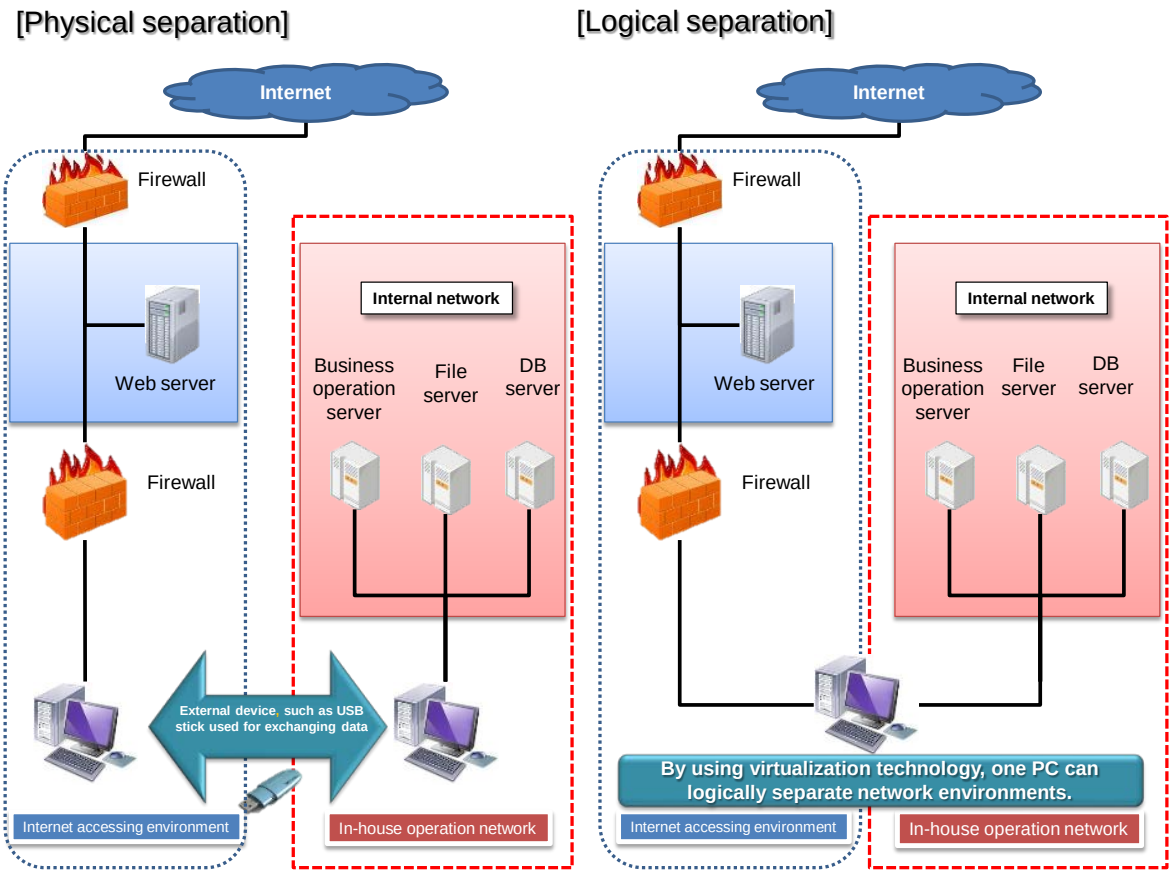
A network for an in-house operation system can be separated and isolated from a network for accessing the Internet in one of two ways: physical separation or logical separation.

[Physical separation]

Physically separating network environments by independently installing terminals, network devices, and communication lines

[Logical separation]

Logically separating network environments by using virtualization technology, while sharing terminals, network devices, and communication lines



Source: Created by FISC based on published materials

⑨ Examples of recent major cybercrimes and attacks

Date of occurrence	Description of attack
March 2011	- DDoS attack against South Korean government agencies
April	- Cyber attack against Sony Online Entertainment (U.S.) - Targeted attack against agricultural cooperative in South Korea
June	- Theft of authentication information for Internet banking from 53 Japanese financial institutions - Unauthorized access to Citibank (North American region) - Cyber attack against International Monetary Fund (IMF) (attack technique unknown)
July	- DDoS attack against National Police Agency of Japan
August	- DDoS attack against Hong Kong Exchanges and Clearing Limited
September	- Targeted attack against Mitsubishi Heavy Industries - Targeted attack against an organization related to Japan's defense ministry - Theft of private information by guiding MasterCard users an illegal website from a URL mentioned in emails
October	- Phishing fraud under the name of a Japanese financial institution - Phishing fraud to steal passwords (such as random number list information) for Internet banking operated by a Japanese financial institution
June 2012	- Illegal access to and defacement of the websites of Japan's Ministry of Finance Japan and Ministry of Land, Infrastructure, Transport and Tourism, and DDoS attack on JASRAC sites.
July	- Man in the Browser (Operation High Roller) attack to illegally transfer money via computers owned by customers of some financial institutions in the U.S. and Europe to the bank account of a third party
September	- DDoS attack against and defacement of websites of Japanese government agencies such as the Supreme court, Ministry of Internal Affairs and Communications, Cabinet Office, and Tokyo Metropolitan government office following nationalization of the Senkaku Islands by the Japanese government - DDoS attack against websites of some Japanese private firms, including newspaper companies, banks, and airlines
October to December	- Theft and illegal money transfer via some infected computers owned by customers of Japanese Internet banking websites using a process that displays a false screen and requests random number list figures. - In Japan, crime notice and threats were posted to bulletin boards and sent via emails by spoofing from computers infected by illegal programs to facilitate remote control. Although, initially, the owner of the remotely controlled computer was arrested, it was subsequently found that the wrong person had been charged; the real culprit later claimed responsibility.
January 2013	- Leakage of confidential documents concerning TPP negotiations from a remotely controlled official computer of Japan's Ministry of Agriculture, Forestry and Fisheries.
February	- Suspicion of leakage of document information through suspicious communication from a computer of Japan's Ministry of Foreign Affairs to an external server.
March	- Systems at Shinhan Bank and KBS in South Korea went down (ATMs and broadcasting were halted), and data in servers were destroyed.
April	- Leakage of credit card information of customers in the U.S. from a server of the U.S. subsidiary of NTT DoCoMo - Attack on ID management server of Yahoo Japan leading to leakage of ID information of more than 20 million customers
June	- Illegal withdrawal of US$45 million from several ATMs in the U.S. by breaking into pre-paid card system and changing pre-paid cards into unlimited cards (no maximum withdrawal limits)
October	- Network of Adobe Systems (U.S.) came under attack and customer information and source codes of a number of products were illegally accessed (including customer IDs, encrypted passwords, customer names, encrypted credit/debit card numbers and their validity periods and purchasing histories), affecting 2.9 million customers.
December	- In Japan, 1,125 cases of illegal money withdrawal from bank accounts by stealing IDs and passwords for Internet banking were reported from January through November. Total amount of damage ¥1.2 billion (according to the National Police Agency).

Source: Created by FISC based on materials such as press reports

2. Activities by major Japanese public organizations and councils for improving security, including countermeasures against cyber attacks

No	Name	Foundation	Organization	Activities
1	Information-technology Promotion Agency, Japan (IPA)	October 1970	Independent administrative corporation under jurisdiction of Ministry of Economy, Trade and Industry	Ensuring safety and reliability of IT and promotion of IT strategy through development of various security measures and reliable software, and human resources
2	Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)	October 1996	Several dozen information security analysts acting under control of security committee comprising former employees of IT operators, communication operators, and Internet service providers, persons with academic backgrounds and former officials of an administrative agency	Organization founded as Computer Emergency Response Center under the initiative of the then Ministry of International Trade and Industry to respond to computer security incidents and organize coordination among parties concerned with disclosure of vulnerability-related information. Serves as Japanese contact point for receipt of domestic and international reports (requests for coordination) and conducts support activities, such as analyzing the situation and technique of an incident and coordinating technical responses among concerned parties
3	Cyber Force	April 2001	Comprising National Police Agency's cyber terrorism response technical center (known as: Cyber Force Center) and mobile technical groups (cyber force) deployed across Japan	Provides emergency technical responses to cyber attacks (including cyber terrorism and cyber intelligence) as the police technical base. Detects signs of cyber attacks, analyzes situations, and provides Internet observation results to critical infrastructure operators, 24/7
4	Integrated Security Measures Council	December 2001	Private panel sponsored by head of Community Safety Bureau of National Police Agency. Comprising private-sector experts such as university professors, lawyers, systems vendors, information security vendors, and representatives of industry groups	Studies cooperation among industrial circles and police on information security, using experts, from the perspective of ensuring safety and reliability of information communication networks
5	National Information Security Center (NISC)	April 2005	Comprising Assistant Chief Cabinet Secretary (center head), two Cabinet Secretaries (vice center heads), six Cabinet directors, and three information security aides (advisers) selected from private sector	Information security policy execution organization that carries out the following activities based on the First National Strategy on Information Security, formulated in February 2005: - Basic strategy (formulating medium-/ long-term plans and annual plans on information security strategy) - International strategy (liaison for international cooperation on information security policies) - Promotion of comprehensive measures by government organizations (formulation and operation of consistent standards for promoting information security measures in government organizations) - Critical infrastructure measures (gathering, analyzing, and assessing vulnerability information and incident information, and supporting government organizations) - Incident response support (cooperation between public and private sectors on information security based on a critical infrastructure action plan)

No	Name	Foundation	Organization	Activities
6	Information Security Policy Council	May 2005	Comprising experts in various aspects of information security policy and requested by the director-general of Strategic Headquarters for the Advanced Information and Telecommunications Network Society to participate in deliberations, as well as the Chief Cabinet Secretary (chairman), minister in charge of information technology (IT) policy (deputy chairman), National Public Safety Commission Chairman, Minister for Internal Affairs and Communications , Minister for Foreign Affairs , Minister of Economy, Trade and Industry , and Minister of Defense	Set up under the supervision of the IT Strategic Headquarters (Strategic Headquarters for the Advanced Information and Telecommunications Network Society) as a council that decides on matters related to the core of Japan's information security issues. Formulates basic policy related to information security and unitary government safety standards for information security.
7	Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR)	December 2005	Comprising companies and industrial groups involved in critical infrastructure such as finance, information communication, and electricity *Financial field is divided into four CEPTOARs (banks, securities, life insurance, and non-life insurance) and information communication field into three (communication, broadcasting, and cable television). A total 15 CEPTOARs by field exist.	Framework to reinforce information sharing system related to IT vulnerabilities in critical infrastructure fields. Aims to appropriately provide critical infrastructure operators with information provided by the government on IT vulnerabilities, enhancing information sharing by concerned parties and improving responsiveness to incidents.
8	CEPTOAR-Council	February 2009	Comprising industry group representatives of 13 of 15 CEPTOARs. Railways and Medical Services CEPTOARs also participate in the general assembly as observers. Incidentally, this center also participates in the general assembly as an observer.	Seeking to reinforce security measures for critical infrastructure and share information among the respective CEPTOARs, performs the following activities: - Promotion of cross-cutting information sharing - Coordination and management of information sharing system for preventing IT faults in critical infrastructure - Discovery of cross-cutting common issues and development of common understanding
9	Information Security Measures Promotion Council	July 2010	Comprising Chief Cabinet Secretary (chairman), Deputy Chief Cabinet Secretary for Crisis Management, Deputy Chief Cabinet Secretary for Information Communication Policy (vice chairman), and chief information security officers (CISO) in related administrative bodies and official position designated by chairman	Set up under the supervision of the Information Security Policy Council to bolster the functions of chief information security officers (CISO) in government agencies. Studies matters related to the information security policies of government agencies, such as revising unified technical standards, and reporting on and evaluating implementation of countermeasures and important inspections by ministries and agencies
10	Cyber Intelligence Information Sharing Network	August 2011	Comprising National Police Agency, municipal police, and some 5,000 operators with advanced technology across Japan	Information sharing network for exchange of information among operators that could be targeted by cyber intelligence activities and police. Raises operators' awareness of targeted attacks and email attacks by collecting and analyzing information on such attacks.

No	Name	Foundation	Organization	Activities
11	Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP)	October 2011	Comprising five industries – critical infrastructure device manufacturers , power, gas, chemical , and petroleum – and 45 participant organizations	Shares information gathered by a public organization, IPA, on countermeasures against advanced cyber attacks with participating organizations
12	Cyber Incident Mobile Assistant Team (CYMAT)	June 2012	CYMAT is supervised by the head of the National Information Security Center, who is a government CISO, and comprises officials of the Cabinet Office and all ministries and agencies.	Organization set up in the National Information Security Center (NISC) in the event of an emergency. Upon occurrence of an incident requiring concerted response by government agencies, prevents expansion of damage, implements recovery, investigates cause, provides technical support and advice to prevent recurrence, in cooperation with the Cabinet Office and all ministries and agencies.
13	CEPTOAR-Councils Capability for Cyber Targeted Attack Protection (C4TAP)	December 2012	About 350 organizations	Initiative aimed at gathering and sharing increased information on targeted attacks, blocking targeted attacks against critical infrastructure services or mitigating damage, and maintaining or promptly recovering services, by sharing specific information on emails suspected of being related to targeted attacks

Source: 2013 edition of “Financial Information Systems White Paper,” issued by FISC

3. Major information sharing systems in Japan

① CEPTOARs (Capability for Engineering of Protection Technical Operation Analysis and Response) in financial field

Name	CEPTOARs in financial field (Note 1)
Outline of organization	- Information Security Policy Council set up at the IT Strategic Headquarters under the 2005 Action Plan on Information Security Measures for Critical Infrastructures. According to this plan, Capability for Engineering of Protection, Technical Operation, Analysis and Response functions (CEPTOARs) are set up in 10 fields of critical infrastructure (Telecommunications, Finance, Civil Aviation, Railways, Electricity, Gas, Governmental Administrative Services (including local governments), Medical Services, Water Works, and Logistics). NISC is the secretariat for this council. - CEPTOAR in the financial field comprises banks, securities firms, life insurance and non-life insurance companies. - The financial CEPTOAR liaison council (secretariat: Japanese Bankers Association) shares and exchanges information on activities and successful cases handled by individual CEPTOARs. As necessary, relevant organizations participate in the council as observers.
Number of members	- Bank CEPTOAR: 1,561 companies, Securities CEPTOAR: 253 companies and 8 organizations, Life insurance CEPTOAR: 43 companies, Non-life insurance CEPTOAR: 29 companies (including 3 observer companies) (As of the end of March, 2013)
Functional outline	○ Bank CEPTOAR - Organized by operators of settlement systems and all business types of deposit-taking financial institutions - Deposit-taking financial institutions are mutually related through a settlement system, and malfunctioning of settlement due to an IT fault at one institution could be systemically expanded to other institutions. Bank CEPTOAR shares and analyzes information on IT faults and responses to them. ○ Securities CEPTOAR - Membership comprises securities-related institutions, such as securities firms, securities exchange, liquidation and settlement institutions; shares information provided by the government among members. Information is shared among concerned parties as necessary. - Analyzes and ascertains major system fault causes in the securities field, studies measures for preventing occurrence of incidents and expansion of damage in the event of an incident, and shares information among concerned parties through cooperation with informal gatherings of chief information officers (CIOs) of securities firms. ○ Life insurance CEPTOAR - Shares information on IT faults, financial crimes using IT, vulnerability of software and hardware, and viruses. Also shares information on prevention of IT faults and expansion of damage in the event of a fault, rapid recovery, and prevention of recurrence. ○ Non-life insurance CEPTOAR - Shares information on IT faults, financial crimes using IT, vulnerability of software and hardware, and viruses. Also shares information on prevention of IT faults and expansion of damage in the event of a fault, rapid recovery, and prevention of recurrence.

(Note 1) CEPTOAR stands for Capability for Engineering of Protection, Technical Operation, Analysis and Response and is the name of the information sharing and analysis function prepared for each critical infrastructure field.

Source: Created by FISC based on published materials

② Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP)

Name	Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP)
Outline of organization	- Set up in October 2011 as a facility for information sharing and rapid response by manufacturers of equipment used for critical infrastructure (e.g. heavy industry, power generation, etc.) under the supervision of the Ministry of Economy, Trade and Industry (METI). This was a response to the strong demand for construction of a framework for sharing information and measures for strengthening information security against targeted cyber attacks, based on a proposal by METI's Study Group on Cyber Security and Economy, which was launched in 2009, and cyber attacks against Mitsubishi Heavy Industries and government agencies
Members	- Forty-five organizations participating from five industries (critical infrastructure device manufacturers, power, chemical, gas, and petroleum)
Functional outline	- The Information-technology Promotion Agency, Japan (IPA) collects information on cyber attacks that are detected at member companies and its group company (or industry organizations). - IPA analyzes the information source and sensitive information, adds the results of analysis by IPA, shares information having obtained authorization from the information source, and shares with member companies. - IPA provides information to METI or to the National Information Security Center through METI, upon approval from the information supply source, if any damage to participants or the nation is anticipated. - Cooperation with JPCERT Coordination Center upon approval from the information source - Supply of emergency response information and technical reports to general companies and industrial groups

Source: Created by FISC based on published materials

③ Targeted attack information sharing system in CEPTOAR-Council

Name	CEPTOAR-Councils Capability for Cyber Targeted Attack Protection (C4TAP)
Outline of organization	Initiative to collect and share various information on targeted attacks among the critical infrastructure operator attacks, and prevent targeted attacks on critical infrastructure services, mitigate damage, and facilitate prompt recovery
Membership	About 350 organizations (at start of operation) *CEPTOAR groups, companies, organizations, and observers joining CEPTOAR-Council
Services supplied	- Analyzes information supplied by participants on targeted attack emails and provides it to the information supplier and participants. - Information supplier can select the range of sharing for each type of information. - The supplier can remain anonymous if the information contains confidential information.

Source: Created by FISC based on published materials

4. Activities by major overseas public organizations and councils

① U.S. FS-ISAC

Name	Financial Services Information Sharing and Analysis Center (FS-ISAC)
Outline of organization	- Non-profit organization (not government-related), established in 1999 by Executive Order - Over 4,400 member institutions, mainly banks but also including insurance companies and debit/credit card companies - About 600 paying member organizations. Other members are non-paying members.
Operating expenses	- Operations funded mainly by membership fees from paying members (operating expenses are tax-deductible). - Income from sponsors of conferences held by FS-ISAC and business earnings from Web seminars sponsored by FS-ISAC
Membership	- Paying members are classified into several ranks, including platinum, premium, standard, basic, etc. Voting rights and election eligibility of officials differ depending on rank.
Services supplied	- Collecting and analyzing information from financial institutions on damage from and responses to disasters that cause physical damage, such as cyber attacks and natural disasters, and sharing that information with other member financial institutions - Sources of information collected by FS-ISAC ① Information from member financial institutions ② Open sources (published news reports and information from websites) ③ Information delivered by the government or vendors ④ Information delivered by ISACs other than FS-ISAC - Only information in a limited range is available to non-paying members. However, there are cases where the same information for paying members is provided to non-paying members if substantial damage to the whole industry can be assumed (e.g. hurricane damage).
Response to medium-sized and small institutions and mentor system	- Small financial institutions that do not join the FS-ISAC generally receive information from the FS-ISAC through member industry groups in the FS-ISAC (such as ABA, CUNA, SIFMA, and ICBA (Note 1)). - A mentor system has been established to enable major financial institutions to provide expertise in responding to cyber attacks to small financial institutions.

(Note 1) ABA: American Bankers Association, CUNA: Credit Union National Association, SIFMA: Securities Industry and Financial Markets Association, ICBA: Independent Community Bankers of America

Source: Created by FISC based on interview with FS-ISAC

② South Korea financial ISAC

Name	Information Sharing and Analysis Center (South Korea)
Outline of organization	- Under the Information Communication Infrastructure Protection Act, which came into effect in 2001, two organizations were designated as financial ISACs by the then Ministry of Finance and Economy of the Republic of Korea and the Financial Supervisory Commission in 2002: ① Koscom, an Internet-based security company and ② Korea Financial and Telecommunications Clearings Institute, which provides financial settlement functions and electronic authentication services for Internet banking. - The financial ISAC of Koscom has about 70 member companies, including securities firms and related institutions (such as securities exchanges).
Membership	- Membership fee depending on the asset size of a member company and the contents of services
Services provided	- Gathers information on the techniques used in the latest cyber attacks, virus information, infringement accident information, and statistics on detection of and defense against attacks collected from member companies, government agencies, and relevant institutions, and analyzes and provides information to member companies. - Real-time surveillance for DDoS attacks and unauthorized break-ins, 24 hours a day and 365 days a year, using a joint monitoring system - The member financial institution supplies log information on communication networks to the financial ISAC (using installed equipment and circuits for collecting logs). - Gathering and analyzing evidence data, identifying damaged parts, determining if information has been leaked, and using a forensics task force to identify the leak route - Studies and supports recurrence prevention measures to be implemented in the event of damage due to a cyber attack - Provides advice on analysis, diagnosis, and fixes to minimize vulnerability (information security consulting) - Holds workshops and seminars.

Source: Created by FISC based on interview with South Korean financial ISAC

③ Europe

Name	The European Network and Information Security Agency (ENISA)
Foundation	March 2004 (started operating in September 2005.)
Background	Set up, based on EC Regulation № 460/2004 of March 10, 2004, to reinforce response by the EU, its member nations and businesses to issues of networks and information security
Headquarters	Iraklion, Republic of Greece
Number of officials	65 (June 2013)
Outline of operations	- Collects cyber security information and analyzes risks. Also conducts studies on risk assessment activities and risk control. - Supports EU institutions and member nations' jurisdiction authorities (advice, legislation support, cooperation with member nations, and support dialog with industrial sector) - Improving public awareness of ICT security matters - Support for technological research and development and standardization activities - Promotion of international cooperation activities among EU and third countries
Features	- Organization under control of Executive Director (currently Prof. Udo Helmbrecht) - Run by and comprising experts representing stakeholders from areas such as the information communication technology industry, consumer groups, and persons with academic background as members - Supervised by a control committee made up of representatives from EC and member nations - Budget allotted by EU. Annual budget: 8.2 million euro

Source: Created by FISC based on published materials

Name	Financial Institutions-Information Sharing and Analysis Center (FI-ISAC) (Europe)
Outline of organization	- European cooperation initiative formed in 2008 by the European Network and Information Security Agency (ENISA), Centre for the Protection of National Infrastructure (CPNI.NL) of the Netherlands, and stakeholders of ENISA (Hungary, United Kingdom, and Switzerland). - Members include the Computer Emergency Response Team (CERT), law enforcement agencies, and banks in Europe. - Its objective is to promote information sharing on incidents, threats, and vulnerability across the European region. - The Netherlands has a separate FI-ISAC that shares incident information based on its own mailing list (incidents are analyzed by each financial institution on its own responsibility).

Source: Created by FISC based on published materials

Name	Cyber security Information Sharing Partnership (CISP) (United Kingdom)
Outline of organization	- In 2011, following a meeting by the British prime minister with industry leaders, a pilot project was launched with participation by 160 companies across five industries (defense, energy, finance, pharmaceuticals, and telecommunications) with a view to promoting exchange of practical information on and reinforcement of countermeasures against cyber threats. - Following the pilot period, from 2011 through 2012, a framework that comes under the jurisdiction of the Office of Cybersecurity and Information Assurance (OCSIA), an internal organization of the British Cabinet Office, was officially established. - As of January 2014, more than 600 individual members representing about 300 organizations are participating.
Operating expenses	- Financial support from the government based on the National Cybersecurity Programme
Membership	- Individual membership for corporations qualified for admission (several representatives from each corporation)
Services supplied	- Provides an online communication website for exchange of information on threats of cyber attacks, vulnerability, best practices, appropriate responses, etc.

Source: Created by FISC based on published materials

④ Others

Name	Forum of Incident Response and Security Teams (FIRST (Note 1))
Outline of organization	- International non-profit organization established in 1990 to reinforce mutual communication among CSIRTs (Note 2) worldwide and to collect, provide, and share security incident information - 290 CSIRTs representing 64 governments, educational establishments, and businesses worldwide participate as members, including 22 CSIRTs from Japan. (Note 3)
Activities	- Holds Annual FIRST Conference on Computer Security Incident Handling (Annual FIRST Conference) to share knowledge and information on incident response with security experts from around the world. - Non-FIRST members can also participate in the Conference. - In addition to the Annual FIRST Conference, FIRST Symposia, held several times a year focusing on specific regions and FIRST Technical Colloquia on Computer Security Incident Handling are also held to share information about incidents and vulnerability affecting incident response.

(Note 1) Reference URL: http://www.first.org

(Note 2) CSIRT stands for Computer Security Incident Response Team, which is an organization established to respond to incidents related to computer security. It constantly gathers and analyzes information on incidents, vulnerability, and signs of attacks, and formulates guidelines and procedures for responses.

(Note 3) As of the end of December 2013

Source: Created by FISC based on published materials

5. Joint training programs

① Ministry of Economy, Trade and Industry

Name of program	Cyber security training by the Ministry of Economy, Trade, and Industry (electricity, gas, and buildings)
Conducted by:	Sponsored by: Ministry of Economy, Trade, and Industry Secretariat: Mitsubishi Research Institute, Inc.
Dates and frequency	(Electricity): March 12, 2013 (Gas): February 5, 6, 14, and 15, 2013 (Buildings): February 25, 2013
Objectives	- To reinforce response to cyber attacks aimed at suspending or damaging operation of control systems used for critical infrastructure - To enhance awareness regarding security threats with the potential to seize control of systems, and countermeasures against them
Participants	Ministry of Economy, Trade, and Industry Electricity, gas, and building industry groups Electricity, gas, and building research institutes Electricity, gas, and building operators Control system vendors
Description and method of training	- Lecture and exercise on security - Exercise on security incident response activities based on a scenario, using a control system simulator - Although training was conducted separately in each field in 2013, it is planned to use the Tagajo Headquarters of the Control System Security Center (CSSC), in Tohoku, in 2014.

Source: Created by FISC based on interview with the Ministry of Economy, Trade and Industry

② Joint training program organized by Ministry of Internal Affairs and Communications

Name of program	Cyber Defense Exercise with Recurrence (CYDER (Note 1))
Conducted by:	Ministry of Internal Affairs and Communications
Date and frequency	Started in September 2013 The first exercise was conducted in September 2013. A total six exercises are planned within the fiscal year.
Objectives	- To improve the incident response capability of LAN managers and LAN operators in ministries, agencies and private enterprises - To develop skilled information system administrators who can respond to attacks that threaten continuous system operation while taking its daily operation into consideration
Participants	Central ministries and agencies, independent administrative corporations, and private enterprises
Description and method of training	- Practical cyber defense exercise simulating a large-scale organization network with several thousand officials participating and a large-scale environment - Practice responding to an attack with a team of two to four members participating from each agency and experiencing incident handling using an actual machine - Guidance in the morning of Day 1 and an exercise using an actual machine in the evening. Evaluation of individual teams' responses on Day 2 and sharing of the results with all participants

(Note 1) CYDER stands for CYber Defense Exercise with Recurrence.

Source: Created by FISC based on published materials

③ Joint training program organized by NISC

Name of program	CEPTOAR (Note 1) training
Conducted by:	National Information Security Center (NISC)
Date and frequency	Conducted from July through December 2012 (The first training program was conducted in 2006; 2012 marked the seventh.)
Objectives	- To maintain and improve the information sharing system among CEPTOAR, NISC, and critical infrastructure sector-specific ministries (Maintenance of contact network and skills improvement) - To identify areas for improvement or issues to be resolved, such as the procedures of each CEPTOAR and on each route, and to check the information sharing system
Participants	- 11 CEPTOARs and participating operators (about 1,570 groups) (Operators, including group companies in charge of the information system, to participate in the training program are selected by each CEPTOAR.) - Persons in charge at ministries and agencies supervising critical infrastructure, liaison, (Note 2) and person in charge at NISC
Description and method of training	- Periodically provides an opportunity to check communication functions in order to maintain and improve an information sharing system based on details of implementation. - Sends e-mails (Note 3) from NISC via liaison to each CEPTOAR to provide information to the participants. - Uses simulation information created by NISC for training (information sharing level: Green (Note 4)) and customizes simulation information for some CEPTOARs. - The simulation information may be partially changed by a CEPTOAR or the training can be conducted without prior notice if requested by a CEPTOAR.

(Note 1) CEPTOAR stands for Capability for Engineering of Protection, Technical Operation, Analysis and Response. It was decided in the Action Plan on Information Security Measures for Critical Infrastructures (2005) at the Information Security Policy Council of National Information Security Center (NISC) that a CEPTOAR would be prepared for each critical infrastructure field. There are 14 CEPTOARS: Information Communication, Railways, Banking, Securities, Life Insurance, Non-life Insurance, Airlines, Electric Power, Gas, Government/Administrative Services (including municipal governments), Water Services, Medical Services, and Logistics.

(Note 2) The liaison runs between the NISC, critical infrastructure sector-specific ministries and CEPTOARs.

(Note 3) Time of viewing information by e-mail was reported in order to accurately ascertain the time of arrival of conveyed information.

(Note 4) Information sharing levels (Traffic Light Protocol) are classified into Red, Amber, Green, and White, in descending order of confidentiality.

Source: Created by FISC based on published materials

④ Joint training program organized by three markets

Name of program	3-market joint training
Conducted by:	- Japanese Bankers Association - Tokyo Foreign Exchange Market Committee - Japan Securities Dealers Association
Date and frequency	From February 2010
Objective	To prepare a system for cooperation among markets when BCP is exercised
Participants	- Ministry of Finance Japan, Financial Services Agency, Bank of Japan - 188 members of Japanese Bankers Association - 33 members of Tokyo Foreign Exchange Market Committee - 394 members of Japan Securities Dealers Association
Description and method of training	- Conducts training in virtual time based on an assumption that the three markets are simultaneously hit by the same disaster (earthquake directly striking Tokyo). - Confirms response if BCP on the three markets is exercised simultaneously by members and secretariats. - Shares information among markets and confirms cooperation system.

Source: Created by FISC based on published materials

⑤ Bank of Japan

Name of program	Backup center switchover training
Conducted by:	Bank of Japan
Date and frequency	To be conducted about once a year
Objective	- Practical training to improve effectiveness of business continuity plan based on assumption of various disasters
Participants	- Bank of Japan - Financial institutions - Private settlement system
Description and method of training	- Training on switching over to backup system and connecting customer computers on assumption of a system failure in Bank of Japan's network

Source: Created by FISC based on "Settlement System Report 2012-2013" published by the Bank of Japan

⑥ Cross-sector exercises CIIREX 2013

Name of program	Cross-sector exercises CIIREX 2013(Note 1)
Conducted by:	National Information Security Center (NISC)
Date and frequency	Conducted December 9, 2013 (The first exercise was conducted in 2006. The exercise in 2013 was the eighth.)
Objectives	- To improve protection of critical infrastructure against IT faults - To verify responses to IT faults, information sharing system (including signs), and method of initiating and implementing business continuity plans (BCP)
Participants	- Critical infrastructure operators, etc., in 10 fields (information communication, finance, airlines, railways, electric power, gas, government and administrative services, medicine, water supply, and logistics) - Fifteen CEPTOARs (communication, cable TV, broadcasting, banking, etc., securities, life insurance, non-life insurance, airlines, railways, electric power, gas, municipalities, medicine, water supply, and logistics) - Critical infrastructure ministries and supervisory agencies (financial services, internal affairs, health and labor, economy and trade, and transport) and NISC
Description and method of training	- Exercise using practical scenario simulating the latest example of an IT fault - Information sharing and response in cooperation with assembled operators in 10 fields of critical infrastructure - Exercise scenario assuming a situation where several signs of threats to IT systems are detected, a large-scale IT fault occurs, and services in several fields are affected. - Verifies cooperation between public and private sectors to maintain business operation, and their responses to such a situation

(Note 1) CIIREX (Critical Infrastructure Incident Response Exercise) is the abbreviation of "cross-sector exercises for protecting critical infrastructure".

Source: Created by FISC based on published materials

⑦ U.S.

Name of program	Quantum Dawn 2
Conducted by:	SIFMA (U.S. Securities Industry and Financial Market Association)
Date	July 18, 2013
Participants	Over 500 persons from more than 50 organizations, including financial institutions, Department of the Treasury, securities exchanges, Department of Homeland Security (DHS), Federal Bureau of Investigation and Securities and Exchange Commission (SEC)
Location	U.S. (from each participant's offices)
Training scenario	The stock market had been hit with multiple simultaneous cyber attacks that affected market transactions in a chain reaction, culminating in a market shutdown.
Description of training	- A dedicated training platform was used. "DECIDE-FS (Distributed Environment for Critical Infrastructure Decision-making Exercises - Finance Sector)". - Participants made decisions in response to the situation displayed on DECIDE-FS as the scenario progressed. Based on their reactions, participants shared information, contacted and coordinated with the others.

Source: Created by FISC based on published materials

⑧ United Kingdom

Name of program	Waking Shark II
Conducted by:	Sponsor: Securities Industry Business Continuity Management Group (SIBCMG) Supervisors: Bank of England (BOE), HM Treasury, Financial Conduct Authority (FCA)
Date	November 12, 2013
Participants	About 100 persons from several dozen organizations, including banks, settlement organizations, security exchanges, vendors outsourcing to banks
Location	London City district (meeting training)
Training scenario	- A number of attacks targeting securities markets (including a simulation of a DDoS attack emanating from a fictitious foreign government) affected the whole financial system in a chain reaction. - Preparedness for response to cyber attacks across the entire British financial system was examined (scenario created by Credit Suisse).
Description of training	- Scenario details were not revealed until the day of the training exercise; it was explained to the participants over the course of several hours on the day, then followed up with a training session that lasted for five and a half hours. - Participants shared information by sending damage reports to their companies' portal sites in accordance with the training scenario.

Source: Created by FISC based on published materials

6. Countermeasures by major Japanese banks against illegal money transfer

	The Bank of Tokyo-Mitsubishi UFJ			Mizuho Bank
Measures	Distribution of security software (for computers) to prevent unauthorized programs being installed	System for detecting infection by unauthorized programs	One-time password using software token	Mail type one-time password
Description	- Customers can download the software free of charge from BTMU's website - Extermination/prevention of infection by unauthorized program accessing computers	- System for detecting infection by unauthorized programs is installed on the bank's system. - The bank checks the transactions of customers and, notifies customers when they log in to the system if something illegal is detected	- Displays a one-time password in an application for smartphones - Used when money is transferred using Internet banking (Note 1)	- Sends a one-time password by e-mail - Used for transactions which are suspected of unauthorized access and attempts to deposit money in unregistered accounts
Effects	- Extermination/prevention of infection by unauthorized program accessing customers' computers	- Blocking transactions from computers infected by unauthorized programs	- Prevention of spoofing by stealing a password or a random number list	- Prevention of spoofing by stealing a password
Period	December 15, 2013	December 2013	Within 2014 (planned)	October 6, 2013
Features	- Can directly counter unauthorized programs infecting customers' computers	- Can comprehensively protect all customers by using the bank's server	- Less expensive for storage and delivery, and easier to upgrade than hardware token	- Fast, easy implementation simply by sending emails - Load on the financial institution is reduced because the password can be introduced at lower cost than hardware tokens
Remarks	- Free distribution - The bank does not intend to force customers to install the software on their computers or suspend the accounts of those who do not wish to install it	- Whether or not usage is to be stopped when an infection or illegality is discovered is still under consideration	- No plan to introduce hardware tokens	- Targets are all Internet banking customers - Mobile banking customers are excluded - Customers using conventional hardware tokens are excluded

(Note 1) Internet banking is a transaction using a computer or a smartphone.

	Sumitomo Mitsui Banking Corporation		Resona Bank	
Measures	Distribution of password cards	SMBC Direct Light (exclusive inquiry service)	One-time password using software token	Internet banking service without money transfer function
Description	- Displays one-time password on card-shaped hardware token - Used for money transfer via Internet banking or mobile banking	- Internet banking with functionality limited to viewing balance information and inquiring about deposit/withdrawal details - Cannot be used for applications such as money transfer, products, or changing address details	- Displays one-time password on dedicated application for smartphones - Used for money transfer via Internet banking or mobile banking	- View balance information, view transaction history, and product exchange (fixed deposit, foreign currency deposit, investment trust, etc.) can be used - Money transfer is not available
Effect	- Prevention of spoofing by stealing password	- Disables illegal money transfer by excluding transfer function from the services	- Prevention of spoofing by stealing password	- Disables illegal money transfer by excluding transfer function from the services
Period	October 21, 2013	October 21, 2013	January 6, 2014	April 2014 (planned)
Features	- Hardware token offers a high level of security because it is physically independent, does not communicate, and has no room for intervention by criminals - Easier to carry than conventional key holder type	- Meets demands from customers concerned about security against illegal withdrawal, etc.	- More convenient than hardware token because password can be used with smartphones or cell phones that travel about with customers. Lower cost than hardware token	- Measure aimed at simplifying operations to enter settings for first use, and at promoting use of Internet banking. This service, having no money transfer function, also meets demands from customers concerned about security, as an ancillary effect
Remarks	- Distributed to all new customers and existing customers on request - Existing hardware token one-time password became free of charge as of January 2013	- Based on same system as the existing full-service Internet banking with money transfer function removed	- Existing hardware token one-time password became free of charge as of October 2013	- Based on same system and existing full-service Internet banking with money transfer function removed

Source: Created by FISC based on interviews with officials at The Bank of Tokyo-Mitsubishi UFJ, Mizuho Bank, Sumitomo Mitsui Banking Corporation, and Resona Bank

7. Activities by major overseas financial institutions, etc.

	U.S.	Europe	South Korea
Countermeasures against targeted attacks	- Checking suspicious behavior by monitoring and analyzing logs - Sharing information of global intelligence team on cyber attacks around the world and studying techniques used in cyber attacks - Reinforcement of incident response preparedness against situations where damage actually occurs or hidden unauthorized programs are found (preparation for procedure and training for incident response) - Providing seminars and training to counter phishing and targeted attack e-mails to employees - Shortening application periods of patches and software designed to counter unauthorized programs - Reinforcement of countermeasures against cyber attacks at outsourcing companies	- Checking suspicious behavior by monitoring and analyzing logs - Sharing information of global intelligence team on attacks around the world and studying techniques used in attacks - Reinforcement of incident response preparedness against situations where damage actually occurs or hidden unauthorized programs are is found (preparation for procedure and training for incident response)	- Checking suspicious behavior by monitoring and analyzing logs - Sharing information of intelligence team on attacks around the world and studying techniques used in attacks - Reinforcement of incident response preparedness against situations where damage actually occurs or hidden unauthorized programs are found (preparation for procedure and training for incident response) - Reinforcement of verification when patches are applied - Separation of networks for external connection systems from in-house systems - Reinforcement of in-house regulations on accessing websites (expansion of blacklist <list of websites that must not be accessed>, introduction of whitelist system <system to restrict in advance websites that may be accessed>) - Reinforcement of verification of countermeasures against cyber attacks at outsourcing companies
Countermeasures against DDoS attacks	- Monitoring by global intelligence team for signs of DDoS attacks - Overseeing and selecting network transactions and bypassing attack transactions to networks of external outsourcing vendors - Upgrading infrastructure through capacity management	- Monitoring by global intelligence team for signs of DDoS attacks - Overseeing and selecting network transactions and bypassing attack transactions to networks of external outsourcing vendors	- Monitoring signs of DDoS attacks - Blocking transactions in the event of DDoS attacks - Cooperating with financial ISAC to counter attacks that the institution alone cannot cope with
Countermeasures against illegal use of Internet banking	- Overseeing transaction statuses of customers (checking suspicious actions and access attempts from different locations) - Confirmation with customers by phone if any irregular activity is observed - Checking system environments of customers' terminals (patching status of OS, version of browser, etc.) (some institutions only) - Suspending websites suspected of phishing (requesting ISP to close an such website as soon as it has been identified) - Authorizing different routes for some transactions (some institutions only)	- Overseeing transaction statuses of customers (checking suspicious actions and access attempts from different locations) - Suspension of transfer and confirmation with customer by phone if any irregular activity is observed - Supplying and recommending use of security tools such as software designed to counter unauthorized programs to customers (voluntary use) - Closing websites suspected of phishing (requesting ISP to close any such website as soon as it has been identified)	- Overseeing transaction statuses of customers (checking suspicious actions and access attempts from different locations) - Suspension of transfer and confirmation with customer by phone if any irregular activity is observed - Delaying transmission of money transfer guidance data for about 30 minutes instead of sending it immediately after accepting transfer processing (halting transfer if a customer reports damage during this period) - Restricting terminals or authorizing different routes for large-lot transactions - Checking system environments of customers' terminals (whether firewall software or software to counter unauthorized programs is installed) - Introduction of mechanism that blocks transactions if a customer's terminal does not meet prescribed conditions, unless check box (transaction on own responsibility) on the website page is checked - Alerts customers by displaying pop-up screen

	U.S.	Europe	South Korea
Sharing and exchanging information with other financial institutions	- Information sharing by FS-ISAC (via industry group <FS-ISAC member> with non-member medium-sized and small financial institutions). Information to be shared includes not only incidents related to cyber attacks but also those related to natural disasters. - The concept of sharing incident information widely throughout the industry rather than among individual institutions is gaining common acceptance as an effective way to improve security levels industry-wide	- Information sharing among European financial institutions via FI-ISAC (Financial Institutions Information Sharing and Analysis Center) (led by the Netherlands) - Unofficial information exchanges with CSIRTs of each financial institution and human connection in financial industry	- Sharing extensive information on security of financial institutions with financial ISAC - Latest information collected and maintained by KISA (Korea Internet & Security Agency) on vulnerability and malicious websites is used by each financial institution
Participation in joint training	- Participation in Quantum Dawn 2, held by SIFMA (Securities Industry and Financial Markets Association) - Participation in various joint training sessions and exercises conducted by each industry group, in addition to above	- Participation in Waking Shark II, held in the UK in November 2013 (European banks other than those located in the United Kingdom also participated.) - Participation in BCP joint training programs (Note 1) on an annual basis to verify responsiveness to large-scale disasters	- Participation in training assuming a DDoS attack or infection by malicious codes, for members of financial ISAC

(Note 1) This joint training does not necessarily specialize in cyber attacks.

Source: Created by FISC based on published materials

8. Record of Councils held

(1) Members of Council of Experts on Countermeasures against Cyber attacks on Financial Institutions

(without honorifics)

Chairman	Kiyoshi Yasutomi	Professor, Law School, Keio University J.D., LL.M., S.J.D, Attorney
Members	Ryoichi Sasaki	Professor, School of Science and Technology for Future Life, Tokyo Denki University Advisor on Information Security, Cabinet Secretariat, Government of Japan Doctor of Engineering
	Tetsutaro Uehara	Professor, College of Information Science & Engineering, Ritsumeikan University
	Itsuro Nishimoto	CISSP, CTO (Cybersecurity), Lac Co., Ltd.
	Daisuke Inoue	Director, Cybersecurity Laboratory, Network Security Research Institute, National Institute of Information and Communication Technology
	Junko Hayakashi	Executive Director, Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
	Haruki Nakamura (up to 2nd Council)	Managing Executive Officer, Mizuho Financial Group, Inc.
	Kouji Yonei (from 3rd Council)	Executive Officer and General Manager of IT & Systems Planning Division, Mizuho Financial Group, Inc.
	Hiroki Yonezawa	Director, System Division, The Bank of Kyoto, Ltd.
	Yuji Ishida	General Manager, Business Promotion Department, National Association of Shinkin Banks
	Keiji Sakagami	Managing Director, IT Governance & Corporate Security Dept.,, Nomura Holdings, Inc.
	Tetsuya Koide	Head of IT Business Process Risk Management Center, IT Business Process Planning Department, Dai-ichi Life Insurance Company, Limited Chairman, Information System Department, Life Insurance Association of Japan
	Toshiya Yanase	General Manager, Information Technology Planning Department, Mitsui Sumitomo Insurance Co., Ltd.
	Hiroki Kawai	Director, IT Development Department, Tokyo Stock Exchange, Inc.
Observers	Tomoo Yamauchi	Counselor, National Information Security Center, Cabinet Secretariat, Government of Japan
	Kosuke Uchida	Deputy Director, Policy and Legal Division Planning and Coordination Bureau, Financial Services Agency
	Tomonori Iwasa	Director, Head of Security Control Center, System Planning and Coordination Division, Information System Services Department, Bank of Japan

(2) Outline of activities

First Council

June 24, 2013

① Explanation on rules of Council of Experts on Response to Cyber Attack

② How to proceed with future councils

③ Outline of result of joint study by Financial Services Agency and FISC in 2012

④ Council of experts on response to cyber attack, memo on agenda (draft)

⑤ Joint study by Financial Services Agency and FISC in 2013 Questionnaire on cyber attack response preparedness

Second Council

August 1, 2013

① "Threats to financial information systems and activities of NICT"
Lecturer: Member Inoue

② "Response to cyber attacks on local financial institutions"
Lecturer: Member Yonezawa

③ Overseas rules concerning cyber attacks

④ Correction of agenda memo

⑤ Discussion on agenda memo

Third Council

September 26, 2013

① "Example of our activities – Cyber attack response training"
Lecturer: Mr. Hidetsugu Kuroda, deputy general manager, Cybersecurity Team, IT & Systems Planning Division, Mizuho Financial Group

② "Trends of cyber attacks today and in the past and introduction of overseas examples"
Lecturer: Mr. Mitsuyoshi Sugaya, executive director and manager, Consulting Business Department, NRI Secure Technologies, Ltd.

③ "Improvement of multiple-risk communicator MRC and its application to countermeasures against targeted mail attacks"
Lecturer: Member Sasaki

④ Report on survey in South Korea "Cyber attack response preparedness at financial institutions, etc., in South Korea – based on interview in August 2013"

⑤ Explanation on corrections to agenda memo

⑥ Discussion on agenda memo

Fourth Council

October 26, 2013

① “Countermeasures against cyber attacks – Past experience and future plan”
Lecturer: Member Sakagami

② “Protection of critical infrastructure and cyber-security”
Lecturer: Observer Yamauchi, National Information Security Center

③ Explanation on corrections to agenda memo and discussion

Fifth Council

November 14, 2013

① “Our countermeasures against cyber attacks and problems”
Lecturer: Mr. Kunihide Takahashi, Manager, IT Management Team, Information Technology Planning Department, Mitsui Sumitomo Insurance Co., Ltd.

② “Global Information Security”
Lecturer: Mr. Dan Antilley, Bank of America

③ Outline of result of questionnaire on cyber attacks

④ Study of draft of gist of report

Sixth Council

January 21, 2014

① Report on survey in the U.S. and Europe “Cyber attack response preparedness in Europe and U.S.”

② Study of draft of report

Seventh Council

February 21, 2014

① Study of draft of report

② Future work related to cyber attack response

(3) Secretariat, Center for Financial Industry Information Systems

Standing director Tatsuro Watanabe

Standing director Tadashi Nunami

Research Department	Director General	Takashi Arai
Security & Audit Department	Director General	Toshinobu Nishimura
General Admin. & Planning Department	Director General	Haruhiko Nakada

◆ Secretariat staff

Tsuyoshi Hattori, Shusuke Araki, Katsumi Kito, Masaaki Shiga, Nobuyuki Ooyama, Hiroyuki Kakei (up to 3rd Council), Izumi Ikeda (from 4th Council), Hideaki Nara, Koichi Watanabe, Yasuhiro Hamamoto, Kazuto Soma, Haruhisa Unno (from 3rd Council), Takeo Ishii, Takahiro Watanabe