Improvement of Financial Service Safety by Promoting Cyber Security Measures

MIYAKAWA Koichi, SATO Takamichi, AGA Kouichi, SUGIYAMA Yohei

Abstract

The recent advancement of IT and Internet and the expansion of the scope of service applications has tended to support an increase of cybercrimes that aim at obtaining money or obstructing businesses and services. This trend has resulted in suitable countermeasures becoming an important issue for society.
In particular, attacks on critical infrastructures are increasing on a worldwide scale. Among them, the increase in attacks that are targeting financial institutions with the aim of obtaining money are most noticeable.
This paper describes the latest trend in cyber security threats and reviews the potential proposals and issues of financial institutions based on the guidelines given by the Japanese Financial Services Agency. NEC's approach to issues of cyber security for financial institutions is also introduced.

Keywords

cyber security, IoT, DDoS, malware, ransomware, illegal money transfer, AI, financing

1. Introduction

Cyberattacks and associated crimes are recently increasing at a worldwide scale and their damage is also expanding. They have a potential of exerting critical damage to national life, particularly in the operators of critical infrastructure of thirteen fields. They include information communications, financing, aviation, railroad, electricity, gas, governmental/administrative services, medical care, water supply, logistics, chemistry, credit and oil. The Japanese Cabinet adopted the "Cyber Security Strategy" as a national strategy on Sept. 4, 2015 in order to systematically promote cyber security measures on a project basis.

While Japan is attracting attention because of the major international events to be held there in the future, it is also becoming an important target of interest to malicious people and the risk of cyberattacks is increasing in severity.

2. Latest Threat Trends

On December 2016, the Japan Network Security Association (JNSA) announced the Top Ten Security News items (**Table 1**).

Among these, the threats that invite special note from the viewpoint of cyber security of financial institutions are: "DDoS attacks at the largest-ever scale by IoT devices has become apparent" ranked first, "Attention-seeking announcement from Information-technology Promotion Agency (IPA) against attacks aiming at ransomware infection" ranked second, and "Cyberattacks to the information infrastructures of Japan Defence Agency and Self Defence Forces (attacks of national critical infrastructures), which is ranked sixth and is the attack intended to threat key governmental ministries and agencies. All of these need to be assessed continuously as currently being the most important trend threats.

Although not included in this ranking, illegal money transfers through Internet banking also became a significant news item in 2016, as a threat to financial institutions. In the following sections, the authors describe the main threats related to financial institutions.

Table 1 JNSA 2015 Top Ten Security News Items.

Ranking	2016 Top Ten Security News Items
[1st]	Oct. 14: DDoS attacks of the largest-ever scale by IoT devices has become apparent - Security of IoT devices such as surveillance cameras is an urgent key issue.-
[2nd]	Apr. 13: Attention-seeking announcement from IPA against attacks aiming at ransomware infection - Ransomware threats make your data completely unavailable. -
[3rd]	July 20: Attention-seeking announcement from Government for "Pokémon GO" users - GO! for improvement of national security awareness. -
[4th]	Mar. 12: AI completely beating the world-top pro *go* player. - Do AI dream of becoming Big Brothers? -
[5th]	Oct. 24: IPA started acceptance of applications for new national qualification "Registered Information Security Specialist". - Can this be the trump card for the shortage of security specialists? -
[6th]	Nov. 28: Cyberattacks to the information infrastructures of JDA and JSDF - Invading the main castle via a publicly open defence university PC? –
[7th]	Nov. 8: Mr. Donald Trump winning the U.S. Presidential Election - Is the Trump Phenomenon a headwind for Japanese security situations? –
[8th]	June 27: Illegal access damage made public by Saga Prefectural Board of Education - Committed by a 17-year-old boy, a gap between the dark side of society and the virtual game world –
[9th]	June 14: Suspicion of a massive personal information leak from a JTB Group website - Sophisticated targeted attack mails put routine preparation in question. -
[10th]	Apr. 14: Official adoption of EU General Data Protection Regulation (EU privacy regulation) - New rules to meet changes in personal data and the spread of threats –

(Source: Japan Network Security Association (JNSA))

2.1 DDoS Attack by IoT Devices

Although the DDoS attack is an old attack technique the latest attacks are often using IoT devices as the attack source.

In late September 2016, the U.S. information security site "Krebs on Security" was put down by the heaviest DDoS attack to date. The malware used in this attack (botnet*), named "Mirai," was used to attack the site by forming a botnet on the IoT devices turned IP-based, such as web cameras, routers and digital video recorders (**Fig. 1**). According to the blog of Mr. Krebs, the site owner, the Akamai protecting the site observed at the peak nearly twice the maximum scale of traffic it had experienced in the past (max. 620 Gbps). This attack was accompanied with a subsequent topic when the Mirai source code was published in a hacker forum. The source code was reprinted in the GitHub (shared web service for software developers) so that all may see the details.

As this event suggests that any engineer with a certain knowledge of IT can easily perform a similar attack, it should be considered as a major threat.

The basic environment enabling such an attack is the situation in which the initial ID passwords of IoT devices are not changed and those in which vulnerable ID/password combinations are used with a hard-coded built-in account (**Table 2**).

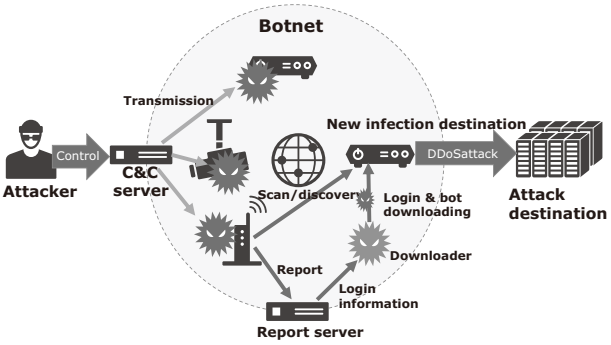

Fig. 1 Image of Mirai botnet.

Table 2 Examples of frequently used careless IoT device passwords.

Username	Password	Username	Password
666666	666666	administrator	1234
admin	(None)	Administrator	admin
admin	1111	guest	12345
admin	1234	guest	guest
admin	12345	mother	fucker
admin	54321	root	(None)
admin	7ujMko0admin	root	0
admin	admin	root	1111
admin	admin1234	root	1234
admin	pass	root	54321
admin	password	root	7ujMko0admin

What is necessary for the financial institutions, is for example to re-inspect if the surveillance camera watching the ATM machines use an ID/password combination as described above.

If a financial institution is exposed to a large-scale DDoS attack, then faults causing direct damage to the users, such as the shutdown of the Internet banking service, are predictable.

2.2 Ransomware

Ransomware(**Fig. 2**) is a kind of malware that locks the infected PC or prevents specific files from being opened. As indicated by the name of "ransom," the attacker requests a ransom payment to solve the infection. The ransom is often requested in a virtual currency, which is hard to be traced and easy to be cashed.

The ransomware is not executed directly by the developer, but is distributed using a mailing list after passing through many affiliates.

*1 Botnet: Group of computers remote controlled by instructions sent through the Internet.

When the ransomware is executed and the developer receives money, part of it is kicked back to the affiliates.

The use of ransomware is increasing rapidly because it can easily be turned into cash and it is therefore very convenient for the attackers.

If you are infected by ransomware, it is recommended never to obey to the money request and to quickly study means of restoration using backup. This will necessitate a review of the overall backup plan, so that it covers not only PCs but server devices and smartphone devices as well.

2.3 Illegal Money Transfer Using Malware

The Year 2016 saw an outbreak of malware "Gozi" (known as also "Ursnlf", "Snifula" or "Papras") targeted at Internet banking causing illegal money transfer damage to many financial institutions.

What is special with this malware is that it is infected by a fishing mail sent in the disguise of a bill. When the user accesses the Internet banking, the ID/password information is taken and used for an illegal money transfer (**Fig. 3**). In addition, there is also a risk that other kinds of personal information may be taken from the infected terminal. There is also similar malware that can itself execute illegal money transfers. Attacks using various other techniques are also anticipated in the future.

Fig. 2 Example of screen display of Crypt Locker ransomware.

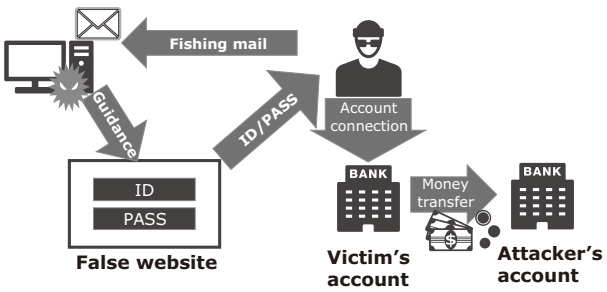

Fig. 3 Illegal money transfer fraud method.

The countermeasures for avoiding damage from banking malware are mainly taken by the user side. These include carefulness of users and the use of multi-factor authentication, but technology for defence using AI is recently under R&D.

3. Proposal to Financial Institutions

In its FY2016 Financial Administration Guidelines the Japanese Financial Services Agency has requested the enhancement of cyber security as well as measures for promoting the FinTech. On June 15, 2016 at the Critical Infrastructure Expert Panel (7th meeting) of the National Centre of Incident readiness and Strategy for Cybersecurity (NISC), the FSA presented a report entitled "Cybersecurity Measures adopted by Financial Institutions" (**Fig. 4**).

Upon receiving these guidelines, NEC identified the following issues that require solution.

(1) It is necessary to deepen the understanding of managers of financial institutions about cyber security.

(2) Cyber security is not a transient subject but one that requires continual enhancement. Collaboration across the boundaries between industries are required in anticipation of the big international events to be held in Japan.

(3) The cyber security measures are advanced among major financial institutions but not among the smaller institutions.
For the small and medium financial institutions that have difficulties in affording the management of cyber security budgets, it is required to provide low-price services or human resource cultivation services.

(4) The current support systems of cyber security vendors are concentrated with Tokyo vendors and these are unable to cover the whole country.

Cyber security measures are often considered only after something happens. We might pre-empt adverse events by analysing the expected risks properly from the service planning or design stage and to thereby decide the development budget by foreseeing such measures. Since the risks are not constant, they should be reviewed as required in order to be ready for encountering new types of threats. Cyber security is an issue that belongs to the domain in which managers of financial institutions should be involved positively and it is important to deepen understanding of the associated risks.

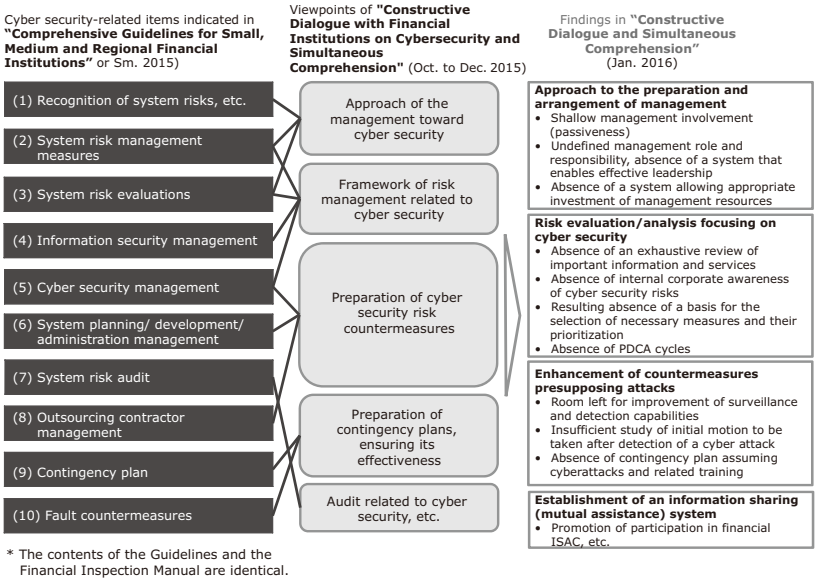

Fig. 4 Cyber security management indicated by FSA guidelines.

4. NEC's Approach to Financial Institutions

Based on the issues recognized in the above, we will deploy the following procedures in our approach to financial institutions.

(1) Encouragement of management, support for human resource cultivation

NEC holds various seminars and promotion activities based on individual visits to encourage management to adopt security measures. We also deploy human resource cultivation activities based on our human resource cultivation programs.

(2) Support for cyber security risk management, provision of technical measures

We offer support for risk management by analysing risks related to cyber security, etc., and we evaluate specific measures based on the analysis results. As a technical countermeasure, we are promoting measures applying the AI technology in "NEC the WISE."

(3) Information exchange with related organizations and information provision service

We exchange information with related organizations including the Japan Cybercrime Control Center (JC3) and the Center for Financial Industry Information Systems (FISC) to obtain the latest threads and incident information quickly, and also to provide associated information.

(4) Support for comprehensive cyber security operations (SOC services)

NEC also deploys independent services via the Security Operation Center (SOC). For the small and medium financial institutions we offer shared SOC services that make use of regional bases. We also support major financial institutions by advancing detection capabilities via use of AI in the SOC operations.

5. Conclusion

In July 2016, NEC's Financial Systems Development Division and Financial Solutions Division developed a cyber security measure promotion system for the financial domain. This system makes it possible to provide financial institutions with safe security solutions as well as enabling them to benefit from the creation of new values.

Authors' Profiles

MIYAKAWA Koichi
Senior Expert
Financial Systems Development Division

SATO Takamichi
Senior Expert
Financial Systems Development Division

AGA Kouichi
Manager
Financial Systems Development Division

SUGIYAMA Yohei
Assistant Manager
Financial Systems Development Division

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.11 No.2 FinTech That Accelerates Digital Transformation

Papers for Special Issue

NEC Information

Vol.11 No.2
June 2017

Special Issue TOP