Developing Key Cyber Security Personnel
- Present and Future -

NEC Cyber Security Journal, Vol.5 2017, Special Edition

NEC Cyber Security Solutions

Futureproof Security

For over a century NEC has been contributing to the development of society
by connecting people with people, people with things, and things with things.

However, the environment in which people and things are connected is now facing serious risks.
To reduce these risks and provide safe and secure cyberspaces,
we need to take a comprehensive approach that includes information,
technology, and personnel.

The latest information gained through international collaborations;
the best security technology in the world;
highly trained personnel with reliable and tenacious problem-solving skills;
and experience and know-how acquired from all parts of the world...

NEC is using these strengths to achieve the total security of clients'
cyberspace and create a brighter and safer future for all society.

Developing Key Cyber Security Personnel - Present and Future -

NEC Cyber Security Journal

Vol. 5 2017,
Special Edition

Contents

Looking back at 2016: Key cyber security challenges are "changing the cybersecurity awareness of top management" and "developing skilled personnel."

In December 2015 the Ministry of Economy, Trade and Industry (METI) and the Information-technology Promotion Agency (IPA) issued the "Cyber Security Management Guidelines." Thus 2016 can be seen as the year that the national government, local governments, companies, and organizations started to seriously address cyber security both individually and collectively. The concept that cyber security measures are not a cost to companies, but are rather an important management task that will raise corporate value is becoming more widely recognized, but this concept has yet to sink in with top management. This is in spite of the fact that we are constantly bombarded with news about information leaks, DDoS attacks, ransomware, and other cyber crimes. Cyber security will also be indispensable to the expansion of the IoT—a key player in the industry of tomorrow.

However, in our quest to accelerate efforts to maintain and manage safe and secure cyberspaces, we are encountering some challenges. For example, in its final report entitled "Securing Human Resources (Development and Employment), the Cross-Industry Function for Cyber Security Human Resources Development" indicated that the development of skilled personnel is an urgent task. Various questionnaires and studies also show that the lack of personnel involved in security is a serious concern within companies.

In this edition of the NEC Cyber Security Journal, we will introduce an assessment of the cyber security risks faced by companies as identified in the management guidelines and look at the challenges involved in eliminating these risks. We will also interview NEC employees who are working at the front lines of security personnel development about NEC's efforts in this area. We hope that this information will be helpful when considering the security measures to be implemented and the development of key security personnel in your company.

* See the NEC Cyber Security Journal website (http://jpn.nec.com/cybersecurity/journal/) for details about this study group.

Corporate challenges identified by the Cyber Security Management Guidelines

Overview of the Guidelines

In December 2015 the Ministry of Economy, Trade and Industry (METI) and the Information-technology Promotion Agency (IPA) issued the "Cyber Security Management Guidelines." These guidelines position cyber security as an important management task, and identify three cyber security principles that top management must adopt and 10 important items that must be executed with a top-down approach. The guidelines target people in top management.
The 10 important items can be divided into four categories: demonstration of leadership by top management and constructing systems for cyber security; determining a framework for cyber security risk management; measures to prevent attacks based on risk management; and preparations for cyber attacks. It goes without saying that while the management guidelines call for measures to prevent cyber attacks on the companies themselves, they also advise top management to implement business-wide measures that include the supply chain (business partners), and devise measures to respond to security incidents such as malware infestations and internal information leaks.

Overview of simple risk assessment

NEC has released a simple diagnostic tool on its website called "Simple Risk Assessment Based on Cyber Security Management Guidelines"*1 (hereafter referred to as the Simple Diagnosis) that can be used to determine the status of the security measures implemented by customers.

Demonstration of leadership by top management and constructing systems for cyber security	
Q1	Does your company have an information security policy (*1), and has it been published within the organization under the auspices of top management?
Q2	Has the information security policy been made public under the name of the president so as to advertise your security policy?
Q3	Does the information security policy include measures against cyber attack threats?
Q4	Is there someone in top management, such as a CISO (*2), who is primarily responsible for security activities?
Q5	Has a security risk management framework (*3) been constructed to respond to cyber attacks?

(*1)…A policy that clarifies the principles and direction of information security within the company or organization as conceived by top management.
(*2)…Chief Information Security Officer. The executive director who is in charge of information security within a company.
(*3)…A framework through which the current information security situation and risks can be grasped, and through which the necessary measures can be implemented.

Excerpt of questions

The Simple Diagnosis consists of twenty yes or no questions in four categories that are based on the 10 important items in the Cyber Security Management Guidelines. The answers are checked against the Guidelines to determine the security measure status of the company. There are six possible results: "The four categories are generally covered"; four types of "Notes concerning the most problematic category"; and "Problems in all four categories." Customers can receive advice on security measures according to their results.

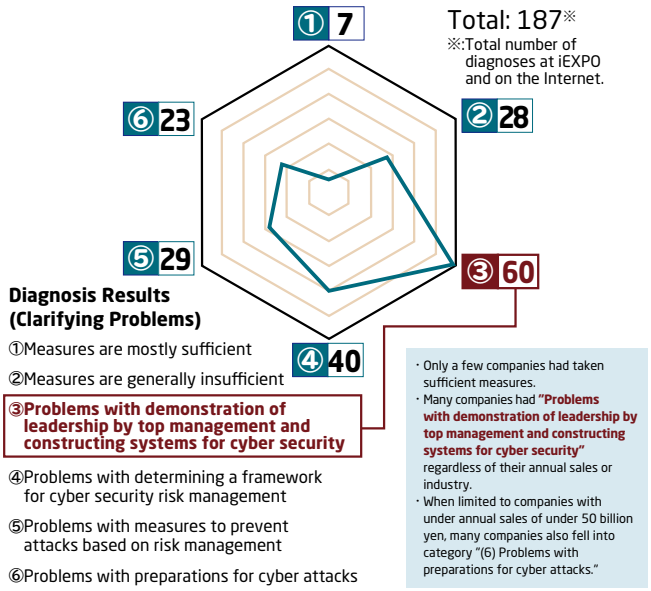
People who have taken the Simple Diagnosis can download an overview of the Management Guidelines and a manual of case studies on the measures that NEC has implemented based on these Guidelines.

◆Excerpt from diagnosis results and advice
"Your procedures for implementing measures to respond to a cyber attack and your practical training for such a case may be insufficient."
"Under your current conditions, if a cyber attack were to occur you would not be able to promptly determine the cause or scope of the damage, so that the damage may spread. Once the damage spreads, it will take longer than necessary to recover, which will increase the severity of the damage."

Summary of diagnosis results

In the approximately three months since the Simple Diagnosis was released publicly in September 2016, we have tallied about 200*2 results. Looking at the six different result categories, about one third of the respondents had problems with "Demonstration of leadership by top management and constructing systems for cyber security."
The top ranking problems were that measures were not thorough at

*1 https://www2.nec.co.jp/cgi-bin/e-diagnosis/cybersecurity01/edia_top.cgi
*2 Total of respondents who did the Simple Diagnosis on the Web or who did the Simple Diagnosis at our booth at the C&C User Forum & iEXPO 2016.



Diagnosis results

group companies, business partners along the supply chain, and IT system management vendors, and that the systems and personnel were not available for when security incidents occurred.

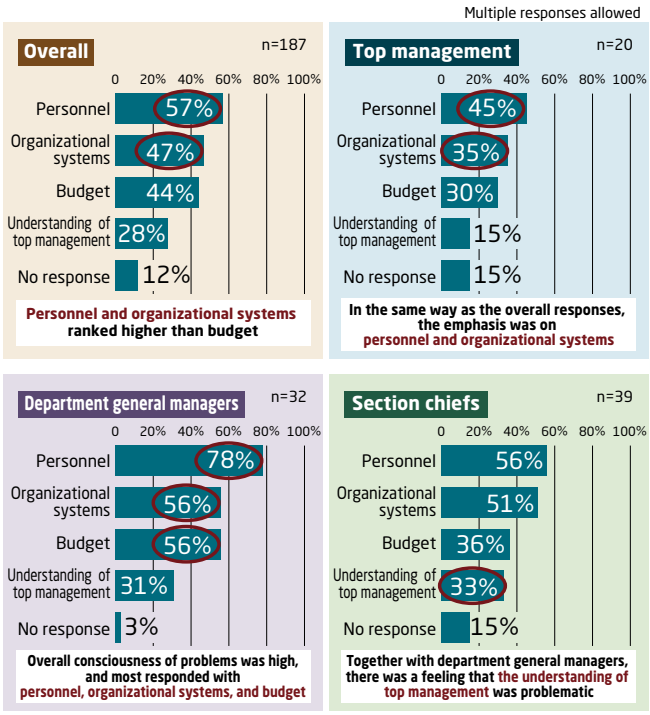
The question with the lowest positive response rate (over 70 percent of respondents replied "no") was, "Do you have an agreement for security measure contents and do you share your measure implementation status with group companies and business partners along your supply chain?" This told us that there are many problems, including that companies have not been entering into agreements with an awareness of security and they do not understand their security measure implementation status; that they do not understand how to make their subcontractors aware of the necessity for security measures; and that they do not know how far to go with mandatory measures and sharing of information.

The results of the Simple Diagnosis and a short questionnaire that was conducted concurrently showed that about 80 percent of companies answered "already implemented," "currently implementing," "considering implementation," and "collecting information," indicating that they were very interested in the Guidelines and would proactively implement them. Since the contents of the Guidelines will be revised in the future and the IPA will issue explanations, it is likely that companies that said they are "collecting information" will also implement the Guidelines.

In response to the item "Problems with your company's cyber security measures" in the short questionnaire (multiple responses allowed), more companies responded that they had problems with "developing security personnel" for normal and emergency situations (57%) and their "organizational system" for when incidents occur (47%) rather than with their "budget" for security investments (44%). This was similar to the response in the Simple Diagnosis and proves that development of security personnel and organizational systems are still lacking.

Status of Cyber Security Management Guidelines implementation

Even when these questions are posed to top management, the results are the same, with problems being identified in the areas of "personnel" and "organizational systems." Moreover, department general managers also find problems with "budgets," and both department general managers and section chiefs see problems with the "understanding of top management."



Problems with your company's cyber security measures (multiple responses allowed)

In conclusion

How should companies cope with the problems of developing personnel and constructing systems that have been identified from the Simple Diagnosis and short questionnaire? In the following pages, we will introduce the concepts and approaches taken by NEC for developing security personnel. Please be sure to study them, because they might hold clues as to how your company can develop its own security personnel.

The Simple Diagnosis tool that was introduced here is available on our website. Please use it if you have yet to gain an understanding of your company's security measure situation.

NEC provides detailed risk assessment services based on our Management Guidelines. In these services, security professionals assess risks from many different angles, discover problems in our customers' organizations, and provide security solutions. We believe that NEC's strength lies in our ability to use our knowledge and know-how of many different businesses and systems, and propose the best possible security measures for our customers. If you are unsure about where to start or what specific actions to take, please contact us.

Roundtable discussion

Developing Cyber Security Personnel

~What is the key to success?~

Advanced Persistent Threat (APT) attacks that target specific companies or organizations are increasing in number around the world. In the era of IoT when all things will be connected to the Internet, damage from cyber attacks will not be limited to single companies; it will affect all of society. For many years NEC has been maintaining and improving its multilayered and dynamic cyber security measures in order to protect the important information assets and systems of its customers. In this roundtable discussion, the key people working on the front lines talk about their efforts to reinforce our systems, and how to develop advanced cyber security personnel.

Part 1

Cyber security personnel are not developed in a day. The front lines of security personnel development as told by pioneers in the field.

Since cyber attacks are becoming more sophisticated by the day, NEC has been reinforcing its development of security personnel in order to improve security measures for products, systems, and services, and also to contribute to the safety and security of its customers in many different fields. We asked Tetsuji Tanigawa and Takeo Tagami—both of whom have been working in the systematic development of security personnel since the dawn of security measures when there were no role models available—about the importance of developing security personnel and the keys to doing so.

People create both the threats and the measures

Damage from cyber attacks is increasing around the world. It is necessary to reinforce cyber security measures from many different points of view, and urgently develop personnel dedicated to cyber security. Executive Security Specialist Tetsuji Tanigawa of the NEC Management Information Systems Division and Cyber Security Strategy Division gave us some background to this topic.

Tetsuji Tanigawa
Executive Security Specialist
NEC Management Information Systems Division and Cyber Security Strategy Division

"APT attacks, unauthorized accesses, and denial of service attacks that are increasing recently cannot be prevented with conventional methods such as firewalls and security patches," he says. "This is because the attack methods change dynamically."

To respond to these ever changing attack methods, the IT departments and Computer Security Incident Response Teams (CSIRTs) at companies collect intelligence (information), analyze attack methods, and find solutions that can lead to effective protective measures.

"Security personnel are required to have special skills that differ from general IT engineers, such as information collection and diagnosis, monitoring, incident response, forensics, and analysis skills" says Tanigawa. "They must also have the same level of knowledge and abilities as the attackers in order to respond to the attacks. This is why personnel that specialize in cyber security are necessary."

There is always an attacker in a cyber attack. To cope with attackers who do not show their hand and who always try to do the unexpected, "protectors" who can use technology and information to respond in different ways are necessary. Because both the threats and the responses to the threats come from people, another key point in addition to technology and information is the quality of the people.

The importance of personnel development is pointed out in the "Cyber Security Management Guidelines"

The importance of developing security personnel is also emphasized in the "Cyber Security Management Guidelines" jointly issued by the

Ministry of Economy, Trade and Industry and the Information-technology Promotion Agency (IPA) in December 2015.
Specifically, the Guidelines position cyber security as an important management task, and identify three cyber security principles that top management must adopt: (1) demonstrate leadership in security measures, (2) implement business-wide measures that include the supply chain, and (3) implement appropriate communications, such as information disclosure and sharing.
"With the increasing number of cyber attacks every year, it is becoming more difficult to acquire cyber security personnel with advanced skills," says Takeo Tagami, Senior Manager in the NEC Management Information Systems Division and Cyber Security Strategy Division. "This is why the government is emphasizing that top management must clearly understand the need for such people, create a career path that allows security personnel to demonstrate their abilities, and develop mechanisms and systems to provide continuous training and education."

"Bridging personnel" who can connect top management with front line personnel

However, not just anybody can become cyber security personnel. In many cases cyber attacks come from overseas, and the perpetrators are located in places where the Japanese police does not have authority. They also carry out complex attacks that are impossible to predict.
"To handle these complex and advanced attacks, the responders must acquire a big picture of the entire attack, have the knowledge and sensitivity to make detailed technological adjustments, and the strong will and enthusiasm to devise measures without breaking down under pressure," says Tanigawa. "I believe that these are the necessary requirements for cyber security personnel."
Furthermore, there is more than one type of cyber security personnel. NEC defines a "security engineer" as a person with specialized cyber security knowledge and the skills to cope with attacks. This category includes "analysts" who can stop various types of cyber attacks with a wide range of knowledge and analytic skills, and "top guns" who have extremely advanced skills.
In addition, there are "bridging personnel" who in their role as security engineer leaders must have both management and consulting abilities, and act as a bridge between top management and actual front line personnel. This level of personnel is also deemed necessary in Japan's national policy and Management Guidelines.
"To utilize cyber security concepts in all corporate operations, top management and front line personnel must both share the problems they are facing with regards to cyber security, and the direction that solutions need to take," explains Tagami. "Bridging personnel explain the risks within the company to top management and the Chief Information Security Officer (CISO) in language that they can understand, make proposals for security investments based on front line problems, and reflect the will of top management in the front lines."
Developing this level of personnel requires considerable time and the right environment, because these people are specialists who require comprehensive abilities that include advanced knowledge about IT and security, and management skills.

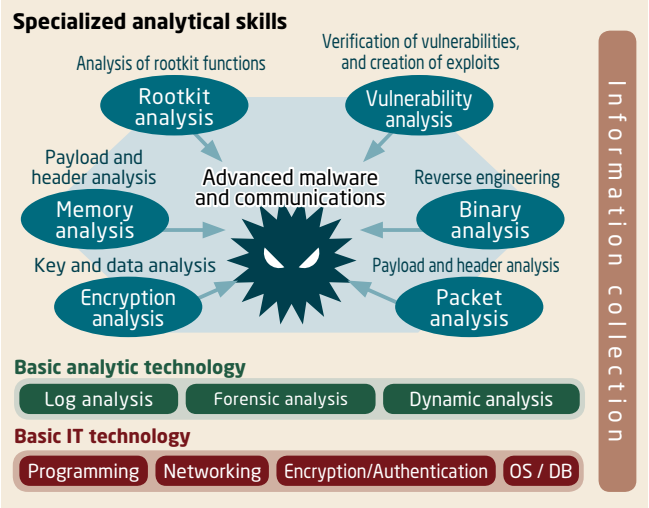
Early development of hybrid personnel

Takeo Tagami
Senior Manager
NEC Management Information Systems Division and Cyber Security Strategy Division

Since NEC has made the security business one of its management pillars, how does it develop its security personnel?
"We have been developing security technologies for some time, but a major turning point was in July 2002 when we introduced the CSIRT, which would act as the command post for cyber security measures," explains Tanigawa. "That is when we started collecting and storing information about potential internal vulnerabilities, honing our technological capabilities and acquiring experience, and connecting with external organizations."
At the same time, NEC was steadily strengthening its CSIRT personnel and organization. From 2011 the number of targeted attacks grew rapidly, and even if the attacks were detected, there were not sufficient personnel available to cope with all of them. It was then that, as part of its CSIRT activities, NEC defined a skill map of the special skills necessary, proactively recruited personnel with advanced skills from Group companies, and accelerated efforts to develop security professionals.

Developing security professionals was a difficult task

However, developing security professionals was not that easy. Looking at the technological requirements of the skill map that NEC defined, advanced analytic skills and a wide range of knowledge was required. The basic IT skill requirements alone included knowledge from numerous layers, including programming, networking, OS/DB, and encryption and authentication.
"This wide range of knowledge is required because cyber attacks combine different types of technologies," says Tanigawa. "You will always made mistakes if you try to respond to an attack with only



Specialized skills required for CSIRT activities

fragments of knowledge, such as knowledge only about networks or OSs. In addition to this wide range of knowledge, security personnel also need knowledge of advanced programming languages so that they can implement actual analysis and measures."

That is not all. It is also necessary to improve judgment and communication capabilities. This is because after a server that has been infested with malware is analyzed, the system administrator must be told what kind of improvements and operations must be made in the short and long term.

"When a service must be temporarily stopped, a decision must be made when to stop it," explains Tagami. "The system administrator's situation must be considered when making such decisions."

In order to develop these comprehensive abilities, NEC has recruited many of its CSIRT members from its own divisions. After they are recruited, they often proceed to have a very diverse career. From the CSIRT, they move on to becoming security consultants for customers, or might even be put in charge of developing specialists at government organizations. Some of them come back to the CSIRT, and there are others who are involved in the security business in other parts of NEC. It is through this wide range of experience that security professionals are developed.

"It would be very difficult to develop this level of cyber security personnel at regular companies," says Tagami. "People like these tend to be concentrated in large ICT vendors and dedicated security vendors. Because NEC must defend its own information systems and also provide advanced cyber security services to its customers, it has always had access to personnel with the right aptitude and talent. That is another major factor in our success."

Providing practical education and creating a career path system

No matter how good the person or the training, not everyone can become an analyst or a top gun. The important thing is to create a system to develop enough cyber security personnel to provide the company with the depth it needs. To that end, NEC prepares training programs according to each individual's skills, so that each individual can develop his or her skills accordingly.

For example, security engineers share information on the latest incidents and malware on a daily basis through mailing lists and in-house communities. They can use that information to accumulate their own know-how and for their own research activities. The CSIRT holds study groups for analysts once every two weeks. About one hundred people participate in these groups and study malware analysis methods, forensic methods, and how to respond to incidents.

"To further their practical skills, we ask for volunteers to take part in Capture the Flag (CTF) security contests that are held on almost a weekly basis around the world," says Tanigawa. "Top gun class white hat hackers take part in these global competitions, so that is motivation for our employees to participate. These competitions create great study opportunities."

At the same time, NEC holds its own internal CTF events. In February 2016, the company held an online CTF competition for two weeks that any NEC Group employee could take part in. Participants were presented with a total of 97 problems concerning encryption, OSs, networks, web applications, and security incident analysis.

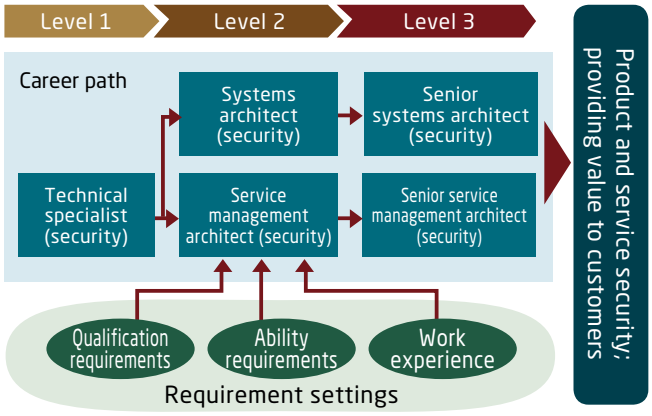
Example internal CTF problem

Scene from the awards ceremony

"We were really surprised when about 600 employees ended up participating," says Tanigawa. "I think this is proof that awareness of security has spread throughout our entire Group."

In addition to training programs like these, NEC has also prepared a diverse career path system. Many different positions are defined in detail, including security analysts who monitor security and analyze it; security architects who develop security products, integrate systems, and are in charge of service operations; security consultants who visualize customer problems from the point of view of security, and propose road maps and measures to solve the problems; and security planners who develop cyber security businesses and plan solutions. Personnel systems are in

place for the development of each type of career.
Furthermore, the skills that each individual has acquired are recognized through the NEC Professional Certification System, which designates personnel as "system architects," who assure the security quality of information systems, and "service management architects," who conduct security management and incident response.
"Cyber security personnel are expected to play many roles in NEC's diversified businesses," says Tagami. "We have therefore set things up so that they can form their own careers from many different options and increase their levels of experience".



- Systems architect (security): Assuring security quality for information systems
  - Analysis of threats and vulnerabilities; definition of security requirements; architecture design; etc.
- Service management architect (security): Assuring security quality for IT service operations
  - Security management, monitoring, handling incidents, etc.

Professional Certification System (Security)

Expanding to 1200 security personnel

The cyber security personnel that NEC develops do not only protect the information systems of the NEC Group. They are also involved in security design, installation, and proposals for products, systems, and services that are provided to enterprises, national and local governments, and individual customers. NEC therefore plans to double the number of security personnel by fiscal 2017.
Because it takes such a long time to develop security personnel, the company's needs cannot be met through internal development alone. NEC has therefore added the Cyber Defense Institute boasting Japan's best cyber security engineers and Infosec, a leader in corporate risk management, to the NEC Group to boost advanced security personnel numbers.
NEC is also operating a Cyber Security Factory that connects the NEC Group and external security partner companies to provide one-stop advanced cyber security measures. This organization is a collection of experts well versed in cyber security, and NEC is using it effectively as a place to develop security professionals.
"It goes without saying that a single company cannot handle cyber attacks that could damage entire supply chains and all of society," says Tanigawa. "Therefore, NEC's CSIRT shares daily incident information with JC3 (Japan Cybercrime Control Center), NCA (Nippon CSIRT Association) and other public organizations, companies, and universities."
"We also hope to spread the development of cyber security personnel and knowledge to NEC's overseas subsidiaries," adds Tagami. "We are already promoting the development of local personnel who can be in charge of cyber security."
Going forward, NEC will continue to strengthen its security professionals, and hopes to provide total solutions to its customers that include consulting, security measures, security operations, and incident response.

Enhancing information security skills through CTF

CTF (Capture the Flag) is a competition involving information security skills. In many cases, competitors use their security skills to analyze problems for hidden answers (flags), which they then send to the competition server. It is possible to take part in many overseas CTF competitions through the Internet. Famous competitions include SECCON in Japan and DEFCON abroad, and these competitions serve as ways to unearth new security personnel. NEC internally distributes cyber security information, including CTF problems. The purpose of distributing CTF problems is to expand the number of people involved in CTF, and to improve the information security skills of NEC employees. NEC also conducts monthly in-house CTF study groups that take the form of practical problem solving sessions for beginners and intermediate/advanced competitors, and allow employees to study information security skills and techniques in an enjoyable way. Also, by studying the way attackers think, participants are able to gain knowledge from a perspective that differs from their conventional system design and construction perspective. They can then use that knowledge to devise more realistic security measures.

Part 2

Reaching the pinnacle of security work: Professional attitude and approach as told by CSIRT members

NEC has cyber security personnel from diverse backgrounds and with diverse skills. It goes without saying that none of them had the talent to be professionals from the start. They had to gain experience and work hard to develop their skills and achieve their goals. We interviewed two security engineers and asked them how they improved their technological abilities and gained the resourcefulness to become cyber security professionals.

Entering the security world after many different experiences

Michibi Uehama and Jun Kodama are respectively veteran and new members of NEC's CSIRT, the company's front line cyber security team. However, contrary to expectations, neither of them started out in the security field.

Uehama majored in software engineering at university. Because he was more interested in system construction than software development, he joined NEC Networks & System Integration Corporation (NESIC) after graduating. He became interested in the security field after coming into contact with remote access and authentication technology when he was an SE in charge of system integration for network infrastructure and teleconferencing system clients. After working as an SE for over ten years, he wanted to become a specialist in something, so he transferred to a job that involved consulting with customers on ISMS certification (ISO/IEC 27001).

"Because I was inexperienced, I was frustrated because I was not able to communicate the risks and true nature of security measures to top management and the front line workers," explains Uehama. "It was at that time that the company told me that I should study how NEC's CSIRT responds to security incidents to improve my security skills. So that is when I transferred to the CSIRT."

Michibi Uehama
Expert
NEC Cyber Security Strategy Division

Kodama has always been recognized as a personal computer expert. As an undergraduate and a graduate student he majored in information systems and networking, and received specialized education in UNIX operating systems before entering NEC.

"In addition to my classes, I also worked part time in the university computer room, so I was really immersed in computers," says Kodama, looking back. "I made an e-learning video distribution system, and an application to distribute contents on the web as well as some other things."

In his first two years at NEC he was assigned to sales. However, he just could not get used to sales work and asked to be transferred to development, so he was transferred to the data center of a Group company. After working on assessments of storage systems and developing virtual environments, he returned to one of NEC's infrastructure divisions, and was also assigned to work with the CSIRT.

Both of these men entered the world of security after gaining a wide range of experience elsewhere, but neither of them had much of a problem making the transition. Both of them agreed that "It was very easy to blend in because everyone told us that we should ask if we had any questions. There were many training courses and study groups, and we felt reassured because some of Japan's top professionals were our colleagues. The CSIRT is often about teamwork, so there are plenty of opportunities to learn different skills from others, and the environment is conducive to gaining the knowledge we need about security engineering in a structured way."

Jun Kodama
NEC Platform and Engineering Division

Asking yourself day after day what skills you don't have

However, because their workplace was the pinnacle of security work, they both spent many days wondering what knowledge and skills they lacked.

"One big stumbling block for me was that I did not have enough program development experience," admitted Uehama. "Sometimes, work at the CSIRT involves examining tens of thousands of lines of logs to discover abnormal character strings that would lead to the discovery and analysis of malware. Therefore, it is necessary to understand what a normal program looks like.

"Today, I am able to read some code, but because we need to learn so many programming languages I am always asking myself what knowledge and skills I am lacking," he continued. "So, I keep trying to fill the gaps by learning the things that have the highest priority."

Kodama is battling attackers on a daily basis, but strongly feels that he is lacking in many skills. However, he says that that fact stimulates him.

"Even in my immediate surroundings there are experts who I cannot compare myself with. At their level, they will find hints in data that looks like meaningless character strings, and then they will use numerous analysis methods to quickly find characters that mean something. I also have the chance a number of times every year to take part in CTF (Capture the Flag) contests in which security specialists from around the world compete, but the problems presented are much more difficult than actual malware analysis. The reason is that CTF involves research on attack methods that are expected to be developed in the future, so it is like being confronted with malware from several years in the future. That is why among my NEC CSIRT teammates I am not yet at the level where I can score points. However, I want to reach that level some day," he laughs.

Battling opponents that you cannot see

NEC's CSIRT members also work on responding to attacks on customers, so they must be ready to handle actual attacks at any time. Immediately after he was assigned to the CSIRT, Kodama was given the task of analyzing ransomware, which was just starting to proliferate at that time.

"I was fortunate to be able to work on a relatively easy-to-solve attack, so that gave me a feel for what I needed to do," he says. "After that, attackers upped their game every few months, but gradually I learned what the attackers were thinking and could understand how they would change their attacks. I was truly battling an opponent that I could not see."

Sometimes the work involves a customer's actual business.

"We once received a request to analyze the possible illegal doctoring of a web site. Upon analyzing the problem, I thought the situation was very serious," recalls Kodama. "After confirming my assessment and consulting with team members, we made the decision to shut down the customer's service. It was a large scale service so it was very nerve racking."

The result was that the team was able to minimize the damage, for which the customer was very thankful. It was a moment when Kodama felt a sense of achievement because he was able to demonstrate the technological ability that he had been working on.

Uehama feels a sense of worth because he is able to prevent many attacks on customers by using his experience with the malware attacks detected by NEC and the corresponding incidence response. In this type of work, past experience is often valuable.

"When explaining risks and measures, I naturally use words that are easy for customers to understand, and customers sometimes thank me for that," he says. "This might be from my experience as an SE and in consulting. Security work requires a broad range of knowledge, so that past knowledge and experience is often invaluable. What I really like, however, are those moments when I can really feel that I have gotten better than I was a year ago or several months ago."

Wanting to become a specialist who will keep the company safe and secure

Both of these employees are improving themselves at the forefront of security, but how do they see their careers developing?

Kodama is aiming to become an engineer at the highest level; that is, he is aiming to become a top gun. "That is what I have been aiming for since I entered this field. To that end, there are still many technical aspects that I must absorb. However, the important things are protecting information, business, and society. So, I believe that it is my mission to protect all social systems from cyber attacks by encouraging CSIRT members to help each other become better by always sharing information."

Kodama talks this way because he believes that cyber security is already a part of the social infrastructure. "Unless measures to protect against malevolent attacks become standard, then neither business nor social life can continue," he concludes.

Uehama says that he aims to become an expert "bridging security personnel" who will connect top management and security workers. "To achieve this I have to always be aware of the latest security technologies and trends, and make continuous efforts to improve my knowledge and skills," he explains. "In describing the latest risks and the front line conditions to top management, including the top management of customers, I need to use my own words and judgment and not just parrot someone else. I also need to communicate accurate information. It goes without saying that I will have to improve my management skills and communication abilities as well."

The forefront of security is not a place that attracts a lot of attention. However, both of these men understand that they are doing something that helps the entire world, and they have the pride and goals that come with being professionals as they and their CSIRT colleagues continue to battle an enemy that they cannot see.

Futureproof Security

NEC Cyber Security Solutions help achieve the total security of clients' cyberspace, and create a brighter and safer future for all society.

Publisher

NEC Cyber Security Strategy Division

E-mail : info@cybersecurity.jp.nec.com
URL : http://www.nec.com/cybersecurity