Futureproof Security

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

Trend and the Future Outlook

Increased cyber security awareness

The year 2015 was the end of the beginning of the age of cyber security. When Tokyo was awarded the 2020 Olympic and Paralympic Games in 2013, there was a sudden increase in awareness of the need to guard against terrorists and cyber attacks. That led to the enacting of The Basic Act on Cybersecurity in November 2014, and in October 2015 the My Number Individual Identification Number System (social security and tax number system) came into effect. Hardly a day has gone by without some news about cyber security in which a cyber attack has led to large scale leakage of information. In addition, cyber security is not limited to the ICT field. Security must be reinforced for control systems and the growing Internet of Things (IoT).

What measures should companies take?

Today, security measures are a part of all corporate activities. They include a wide range of organizational measures from business continuity plans (BCP), IT planning, information security management systems (ISMS), and security audits, as well as system-based measures covering all aspects from system introduction plans to procurement and operation. Once an incident occurs, not only the IT department, but also top management and various other departments including the legal, promotion and sales departments, must work together to respond to the incident. It is therefore important for companies to understand that cyber attacks are a risk to overall corporate activities, and that investments must be made in cyber security as a facet of risk management in order to expand and continue business. When considering such investments, it is recommended to refer to best practices such as the Cybersecurity Framework published by the National Institute of Standards and Technology (NIST) and the Cyber Security Management Guidelines* published by the Ministry of Economy, Trade and Industry (METI) and the Information-technology Promotion Agency (IPA).
Increased cyber security awareness

The year 2015 was the end of the beginning of the age of cyber security. When Tokyo was awarded the 2020 Olympic and Paralympic Games in 2013, there was a sudden increase in awareness of the need to guard against terrorists and cyber attacks. That led to the enacting of The Basic Act on Cybersecurity in November 2014, and in October 2015 the My Number Individual Identification Number System (social security and tax number system) came into effect. Hardly a day has gone by without some news about cyber security in which a cyber attack has led to large scale leakage of information. In addition, cyber security is not limited to the ICT field. Security must be reinforced for control systems and the growing Internet of Things (IoT).

What measures should companies take?

Today, security measures are a part of all corporate activities. They include a wide range of organizational measures from business continuity plans (BCP), IT planning, information security management systems (ISMS), and security audits, as well as system-based measures covering all aspects from system introduction plans to procurement and operation. Once an incident occurs, not only the IT department, but also top management and various other departments including the legal, promotion and sales departments, must work together to respond to the incident. It is therefore important for companies to understand that cyber attacks are a risk to overall corporate activities, and that investments must be made in cyber security as a facet of risk management in order to expand and continue business. When considering such investments, it is recommended to refer to best practices such as the Cybersecurity Framework published by the National Institute of Standards and Technology (NIST) and the Cyber Security Management Guidelines* published by the Ministry of Economy, Trade and Industry (METI) and the Information-technology Promotion Agency (IPA).
Global trends in cyber security

Cyber security in global discussions

The year 2015 saw an increased interest in cyber security around the world, with many different themes being actively discussed. It goes without saying that countering ever more sophisticated cyber threats and cyber attacks is an urgent issue; however, the recent focus has also been on organizational resilience. Resilience not only means having robust defensive measures; it also indicates how resilient and flexible organizations are when an emergency occurs and how quickly they can take action and recover. This has become a major theme of cyber security measures.

NEC has participated in many international meetings, conferences and forums concerning laws and regulations, policies, organizational theories and the latest technical trends in cyber security, and has discussed the latest actions taken around the world aimed at making organizations more resilient, in particular, internet governance, information sharing frameworks, cyber crime, the Internet of Things (IoT), and IoT security have become globally common keywords and are all being talked about. Many such discussions are sure to continue in 2016 as this global trend continues.

At the same time, sharing information with developing countries that have suffered serious damage and providing them with technical support for implementing countermeasures are also important themes. Issues shared by the entire world are at the top of the agenda in discussions held by international organizations, and there are high hopes for appropriate support measures at both the local and national level.

Establishing a legal framework for cyber security

- Improving user awareness and promoting ICT education programs
- Support for the creation of National CERT/CSIRT
- Technical support for combating cyber threats

Cyber security as a component of risk management

To be a resilient organization, it is necessary to consider organizational and human resource aspects in addition to technical measures based on “security by design.” (Refer to the figure on page 4.)

The keys to effectively implementing these aspects in an organization are strong leadership and proper understanding by top management. Considering the fact that cyber attacks generate risk for all corporate activities, top management must understand that cyber security is an important corporate risk management issue and also demonstrate leadership to take action.

As mentioned in the previous session, security measures must be implemented in all related departments and must cooperate in handling any incidents that occur. In other words, the entire organization of a company, starting with top management, must know how to properly manage cyber security risks. Best practices and guidelines that can be referred to are listed on the following pages.

---

Cyber Security Management Guidelines

These are guidelines that were issued by the Ministry of Economy, Trade and Industry (METI) and the Information-technology Promotion Agency (IPA) in Japan in December 2015. The guidelines have been written for large and small-to-medium sized companies (they do not target small-scale enterprises) that supply systems and/or services related to IT and computer technology or IT is indispensable for their management strategies.

The guidelines clearly state that cyber security is a management issue and indicate three principles that top management must be cognizant of and ten important items that the security administrator must ensure are implemented by all staff. Companies are also required to handle cyber security incidents in accordance with these guidelines.

1. How much cyber attack risk is acceptable and how much will be invested in cyber security? Unless measures are promoted top management, risks that might affect the company will be overlooked.
2. Security measures must not be limited to just one company, but must include group companies and business partners across the supply chain.
3. Appropriate communications concerning security measures must be maintained with related parties, including disclosing information about security measures at normal times.

Cyber Security Management Guidelines
(This document is currently only available in Japanese.)

---

Information Security Management Systems (ISMS)

- ISMS Related International Standardization Trends at ISO/IEC JTC1 SC27 (IT Security Techniques)

ISMS is a management system that was internationally standardized by ISO/IEC, and is widely accepted in Japan as a means of managing information security within an organization. ISMS helps an organization determine the necessary level of security to implement based on risk assessments, plan measures, assign resources, and maintain and improve the system. (PDCA cycle implementation)

ISMS has been standardized in the ISO/IEC 27000 series centered on ISO/IEC 27001:2013 (ISMS Requirements). The main documents are as follows:

- ISO/IEC 27001:2013 (Information security management systems - Requirements)
- ISO/IEC 27002:2013 (Code of practice for information security controls)
- ISO/IEC 27005:2011 (Information security risk management)
- ISO/IEC 27014:2014 (Governance of information security)
- ISO/IEC 27017:2015
- ISO/IEC TR 20232 Revised

Mapping of ISO/IEC 27001 and ISO/IEC 27002

---

* Assuring security from the system planning and design phase. (From Cybersecurity Strategy, September 2015)
Global trends in cyber security

Cyber security in global discussions

The year 2015 saw an increased interest in cyber security around the world, with many different themes being actively discussed. It goes without saying that countering ever more sophisticated cyber threats and cyber attacks is an urgent issue; however, the recent focus also has been on organizational resilience. Resilience not only means having robust defensive measures; it also indicates how resilient and flexible organizations are when an emergency occurs and how quickly they can take action and recover. This has become a major theme of cyber security measures. NEC has participated in many international meetings, conferences and forums concerning laws and regulations, policies, organizational theories and the latest technical trends in cyber security, and has discussed the latest actions taking place around the world aimed at making organizations more resilient. In particular, internet governance, information sharing frameworks, cyber crime, the Internet of Things (IoT), and IoT security have become globally common keywords and are all being talked about. Many such discussions are sure to continue in 2016 as this global trend continues. At the same time, sharing information with developing countries that have suffered serious damage and providing them with technical support for implementing countermeasures are also important themes. Issues shared by the entire world are at the top of the agenda in discussions held by international organizations, and there are high hopes for appropriate support measures at both the local and national level.

- Establishing a legal framework for cyber security
- Improving user awareness and promoting ICT education programs
- Support for the creation of National CERT/CSIRT
- Technical support for combating cyber threats

Cyber security as a component of risk management

To be a resilient organization, it is necessary to consider organizational and human resource aspects in addition to technical measures based on "security by design." (Refer to the figure on page 1.)

The keys to effectively implementing these aspects in an organization are strong leadership and proper understanding by top management. Considering the fact that cyber attacks generate risk for all corporate activities, top management must understand that cyber security is an important corporate risk management issue and also demonstrate leadership to take action. As mentioned in the previous session, security measures must be implemented in all related departments and must cooperate in handling any incidents that occur. In other words, the entire organization of a company, starting with top management, must know how to properly manage cyber security risks. Best practices and guidelines that can be referred to are listed on the following pages.

![Map of international meetings, conferences and forums attended in 2015](image)

National Institute of Standards and Technology (NIST) Cybersecurity Framework

This is a framework created jointly in 2013 by the U.S. Government and private sector working together based on Presidential Executive Order 13636, Improving Critical Infrastructure Cybersecurity. This framework is meant for private sector companies and provides guidance in managing cyber security risks.

The framework is a collection of effective industry standards, guidelines and best practices, and provides a variety of organized and structured cyber security approaches. (It is therefore not limited to use by a single industry or country; companies outside the United States can also use it.) Introduction of measures will differ because each company has unique risks. However, by using the framework below to specify the necessary measures, and then by iterating according to their priority, the effectiveness of investments can be maximized.

- **Framework Basics**
  - **Framework Core**
    - A summary of best practices for common cyber security measures, their expected outcomes, and reference information about their range of application. This is made up of five functions that are executed concurrently and continuously: Identify, Protect, Detect, Respond, Recover.
  - **Framework Implementation Tasks**
    - Indicates how companies handle cyber security risks and the kinds of processes they use to manage those risks.
    - Indicated at Tier 1 (partial) to Tier 4 (adaptive).
  - **Framework Profile**
    - Represents the outcomes (implementation of security measures) based on business needs that an organization has selected from the framework.

Cyber Security Management Guidelines

These are guidelines that were issued by the Ministry of Economy, Trade and Industry (METI) and the Information-technology Promotion Agency (IPA) in Japan in December 2015. The guidelines have been written for large and small-to-medium sized companies (they do not target small-scale enterprises) that supply systems and/or services related to IT and companies for which the utilization of IT is indispensable for their management strategy.

The guidelines clearly state that cyber security is a management issue and indicate three principles that top management must be cognizant of and ten important items that the security administrator must ensure are implemented by all staff. Companies are also required to handle cyber security incidents in accordance with these guidelines.

The three principles that top management must be cognizant of (Excerpt):

1. How much cyber attack risk is acceptable and how much will be invested in cyber security? Unless measures are promoted by top management, risks that may affect the company will be overlooked.
2. Security measures must not be limited to just one company, but must include group companies and business partners across the supply chain.
3. Appropriate communications concerning security measures must be maintained with related parties, including disclosing information about security measures at normal times.

Cyber Security Management Guidelines


ISMS is a management system that was internationally standardized by ISO/IEC, and is widely adopted in Japan as a means of managing information security within an organization. ISMS helps an organization determine the necessary level of security to implement based on risk assessments, plan measures, assign resources, and maintain and improve the system. (FDC cycle implementation)

ISMS has been standardized in the ISO/IEC 27000 series centered on ISO/IEC 27001:2013 (ISMS Requirements). The main documents are as follows:

- ISO/IEC 27001:2013 (Information security management systems - Requirements)
- ISO/IEC 27002:2013 (Code of practice for information security controls)
- ISO/IEC 27005:2011 (Information security risk management)
- ISO/IEC 27004:2010 (Measurement of information security)
- ISO/IEC 27006:2015 (Requirements for bodies providing audit and certification of information security management systems)
- ISO/IEC TR 27023 Revised (Mapping of ISO/IEC 27001 and ISO/IEC 27002)

Assuring security from the system planning and design phase (From Cybersecurity Strategy, September 2015)
Cyber attacks, particularly Advanced Persistent Threats (APTs), have been occurring frequently in Japan. In many cases, these attacks have a serious effect on their organizations. What kinds of issues are involved and what kinds of measures are being taken on the front lines of security? How do security experts fight against invisible enemies and adversaries? NEC gathered together some of its top domestic and foreign security experts who have a deep and unique understanding of cyber security to talk about the frontline issues they are facing. (Moderator: Jun Goto, Senior Expert, Cyber Security Strategy Division. Panelists: CSIRT supervisor; malware analysis manager; IR (Incident Response) manager; SOC (Security Operation Center) manager; forensics manager; web diagnosis manager; and secure development and operations manager. The discussion was conducted in October 2015.)

**Theme 1: What are some of the current threats to security and what are the issues faced by the CSIRT?**

More companies and organizations are establishing a Computer Security Incident Response Team (CSIRT) to handle problems that conventional IT departments cannot solve. Once a security incident occurs, top management and staff on the front lines must work together to take measures to handle media fallout and any legal ramifications. However, although many companies are establishing CSIRT units, in reality, members of these units also often have regular work responsibilities, which can cause problems with the functionality of the CSIRT. How are security threats changing and what kinds of issues are there with CSIRT?

**Security threats are becoming more complex and sophisticated.**

**Goto:** Targeted attacks on companies and government agencies are becoming more complex and sophisticated every year. What do the members of the roundtable think about these changes?

**CSIRT supervisor:** Since 2011, NEC also has been the target of intermittent attacks. Over the last year in particular, the number of attacks by unknown malware that are not caught by conventional virus definition databases has increased. For instance, it is very difficult to detect malware in password protected zip files that are attached to e-mail. Even if we take countermeasures, the attackers will immediately change their attack patterns, so it is like chasing your tail.

**Malware analysis manager:** In June 2015, damage caused by the remotely operated virus “Emdivi” was a big story in Japan. The infamous information leak from a government organization was one of the incidents traced to this attack, but the number of industries targeted by this virus keeps growing, and today it has become a widespread problem in all types of companies of every size. The feature of Emdivi is that it can be remotely operated from the outside, so that once it is inside an organization’s network, it will search the information on the computers within the organization and send the internal data of the targeted company to the external attack server. There are cases in which all data was stolen in hours, and other cases in which the virus resided within a system for over a year in multiple computers while conducting these illegal searches. NEC has been exchanging information with government-related external organizations and various security vendors, and we are working day and night to prevent damage to our customers.

**CSIRT supervisor:** When unknown malware is detected, for example a targeted e-mail attack, we not only depend on sandbox products; our security staff also try to determine the nature of the attack from past attack trends and know-how based on analysis of changing attack methods. The IT departments at regular companies simply do not have the human resources to defend against these types of attacks.

**Columns: What are the roles of SOC and CSIRT?**

Currently, the number of companies establishing or considering establishing a SOC or CSIRT is growing. At the same time, there are also many companies that have established these centers/teams but are not operating them effectively. SOC (Security Operation Center) is a generic term for an organization that monitors security appliance products and server logs to discover incidents, and it acts as a guard. CSIRT (Computer Security Incident Response Team) is a generic term for an organization that handles any discovered incidents, and it plays the role of an investigator that prevents damage from spreading.

**CSIRTS need to be operated properly.**

**Goto:** CSIRT units monitor and improve internal environments when things are normal, and once an incident occurs, they play a central role in implementing countermeasures. However, many companies and organizations seem to have problems operating their CSIRTS.

**CSIRT supervisor:** It is a good trend for us that people are paying attention to CSIRT, but in many regular companies, CSIRT staff are selected from various departments and asked to double as members of CSIRT. There are even cases when a single individual is given all the responsibility. Even if an expert is designated, that person needs a human network within the organization who should be trained on a regular basis, otherwise things will not go smoothly if an incident occurs and the damage will spread.

**SOC manager:** SOC staff provide incident information to the CSIRT or IT department. The department that was contacted takes initial action to respond to the incident and coordinates with related departments. However, this is often the area that is not working. Specifically, we once had a case where a customer left decision-making completely up to us saying, “We will leave all security work up to you,” with the result that even though our job was only monitoring the equipment, we were forced to do the subsequent investigative work. There have also been cases in which even though a CSIRT was established, the logs necessary for investigative analysis were not stored appropriately, so investigative analysis could not be conducted.

**Goto:** In other words, it’s not just a matter of making a CSIRT and then forgetting about it.

**SOC manager:** That is correct. Security threats are evolving on a daily basis and attackers use one new attack method after another. Therefore, the people in CSIRTS must watch the attack trends and gain the expertise and know-how to handle sudden incidents.

**It is vital to make frontline risks visible in companies and organizations, and for top management to understand the issues involved.**

CSIRT supervisor: With respect to protecting internal business information from security threats, NEC is in the same boat as its customers. That is why NEC has been researching advanced security technology since the 1990s and developing and improving its internal organization. We also have a long history of operating a CSIRT since we first established one in 2002. We have been building a database that will allow us to take immediate action by comprehensively collecting and storing new incident information, and information about threats and vulnerabilities. We also have an organization that will allow immediate use of the tens of thousands of pieces of information collected so far if necessary.

**IR manager:** It is important to get top management to better understand the risks involved in information security. It is said that the cost effectiveness of security measures is hard to see; however, by visualizing the impact on management when certain kinds of incidents occur, it will be easier for top management to make investment decisions. It is necessary for top management to recognize the minimum human resources required to prevent or minimize damage. In addition, if an incident should occur, top management should cooperate with the CSIRT to make important corporate activity decisions and to demonstrate leadership.

**Goto:** So, it is important that top management accurately understands current problems in the work place.
Cyber attacks, particularly Advanced Persistent Threats (APTs), have been occurring frequently in Japan. In many cases, these attacks have a serious effect on their organizations. What kinds of issues are involved and what kinds of measures are being taken on the front lines of security? How do security experts fight against invisible enemies and adversaries? NEC gathered together some of its top domestic and foreign security experts who have a deep and unique understanding of cyber security to talk about the frontline issues they are facing. (Moderator: Jun Goto, Senior Expert, Cyber Security Strategy Division. Panelists: CSIRT supervisor; malware analysis manager; IR (Incident Response) manager; SOC (Security Operation Center) manager; forensic manager; web diagnosis manager; and secure development and operations manager. The discussion was conducted in October 2015.)

More companies and organizations are establishing a Computer Security Incident Response Team (CSIRT) to handle problems that conventional IT departments cannot solve. Once a security incident occurs, top management and staff on the front lines must work together to take measures to handle media fallout and any legal ramifications. However, although many companies are establishing CSIRT units, in reality, members of these units also often have regular work responsibilities, which can cause problems with the functionality of the CSIRT. How are security threats changing and what kinds of issues are there with CSIRT?

**Malware analysis manager:** In June 2015, damage caused by the remotely operated virus “Emidious” was a big story in Japan. The infamous information leak from a government organization was one of the incidents traced to this attack, but the number of industries targeted by this virus keeps growing, and today it has become a widespread problem in all types of companies of every size. The feature of Emidious is that it can be remotely operated from the outside, so that once it is inside an organization’s network, it will search the information on the computers within the organization and send the internal data of the targeted company to the external attack server. There are cases in which all data was stolen in hours, and other cases in which the virus resided within a system for over a year in multiple computers while conducting these illegal searches. NEC has been exchanging information with government-related external organizations and various security vendors, and we are working day and night to prevent damage to our customers.

**CSIRT supervisor:** When unknown malware is detected, for example a targeted e-mail attack, we not only depend on sandbox products; our security staff also try to determine the nature of the attack from past attack trends and know-how based on analysis of changing attack methods. The IT departments at regular companies simply do not have the human resources to defend against these types of attacks.

**Goto:** Targeted attacks on companies and government agencies are becoming more complex and sophisticated every year. What do the members of the roundtable think about these changes?

**CSIRT supervisor:** Since 2011, NEC also has been the target of intermittent attacks. Over the last year in particular, the number of attacks by unknown malware that are not caught by conventional virus definition databases has increased. For instance, it is very difficult to detect malware in password protected zip files that are attached to e-mail. Even if we take countermeasures, the attackers will immediately change their attack patterns, so it is like chasing your tail.

**SOC manager:** There are some customers who say, “Our company does not have the kind of information assets that will be targeted.” This, however, is a big mistake. In the past few years, targeted attacks known as watering hole attacks have been on the increase. The web sites of regular companies in Japan have been used as illegal stepping stones to gain access to the actual target companies, and even though these regular companies are also victims, they are sometimes treated as the perpetrators. In those cases, even if security measures were taken, unless those companies can prove that there were illicit activities of which they were unaware, they are likely to lose the trust of their customers and incur damage to their brand image. Because any company can become involved in a serious security incident, activities to protect your own company are very important, and are even one of your social responsibilities.

**CSIRTs need to be operated properly.**

**Goto:** CSIRT units monitor and improve internal environments when things are normal, and once an incident occurs, they play a central role in implementing countermeasures. However, many companies and organizations seem to have problems operating their CSIRTs.

**CSIRT supervisor:** It is a good trend for us that people are paying attention to CSIRT, but in many regular companies, CSIRT staff are selected from various departments and asked to double as members of CSIRT. There are even cases when a single individual is given all the responsibility. Even if an expert is designated, that person needs a human network within the organization who should be trained on a regular basis, otherwise things will not go smoothly if an incident occurs and the damage will spread.

**SOC manager:** SOC staff provide incident information to the CSIRT or IT department. The department that was contacted takes initial action to respond to the incident and coordinates with related departments. However, this is often the area that is not working. Specifically, we once had a case where a customer left decision-making completely up to us saying, “We will leave all security work up to you,” with the result that even though our job was only monitoring the equipment, we were forced to do the subsequent investigative work. There have also been cases in which even though a CSIRT was established, the logs necessary for investigative analysis were not stored appropriately, so investigative analysis could not be conducted.

**Goto:** In other words, it’s not just a matter of making a CSIRT and then forgetting about it.

**SOC manager:** That is correct. Security threats are evolving on a daily basis and attackers use one new attack method after another. Therefore, the people in CSIRTs must watch the attack trends and gain the expertise and know-how to handle sudden incidents.

It is vital to make frontline risks visible in companies and organizations, and for top management to understand the issues involved.

**CSIRT supervisor:** With respect to protecting internal business information from security threats, NEC is in the same boat as its customers. That is why NEC has been researching advanced security technology since the 1990s and developing and improving its internal organization. We also have a long history of operating a CSIRT since we first established one in 2002. We have been building a database that will allow us to take immediate action by comprehensively collecting and storing new incident information, and information about threats and vulnerabilities. We also have an organization that will allow immediate use of the tens of thousands of pieces of information collected so far if necessary.

**IR manager:** It is important to get top management to better understand the risks involved in information security. It is said that the cost effectiveness of security measures is hard to see; however, by visualizing the impact on management when certain kinds of incidents occur, it will be easier for top management to make investment decisions. It is necessary for top management to recognize the minimum human resources required to prevent or minimize damage. In addition, if an incident should occur, top management should cooperate with the CSIRT to make important corporate activity decisions and to demonstrate leadership.

**Goto:** So, it is important that top management accurately understands current problems in the work place.
Theme 2: Surprisingly vulnerable?
The side of corporate systems that only security staff can see

Log management is the foundation of security measures.

Forensics manager: Forensics is called upon when it is determined that an incident has clearly occurred. We are often told, “One of our computers has been infected by a virus,” but when we visit the customer it is more likely that several computers have been infected, and there was even a case when over one thousand computers were infected. In these kinds of cases, forensic investigations usually end with a few computers because of cost concerns. In the cases we have investigated, almost all have had information stolen. Therefore, our work is about proving that there has been damage.

Goto: When holding a discussion such as this, we tend to talk about the sophistication of cyber attacks, but we should know that many could be prevented by taking some basic countermeasures.

IR manager: And one of the major problems is that an awareness of security has not been fostered. There is a feeling that security is somebody else’s problem, and there is not a culture or mindset of paying for security. As a result, even when building new systems or replacing old ones, things are left to low level people or vendors. If top management does not provide a budget for security, then the money must be taken out of the current IT budget. This is what causes weaknesses in security checks and security systems. Security costs are not something that can be paid once in every five years. It is vital that organizations change their awareness about this and create a robust system for maintaining security.

Preparations are vital when implementing security incident measures

IR manager: There is another technical issue. Larger organizations use multilayer proxy servers, and that causes time lags in the logs of different terminals. Recently there are cases of time lags between VMs in a virtual server, and this makes it harder to investigate incidents.
**Theme 2: Surprisingly vulnerable?**
The side of corporate systems that only security staff can see.

**Log management is the foundation of security measures.**

**Goto:** It seems that some companies use the term SOC even if they are referring to their NOCs (Network Operations Centers where network equipment is monitored). SOCs are mainly engaged in categorizing the threats monitored by security products and notifying customers, but what issues are SOCs facing on the front line?

**SOC manager:** When an incident occurs in an SOC, the most important thing to do is to view the logs related to the customer's environment. Without these, it is impossible to correctly grasp the when, where, who, what and how of an incident. Acquisition and management of logs is the foundation of all security measures, but more frequently than not, people do not acquire logs properly.

**IR manager:** That is true. Properly acquired logs may actually be the exception rather than the rule. This is especially true in forensic investigations, but just having the terminal log does not help when it comes to details. It is also necessary to acquire the logs for network equipment. For example, the accuracy of an investigation will depend considerably on how much of the log of a proxy server is available. However, maintaining the huge number of logs output from all the various pieces of equipment incurs significant costs, including those for storing archives. This is the stumbling block for many companies. But it is necessary to maintain logs that are appropriate for the type of operations that an organization is involved in.

---

**SOC manager:** If several logs are retained for even a short period, then we should be able to piece things together. However, if even that is not done, then we have no way of knowing what kind of information was stolen. (See the figure below for examples of recommended log acquisition locations.)

---

**Forensics manager:** Forensics is called upon when it is determined that an incident has clearly occurred. We are often told, “One of our computers has been infected by a virus,” but when we visit the customer it is more likely that several computers have been infected, and there was even a case when over one thousand computers were infected. In these kinds of cases, forensic investigations usually end with a few computers because of cost concerns. In the cases we have investigated, almost all have had information stolen. Therefore, our work is about proving that there has been damage.

Goto: When holding a discussion such as this, we tend to talk about the sophistication of cyber attacks, but it would seem that many could be prevented by taking some basic countermeasures.

**IR manager:** And one of the major problems is that an awareness of security has not been fostered. There is a feeling that security is somebody else’s problem, and there is not a culture or mindset of paying for security. As a result, even when building new systems or replacing old ones, things are left up to low level people or vendors. If top management does not provide a budget for security, then the money must be taken out of the current IT budget. This is what causes weaknesses in security checks and security systems. Security costs are not something that can be paid once in every five years. It is vital that organizations change their awareness about this and create a robust system for maintaining security.

**Preparations are vital when implementing security incident measures**

**IR manager:** There is another technical issue. Larger organizations use multilayer proxy servers, and that causes time lags in the logs of different terminals. Recently there are cases of time lags between VMs in a virtual server, and this makes it harder to investigate incidents.

---

**Outline of the flow of log analysis**

**Forensics manager:** Forensics is called upon when it is determined that an incident has clearly occurred. We are often told, “One of our computers has been infected by a virus,” but when we visit the customer it is more likely that several computers have been infected, and there was even a case where over one thousand computers were infected. In these kinds of cases, forensic investigations usually end with a few computers because of cost concerns. In the cases we have investigated, almost all have had information stolen. Therefore, our work is about proving that there has been damage.

Goto: When holding a discussion such as this, we tend to talk about the sophistication of cyber attacks, but it would seem that many could be prevented by taking some basic countermeasures.

**IR manager:** And one of the major problems is that an awareness of security has not been fostered. There is a feeling that security is somebody else’s problem, and there is not a culture or mindset of paying for security. As a result, even when building new systems or replacing old ones, things are left up to low level people or vendors. If top management does not provide a budget for security, then the money must be taken out of the current IT budget. This is what causes weaknesses in security checks and security systems. Security costs are not something that can be paid once in every five years. It is vital that organizations change their awareness about this and create a robust system for maintaining security.

**Preparations are vital when implementing security incident measures**

**IR manager:** There is another technical issue. Larger organizations use multilayer proxy servers, and that causes time lags in the logs of different terminals. Recently there are cases of time lags between VMs in a virtual server, and this makes it harder to investigate incidents.
Sharing information and an awareness of problems can work as a bulwark against attacks.

Goto: This is where the knowledge and skills of specialists come in. The SOCs at NEC support our customers 24 hours a day, 365 days a year with security specialists who monitor and analyze the equipment at the borders of our customers’ networks in an integrated fashion. Have any of you noticed anything special in our relationships with our customers?
Forensics manager: This is closely related to the status of local storage when incidents occur. Quarantining an infected terminal from a network is fine, but if the power is shut down or an anti-virus program is used to scan for viruses, then the virus is not only removed, but the log of the infected terminal can also be lost. From the viewpoint of investigating the cause and effect in chronological order, the entire scope of the incident should be preserved, and left for specialists to handle. Sometimes there are cases in which the company conducts a partial investigation that overwrites the logs, so that there is no way to trace what happened.

IR manager: I have also been involved in an incident where we got a request to investigate several infected computers, but it turned out to be several thousand.

Goto: When things get that big, it can affect business continuity because sometimes operations have to be temporarily stopped, or a press conference has to be held.

IR manager: This is not a case that we handled, but I heard of a case in which hardly any logs had been acquired and therefore investigations were impossible. The customer then decided, 'There is some evidence that someone infiltrated our system, but there is no evidence that information was leaked. Therefore, there is no need to make this case public.' This is a problem of compliance, and if someone inside the company happened to make these details public, then the company would be charged with systemic concealment of facts. To prevent these kinds of things happening, thorough preparations must be taken so that investigations can be conducted if need be.

### Sharing Information and an Awareness of Problems

**Can work as a bulwark against attacks.**

Goto: This is where the knowledge and skills of specialists come in. The SDCs at NEC support our customers 24 hours a day, 365 days a year with security specialists who monitor and analyze the equipment at the borders of our customers' networks in an integrated fashion. Have any of you noticed anything special in our relationships with our customers?

### Column: What about organizations that have neither an SOC nor a CSIRT?

If the system administrator in your own organization discovers signs of a cyber attack, it is necessary for him or her to stop information leaks, stop the spread of infection within the organization, and handle all other aspects of the attack. The following are the items that require caution during the initial reaction to an incident:

- Deleting all suspicious files that might contain malware
  - Recent malware operates by using multiple files, so if some of the files are deleted in the infected computer, a malware investigation may not be possible.
- Changing settings (including login passwords) on computers and servers
  - Doing this will make it difficult to determine whether a change in settings was made by the malware or not, so that an investigation will be more difficult.
- Installing and executing new security products (anti-virus software or the like that is different from what was initially installed) in order to investigate a computer that is suspected of being infected.
  - Doing this may result in the loss of traces of malware, making malware investigation no longer possible.

Although it is recommended that computers that have possibly been infected with malware be immediately isolated from the network to prevent the spread of damage, in some cases malware will self-delete in order to destroy evidence if the infected computer is cut off from the network. If the infected computer is shut down, then the processes and data that the malware generated in memory will be lost. If the malware and its traces are deleted, then it will be difficult to identify the range of damage and completely deleting the malware will be difficult. Although preventing leaking of secrets and the spread of infection have top priority, depending on the circumstances, it can also be important to consult with specialists.

### Theme 3. Vulnerable websites

**What are the potential problems in web application development?**

Goto: Recently, we are seeing a sudden increase in attacks that utilize the vulnerabilities of websites. What issues are involved in protecting websites?

**Web pentesting manager:** With web application development, the demand for better usability and functional improvements is relentless, making it a constant battle against time. Because work is done on very tight schedules, it is not rare for applications to have vulnerabilities caused by tiny mistakes. When an incident occurs, such as a website being defaced or information leaked, then there can be serious consequences for business, such as having to stop services or pay damages to users. However, countermeasures for vulnerabilities are both labor and cost intensive, and there is a lack of in-house personnel with the requisite specialized knowledge. The fact remains that there are many websites that have not taken the necessary countermeasures.

Goto: Can you give us an example of what you consider is dangerous when performing website penetration tests?

**Web pentesting manager:** This is an extreme example, but I was surprised to see a 10-year-old PHP application running on a Windows Server 2003 computer. There is no more support for this application, and security upgrades are not available, so this is a very dangerous situation. Since there were webpages and files on the site that even the customer did not know about, we asked for more details and discovered that the customer had asked a vendor to handle everything from development to operation and maintenance. Neither the customer nor the vendor understood the problem with vulnerabilities. There are also many companies that keep changing vendors. In these cases, it is not clear who is responsible for maintaining the previous website, and risks are heightened because vulnerabilities that are not fixed become the target of attackers.

**IR manager:** In addition, there are many cases of operational problems being left untied. I was very surprised to find many cases of passwords being left at their default setting, ‘password.’ In this case, I immediately have the customer reset their policy.

**Goto:** Considering all of these issues, what kind of proposals and countermeasures is NEC offering to its customers?

**Secure development and operation manager:** The first step in maintaining safety is understanding the current system and conducting risk assessments. For example, if a person becomes ill, the doctor does not say, “Okay, just take this medicine.” The doctor will rather consider the symptoms and their possible causes and then take the best possible action. Systems must be treated in the same way. Recent cyber attacks have seriously affected the business continuity of companies and organizations. This means that instead of leaving security up to the IT department, the entire company must be responsible for maintaining security. To prevent or minimize damage, it may be necessary to change the awareness of our sales representatives and system engineers as well as our customers. The NEC Security Technology Center carefully investigates the issues faced by our customers, including their system configurations and current operations, and makes proposals according to the apparent security risks and their severity. We also consult with our customers about reviewing development guidelines, creating security policies, repairing web systems, and creating incident countermeasure plans.

### Conclusion

Because of the increasing sophistication of cyber attacks, more companies are purchasing more security equipment and devices from many different vendors, which is increasing the workload involved in IT management. To meet the needs of customers and reduce this workload as much as possible, we plan to develop a range of new solutions and services, one of which is a log relative analysis system. Log relative analysis can of course be used to target identified attacks, mass attacks and attacks on servers accessible from the outside; but is can also be used to discover illicit acts occurring in-house.

What companies must be especially conscious of is the fact that because all things will be connected to the Internet and society will become a sophisticated fusion of the real world and cyber space, security should not be considered a cost, but rather a necessary investment that will increase corporate value and international competitiveness. NEC will continue to promote secure development and operation based on "security by design" concept that advocates the assurance of security from the planning and design phases. Through this and other measures, NEC is working closely with our customers to realize a safe and secure society.
Futureproof Security
NEC Cyber Security Solutions help achieve the total security of clients' cyberspace, and create a brighter and safer future for all society.