Protecting ICT environments from cyber attacks
with a comprehensive combination of technology, experience, and experts.

NEC Cyber Security Solutions

More advanced and sophisticated cyber attacks may strike at the core of your business. Can your company survive with its current measures?

Cyber attacks can cause immeasurable damages to a company. They can cause tangible damages such as stopping services; they can ruin the public's trust in a company; and they can lead to leaks of important information that may affect corporate survival.
In order to prevent a worst case scenario, you must have the proper organization, the proper personnel, and make the proper investments. You must also make business decisions with every aspect of the company in mind.
Do you know what you need to do?

\Orchestrating a brighter world

NEC Cyber Security Solutions

In a society in which all manner of things are connected to the Internet and the real world and cyber world are become blended, addressing cyber security is a social requirement and a must.
NEC helps to achieve an information society that is friendly to humans and the earth by providing safe, secure, and comfortable environments in the cyber world.

Futureproof Security

Fight to protect the value of your company!

Cyber security is a problem for society as a whole.

The Japanese government passed the Basic Cyber Security Act in November 2014, and in September 2015 the cabinet approved the “Cybersecurity Strategy,” a new national strategy for the nation’s cyber security. With the development of the Internet of Things (IoT) in which everything, including home appliances, automobiles, robots, and whole factories, are connected to networks, there is an increased risk that factories and other manufacturing centers, as well as infrastructure, will become targets of cyber attacks. This makes security measures more important than ever before.

Avoiding cyber attacks requires security measures that combine information, technology, and personnel.

Information

- **Stronger international cooperation** to respond to new attack methods
- **Sharing the latest information and coordinating efforts** to understand attack methods and protect against malware

Technology

- **Multilayer defense** that assumes infiltration
- **Emergency response** when incidents are detected

Personnel

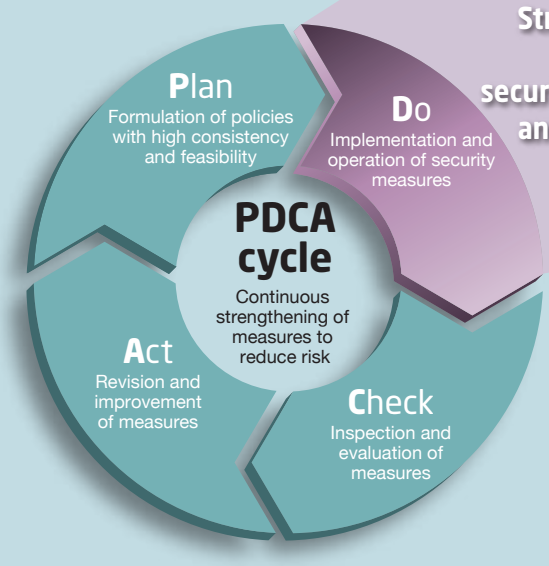
- **Engineer training** for cyber security measures
- **Cooperation between experts** who have specialized knowledge and technology

NEC Cyber Security Solutions provide secure cyber environments by comprehensively combining information, technology, and personnel.

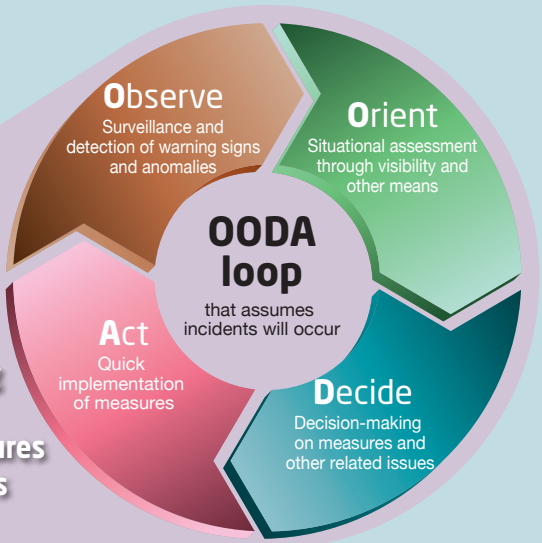
NEC supports effective and continuous security measures, including emergency response that assumes incidents will occur.

We will plan measures that reduce your risks from cyber attacks, and continuously strengthen your entire organization's security.

Simply introducing cyber security measures is not enough. In order to cope with ever more sophisticated cyber attacks, it is important to continuously strengthen your security measures in a planned fashion. In addition to strengthening the security of your entire organization through an effective combination of various security measures, NEC also provides support for continuous measures that reduce vulnerabilities by using the PDCA cycle to plan policies, take measures, verify their effectiveness, and make improvements.



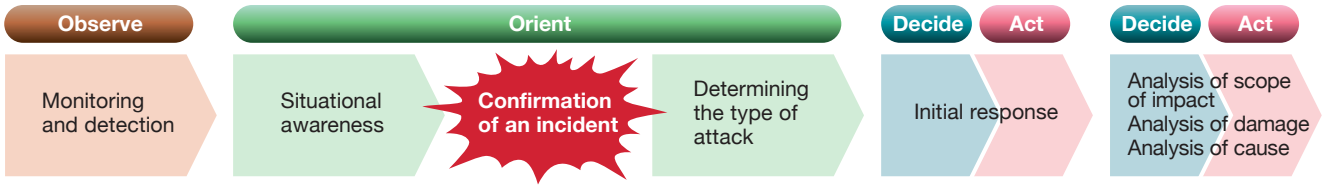
Strengthening of security in measures and operations



NEC supports appropriate situational assessment and prompt response in the event of an incident

In addition to managing security risks with PDCA cycles, what is especially important in preparing for cyber attacks is implementing measures that assume incidents such as illegal intrusions and malware infections will occur. Damage can be minimized by quick detection of abnormal conditions, and timely decision-making and response during emergencies. NEC supports appropriate and speedy handling of incidents through the concept of an OODA loop that includes surveillance and detection, situational awareness, decision-making, and execution of measures.

● Example of incident response

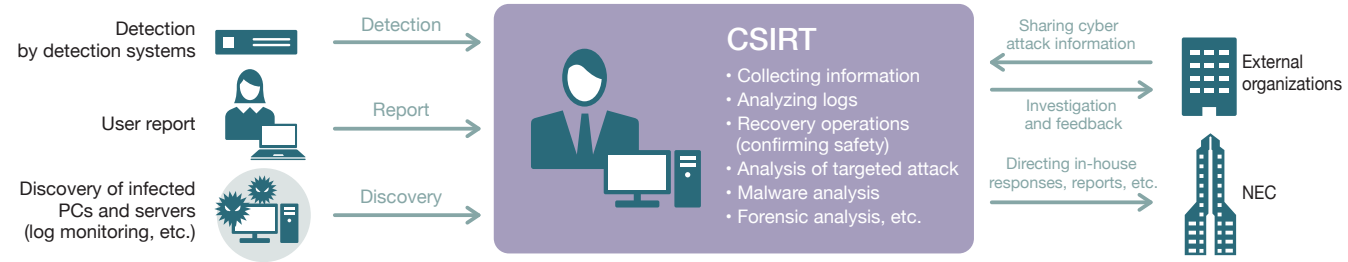


NEC was one of the first companies to implement systematic measures to handle incidents.

Companies today are focusing more strongly on Computer Security Incident Response Team (CSIRT), which is a system of response that assumes incidents that threaten important information assets will occur. NEC started its CSIRT activities in July 2000. We implemented systematic measures at an early stage by cooperating and sharing knowledge with global external organizations, and used our accumulated technologies and experience to configure detection and warning systems, thereby reducing damage. In order to counter ever more advanced and sophisticated cyber attacks, we are promoting advanced responses, such as analysis of detected malware.

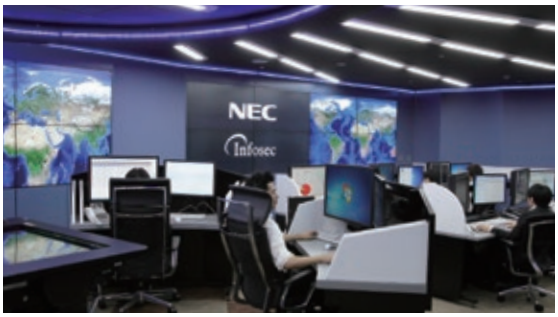
Overview of CSIRT operations

CSIRT : Computer Security Incident response Team



NEC channels intensive internal and external security intelligence into its one-stop cyber security solution: The Cyber Security Factory

When an incident actually occurs, information, technology, and personnel are all needed to implement a quick response. To that end, in 2014 NEC launched the Cyber Security Factory as a center for cyber security measures. This specialized organization coordinates with all companies within the NEC Group and our external security partners, and brings together specialists who are experts in cyber security. This organization collects and shares advanced technologies, the latest attack methods and malware trends, and measure know-how. At the same time, it provides one-stop support that includes introduction and construction of security systems, 24/7 operations monitoring, and emergency response when incidents occur. It also provides realistic cyber training to improve the cyber security response capabilities of corporate security managers.
A new center was opened in Singapore in 2016 to reinforce our global monitoring infrastructure.



Cyber security factory: major functions

- Monitor customers' networks and websites 24/7
- Analyze/evaluate system resilience using cyber attack simulations
- Analyze cyber attack trends, share information and knowledge
- Use advanced techniques to develop sophisticated security technology
- Improve technological understanding of security managers, staff training
- Preserve and inspect evidence through advanced digital analysis

NEC Group

● Cyber Defense Institute, Inc.

CyberDefense

World-class engineers use penetration testing (proactive, authorized exploitation of systems to help evaluate their vulnerabilities) and forensic analysis (analysis of evidence of illegal actions) to devise high-quality security technology services.

● Infosec Corporation

Infosec

Expand the range of security services on offer to include security management and consulting for public sector institutions and private corporations, system design, round-the-clock security monitoring, etc.

Collaborative partners (random order)

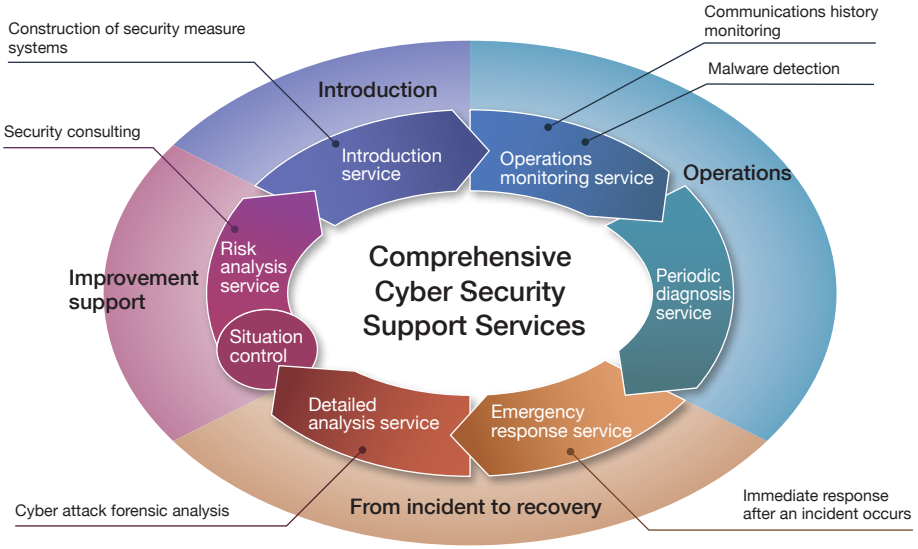
- LAC Co., Ltd.
- FFRI, Inc.
- Trend Micro Inc.
- S&J Corp.
- NRI Secure Technologies, Ltd.

NEC promotes a strong security lifecycle with comprehensive one-stop support services.

NEC's Security Operation Center (SOC) provides advanced security operations monitoring solutions and forensics (analysis of evidence of illegal actions) by world class cyber security specialists. When incidents occur, we also provide emergency incident response solutions implemented by veteran specialists.
We can also link the SOC of our customers (private SOC) with an NEC SOC. This allows us to use both the knowledge accumulated by our customers and our own advanced specialized knowledge for more advanced monitoring and to reinforce the human resource capabilities of our customers.

● Cyber security Total Support Service provided by NEC

Comprehensive one-stop support centered on the NEC Cyber Security Factory



NEC is strengthening its information, technology, and personnel by working together with society to provide secure cyber space.

We share the latest information with specialized cybercrime measure organizations to reinforce security at an international level.

NEC is working with INTERPOL to reinforce international security against cybercrimes.

Image of the Cyber Fusion Centre

In a bid to strengthen the global fight against cybercrime, NEC signed a partnership agreement with INTERPOL in 2012 to fight cybercrime in the INTERPOL Global Complex for Innovation (IGCI) in Singapore. NEC delivered a digital forensic platform and various other technical resources for IGCI, which began full operations in 2015. IGCI offers essential assistance for national authorities in terms of investigating and identifying cyber crimes and criminals, research and development in the area of digital crime, and digital security. NEC is keen to participate in further collaborations between law enforcement and the internet security industry to contribute to the stability of security for businesses and communities throughout the world.

Japan Cybercrime Control Center collaboration (JC3*) links industrial, academic and public sectors.

NEC is a full member of the Japan Cybercrime Control Center (JC3), a non-profit organization seeking to reduce cyber space threats by creating cooperative frameworks between the industrial, academic and public sectors.
JC3 promotes a pre-emptive, comprehensive response to cyber threats by capitalizing on the individual strengths of industry, academic research institutes and law enforcement agencies, and the police's stronger investigative rights.
JC3's ultimate aim is to encourage cooperation and information sharing among relevant institutions worldwide, so they can pinpoint the source of any threat, and localize or minimize any resulting damage.

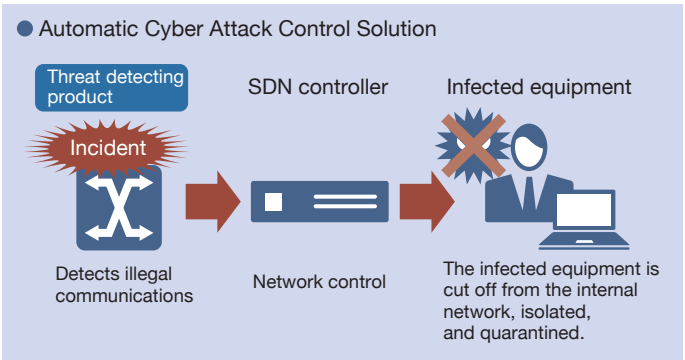
* NEC's Executive Vice President and Chief Marketing Officer, Takaaki Shimizu, was appointed JC3's first Representative Director.

NEC uses its technological expertise and know-how in both ICT and its customers' businesses to develop robust security measures.

As a comprehensive information and communications technology (ICT) vendor, NEC has developed a broad portfolio of hardware and software products. We also have an extensive lineup of solution offerings for many different businesses that are based on our experience and know-how in constructing systems, networks, and providing operations support. It is because we understand the work styles of our customers and have been constructing ICT environments for many years that we can succeed in reducing security risks. In the various development and operations phases, NEC has established development and operations implementation standards to prevent the leakage and falsification of information for systems, products, and services, including social infrastructure. NEC assures security quality by constantly updating its measures for new cyber attacks that occur daily, while also considering international security standards, standards set by the government, and industry guidelines.
For the era of IoT, NEC will provide a safe and secure ICT environment based on our long-established "Security by Design" concept whereby we introduce security measures from the design phase.

NEC is working on reinforcing social infrastructure by conducting proofs of concept (PoCs) for targeted attack measures in Shinagawa Ward.

NEC was an early proponent and is a proactive user of SDN (Software-Defined Networking). When malware infections, website falsification or other problems are detected, the SDN network control functions automatically implement an initial response, such as isolating the communications of infected client PCs and servers, and moving them to a quarantine network.
NEC conducted a joint PoC with Shinagawa Ward to construct new security functions that use SDN, and launched the production system in April 2016.
NEC is aiming to strengthen security measures for social infrastructure through automatic cyber attack control solutions that use SDN.



NEC is developing security professionals with excellent practical skills.

Because cyber attacks become more sophisticated every day, NEC is strengthening its efforts to develop security personnel who can improve the security measures of products, systems, and services, and who can help customers in many different areas.
The NEC Group has defined the security personnel that it requires, and is training professionals in each category. We are continuing to improve this system by cooperating with our customers to define the security personnel that they need. Moreover, we are working together with NEC Group companies, such as the Cyber Defense Institute, and partner companies to prepare training courses for each personnel category, and making these courses available to our customers.

We have established a certification system of our own and encourage our staff to acquire official qualifications.

NEC has established the NEC Certified Professional System to certify personnel who have advanced security expertise. NEC also strongly recommends the acquisition of official qualifications for security, and is expanding the number of staff with CISSP*, which is an international certification, Information-Technology Engineers Examination for Information Security Specialist, and the Registered Information Security Specialist qualification. Employees who have advanced skills, work experience and/or certification in the information security field take the lead in providing customers with optimal solutions.

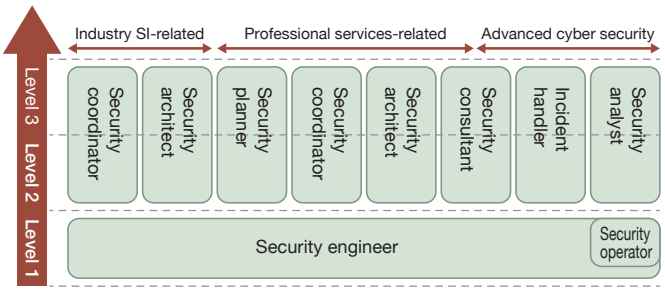
* CISSP Certified Information Systems Security Professional

● Development of professionals

Developing a community of next-generation experts and implementing a companywide CTF

The NEC Group already has a security community made up of over 300 security staff, and follows up on professional development of the next generation through means that include holding regular workshops on topics such as sharing of intelligence and investigation of technology.
We also hold the NEC Security Skill Challenge, an internal Capture The Flag (CTF) competition open to all employees in the NEC Group. In fiscal 2015 about 600 employees took part, and they tried to solve 100 problems in two weeks. About half of the participants were not involved in security work. It is through measures like this competition that we are succeeding to increase our base of security experts.

● Security personnel categories



NEC is working with government agencies, local governments, and academic institutions to develop security personnel and implement training courses.

Working with the Singapore government to train cyber security professionals.

NEC has contracted with the Singapore Economic Development Board to accept trainees for the Strategic Attachment and Training (STRAT) Programme. This program aims to help improve the cyber security of Singapore and surrounding countries, develop personnel with practical skills, and conduct joint research.

NEC has established a JAIST endowed lecture series to train cyber security engineers.

In 2015, NEC provided an endowment to the Japan Advanced Institute of Science and Technology for a course entitled "Cyber Range Organization and Design" to enable advanced research into cyber security, and to develop personnel. Course participants research and develop cyber ranges (cyberspace training areas), and use them to design and develop education programs. The education programs that are developed are made available to other universities and institutions of higher learning.

Cooperating with the MIC's practical exercise to defend against cyber attacks

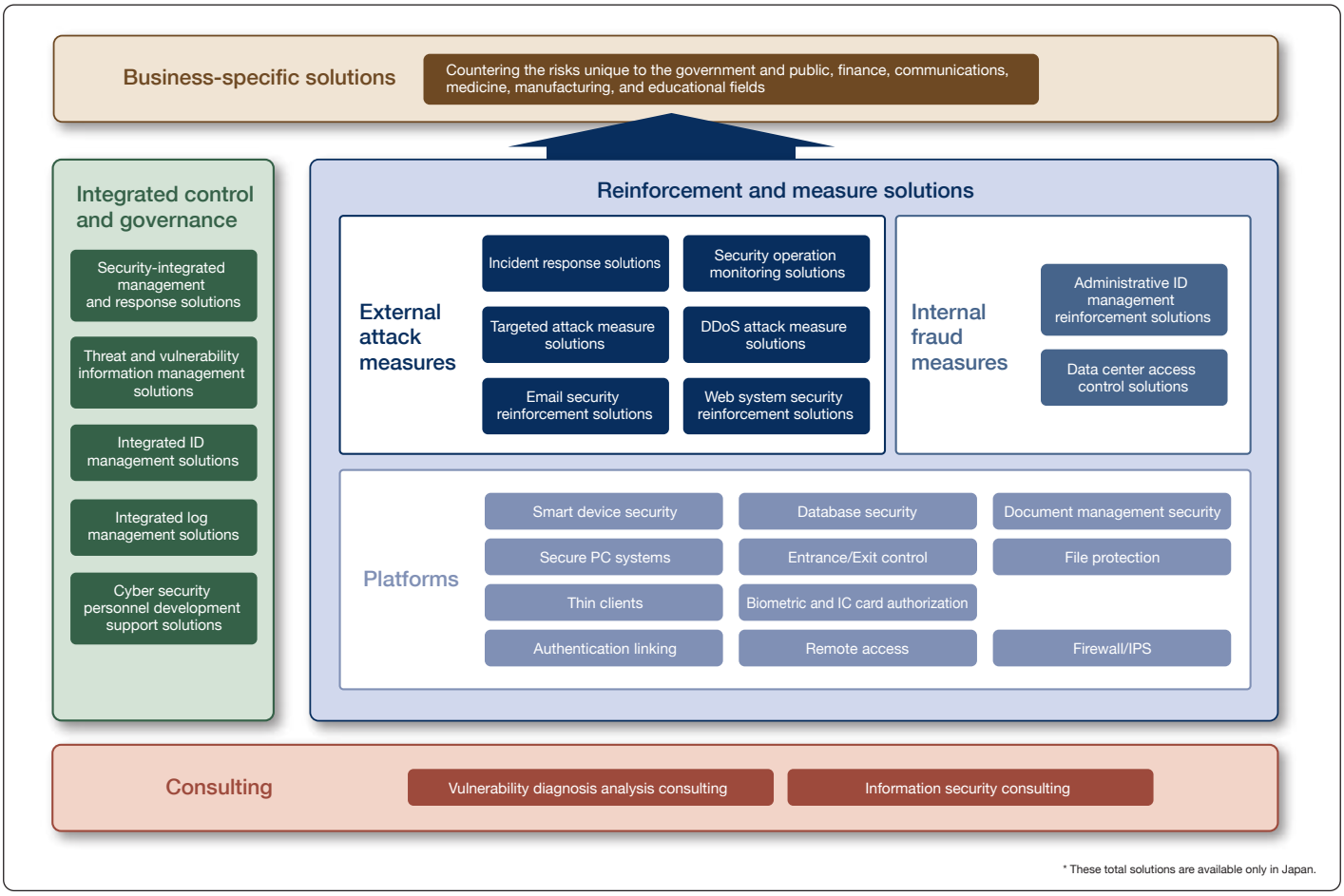
Since 2013 NEC has been cooperating with the "Experimental exercise to analyze and prevent cyber attacks" conducted by the Ministry of Internal Affairs and Communications (MIC). The purpose of these tests is to have system administrators of government and important infrastructure systems conduct Cyber Defense Exercises with Recurrence (CYDER) to protect against targeted attacks in a large-scale simulated ICT environment.
From September 2016, NEC has also been cooperating with CYDER programs for public organizations in 11 areas around Japan, and is helping to improve the incident handling skills of information system managers.

NEC provides total solutions that include cyber security consulting, measures, operations, and incident response.

NEC uses its system-reinforcing and technology development expertise to create standard solutions to counter increasingly sophisticated cyber attacks, and security measures tailored for entire organizations and systems.

NEC provides total solutions to suit entire organizations and systems by focusing on five areas. 1. ***Consulting*** to visualize risks by diagnosing vulnerabilities, propose improvements, and help customers create security policies tailored to their needs; 2. ***Integrated control and governance*** through which companywide control is implemented and security levels are maintained and improved; 3. ***Platforms*** that are the base for realizing the created security policies; 4. ***External attack measures*** which cover the operations and monitoring of systems for protecting against cyber attacks such as targeted attacks and DDoS attacks on web systems, as well as incident response; and 5. ***Internal fraud measures*** to prevent the leakage of information, whether deliberate or unintentional.

NEC also provides security for its customers by reducing the risks unique to various businesses through its "Business-specific Solutions" that include everything from consulting to operations based on our rich experience and system construction know-how.



* These total solutions are available only in Japan.

Consulting: Providing solutions through multifaceted diagnoses

NEC provides support for improving work and creating organizations through multifaceted diagnoses.

NEC analyzes the entire ICT environments of its customers from various angles, confirms the implementation status of existing security measures, and proposes solutions, including those related to work improvements and systems operations.

We also utilize our long experience in operating a CSIRT within the NEC Group, and support our customers by providing emergency responses that assume incidents will occur and building disciplined organizations.

NEC "Cyber Security Management Guidelines" assessment

The "Cyber Security Management Guidelines" were formulated in December 2015 by METI (Ministry of Economy, Trade and Industry), and the independent Information-technology Promotion Agency in Japan. These guidelines position cyber security as an important management task, and summarize the requirements necessary for promotion of measures under the leadership of management. NEC uses these guidelines to assess and clarify the problems of our customers, create policy, and provide appropriate solutions and services.

Integrated control and governance: Systematically managing ICT environments from an administrative point of view.

Fields that require governance are spreading to cloud-based systems and smart devices.

Development of ICT in areas such as the cloud and smart devices has expanded the range of areas that must be covered by company security management. Because the boundary between internal and external systems has become more ambiguous, there is a need for a higher level of regulation, such as access controls that cross boundaries. In this complicated situation, understanding the vulnerabilities of client PCs and servers is more important than ever, and quick response is vital.

NEC's "Count management" helps visualize risks.

By enumerating and visualizing people, ID numbers, client PCs, servers, and even logs, it is possible to understand what kinds of vulnerabilities exist in which locations. Quantification also makes it easy to quickly determine the degree of risk a company faces, and to prioritize measures.

To handle the growing number of threats, including vulnerabilities, targeted attacks, and internal information leaks, NEC provides the know-how that it has acquired through the NEC Group and through its business partners in the form of Proactive Cyber Security Solutions, which provide pre-emptive measures.

Protecting PCs from viruses and malware

Count management

Any deviation in security measure levels becomes a point of vulnerability for cyber attacks. NEC has been using "Count management" to visualize security environments. Count management enables thorough understanding of which equipment is connected to internal networks, making it possible to ensure that all client PCs have security software installed.

In addition, if a client PC without the latest security patches installed is connected to the internal network or if malware is detected on a client PC, that client PC is isolated and cut off from the internal network by a quarantine network. These and other such measures provide valuable peace of mind.

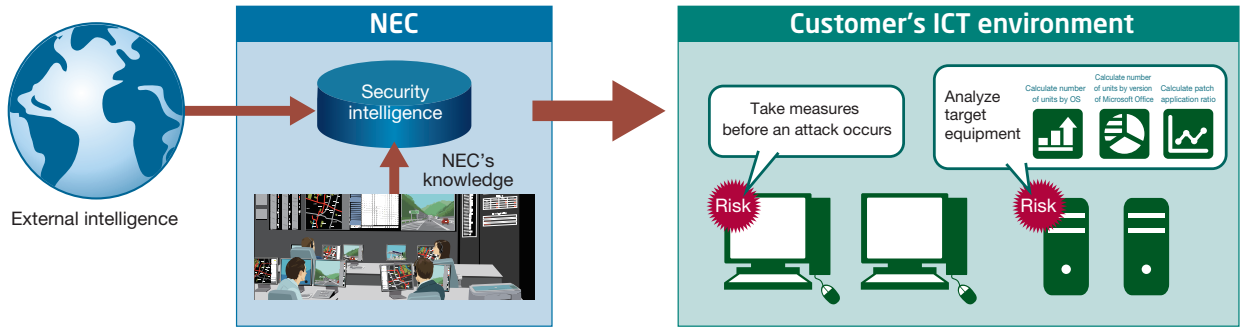
NEC provides new "proactive" cyber security measures based on our internal "Count management" know-how.

Every day, new software vulnerabilities suddenly appear, rendering previously secure ICT environments vulnerable and in need of emergency action. The key to implementing successful measures is to have the latest information on threats and vulnerabilities on hand and control risks to your ICT environment. NEC has been implementing "Count management" for many years. This technology forms the basis of a platform that allows NEC to visualize within one hour which client PCs and servers among the 180,000 units in the NEC Group are vulnerable or have illegal applications installed according to industry reports output daily, and take appropriate and timely action to protect the company's networks. Additionally, NEC's cyber security experts are continually analyzing the latest threat and vulnerability information collected from around the world and adding it to a "security intelligence" database. NEC uses this "security intelligence" combined with our security platform that allows for real time visualization to provide "Proactive Cyber Security Solutions" that implement proactive and effective measures before cyber attacks occur. These solution offerings are known as the "NEC Cyber Security Platform."

ICT environment that leverages the cyber security policy proven on NEC's 180,000-device platform

Practical knowledge that promotes "visualization"

Platform that enables real-time "visualization"



Platforms: Security infrastructure must be convenient to use.

NEC provides infrastructure that functions when and how required to protect your information assets.

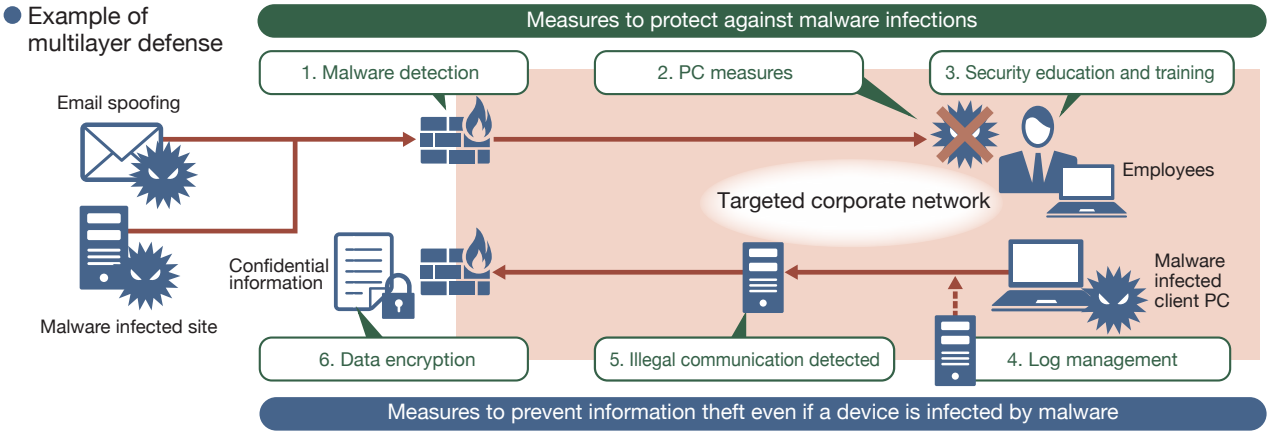
To maintain an ICT environment that supports your business, you need balanced security infrastructure that includes a document management system to protect information assets, physical security, and quarantine systems for PCs that are brought in from outside. NEC leverages the operational know-how of the NEC Group to provide security infrastructure that protects confidential trade secrets and customer information while handling external attacks and internal fraud, and also places importance on maintaining convenience for users.

External attack measures: It is important to assume that there will be intrusions, and combine multiple measures to reduce damage.

Protecting information assets from targeted attacks by using cyber security and HR policies to mount a multilayer defense.

Targeted attacks often use unknown malware that cannot be detected and removed by conventional antivirus software. When a client PC in a company is infected by unknown malware, the infected client PC must be identified and immediate action taken. One measure that is effective against theft of information by this type of unknown malware is "multilayer defense." NEC provides "multilayer defense" that combines technological measures that quickly detect malware activities, and human-based services such as user education and monitoring services.

● Example of multilayer defense



NEC protects the public web systems that are the face of a company.

There are many cases in which victims turn into inadvertent perpetrators when attackers alter websites by exploiting their vulnerabilities and lead users to illegal sites or infect client PCs with malware. NEC visualizes the states of web systems and applications, and proposes measures that classify priorities for new vulnerabilities.

Protecting against ransomware

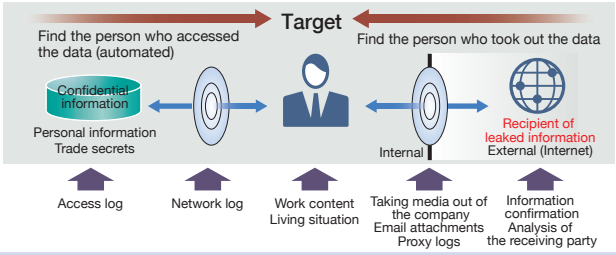
Ransomware is malware that encrypts the data on an infected client PC making it impossible to use. The user is then ordered to pay a ransom in exchange for making the data useable again. Various security measures are necessary based on the concept of multilayer defense in order to reduce the risk of infection. It is also important to have backups just in case a system is infected.

Internal fraud measures: Measures are necessary for risks that are a tradeoff for using the latest ICT to make work more efficient.

Continuously updating all measures, including security policy creation, education and risk analysis, is indispensable.

Email, CD-Rs, thumb drives, cloud storage, and smartphones have allowed us to work much more efficiently. On the other hand, ICT developments have led to information leaks caused by fraudulent acts by employees or through human error. It is necessary to analyze the risks involved in using new devices and services, and continuously reinforce measures, such as updating security policies and educating employees. In addition to measures such as access limits, using thin clients, controlling external media and devices, and encrypting data, introducing operations monitoring and log analysis devices also have a deterrent effect.

● A system to prevent internal information leaks that utilizes deterrent effects

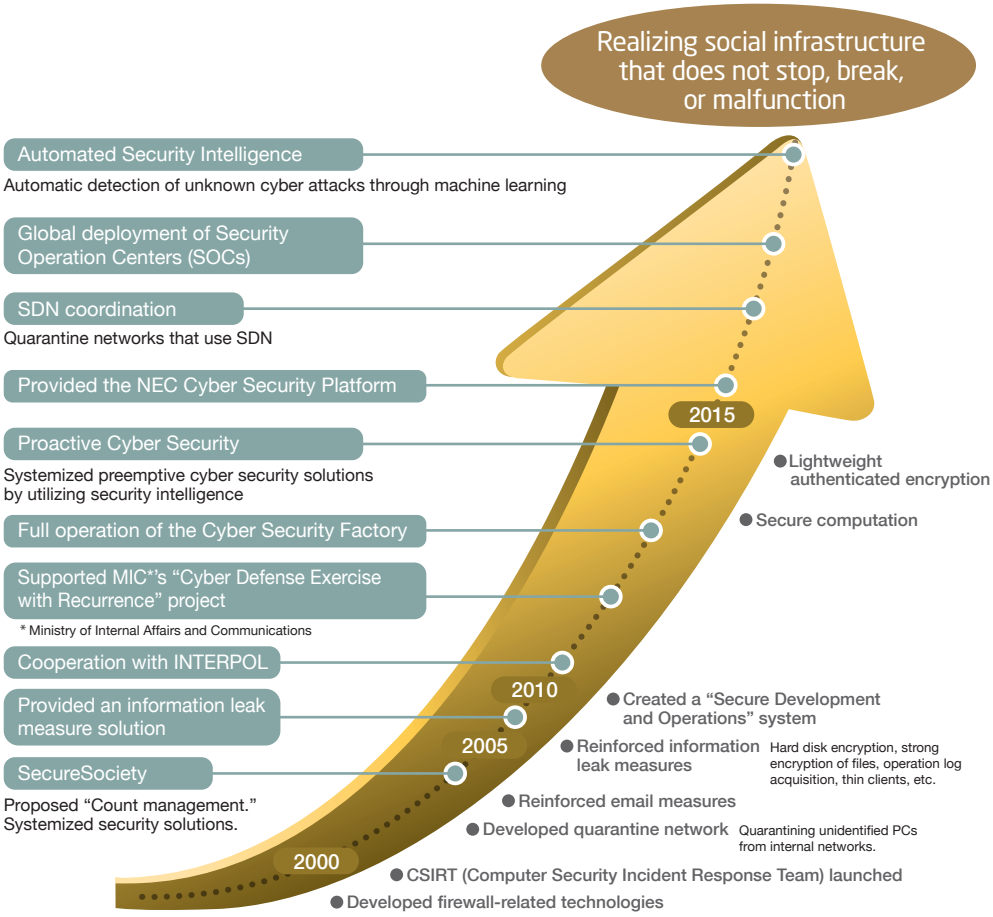


Futureproof Security. Beyond the frontlines of cyber security. See where NEC is going in the future.

NEC will continue to boost the security of social infrastructure with advanced cyber security measures that combine our experience and record of building systems for many customers with our extensive information, technology, and personnel.

The NEC Group has a network system that links 180,000 client PCs and servers. To maintain the safety of this enormous ICT environment, NEC has combined and utilized its original security technologies and solutions. Based on the technologies and know-how proven in our own systems, we are developing and providing solutions that will protect companies and our social infrastructure.

NEC offered the first commercially viable Quarantine Network System in Japan to detect and isolate unauthorized client PCs on a network. In addition, NEC was one of the first companies to propose and implement "Count management," a technology used to quantify and visualize security threats and vulnerabilities. NEC is currently developing cutting-edge technologies that leverage SDN and artificial intelligence (AI). As a leading company in delivering innovative cyber security solutions that create new value, we will never stop providing security and safety to our customers.



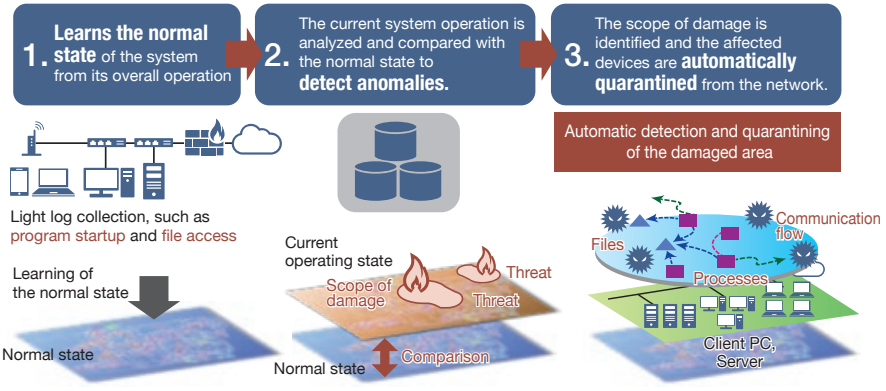
NEC is conducting R&D on technologies that will use AI to automatically detect and quarantine unknown cyber attacks.

NEC is looking to the future. One of the technologies we are developing is "Automated Security Intelligence," a technology that automatically detects unknown cyber attacks by using AI, enabling the scope of damage to be ascertained in less than one-tenth of the time required for conventional manual analysis.

This technology learns the normal state of a network from the complex operations of the entire system, such as the actions of client PCs and servers (program startup, file access, communications, etc.), compares and analyzes the normal state of the system with the current state, and detects when the system acts abnormally.

It can also automatically quarantine only the affected section from the network by using system management tools and SDN.

● Automated Security Intelligence



◎ Even **unknown cyber attacks** are detected in real time.
◎ Identifying the scope of damage takes **less than one-tenth** of the time required for conventional manual analysis.

Futureproof Security

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

For further information, please contact:
NEC Cyber Security Strategy Division
http://www.nec.com/cybersecurity

NEC Corporation 7-1,Shiba 5-chome, Minato-ku, Tokyo 108-8001

Issued May, 2017

Cat.No.J03-17050001E