Safer Cities & Public Services

Commercial facilities as targets:

# New threats to critical infrastructure

The cyber attack on Iranian nuclear installations that occurred in 2010 came as a great shock to industries involved with the establishment and operation of critical infrastructure. Cyber attacks on a state level are characterized by the targeting of critical infrastructure, such as public transportation systems, large-scale constructions, power plants, and dams. Any damage to or cessation/interruption of operation of such critical infrastructure caused by a cyber attack can inflict immense harm on the society. As demonstrated by the spread of IoT and mobile telecommunications, the connectivity of diverse devices and systems to networks also increases the need for security in the critical infrastructure sector. This trend is expanding, as represented by the recent U.S. government's designation of the commercial facilities, which encompasses stations and shopping malls, as one of the critical infrastructure sectors. In particular, cyber attacks are increasing in the area of IoT, including devices connected to information telecommunications networks. Over the coming years, government agencies, enterprises, and other organizations will be required to adopt security measures and cutting-edge technologies for both cyber and physical threats, including protections for critical infrastructure sectors. This report overviews the cyber attack risks to critical infrastructure sectors that Japan and the world are confronted with, as well as specific efforts and sophisticated technologies deployable to reduce such risks.

# Attacks on critical infrastructure are already a reality

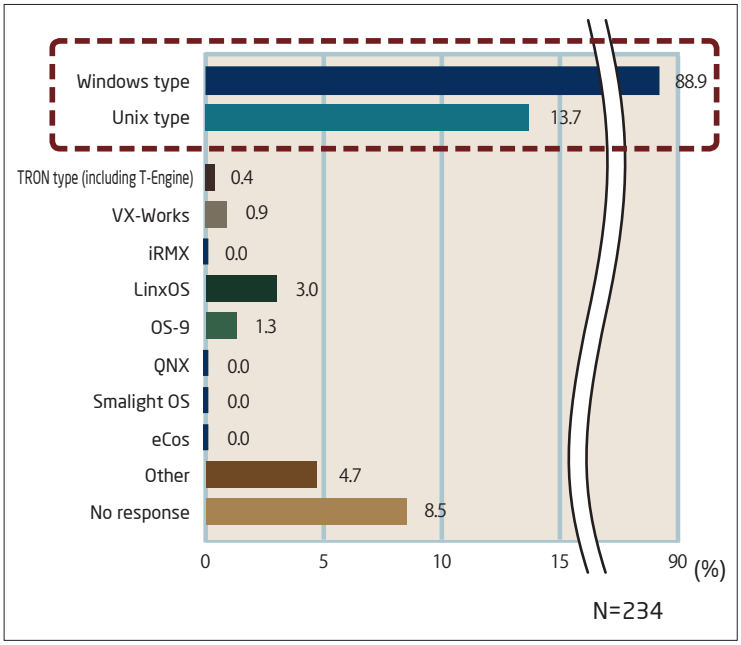
Today, the main current of cyber attacks is shifting from crimes committed by recreational hackers and crimes for money purposes committed by individuals to intelligence and destructive activities suspected to be perpetrated by criminal organizations and states. Looking at cases in Japan, ever since the fact that several defense industry manufacturers' and the House of Representatives' systems received targeted attacks in succession between September and October 2011 came to light, the threat of targeted attacks on intellectual property and state secrets is still expanding. Attacks on critical infrastructure sectors are now a "real" issue.

Furthermore, the system software that controls critical infrastructure primarily runs on Windows and lacks variety. Because this system is relatively closed, the detection of vulnerabilities is often delayed.

Advances in the IoT have propelled factory automations and networking. But at the same time, these advancements increase the risk that an information security incident could develop into a situation that threatens social infrastructure, industrial plants, plant safety, and even environmental conservation. The significance of security is incalculable when considering the possible impact that cyber attacks capable of causing material destruction to critical infrastructure sectors may have.

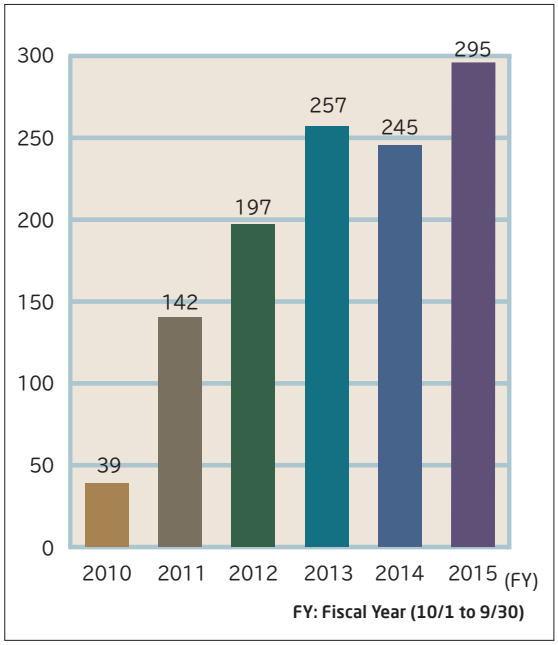
Furthermore, the types of attacks are diversifying and getting more sophisticated and complex year after year. Still fresh in the Japanese people's minds is the incident of the massive information leak from government agencies that occurred in 2015, which was triggered by an artful e-mail disguised as a business statement.

In the U.S., President Obama declared the increase in cyber attacks on the state a "national emergency" in April 2015. The country has heightened the level of vigilance against cyber attacks on critical infrastructure sectors; the federal government redefined their critical infrastructure sectors including complex commercial facilities. Cyber attacks targeting critical infrastructure are not something that Japan can be indifferent about. Immediate actions at a national level are required.




## OS usage (terminals) at industrial plants

*** Created based on Japan's Ministry of Economy, Trade and Industry, "Field Survey Project Report on Threats and Actions for the Application of General-purpose IT in Industrial Equipment, etc. (March 2009)"**




## The number of cyber incidents responses by U.S. ICS-CERT

*** Created based on ICS-CERT's (The Industrial Control Systems Cyber Emergency Response Team; the agency for industrial control system security in the U.S. Department of Homeland Security), Monitor Newsletters**

# What happened in actual cyber attacks around the world?

The world has already suffered multiple incidents of destruction of critical infrastructure that are believed to have been inflicted by cyber attacks. As an example, it is reported that one of the blast furnaces at a German steel mill suffered massive damage following a cyber attack on their network in 2014. The attacker sent targeted e-mails to hack the control system, and as a result, the plant's parts failed, which prevented normal shutdown of the blast furnace and led to the damage.

Since attackers are always devising new attack techniques, preventive actions tend to fall one step behind – this is not limited to critical infrastructure security, but also applies to information security measures as a whole. With that in mind, it is crucial to recognize that cyber attacks are real-life threats targeting control systems, which conventionally were not targets, and that genuine efforts must be put into security measures. To accomplish this, a reliable partner is essential to combat any sophisticated attacks that occur who has the expertise in dealing with them. In selecting a partner, the selecting entity should thoroughly evaluate a candidate's ability to handle user issues and provide appropriate solutions, not to mention have leading technologies to combat modern cyber attacks.

For the future of such enterprises and organizations, it is becoming increasingly important to review their control system security and implement specific protections based on a solid understanding of actual cyber attack incidents targeting critical infrastructure across the world.

**Direct damage to critical infrastructure inflicted by cyber attacks is affecting the real world.**

# Redefining critical infrastructure in Japan for enhanced protection

An endless series of incidents has cropped up to constantly remind us of the need for critical infrastructure security – terrorist attacks on overseas international airports and prolonged flight cancellations due to airline system failure in Japan, to give a few examples. Measures are also being taken against terrorist attacks on citizens in Japan. On November 6, 2014, the Basic Act on Cyber-security was passed by the Diet, which is part of the country's highly publicized cyber security efforts.

Today, a total of 13 areas are defined as critical infrastructure sectors in Japan: Information and communication services, Financial services, Aviation services, Railway services, Electric power supply services, Gas supply services, Government and administrative services, Medical services, Water services, Logistics services, Chemical industries, Credit card services, Petroleum industries. To increase its focus on efforts on critical infrastructure security, the Japanese government has formulated "The Basic Policy of Critical Information Infrastructure Protection (3rd Edition)". Furthermore, there is currently a growing concern for the security of "commercial facilities," which include stations and shopping malls, as a new critical infrastructure sector in addition to the aforementioned 13 areas. In fact, the U.S. government has added the commercial facilities sector to its now 16 critical infrastructure sectors.

In the backdrop of such movements are the frequent cyber attacks using POS malware against various commercial facilities of different scales in the U.S. during 2014. In the same year, it was reported that POS terminals infected with malware were also found in Japan. When a POS terminal is infected by malware, it poses a risk of customers' credit card information being stolen by a malicious third party to be used for wrongful purposes. In the present-day world, POS malware is said to be expanding its target range to airports and railroads in addition to commercial facilities.

Cyber attacks are expanding their targets to include devices connected to networks along with the proliferation of IoT. A new conception is required for actions to be taken to ensure critical infrastructure security in the IoT age.

**Japan**

| Sector | Agency |
|---|---|
| Financial services | Financial Services Agency |
| Information and communication services | Ministry of Internal Affairs and Communications |
| Government and administrative services | |
| Medical services | Ministry of Health, Labor and Welfare |
| Water services | |
| Electric power supply services | Ministry of Economy, Trade and Industry |
| Gas supply services | |
| Chemical industries | |
| Credit card services | |
| Petroleum industries | |
| Aviation services | Ministry of Land, Infrastructure, Transport and Tourism |
| Railway services | |
| Logistics services | |

**U.S.**

| Sector | Agency |
|---|---|
| Chemical | Department of Homeland Security |
| Commercial Facilities | |
| Communications | |
| Critical Manufacturing | Department of Homeland Security |
| Dams | |
| Defense Industrial Base | Department of Defense |
| Emergency Services | Department of Homeland Security |
| Energy | Department of Energy |
| Financial Services | Department of the Treasury |
| Food and Agriculture | U.S. Department of Agriculture and Department of Health and Human Services |
| Government Facilities | Department of Homeland Security and General Services Administration |
| Healthcare and Public Health | Department of Health and Human Services |
| Information Technology | Department of Homeland Security |
| Nuclear Reactors, Materials, and Waste | Department of Homeland Security |
| Transportation Systems | Department of Homeland Security and Department of Transportation |
| Water and Wastewater Systems | Environmental Protection Agency |

**Differences in critical infrastructure between Japan and the U.S.**

Source: National center of Incident readiness and Strategy for Cybersecurity (NISC)
https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

# Key points in security measures sought by enterprises and organizations

Now, enterprises are confronted with new issues, such as how to protect information assets and systems and what to do when they suffer damage from cyber attacks.

Broadly, four key points can be set forth to define the security measures required of enterprises and organizations: (1) "Multilayer defenses" and "monitoring" are key to protect information assets from targeted attacks. (2) Comprehensive security measures that cover organizational and managerial structures and business operation processes, as well as systems, are required for protecting information assets from internal security risks. (3) Experts' presentation of how to address security risks, along with their instantaneous visualization, are crucial to achieve proactive security measures that enable the understanding of and effective protection against such risks. (4) An organization must be structured in such a way that enables quick responses to incidents. This is an undertaking to minimize damage, as exemplified by the computer security incident response team (CSIRT) for centrally managing incidents within the enterprise.

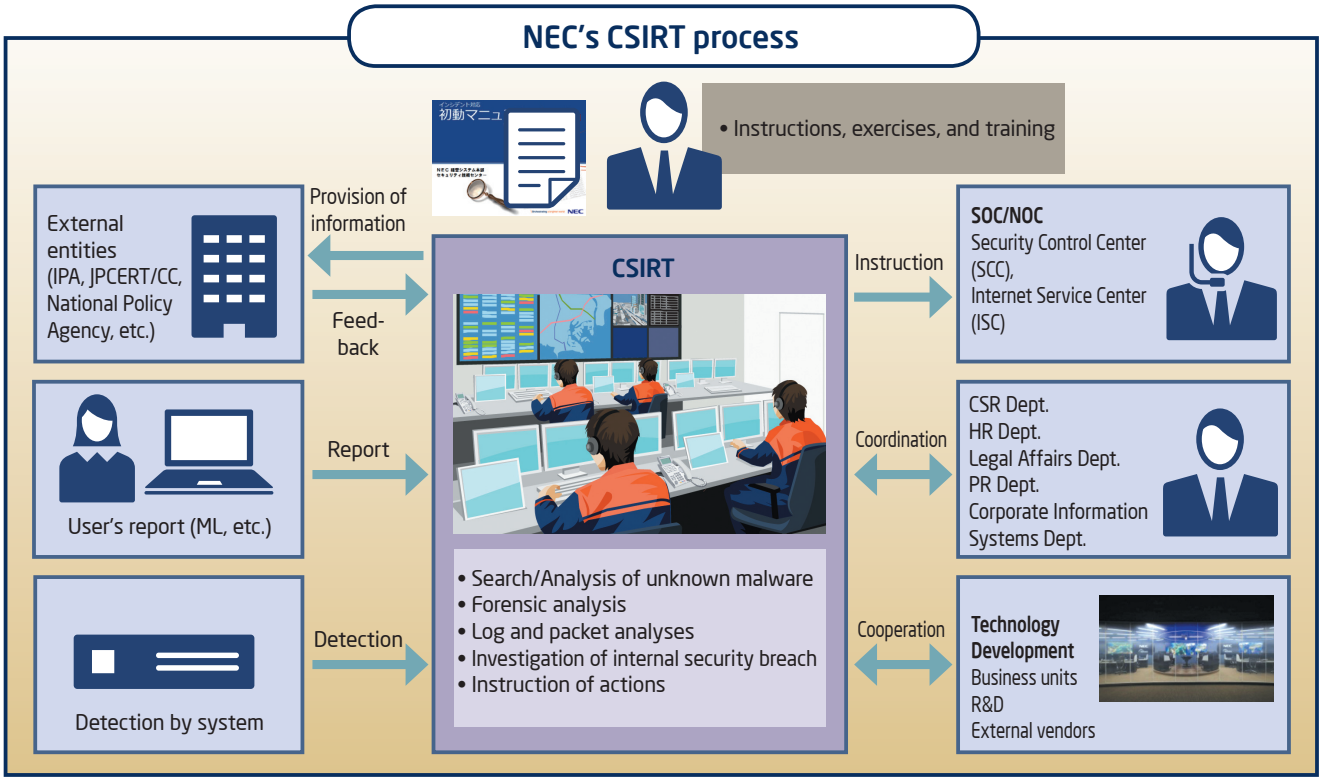
For the resolution of the issue of cyber attacks, NEC provides diverse security products, services, and cyber security solutions that embody extensive solutions to the above four key points.

Needless to say, NEC's solutions also include those for establishing safe, secure critical infrastructure. NEC organized an expert team (CSIRT) that monitors cyber attacks and analyzes the characteristics of attacks and malware, and when an incident arises, preserves evidence and analyzes the attack as well as investigates the cause and brings the situation under control.

NEC was quick to commence its organizational cyber security activities upon establishing and continuing its own CSIRT from July 2000, cooperating with external global institutions, sharing knowledge, and amassing technological and practical expertise to swiftly detect and alert users of security breaches, all to minimize potential damage.

NEC also provides exercises and training for the improvement of technological competence. All of these offerings reflect the techniques and know-how accumulated over the years of security efforts.

Based on such self-cultivated activities, NEC supports the establishment of an optimal organization through in-depth interviews about customers' corporate situation.




* SOC: Security Operation Center NOC: Network Operation Center

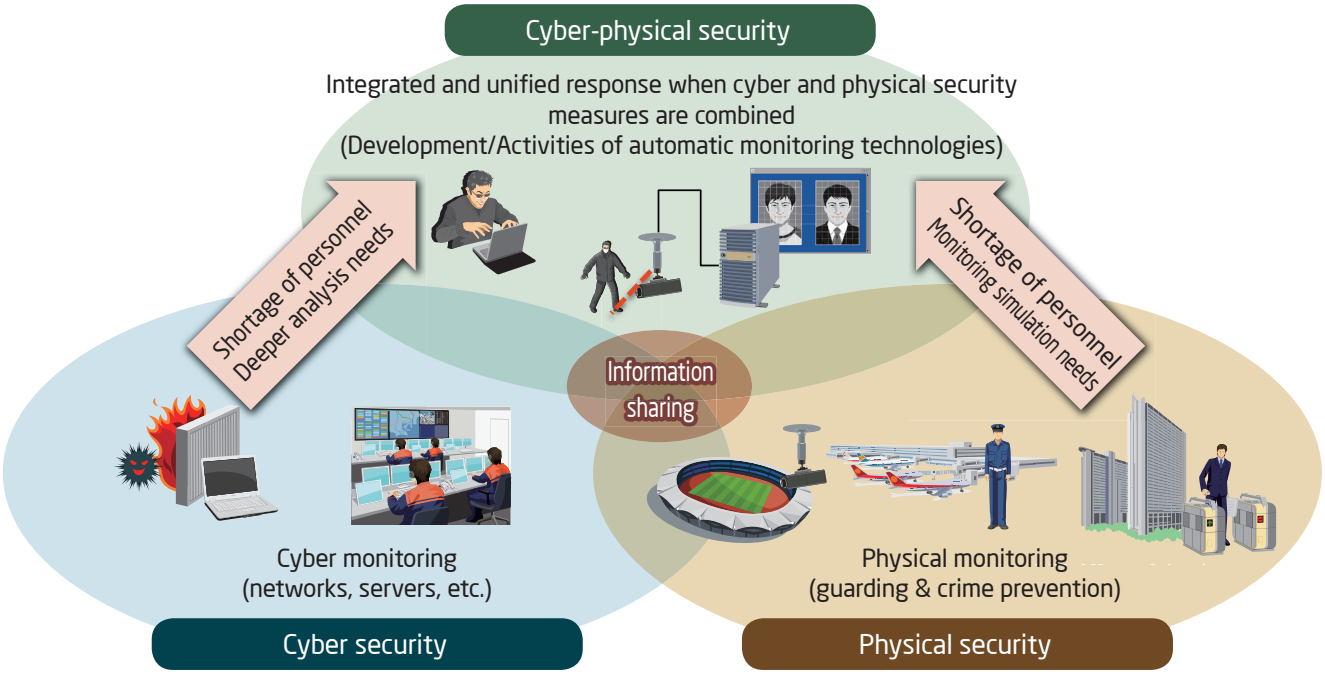
# Cyber-physical security to prevent cyber attacks

As previously outlined, the severity of damages to critical infrastructure inflicted by cyber attacks around the world is trending upwards. Combating today's attack attempts that are steadily getting more advanced and complex is a significant challenge to protecting people's security with only security checks to prevent hazardous objects from entering airports, port facilities, power plants, and other critical facilities and police patrols.

What is attracting attention amid such circumstances as a new approach to combating cyber attacks is cyber-physical security. This aims to block off cyber attacks by driving the latest ICT by combining information from cyber space, which includes cyber attack information, log information, and SNS and other Web information, information from the physical world, such as biometric data, behavioral analysis data, and GPS data. For example, a terrorist's cyber space terrorism plans or access to confidential information by a cyber attack on a critical infrastructure establishment can be detected in advance, and through physical monitoring, including facial recognition, behavior detection, and drone patrolling at the target facility, attacks can be blocked off or promptly dealt with in case an emergency arises.

NEC promotes comprehensive, unified responses for cyber-physical security, with the world's top-class physical security and cyber security as two critical components of an overarching whole. NEC boasts integrated security control and implementation solutions, NEC Cyber Security Platform, Security Operation Center (SOC), and world's number one*1 biometric (facial and fingerprint) authentication technologies, and the world's first behavior detection and analysis technologies. Not only do these options work alone as competitive edges in their respective fields, but they can be combined to respond with their collective strengths. NEC will continue its pursuit to block cyber attacks as well as quickly implement post-attack actions in case of a contingency.

## Comprehensive, unified responses with the world's top-class combination of physical security and cyber security




*1 Ranked 1st in United States' NIST (National Institute of Standards and Technology) benchmark testing.

# Cutting-edge technologies and systems for early detection of cyber attacks

Based on the slogan "Futureproof security. Beyond the frontlines of cyber security," NEC's advanced cyber security response capability offers customers true peace of mind. NEC actively develops system and data security technology to support the formation of a solid, safe base for society, which includes effective regulation systems and the Internet of Things.

Among these activities, NEC's latest concept is "Proactive Cyber Security." We aim to close in on the gap between conventional attacks and the level of security measures by foreseeing and taking pre-emptive actions against attacks.

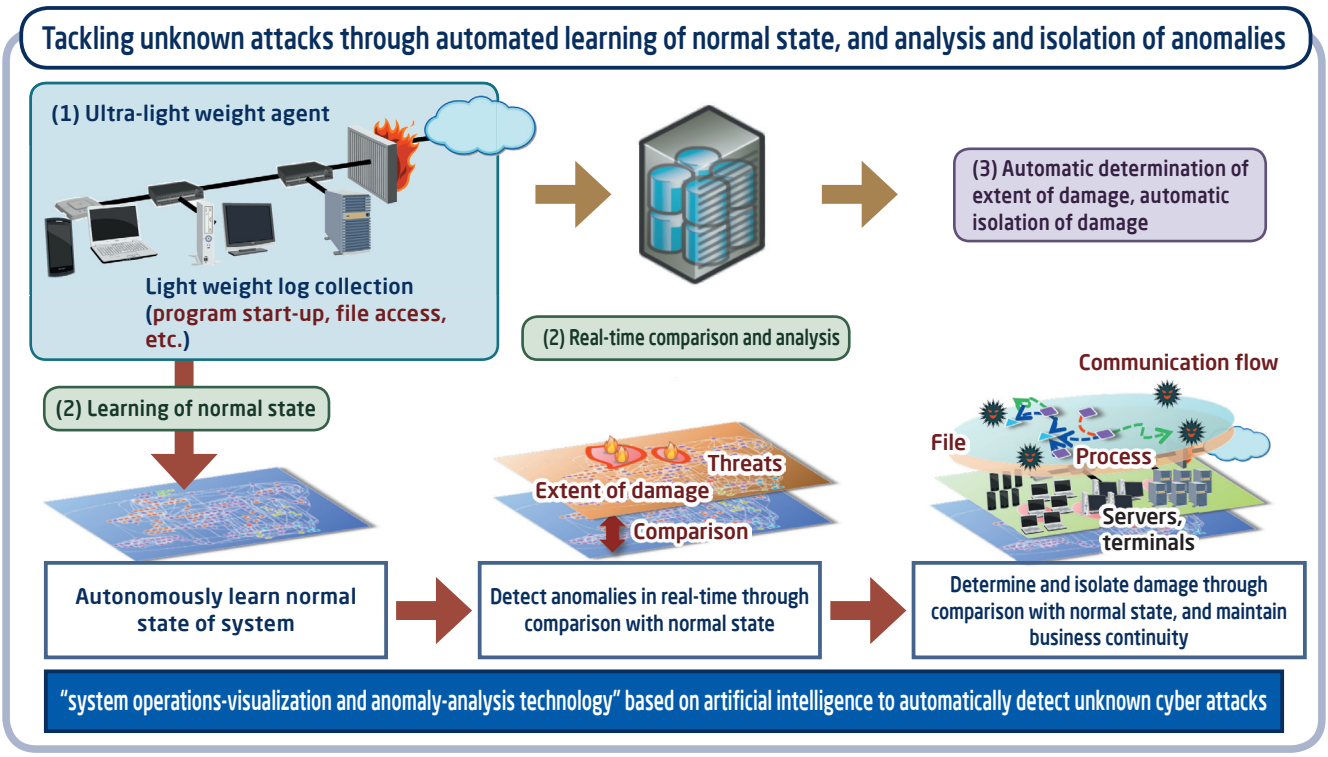
The key to foreseeing such cyber attacks is NEC's security intelligence services, based on information linkage. Experts analyze the information to swiftly identify and respond to potential vulnerabilities in the ICT environment and provide real-time security intelligence.

For example, NEC developed a "system operations-visualization and anomaly-analysis technology" based on artificial intelligence, which draws on artificial intelligence (AI) to automatically detect unknown cyber attacks on social infrastructure and enterprise systems. With this technique, real-time comparison and analysis of the current system operation is conducted vis-à-vis the steady state, which is machine learned from the complex operating status of the entire system, including computers and servers. This enables the detection of deviations from the steady state, and furthermore with the combined use of system management tools and SDN, makes possible the automatic isolation of specified areas from the network. Compared to conventional unaided work, the detailed system operation information allows for the identification of the extent of damage within one-tenth of time needed previously. This technique offers precise anomaly detection and protection that minimize the spread of damage without having to stop the entire system.

NEC has an outstanding record in the area of security based on its cutting-edge technologies that enable early detection of cyber attacks, solutions and systems that constitute comprehensive security, and active partnerships within the industry.

While respecting the essential values pursued by society and by their customers, NEC wishes to work together with everyone and use the ICT to design new societal value, for the sake of a brighter world.

If you have any questions concerning the contents of this report or NEC initiatives, please do not hesitate to contact us.



**NEC Group is focusing its efforts on providing "Solutions for Society" by upgrading the social infrastructure with ICT. NEC defined six megatrends based on a structural observation of the global economy and social trends. Based on the six megatrends, NEC formulated seven themes for social value creation as its mission.**

| | |
|---|---|
|  Sustainable Earth | Establish a sustainable lifestyle base by utilizing limited resources effectively and taking measures to prevent damage to the global environment in order to live in harmony with the Earth. |
|  Safer Cities & Public Services | Help emerging countries build safe and secure cities, and help developed countries mature their societies. Establish a "global" administrative service platform through joint initiatives between the public and private sectors. |
|  Lifeline Infrastructure | Establish ICT systems that resolve disparities of area and delivery time, and build safe and efficient lines for travel, utilities, etc. that can support around-the-clock activities in society. |
|  Communication | Build a platform for information and communications to support the distribution of information and knowledge, which becomes more important as society advances. |
|  Industry Eco-System | Innovate a new industrial ecosystem including connection of industrial machinery with the Internet, 3D printers, crowdsourcing and reverse innovation. |
|  Work Style | Create new work style and relationship with society in which people work together with communities and robots regardless of gender and generation. |
|  Quality of Life | Build a diversified and equal society to support people's enriched and active lives through contributions to education, healthcare and medicine. |

**This Social Value Creation Report is issued for each of the seven themes listed above and summarizes NEC's concepts, efforts, and proposals, in addition to social issues and global trends. NEC hopes that this report can be the first step in establishing cooperative creative partnerships with customers.**

Editorial supervisor: Institute for International Socio-Economic Studies

Please direct any inquiries to the following contact or an NEC marketing representative.

NEC Corporate Marketing Group
nec-vision@crp.jp.nec.com
TEL: +81 (0)3 3454-1111 (main)  http://www.nec.com/en/global/about/vision/index.html