Cybersecurity Consulting Services in the World of IoT

YOSHIFU Kenji, ITOH Mari, YAMADA Tomohide

Abstract

As IoT penetrates the fabric of our reality, transforming the way we live by dramatically increasing the efficiency of industry, improving the responsiveness of business, and enhancing the convenience of daily life, the threat posed by cyberattacks is becoming equally pervasive, posing huge risks to business and making it absolutely indispensable that management redouble its efforts to counter these attacks wherever they may strike, including their supply chains. In this paper, we take a look at the consulting services offered by NEC to help our customers implement appropriate security measures (in IT systems, product development, control systems, etc.) in management and manufacturing after making an assessment based on "Cybersecurity Management Guidelines" formulated by the Ministry of Economy, Trade and Industry (METI).

Keywords

security consulting, cybersecurity, secure development/operation, CSIRT, PSIRT, security education, risk assessment

1. Introduction

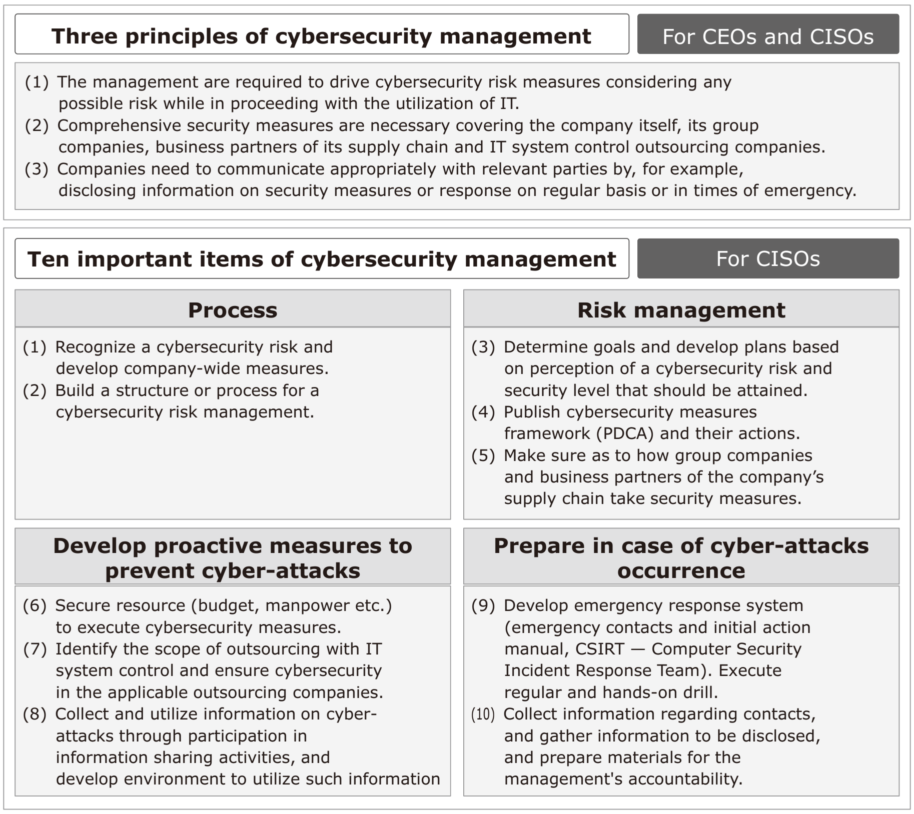
As the world becomes ever more dependent on networks, so too does it become ever more vulnerable to cybercrime. Cyberattacks have been steadily increasing year by year, and information security incidents and accidents have become an issue that can directly connect with management because of their potential to temporarily — or even permanently — shut down an organization's business activities. Given these circumstances, the Ministry of Economy, Trade and Industry (METI) and Information-technology Promotion Agency (IPA) issued "Cybersecurity Management Guidelines"[1)2)] Using these guidelines as a foundation, NEC offers its customer comprehensive cybersecurity consulting services, which are outlined in this paper.

2. "Cybersecurity Management Guidelines"

In November 2014, the Basic Act of Cybersecurity was enacted, stipulating the duties of all the entities concerned (state, municipalities, critical infrastructure operators, cyber-related companies, education and research institutions, etc.). In line with this, the government of Japan decided to lay down basic plans ("Cybersecurity Strategy") regarding cybersecurity. This strategy includes the recommendation that standards and guidelines be implemented according to targets. To address that recommendation, the METI and IPA developed a set of "Cybersecurity Management Guidelines" for the management of private businesses (ver. 1.1 issued in December 2015). These guidelines specify the three cybersecurity-related principles which management needs to recognize and ten important items that the executives responsible should observe (**Fig. 1**).

3. Issues of Cybersecurity and NEC's Commitment

NEC conducted a survey of 200 companies regarding how they were dealing with "Cybersecurity Management Guidelines." Based on their responses, it is clear that many companies — regardless of annual turnover or business type — suffer from a lack of leadership in this area and are unsure how to build a secure structure or implement the appropriate processes. Of the ten important items listed in the guidelines, those ranked highest



Three principles of cybersecurity management

For CEOs and CISOs

(1) The management are required to drive cybersecurity risk measures considering any possible risk while in proceeding with the utilization of IT.
(2) Comprehensive security measures are necessary covering the company itself, its group companies, business partners of its supply chain and IT system control outsourcing companies.
(3) Companies need to communicate appropriately with relevant parties by, for example, disclosing information on security measures or response on regular basis or in times of emergency.

Ten important items of cybersecurity management

For CISOs

Process

(1) Recognize a cybersecurity risk and develop company-wide measures.
(2) Build a structure or process for a cybersecurity risk management.

Risk management

(3) Determine goals and develop plans based on perception of a cybersecurity risk and security level that should be attained.
(4) Publish cybersecurity measures framework (PDCA) and their actions.
(5) Make sure as to how group companies and business partners of the company's supply chain take security measures.

Develop proactive measures to prevent cyber-attacks

(6) Secure resource (budget, manpower etc.) to execute cybersecurity measures.
(7) Identify the scope of outsourcing with IT system control and ensure cybersecurity in the applicable outsourcing companies.
(8) Collect and utilize information on cyber-attacks through participation in information sharing activities, and develop environment to utilize such information

Prepare in case of cyber-attacks occurrence

(9) Develop emergency response system (emergency contacts and initial action manual, CSIRT — Computer Security Incident Response Team). Execute regular and hands-on drill.
(10) Collect information regarding contacts, and gather information to be disclosed, and prepare materials for the management's accountability.

Fig. 1 Outline of "Cybersecurity Management Guidelines."

were implementation of security measures throughout group companies and supply chains, development of an emergency response system in case of an accident, and acquisition of manpower resources (**Fig. 2**).

Focusing on the ten important items described in "Cybersecurity Management Guidelines," all the divisions and departments concerned at NEC Group work together under the leadership of our Chief Information Security Officer (CISO) to improve the information security not only of our in-house environment and that of our partners, but also the systems, services, and products we offer to our customers. In so doing, we endeavor to ensure security in outsourced projects, support secure development and operation, improve the NEC-CSIRT structure to better respond to accidents, and train high-level security manpower through certification and education programs. The knowledge we have gained through our own cybersecurity activities at NEC Group is incorporated in our cybersecurity consulting services.

4. Cybersecurity Consulting Services

In circumstances where cybersecurity is positioned as a critical management issue, NEC offers consulting services to support corporate security (**Fig. 3**).

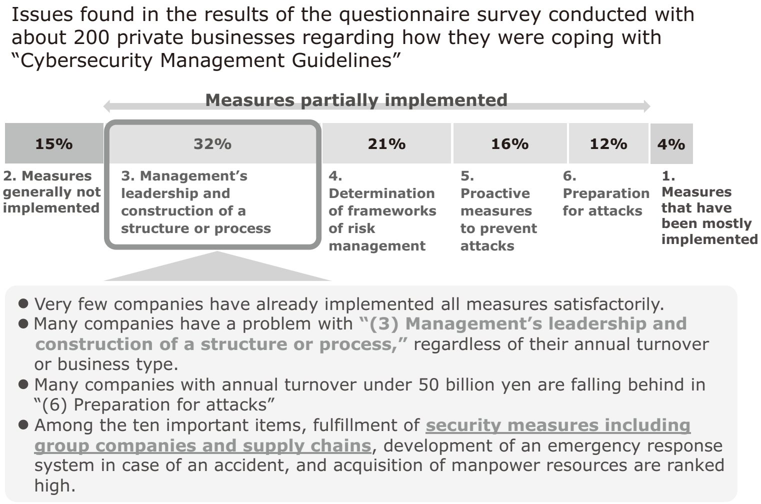
Our services provide security consultation that covers the following three domains: the IT system domain — which centers around the organization's information system division, the product development domain, and the control system domain — which is intended for industrial control systems including factories. We also offer an assessment service for "Cybersecurity Management Guidelines" in order to visualize security issues in organizations on an overall basis.

When we conduct an assessment, we propose measures according to the degree of impact of risk by analyzing and evaluating the risk based on the ten important items in "Cybersecurity Management Guidelines." To analyze and evaluate the risk, we use our original checklist based upon the responses to "Cybersecurity Management Guidelines" at NEC. Solutions derived from this analysis and evaluation include technological solutions and domain-specific support services. We will review some representative domain-specific support services in the following section.

4.1 Services for IT Systems

(1) CSIRT construction/operation support service

NEC launched an in-house CSIRT in 2002 and has


Issues found in the results of the questionnaire survey conducted with about 200 private businesses regarding how they were coping with “Cybersecurity Management Guidelines”

Measures partially implemented
15%
2. Measures generally not implemented
32%
3. Management’s leadership and construction of a structure or process
21%
4. Determination of frameworks of risk management
16%
5. Proactive measures to prevent attacks
12%
6. Preparation for attacks
4%
1. Measures that have been mostly implemented

- Very few companies have already implemented all measures satisfactorily.
- Many companies have a problem with **“(3) Management’s leadership and construction of a structure or process,”** regardless of their annual turnover or business type.
- Many companies with annual turnover under 50 billion yen are falling behind in “(6) Preparation for attacks”
- Among the ten important items, fulfillment of **security measures including group companies and supply chains**, development of an emergency response system in case of an accident, and acquisition of manpower resources are ranked high.

Fig. 2 Issues highlighted by the results of the questionnaire.

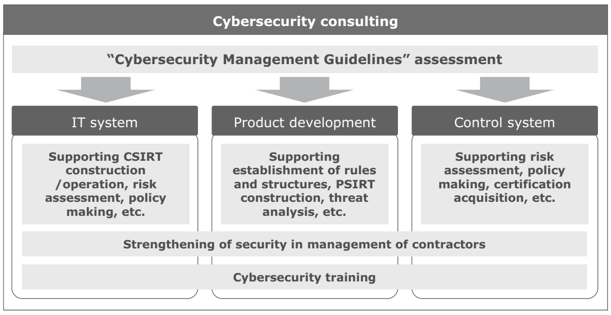

Cybersecurity consulting
“Cybersecurity Management Guidelines” assessment
IT system
Supporting CSIRT construction /operation, risk assessment, policy making, etc.
Product development
Supporting establishment of rules and structures, PSIRT construction, threat analysis, etc.
Control system
Supporting risk assessment, policy making, certification acquisition, etc.
Strengthening of security in management of contractors
Cybersecurity training

Fig. 3 Cybersecurity consulting services.

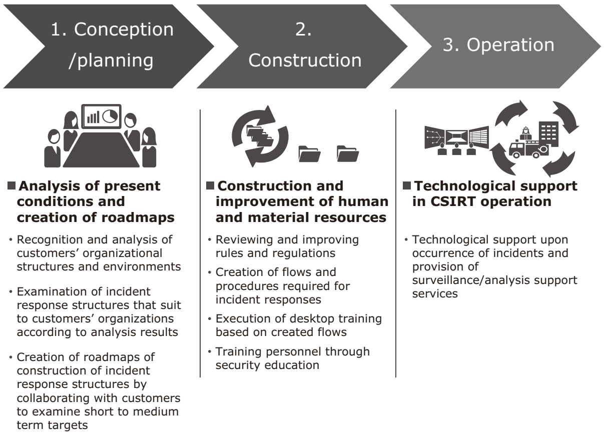

1. Conception /planning
2. Construction
3. Operation
■Analysis of present conditions and creation of roadmaps
・Recognition and analysis of customers’ organizational structures and environments
・Examination of incident response structures that suit to customers’ organizations according to analysis results
・Creation of roadmaps of construction of incident response structures by collaborating with customers to examine short to medium term targets
■Construction and improvement of human and material resources
・Reviewing and improving rules and regulations
・Creation of flows and procedures required for incident responses
・Execution of desktop training based on created flows
・Training personnel through security education
■Technological support in CSIRT operation
・Technological support upon occurrence of incidents and provision of surveillance/analysis support services

Fig. 4 CSIRT construction/operation support service.

had operation results for ten-odd years since then. We have also offered IT systems and operation services to many customers. Based on this technological expertise and know-how, we are able to provide our customers with a service that supports construction and operation of in-house CSIRTs that are designed to be operated by the customer (**Fig. 4**).

4.2 Services for Product Development

(1) Support service for creation of rules for secure development and establishment of structures for it

To effectively promote secure development and operation, it is important to establish basic policies and trans-divisional rules while constructing structures that examine, deploy, and improve various policies, including these policies and rules. Successful construction of an efficient security structure requires effective communication between all departments concerned (IT division, quality promotion/management division, procurement division, etc.) as well as establishment of working groups to discuss and decide on policies and appointment of staff in charge of the promotion at the divisions. Based on our own promotion know-how at NEC, we support the creation of rules and guidelines for secure development and operation and construction or organizational structures (**Fig. 5**).

(2) Support service for construction of PSIRT/vulnerability management processes

To prevent accidents caused by vulnerabilities in products and systems and minimize the impact if there is such an accident, any vulnerabilities found by customers as well as third parties should be immediately addressed. In addition, all vulnerability data — both those that have been publicized and those that have not — is collected and appropriate measures

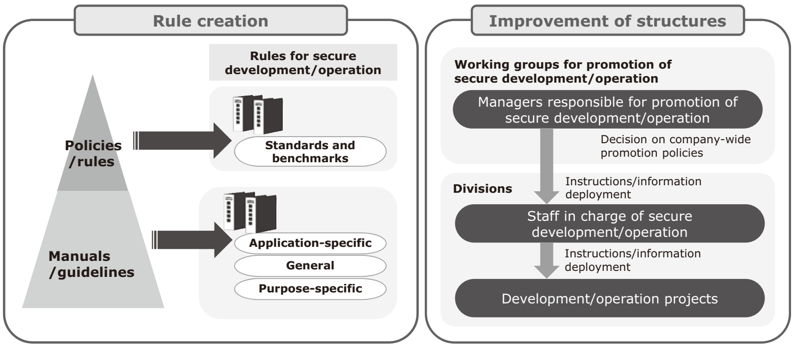

Rule creation
Rules for secure development/operation
Policies /rules
Standards and benchmarks
Manuals /guidelines
Application-specific
General
Purpose-specific
Improvement of structures
Working groups for promotion of secure development/operation
Managers responsible for promotion of secure development/operation
Decision on company-wide promotion policies
Divisions
Instructions/information deployment
Staff in charge of secure development/operation
Instructions/information deployment
Development/operation projects

Fig. 5 Support service for creation of secure development rules and establishment of structures.

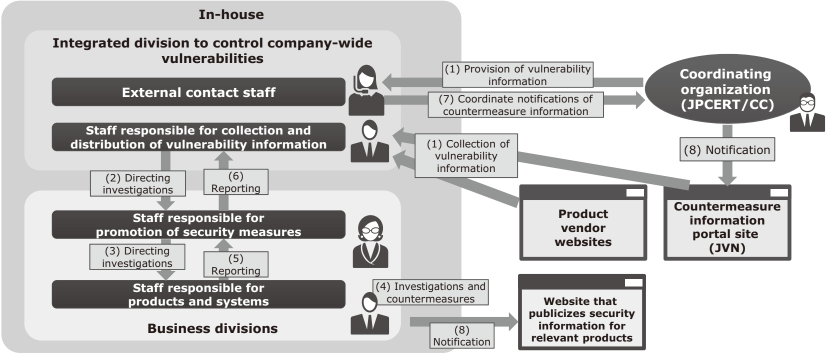
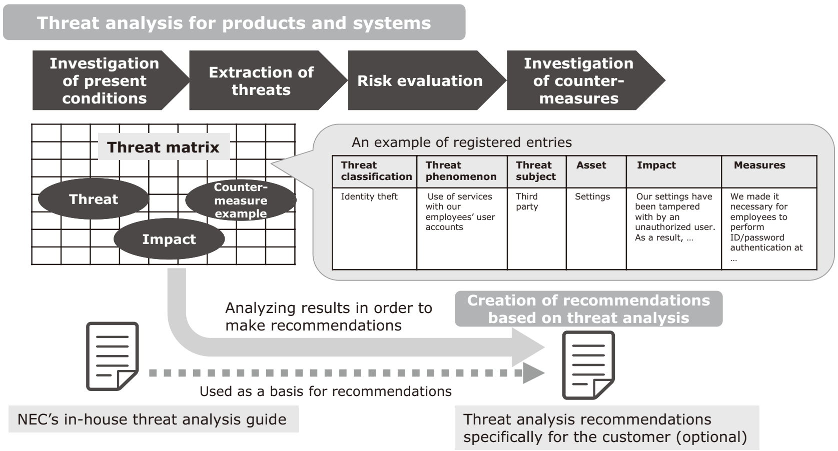

In-house
Integrated division to control company-wide vulnerabilities
External contact staff
Staff responsible for collection and distribution of vulnerability information
(2) Directing investigations
(6) Reporting
Staff responsible for promotion of security measures
(3) Directing investigations
(5) Reporting
Staff responsible for products and systems
Business divisions
(1) Provision of vulnerability information
(7) Coordinate notifications of countermeasure information
Coordinating organization (JPCERT/CC)
(8) Notification
(1) Collection of vulnerability information
Product vendor websites
Countermeasure information portal site (JVN)
(4) Investigations and countermeasures
(8) Notification
Website that publicizes security information for relevant products

Fig. 6 Support service for construction of PSIRT/vulnerability management processes.


Threat analysis for products and systems
Investigation of present conditions
Extraction of threats
Risk evaluation
Investigation of counter-measures
Threat matrix
Threat
Counter-measure example
Impact
An example of registered entries
Analyzing results in order to make recommendations
Creation of recommendations based on threat analysis
Used as a basis for recommendations
NEC's in-house threat analysis guide
Threat analysis recommendations specifically for the customer (optional)

Threat classification	Threat phenomenon	Threat subject	Asset	Impact	Measures
Identity theft	Use of services with our employees' user accounts	Third party	Settings	Our settings have been tampered with by an unauthorized user. As a result, …	We made it necessary for employees to perform ID/password authentication at …

Fig. 7 Support service for analysis of threats for products and systems.

are implemented. Based on NEC's know-how in construction and operation of a product security incident response team (PSIRT) — a taskforce to cope with vulnerabilities in a company's products and systems — this service supports the formation of PSIRTs and the construction of management processes for the customer's products and systems (**Fig. 6**).

(3) Support service for analysis of threats for products and systems

As more and more devices and systems are converted to IoT, the number of security threats are increasing exponentially. Cases where scenario-based threat analysis for the entire environment of network-connectable devices is performed are more

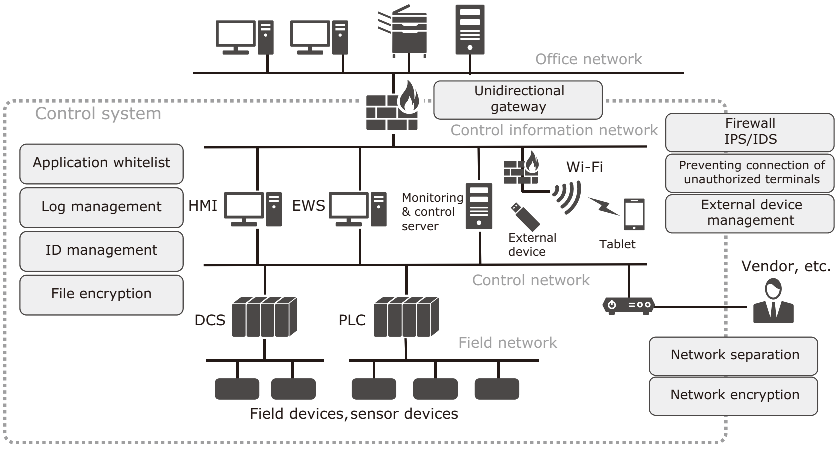


Fig. 8 Concept diagram of a control system and example of security measures.

common than ever. To help companies manage risks in this environment, NEC provides a service to help conduct threat analysis, as well as providing training of threat analysis specialists (**Fig. 7**).

4.3 Services for Control Systems

(1) Control system security assessment service

Based on IEC62443, the NIST Cybersecurity Framework, etc., which are the international standards for security of control systems, we locate security risks in terms of both organizational and system aspects, as well as indicate detected risks and propose countermeasure roadmaps.

(2) Control system security consulting service

We also provide security measures that take into consideration the specific environment and available tools. These range from construction of control systems to implementation of each phase until the system is operating successfully, management of contractors, incident detection, and countermeasures when an incident occurs (**Fig. 8**).

4.4 Interdisciplinary Services

(1) Support service for enhancing security in outsourcing companies

We support the enhancement of the security of outsourcing companies used by the customer by analyzing the present conditions in accordance with NEC's experience-based model processes for management of outsourcing companies. We also propose new processes and develop manuals to help our customers deal with the issues they are facing (**Fig. 9**).

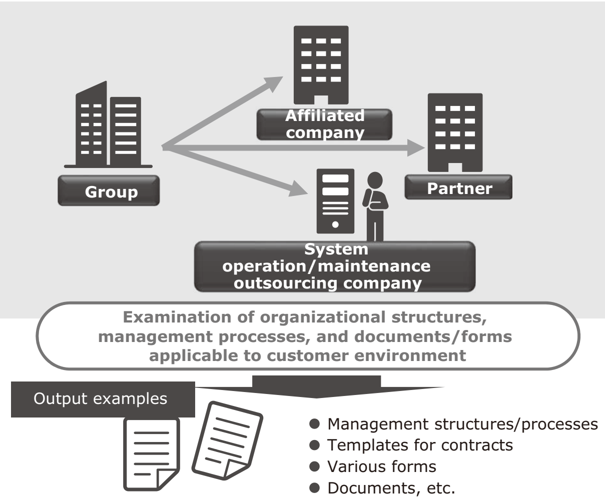

Affiliated company
Group
Partner
System operation/maintenance outsourcing company
Examination of organizational structures, management processes, and documents/forms applicable to customer environment
Output examples
● Management structures/processes
● Templates for contracts
● Various forms
● Documents, etc.

Fig. 9 Support service for enhancing security in outsourcing companies.

(2) Cybersecurity training service

We offer training menus to teach a variety of knowledge and skills — ranging from basic knowledge in information security to expert knowledge to protect information systems from illegal attacks — through lecturers and machine practices. We meet a wide spectrum of needs including specialized requirements such as incident response simulations and malware infection training, as well as generic requirements such as improvement of the security level of the entire organization.

5. Conclusion

As we have seen, NEC is offering various consulting services that support customers' security measures by leveraging our know-how — which has been gained through years of experience in our in-house information security measures, operation of CSIRTs, and our commitment to secure development and operation to ensure the security of NEC Group’s products, systems, and services.

We will continue to offer services that help solve problems in cybersecurity management and support the introduction of more sophisticated security measures.

Reference

1) The Ministry of Economy, Trade and Industry (METI): “Cybersecurity Management Guidelines”
http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guidelines_v1.1_en.pdf
2) Information-technology Promotion Agency (IPA): “Description of Cybersecurity Management Guidelines” (in Japanese)
https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html

Authors’ Profiles

YOSHIFU Kenji
Senior Manager
Cyber Security Strategy Division

ITOH Mari
Expert
Cyber Security Strategy Division

YAMADA Tomohide
Assistant Manager
Security Engineering Center
Cyber Security Strategy Division

Information about the NEC Technical Journal

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

Link to NEC Technical Journal website

Japanese

English

Vol.12 No.2 Cybersecurity

- Building Futureproof Security to Support Business Safety and Reliability -

Remarks for Special Issue on Cybersecurity
Developing Fundamental Solutions to Combat the Rise in Cybercrime: What role can a third-party all-Japan industry-academia-government organization play in containing the threat posed by cybercrime?
Trends in Cybersecurity and NEC’s Commitment to Developing Solutions

Social trends & NEC’s approach
An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures
Latest Cyberattack Trends 2017 - Model Applying NEC Cyber Threat Intelligence -
The Measures Applied Internally by the NEC Group to Forestall and Prevent Cybersecurity Incidents

Cybersecurity solutions
Security Operations Center (SOC) and Security Monitoring Services to Fight Complexity and Spread of Cyber Threats
Incident Response Solution to Minimize Attack Damage
Enhancement of Incident Handling Capabilities by Cyber Exercise
Integrated Security Management/Response Solution – “NEC Cyber Security Platform”
Cloud-based File Encryption Service – ActSecure Cloud Secure File Service –
Security LCM Services
Secure Mobile Work Solutions That Exploit EMM
Cybersecurity Consulting Services in the World of IoT

Applications of AI technology to cybersecurity
Countermeasures against Unknown Cyberattacks Using AI
The Potential of AI to Propose Security Countermeasures
Detection, Auto Analysis of Cyber Threats Using Open Source Intelligence
Cyber-Physical Integrated Analysis Technology for Criminal Investigation Support

In-house efforts provide safety and security for customers
Efforts to Provide Safe, Secure Products and Services for Customers – Secure Developments/Operations –
Talent Management: Managing Cybersecurity Human Resources

\Orchestrating a brighter world NEC
NEC Technical Journal
Cybersecurity
- Building Futureproof Security to Support Business Safety and Reliability -
Vol.12 No.2

Vol.12 No.2
January 2018

Special Issue TOP