Total Cybersecurity in the DX Era

YOSHIFU Kenji, SUZUKI Akinori, OKAZAKI Takumi, NISHINO Shinichiro, OGAWA Kenichi, USUBA Toshimitsu

Abstract

While companies and other organizations are furthering a commitment to digital transformation (DX), they are becoming increasingly vulnerable to cyberattacks, making cybersecurity a more critical management issue than ever before. To help customers better deal with this situation, NEC provides various services and DX offerings to achieve a robust security system required for DX era, while providing all sorts of solutions based on security-by-design principles, in which security is considered and built in from the planning and designing phase. By supporting DX at companies and other organizations, NEC contributes to the achievement of a safe and secure society.

Keywords
security by design, zero trust, cyber hygiene, security consulting, professional service, managed security service, security human resource development

1. Introduction

The importance of cybersecurity awareness has been increasing accompanied by the further advancement of digital transformation (hereinafter referred to as DX) at companies and other organizations.

This paper introduces the trend of cybersecurity underlying in the background and the features of NEC's cybersecurity businesses, as well as security services to support DX and our unique menu of DX Offerings.

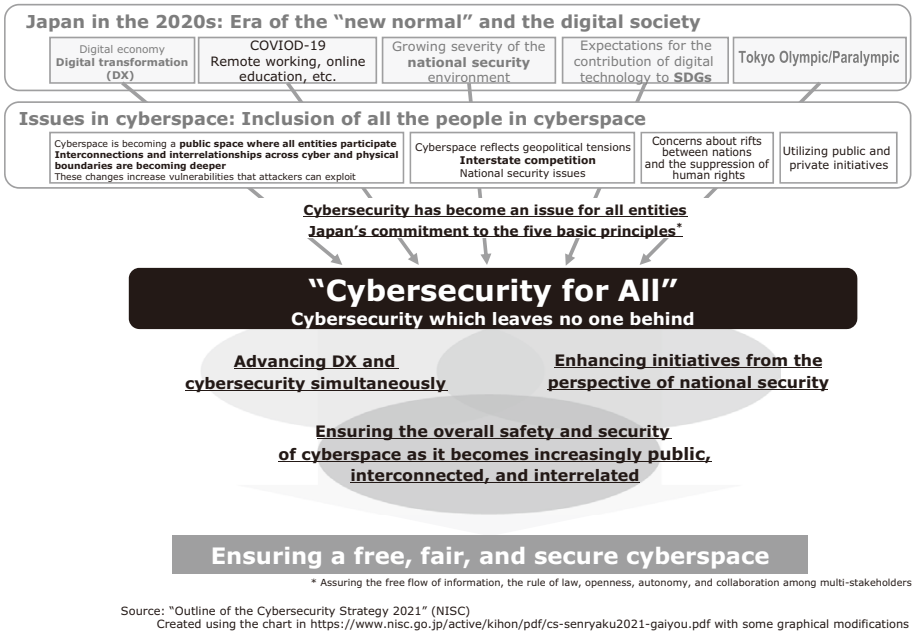
2. Trend of Cybersecurity

As companies and other organizations push forward DX, various systems are now connected with each other, further accelerating the use of PCs and other devices both in the office and remote locations. So, there are more devices connected to the Internet, and from the attacker's point of view, this means that there are more targets that can be attacked, and it is easier to penetrate more deeply into the network once they succeed in compromising the system. In addition to conventional attackers whose purpose is to get money, there are an increasing number of highly skilled attackers whose purpose is to harm the economic security of the targeted country.

Companies and other organizations are now exposed to cyberattacks that jeopardize their operations, making cybersecurity a bigger management issue than ever before.

To address these situations, the Japanese government proposes three directions including "advancing digital transformation and cybersecurity simultaneously" to ensure free, fair, and secure cyberspace in *Cybersecurity Strategy*[1)] released in September 2021 (**Fig. 1**). This report discusses the concept of security by design (SBD) that ensures cybersecurity from the stages of planning and designing systems for various tasks, products, and services and the need for concurrently promoting the commitment to digitalization and cybersecurity — that is the strategy called "DX with Cybersecurity".

In other words, companies and other organizations will be needed to achieve DX with cybersecurity and continue operations while cyberattacks are becoming more intensified and advanced. To achieve this, a mere addition of cybersecurity measures will not suffice. It is instead required that cybersecurity be considered, introduced, and operated from the stage of planning a sys-



Source: "Outline of the Cybersecurity Strategy 2021" (NISC)
Created using the chart in https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021-gaiyou.pdf with some graphical modifications

Fig. 1 Issues and directions of the Japanese government's cybersecurity strategy.

tem to be prepared for incidents and accidents that may occur in the future.

3. Features of NEC's Cybersecurity Operation

We have broken down the concept of SBD into creation of secure products, maintain security of products, and protection from attacks (**Fig. 2**) based on our belief that the topmost importance is not to stop our customers' businesses. Not only do we sell products, we also offer various services that cover the entire lifecycle of a system ranging from planning and design to development, management, and monitoring.

Whereas PCs and other devices as well as business applications all exist in-house in a conventional office environment, it should now be assumed that a company's system is accessed from devices outside the company and a third-party cloud is used in a DX and telework environment. The conventional idea of thinking that it is safe as long as the system exists in-house is no longer valid. It is now required that all the communications from devices to applications be checked to see if there is any problem in terms of security (zero trust). It is also necessary to implement an activity to eliminate vulnerability of devices and systems all the time (cyber hygiene).

Based on this concept, we have put together our knowhow and technology for products and services to solve the security issues of our customers (**Fig. 3**) and provide a menu of DX offerings. In Section 4 and thereafter, we introduce the services to be provided at each stage of system planning, building, and operation, as well as the human resources development programs which foster cybersecurity talent.

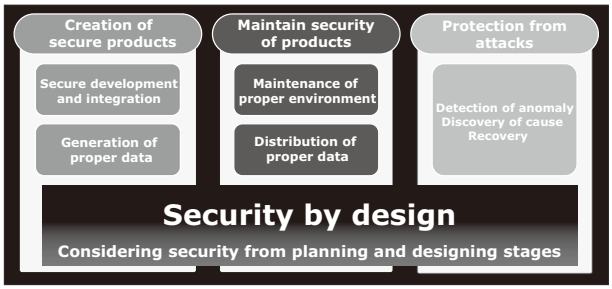


Fig. 2 Required cybersecurity measures.

4. Security Consulting Service

To achieve DX with cybersecurity, it is not enough just to provide strategies to prevent cyberattacks that are becoming increasingly sophisticated and skillful. It is also necessary — from the planning and conception stage of DX — to examine protection of privacy and basic compliance policies for security regulations and guidelines set forth by a government agency.

At NEC we offer a variety of security consulting services for information system departments (IT), product

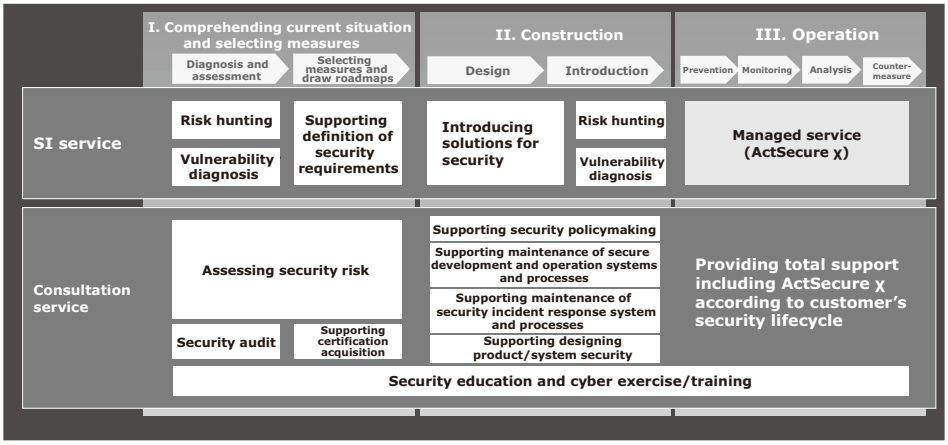


Fig. 3 NEC's security service.

development departments (IoT), and production departments (OT) of our customers who are committed to DX. These services feature: (1) utilization of knowhow gained through security measures in our in-house systems that have been built and operated for a long time, (2) numerous results of consultations by the holders of security certifications such as Certified Information Systems Security Professional (CISSP) and Registered Information Security Specialist (RISS), as well as the members of international standardization committee members, and (3) compliance with various security regulations and guidelines.

We also offer various DX-focused consultation services, including assessing security risk, supporting security policymaking, supporting maintenance of secure development and operation systems and processes, supporting maintenance of security incident response systems and processes, and supporting designing of product/system security. Now let's take a look at a case in which security assessment and maintenance of secure development processes was introduced.

One of our customers in the financial industry was having an issue of strengthening the security measure of their IT system in apprehension of risk of cyberattacks when transitioning the system to the cloud due to DX. So we conducted a security assessment (threat analysis) of the DX system and found a few dozens of vulnerabilities for threats such as spoofing and unauthorized access, making it clear that measures against threats were insufficient. Consequently, we proposed various security enhancement measures based on zero trust principles. We also supported the construction of secure development processes for their IT system based on the SBD concept. As a result, security was taken into consideration from the upstream stage of the development of their newly developed IT system, thereby reducing the number of vulnerabilities detected in testing processes and operation stages and reducing backtracking man-hours.

In addition to this case, we have also contributed to the strengthening of security by supporting secure IoT product development in manufacturing and OT policymaking in critical infrastructure.

5. Professional Service

This is a total support service by our security professionals that supports a wide range of stages from planning and design to construction and operation.

To achieve the above-mentioned zero trust and cyber hygiene, it is not the best way to introduce products and services individually. It is necessary to properly set products and services and having them operate in concert in order to perform continuous and secure observation of the system communications and eliminate their vulnerabilities.

This requires advanced expert knowledge regarding design, construction, and operation in security. The lack of this knowledge may cause security risk due to erroneous setting, for example.

The Professional Service offers risk-related support and features the following.

- Supporting design, construction, and operation based on the SBD concept.
- Leveraging the expertise of experienced engineers who have introduced, built, and operated numerous products

Taking advantage of the wealth of knowledge, we provide a menu of DX offerings that helps achieve prompt introduction of security measures. For instance, we of-

fer the Professional Service to help introduce the cloud security edge (Zscaler Internet Access) service. This supports a series of operations including hearing requirements, setting parameters, and implementing and testing a system, as well as giving operational instructions to customers' administrators, pertaining to Zscaler Internet Access designed to build a secure Internet access environment. We also provide a menu of DX offerings for Microsoft's cloud services.

In the future, we will add operation support services to the Professional Service to continue to provide total support. At the same time, we will continuously improve our menu of DX offerings and security services that help our customers shift to cloud services of providers such as Microsoft and AWS.

6. Managed Security Service

In addition to firewalls that are already subjects of monitoring, devices brought outside the office by employees (endpoints) and their access operations to clouds now need to be monitored critically due to the increase of telework and shifting to clouds-based workstyle. This has resulted in further advancement in security management and monitoring operations and increased workload as well. NEC offers managed security services that address these issues.

The ActSecure χ Managed Security Services (**Fig. 4**) support our customers' safe use of clouds by monitoring security logs from clouds to endpoints.

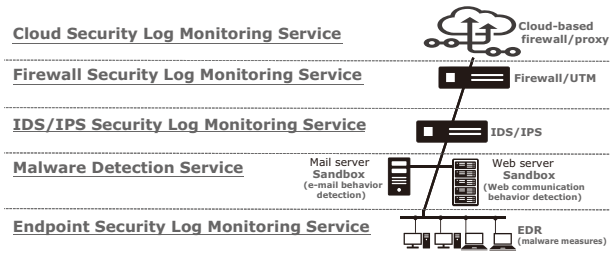


Fig. 4 ActSecure χ Managed Security Services.

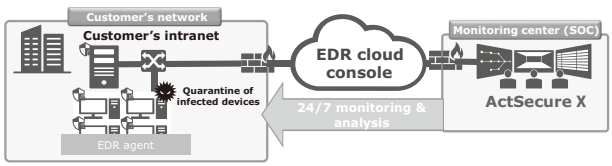


Fig. 5 Endpoint Security Log Monitoring Service.

One of our DX offerings, the Cloud Security Log Monitoring Service monitors alerts generated from firewall/proxy services on clouds. When alerts are detected, their importance is judged and reported to the customer. In the meantime, the communications for which alerts are generated are blocked. Besides, the Endpoint Security Log Monitoring Service (planned for release) judges the importance of alerts generated from security tools installed on devices and promptly implement initial measures such as quarantine of devices and interruption of suspicious processes (**Fig. 5**).

The ActSecure χ Managed Security Services combine our proprietary intelligence employed for monitoring NEC offices, AI and security analysts. In consequence, it offers quick and efficient monitoring at high precision on a 24/7 basis and support the improvement of our customers' security.

7. Security Human Resource Development

In order that companies and other organizations may accelerate DX securely, it is essential to develop adequate human resources. They are expected to promote the design and implementation of security of systems based on the SBD concept and to execute them in practice. Many of security exercises, however, focus on follow-up measures after the occurrence of an incident. So NEC Group has developed practical exercises to incorporate security design and implementation effectively and incorporated them into the human resource development program (**Fig. 6**).

Taking the initiative in the industry, NEC launched a permanent exercise environment for system engineers called the NEC Cybersecurity Training Ground in 2019. Since then, more than 2,800 people participated in this program. The participants learn the importance of secure construction through the experience of first building their own robust systems with secure architectures, and then going through an exercise in which their system is actually attacked. Then they carefully review their experiences and acquire practical security design and implementation capabilities and incident response skills.

Also we have been holding an in-house contest called NEC Security Skill Challenge, in which more than 5,000 people have participated since 2015, to visualize the skills of our employees. The results are linked to professional profiles systemized by governmental and industrial institutions* to find and train potential candidates for security personnel.

* Security Body of Knowledge (SecBoK) human resource skill map (NPO Japan Network Security Association), i Competency Dictionary (Information-technology Promotion Agency, Japan), etc.

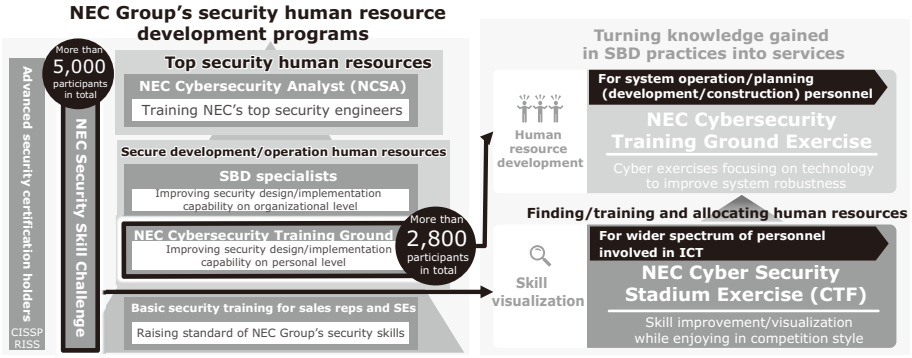


Fig. 6 NEC Group's security human resource development programs.

What's more, we have turned these practical training programs provided for NEC Group engineers into services in the menu of DX offerings available to customers. They are NEC Cybersecurity Training Ground Exercise and NEC Cybersecurity Stadium Exercise, which is a capture-the-flag (CTF) competition. By using these services, our customers can improve their practical skills to build secure architecture and take incident prevention measures as well as find and develop employees who have potential skills.

For example, we conducted the NEC Cybersecurity Training Ground Exercise at Tokyo's Shinjuku City Office using a version customized to their needs. The result not only exhibited improved skills of the city office personnel but also their increased awareness in operational issues they face such as information sharing.

8. Conclusion

This paper has discussed the increasing importance of cybersecurity accompanied by the advancement of DX, the need for companies to introduce comprehensive security measures from planning to operation based on the SBD concept, as well as a variety of NEC's security services and DX offerings that meet that need. While continuing to support DX at companies and other organizations, NEC will contribute to the achievement of a safe and secure society.

* CISSP is a registered trademark of International Information Systems Security Certification Consortium.
* Microsoft is a registered trademark or a trademark of Microsoft Corporation in the U.S. and other countries.
* All other company names and product names that appear in this paper are trademarks or registered trademarks of their respective companies.

Reference

1) National Center of Incident readiness and Strategy for Cybersecurity: Japan's Cybersecurity Strategy 2021 (Overview), September 2021
https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-gaiyou-en.pdf

Authors' Profiles

YOSHIFU Kenji
Senior Expert
DX Strategy Consulting Division

SUZUKI Akinori
Senior Expert
Cyber Security Division

OKAZAKI Takumi
Manager
Cyber Security Division

NISHINO Shinichiro
Manager
Cyber Security Strategy Division

OGAWA Kenichi
Assistant Manager
Cyber Security Division

USUBA Toshimitsu
Assistant Manager
Cyber Security Strategy Division

The details about this paper can be seen at the following.

Related URL:

Professional Security Services (Japanese)
https://jpn.nec.com/cybersecurity/professionalservice/index.html

ActSecure χ Managed Security Services (Japanese)
https://jpn.nec.com/actsecure/actsx_mss.html

Security Education and Cyber Training (Japanese)
https://jpn.nec.com/cybersecurity/professionalservice/education/index.html

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.16 No.2 Special Issue on DX Offerings to Accelerate the Digital Transformation of Society

Papers for Special Issue

NEC Information

Vol.16 No.2
June 2022

Special Issue TOP