Talent Management: Managing Cybersecurity Human Resources

MINEGISHI Makoto

Abstract

For several years now, NEC has been actively working to augment cybersecurity human resources. These efforts include promoting the expansion/deployment of training programs, improving the NEC Certified Professional (NCP) system, and encouraging the acquisition of certifications such as Certified Information Systems Security Professional (CISSP) and Registered Information Security Specialist (RISS). In this paper, we will review these policies and discuss our "talent management" program, that is, how we manage our cybersecurity human resources at the NEC Group including management of career paths and human resource exchanges.

Keywords

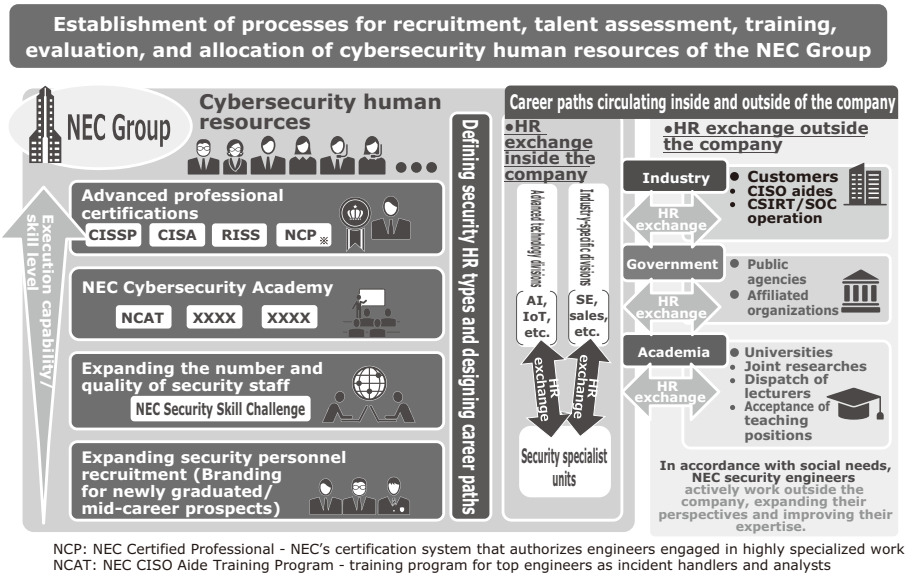
cybersecurity human resources, human resource training programs, NEC Certified Professional (NCP), Capture the Flag (CTF), Certified Information Systems Security Professional (CISSP)

1. Introduction — NEC Group Talent Management

The importance of talent management has been a big topic lately in the HR industry and at relevant conferences and events. The definition of talent management varies. The Society for Human Resource Management (SHRM), the world's largest HR professional society in the United States, has defined talent management as "the implementation of integrated strategies or systems designed to improve processes for recruiting, developing and retaining people with the required skills and aptitude to meet current and future organizational needs." NEC interprets talent management as the achievement of compatibility between overall business expansion and individual career formation. This involves evaluating and appropriately allocating personnel after finding, recruiting and training them in accordance with the strategic requirements of the organization as noted in the SHRM's definition (**Fig. 1**).

It has been quite a while since NEC first established its policies for talent management of professional human resources. For example, the NCP certification system is a system that authorizes high-achieving professionals with high market value based on their technological expertise. At the same time, this system also enables individual workers to take charge of their own careers by determining their career path goals and by defining the experience and skills needed to achieve those goals. Moreover, this system provides a process framework that enables staff to adjust their mid-term career plans and transfer requests with their superiors — through a career review (performed once a year) and other programs (**Fig. 2**).

Meanwhile, it is important to train personnel — who will create social value as cyber professionals working in advanced technologies such as AI, data science, and IoT — on the basis of talent management systems that are common company-wide. It is also important to establish talent management systems specific to the various fields of technical expertise and to the business strategies of the company. Below, we discuss best practices for talent management of professional human resources, focusing specifically on cybersecurity.



NCP: NEC Certified Professional - NEC's certification system that authorizes engineers engaged in highly specialized work
NCAT: NEC CISO Aide Training Program - training program for top engineers as incident handlers and analysts

Fig. 1 Talent management of cybersecurity human resources.

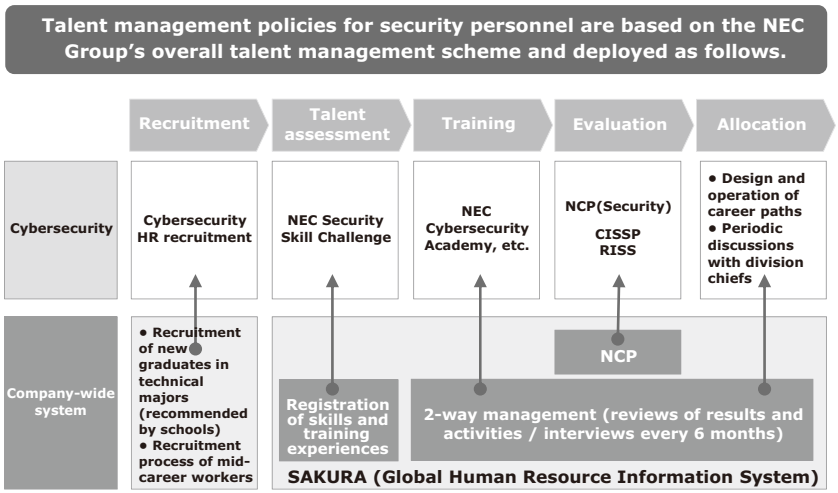


Fig. 2 How cybersecurity HR talent management is linked with NEC's overall scheme.

2. Talent Management of Cybersecurity Human Resources

2.1 Collaboration with the NEC Group's Cybersecurity-Related Organizations

NEC has various divisions engaged in cybersecurity operations and technologies. They include a cybersecurity-related product development division, marketing division, integration division, consulting division, etc.

In some cases, security teams are embedded in business units and divisions dedicated to specific industries. In addition, many NEC Group companies have their own cybersecurity engineers to share and promote security operations that take advantage of their respective strengths.

2.2 Acquisition of Cybersecurity Human Resources

As noted above, many different divisions now require security personnel. To supply those needs, the Cyber Security Strategy Division serves as the core recruiting structure, targeting new graduates and mid-career workers and introducing prospective candidates to the divisions and proposing the best matches among those candidates. Key aspects of this strategy include: (1) classification of human resource requirements in

each division, (2) application of a go-to-market (GTM) strategy for recruitment activities, and (3) execution of planning and management of recruitment events. For example, when recruiting mid-career workers, we not only use employment agencies but also engage in direct sourcing that utilizes staffing databases. When recruiting new graduates, we run an internship program that lasts for about two weeks, as well as career supporting events. Through such endeavors, we strive to persuade new graduates who aspire to become cybersecurity engineers and mid-career workers who can immediately become valuable assets to NEC's cybersecurity operations to join us after explaining to them the positioning (importance) of NEC's cybersecurity operations and outlining the wide range of career paths NEC has to offer.

2.3 Expanding and Discovering Cybersecurity Human Resources

The NEC Group has about 40,000 SEs and software developers. Although they are not cybersecurity engineers, they are responsible for secure design and development of systems when they carry out their duties of SI and service operations. Moreover, because many of them have a background in networks, OSs, and programming, they have excellent potential as cybersecurity engineers. In order to expand the range of cybersecurity human resources and discover competent people, we hold a competition called the NEC Security Skill Challenge (**Fig. 3**).

This competition takes the form of an online capture the flag (CTF) game. The degree of difficulty is set at a level suitable for beginners in cybersecurity, rather than at a level where security experts compete with each other to improve their skills. This is because the main purpose of this competition is to expand the range of cybersecurity human resources. We also put an emphasis on training. For example, we try to encourage beginners to learn on their own by allowing them to look at the hints and answers.

The NEC Security Skill Challenge started in FY 2015. More than 1,000 NEC Group employees participated in FY 2016. Among them, about 70% were SEs and software developers. We believe that by continuing this competition we can contribute to the improvement of the skills of the personnel who participate.

2.4 Training Cybersecurity Human Resources

NEC has been running human resource training programs pertaining to basic security technology, security risk assessment, vulnerability diagnosis, and secure development/operation at the Security Technology Center of the Cyber Security Strategy Division for several years now. A wide range of training programs including analysis regarding cybersecurity and incident handling are also deployed also at NEC Management Partner and NEC Solution Innovators.

After systemizing these training programs, we established the NEC Cyber Security Academy which offers both lectures and basic training exercises. Moreover, we have also established a program — called NCAT which stands for NEC CISO Aide Training — to train core personnel for NEC's cybersecurity service operations. Designed to offer advanced courses, NCAT offers elite training courses at the NEC Cyber Security Academy that incorporate advanced exercises as well as on-the-job training at security-specialized organizations. In addition to skills of personnel defined as a mediator by the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), the NCAT programs consist of programs to improve the skills of security analysts and incident handlers required by security vendors. We are deliberately assigning our NCAT-trained personnel to positions that will enable them to further improve their

An internal CTF competition is held by the volunteer committee. The purpose of this competition is to discover a competent segment of workers and to utilize the results for quantitative parameters for training security human resources. CTF:Capture The Flag

Period held	2 weeks (February 1 to 14)
Number of participants	**More than 1,000** Workers engaged in non-security tasks: **700** Workers involved in security operations: 300
Participation style	Online (Accessible from home) Individual matches
Number of questions	100
Categories	OS, network, web, apps, accident analysis, encryption, binary, miscellaneous, trivia

<Top screen>

<Ending ceremony>

Fig. 3 NEC Security Skill Challenge.

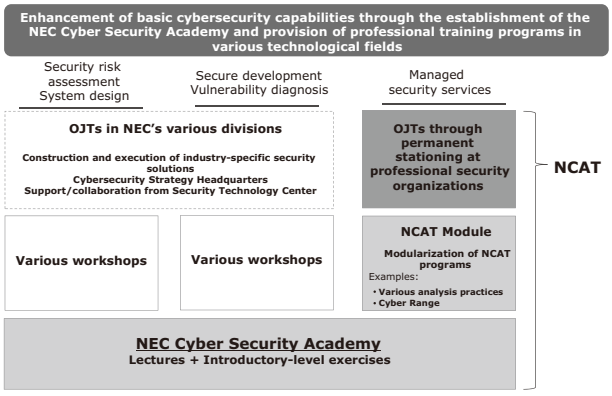


Fig. 4 NEC security personnel training system.

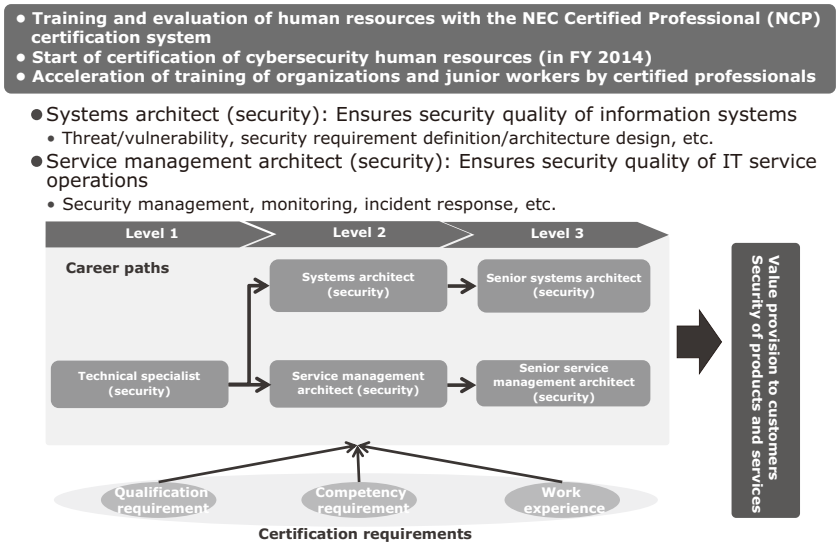


Fig. 5 Advanced professional certifications.

skills as cybersecurity engineers by proving support to government agencies and major corporations, as well as participating in various projects (**Fig. 4**).

2.5 Evaluation of Cybersecurity Human Resources

Now, let's take a general look at how we certify personnel who can play active roles as advanced professionals from among those who have substantial experience (**Fig. 5**). As mentioned in section 1, NEC certifies advanced professionals in the NCP certification system. As for security engineers, NEC also certifies professionals in areas of SI and service design/operation.

In addition, the NEC Group has a few dozen employees who have received Certified Information Systems Security Professional (CISSP) certification — which is an internationally recognized certification. There are also several hundred employees certified as a Registered Information Security Specialist (RISS) — a Japanese certification. All of these cybersecurity professionals are contributing to the expansion of NEC's security business operations.

3. Conclusion
— Career Paths (Allocations) of Cybersecurity Human Resources

As we have seen, NEC is reinforcing cybersecurity human resources through discovery, acquisition, development, training, and evaluation of candidates. Now, we examine how we help them forge their own career paths while they contribute to our operations. We think that the career paths of the cybersecurity human resources at the NEC Group have, when roughly divided, three major features (**Fig. 6**).

First of all, cybersecurity specialists need to be turned into multi-skilled workers. The NEC Group is fully equipped with various functions and solutions for cybersecurity — such as marketing, business development, R&D, consulting, SI, administration, etc. Thanks to this versatility, our security engineers can experience various occupational types without limiting themselves to specific types of jobs. For example, a worker who joined us as a developer of security products can be grown into an analyst, and a worker who was responsible for security design can become a consultant or business developer. In other words, our workers can improve their comprehensive competencies by experiencing multiple types of job positions in the operational domain of cybersecurity.

Secondly, we have active personnel exchanges with industry-specific SI and service businesses and other advanced technology fields. For example, there are cases in which industry-specific SEs learn security skills and start a double career as SEs who are versed in security. We are also beginning to see cases where security engineers encounter leading-edge technology such as AI, data science, and IoT and eventually create new architectures and innovative solutions. By working with businesses in other fields and by becoming adept with different types of technology, cybersecurity engineers are able to play active roles across a much broader range of fields than ever.

Third and finally, the establishment of career paths that circulate outside and inside the company is now becoming popular. When certain projects and clients call

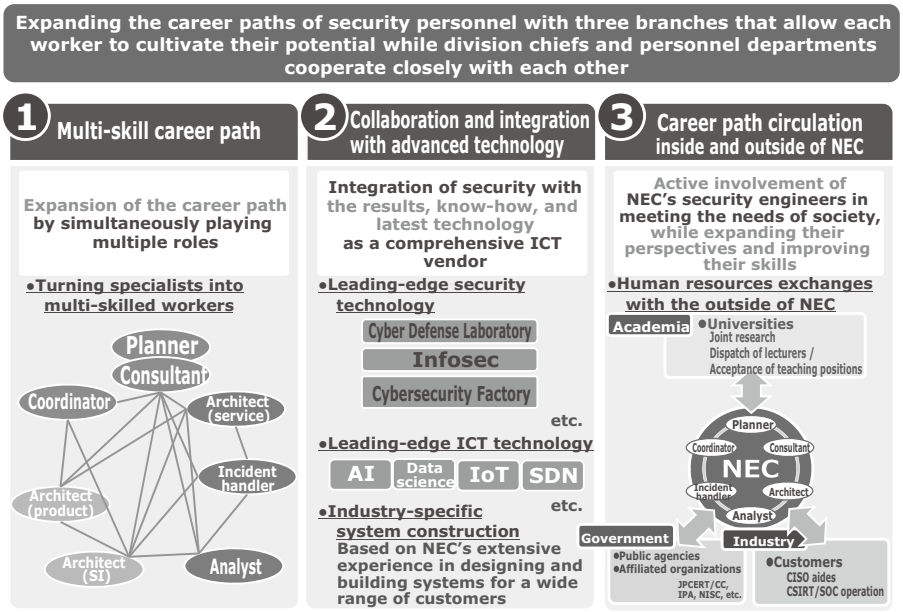


Fig. 6 Expansion of career paths.

on us, the NEC Group security engineers are dispatched to government agencies, various affiliated organizations, and major corporations where they help implement security operations and establish security policies. We have also recently begun dispatching them as lecturers to society meetings and various universities, as well as in placing them as instructors at universities. In this way, we are creating a favorable circulation of expansion and improvement of the NEC Group's cybersecurity operations by not confining our engineers to the NEC Group, but rather by encouraging them to be active in the wider world so that they can come back to us with an expanded horizon and broader perspective.

As we have discussed, NEC develops the human resources needed for cybersecurity operations by rotating the cycle of discovery, acquisition, development, evaluation, and allocation to expand the potential of the career of each employee in this field. That's the framework of our talent management of cybersecurity human resources. We will continue to contribute to operations from a human perspective by further advancing this cycle of talent management, while working collaboratively with various division chiefs and experts in relevant fields.

Authors' Profiles

MINEGISHI Makoto
Manager
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 -

Vol.12 No.2
January 2018

Special Issue TOP