■ Hiroki Takakura, Professor, Information Systems Architecture Science Research Division

## 【Cyber Security Research to Prepare for the Dark Side Rather Than the Light Side】

I was more of a humanities type when I was in high school, but my interest in amateur radio grew, and I eventually ended up going to a university and studying in the information engineering department. By chance, my graduation research project involved computer research. I worked in various fields after that before starting research in cyber security ("security") as an associate professor. That's the research I'm currently involved in. Security requires a broad range of knowledge, so the past experience and knowledge I've acquired continue to help me even today, including the experience and knowledge gained through my interests in the humanities.

### Today's Internet Where Even Cars Are Hijacked

Universities and research institutions handle a great deal of information, including personal information related to education, like student addresses and grades, and other information that has to be protected, like information related to research and information related to organizations and administration. In response to the risks of various cyber attacks, universities and research institutions have to anticipate and make advance preparations. When problems occur, they have to respond right away to minimize the damage. This was my area of research in the 2000s.

However, entering the current decade, there's been a lot of activity in the area of the Internet of Things, or IoT, which seeks to connect just about everything to the Internet and to implement sensing and control through Internet communications. In the US, which was especially fast to jump into this area, even electronic billboards on freeways, cars, coffee makers, TVs, and control systems at chemical plants are directly connected to the Internet. Of course, measures have been taken to ensure that—for example—the engine control of a car won't be affected even if its navigation system is subject to a cyber attack. But if the considerations by the developer aren't rigorous, someone launching a cyber attack could actually seize control of the car. Attacks like this have actually occurred and led to the recall of several million cars.

In Japan, due to Internet conditions and differences in ways of thinking among manufacturers, dangerous situations like this haven't happened so far, fortunately, though various problems do occur. But given the march of globalization, we can't afford to let our guard down.

## A Focus on Training the Necessary Personnel and Training Methods

One of the most serious problems in Japan right now with respect to security is personnel training. Some people of exceptional technical ability emerge from time to time, but often there's no opportunity to acquire management skills. What's in short supply right now in Japan are personnel who understand the technologies and the job types of capable engineers, who can make the best use of those engineers' talents, and who have a certain degree of knowledge and understanding of technology, law, and management. These abilities allow them to explain security-related information to corporate management in a way that's easy to comprehend, which would allow use of the information to help make management-related decisions. In Europe, North America, and South Korea, they already have courses of study for training security management personnel, which are different from those for training engineers. There's probably a limit to the Japanese style cultivation of human resources, where there's a sense that if you train hard as an engineer, the management ability will follow.

In the world of security, things never start perfectly and continue to be perfect after that. The reality is somewhere between absolutely secure and completely at risk. For both security and the training of security personnel, I believe we need to move forward while striking a balance between the two.

(Article researched and organized by Yoshiko Miwa)