Overview

Hitachi's Efforts to Optimize Security in the Post-COVID-19 Societies

Tatsuya Yoshida
Yoshinori Ikeda

1. Introduction

Companies have recently been turning to the use of public clouds such as Amazon Web Services[*1] and Microsoft Azure[*2].

Although the COVID-19 pandemic has made it even more widespread, this trend has been on the rise for years as the result of factors such as companies reducing their on-premises system management loads, and work styles becoming less tied to specific locations.

For security purposes, office work is traditionally seen as an activity done by employees, partners, and other designated parties coming together at an office or other designated location to perform operations using designated equipment provided by the company. So security has always been an activity done by bringing people together at an office to ensure the safety of confidential information and other assets.

Meanwhile, the rapid rise of remote work has overturned all these assumptions—with non-company workplaces now mainstream, it has become possible in theory for anyone to access their work on a public cloud via a public network. Some companies have also started to permit the use of the bring-your-own-device (BYOD) work style where employees use devices that they personally own (or acquire).

These developments have been accompanied by a corresponding rise in awareness of the concept of zero trust—a lack of trust in connections from any device or person.

Since zero-trust environments permit access by anyone from anywhere, they require more powerful personal authentication than was previously needed. A group of designated people must be present in the office. Password authentication has usually been used for authentication in the past. While there is a need for advanced password authentication, it creates a tradeoff between security and convenience as increasingly complex passwords tend to lower convenience. Users have been heavily burdened by the need to use a different complex password for each security need, along with frequent password change requests. This problem is resulting in a recent shift toward biometric authentication technology-based multifactor authentication and other methods designed for both security and convenience.

For system administrators, migrating systems to cloud environments has enabled log displays and automated analysis while also facilitating security monitoring to enable system-wide security augmentation and labor-saving. These benefits are also assisting behavior detection and other new methods of combating cyberattacks.

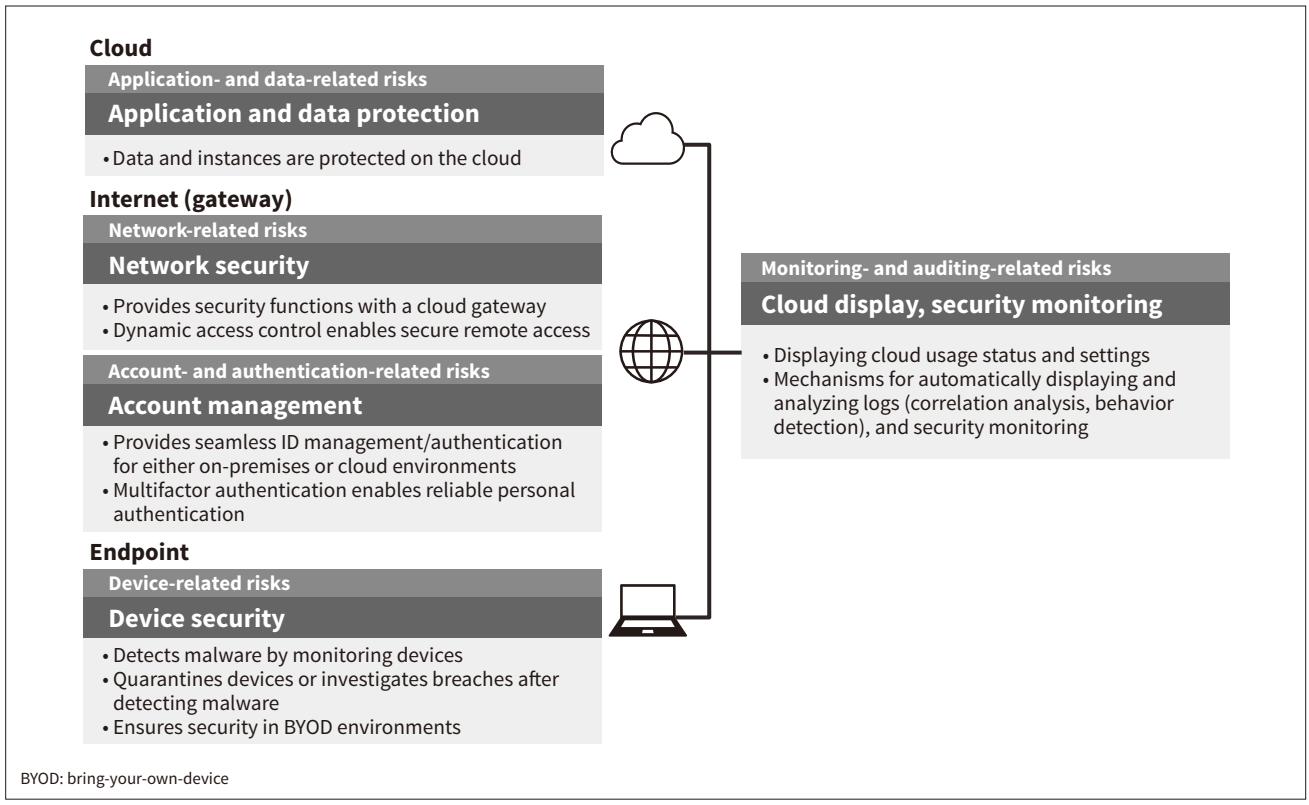
The increasing use of the cloud is also resulting in the growth of outsourced monitoring work, with some providers able to offer advanced and rapid expert analysis and responses.

While discussions of the benefits of cloud and open network environments tend to focus on the risk of attacks from outside, these environments are also evolving in a way that is generating benefits from augmented security for both system operators and users (see **Figure 1**).

*1 Amazon Web Services is a trademark or registered trademark of Amazon.com, Inc. or its affiliates in the US and other countries.
*2 Microsoft Azure is a trademark or registered trademark of Microsoft Corporation or its affiliates in the US and other countries.

Figure 1 — Main Security Measures Used by Zero Trust

The zero-trust concept uses security measures in the cloud, Internet (gateway), and endpoint domains. It provides overall system transparency and security monitoring.



2. Real-world Impact of Increasing Diversity of Attack Victims

Cyberattacks have recently begun to have real-world impacts, bringing security issues to a new level of severity.

Ransomware is a common type of cyberattack. Most of the damage caused by it was previously limited to electronic data, but it has recently started to cause other types of damage as well. Cyberattacks in the USA caused many problems in the first half of 2021 alone. There were attacks with major impacts on the oil supply, along with attacks on water facilities involving unauthorized operation of drinking water component adjustment systems by remote control.

Many of the control systems underpinning this type of public infrastructure have so far tended to not actively embrace security measures due to their nature as special systems or closed systems. However, it has now become essential for these systems to take the same security measures as IT systems due to the occurrence of advanced persistent threats (APTs) and other special types of attacks that identify their targets, along with real damage caused to economic activities and daily life.

Many facility sites use security measures that conform to the IEC 62443 series of security standards for control systems. The IEC 62443 series covers the security functions of control systems and the components themselves. It also covers development processes used by control system and component developers, along with the management and operation processes of control system operators.

The same trend is occurring among the wide array of devices compatible with the Internet of Things (IoT). In the auto industry for example, the number of computer-controlled components has grown so much that semiconductor supply problems are being reported in the media. This growth is resulting in over-the-air (OTA) and other methods of wireless software updates becoming commonplace. Initiatives anticipating autonomous driving in the future have emerged as a result. Regulations have been specified by the World Forum for Harmonization of Vehicle Regulations Working Party 29 (WP29), and international standards such as ISO/SAE 21434 have been created. Automotive manufacturers and suppliers are also being called on to devise measures for handling product security (see **Figure 2**). The world is entering an era in which security measures will be needed for a wide array of devices as components once seen as unrelated to computing rapidly become part of IoT systems.

3. Hitachi's Security Project Work

As mentioned above, modern security requires measures for a wide array of devices in areas such as operational

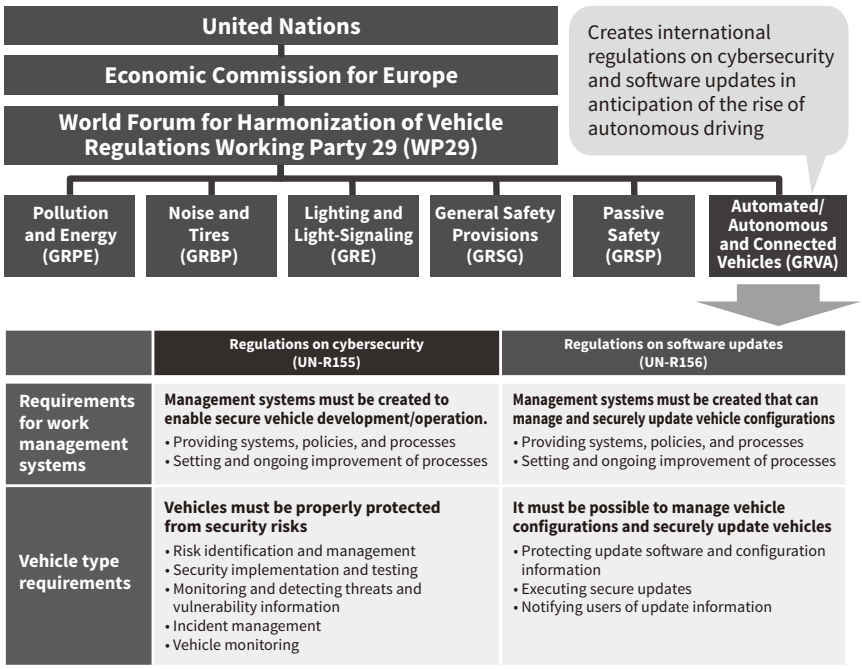


Figure 2 — Overview of Automotive Cybersecurity Standards

The World Forum for Harmonization of Vehicle Regulations Working Party 29 (WP29) has created security standards for today's increasingly connected vehicles.

technology (OT) and the IoT as well as just IT. It's important to implement these security measures by using multiple connected methods rather than just using a single solution.

Hitachi is working to solve this issue by creating an organization for coordinating the work done among business units within the Hitachi Group. It will unify the group's security solutions and enable teamwork for providing security and safety (see **Figure 3**).

Hitachi has the following three strengths in the security domain:

(1) Security knowledge protecting the global IT infrastructure of about 350,000 Hitachi Group employees
(2) In-depth domain-specific expertise in a wide range of business areas (IT, OT, and IoT systems in various areas)
(3) In-house development of original biometric authentication technologies that underpin the core security process of authentication

Hitachi believes that implementing advanced security takes more than just a high level of security technology. It also takes a detailed understanding of the business areas

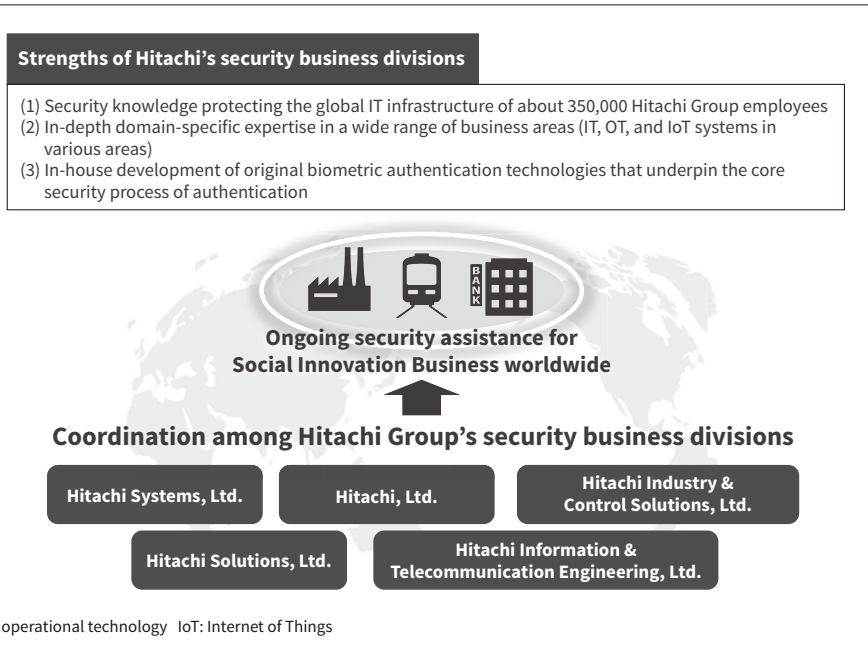


Figure 3 — Coordination among Hitachi Group's Security Business Divisions

The Hitachi Group's security business divisions work as a team to carry out and improve security-related work.

and systems it is being added to, along with convenience and continuity during actual use.

So by drawing on a track record of building and operating many different public infrastructure facilities, Hitachi provides clients with practical security measures using cybersecurity technology underpinning about 350,000 Hitachi employees along with knowledge gained through organizations such as Security Operation Centers (SOCs) and Security Incident Response Teams (SIRTs). These measures also include physical security technologies such as surveillance cameras and access control systems. Customer assets are protected from various threats in a multifaceted manner by combining solutions that use facial recognition or behavior detection technologies to discover suspicious people or objects and prevent behaviors. In the future, Hitachi will provide security solutions that go beyond just protection. These solutions will help enable safer or more efficient work processes by drawing on experts with advanced knowledge and experience and artificial intelligence (AI) driven log analysis/behavior detection technology.

4. Privacy Protection and Ethics Considerations Arising from Fusion of Security and AI

The security industry has recently been using AI to achieve more advanced risk detection for both cybersecurity and physical security. For cybersecurity, it has become possible to identify unknown malware by detecting the type of behaviors exhibited by programs. For physical security, it has become possible to use AI for new economic activities such as marketing driven by facial recognition or history analysis.

Meanwhile, these uses also require consideration of privacy and other ethics concerns. When using the physical security technology mentioned above for example, surveillance cameras that previously only provided monitoring can be combined with AI to enable authentication of individuals. While this technology is effective for detecting suspicious people, it also enables behavior tracing of individuals by technological means. Cases of misidentification resulting in innocent people being excluded from event venues have already come to light, and critics warn that combining security technology and AI might lead to various problems in future.

Countries around the world are responding by creating guidelines on ethical AI use. In February 2021, Hitachi created "Principles guiding the ethical use of AI in Social Innovation Business." They are designed to ensure well thought-out handling of the issues accompanying today's increasingly diverse and complex AI.

Proper handling of privacy information such as personal authentication and behaviors is a key element in many different systems. Hitachi is continually working to provide effective measures by drawing on many years of expertise in privacy protection measures along with cybersecurity and physical security technologies to create systems that do not infringe on personal privacy or interests.

5. Conclusions

Today's world of radically changing lifestyles and working styles demands security measures that continually evolve as security grows in importance. Cybersecurity and physical security have now become more than just expenses required to prevent attacks. They have transformed into measures used as tools to generate next-generation innovations such as new work styles made possible by the zero-trust concept.

Hitachi will continue to evolve and help innovate the world as a way of providing customers with the security technologies and solutions presented in this feature while offering security, safety, and a high level of convenience in the post-COVID-19 societies.

References

1) Hitachi News Release, "Hitachi Establishes Principles Guiding the Ethical Use of AI in Its Social Innovation Business" (Feb. 2021), https://www.hitachi.com/New/cnews/month/2021/02/210222.html

2) Hitachi, Ltd., "The Trend in Standardization of ICS Security System —The Introduction and Updates of IEC 62443—" (Feb. 2020) in Japanese, https://www.jpcert.or.jp/present/2020/ICSR2020_04_HITACHI.pdf

Authors

Tatsuya Yoshida
Security Business Division, Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research:* Cybersecurity sales and marketing. *Certifications*: CISSP.

Yoshinori Ikeda
Smart Infrastructure Consulting Department (2nd), Hitachi Consulting Co., Ltd. *Current work and research:* Cyber-security strategy consulting. *Certifications*: Registered Information Security Specialist.