Hitachi’s Initiatives for Cyber Resilience

While the massive amounts of highly diverse data produced by the digital economy generate value, threats to safety and security have also risen dramatically. Radical changes in work styles such as the recent rise of remote work accompanying the COVID-19 pandemic are also creating the need for security reforms. To enhance cyber resilience in anticipation of the world of the “new normal,” Hitachi is currently working on a lineup of cybersecurity strategies that can be thematically divided into the areas of governance, co-creating security, and “*jibungoto*” (taking ownership). This article looks at these strategies.

Atsushi Murayama
Takeshi Nishimura
Mari Watanabe

1. Introduction

Digital transformation (DX) and work style reforms are two recent trends in the corporate world that have important ramifications for security. DX security measures need to be designed differently from the traditional measures centered around on-premises environments. They should support today’s rapidly growing Internet of Things (IoT) and artificial intelligence (AI) technologies, along with IT platform cloud use and digitalization at production, manufacturing, and development sites. The probability of attacks will likely rise significantly as the devices connected to these cloud platforms become increasingly diverse and commonplace. Security measures for work style reforms need to enable work to be done efficiently and securely when the spread of COVID-19 forces companies to adopt new work styles.

Next, looking back, FY2020 was an eventful year for security threats. Targeted attacks are becoming more advanced and varied than ever. Conventional attack methods are being used together in combination, such as by using ransomware-based threat methods for information theft. Social infrastructure has also experienced many large-scale attacks.

Flexibly adapting to a radically changing environment and responding effectively to the recent risks of cyberattacks will require the creation of cybersecurity strategies that analyze these risks proactively while enhancing cyber resilience premised on the understanding that cyberattacks will impact business.

This article describes how Hitachi is responding to the current environment by working to enhance cyber resilience. The discussion is thematically divided into the areas of governance, co-creating security, and “*jibungoto*” (taking ownership).

2. Governance: Zero Trust Security Initiatives

The general concept behind these initiatives is the ongoing and steady execution of security measures that treat cybersecurity as a management issue. These measures recognize that perfect security does not exist, while providing enough resilience to enable rapid recovery in the event of an incident. The work done to actualize this concept is described here.

Hitachi has implemented a number of measures to combat security risks such as the targeted attacks that have recently become mainstream. In 2011, the company responded to the rise of targeted attacks by improving measures to combat information theft at interfaces. Then, in 2017, Hitachi responded to WannaCry ransomware incidents by improving measures against system destruction, and worked on improving security governance by defining cybersecurity as a management issue.

The company is now starting work on new security measures in response to worldwide trends and increasingly advanced and complex cyberattacks. Central to these efforts is the implementation of zero trust security measures being put in place as IT platforms are moved to the cloud.

When implementing these measures, the increasing use of cloud-based business systems and the trend toward work style reforms led to a major change in approach resulting from the realization that the conventional perimeter-based IT infrastructure design would need to be transformed. **Figure 1** shows the specific approach used.

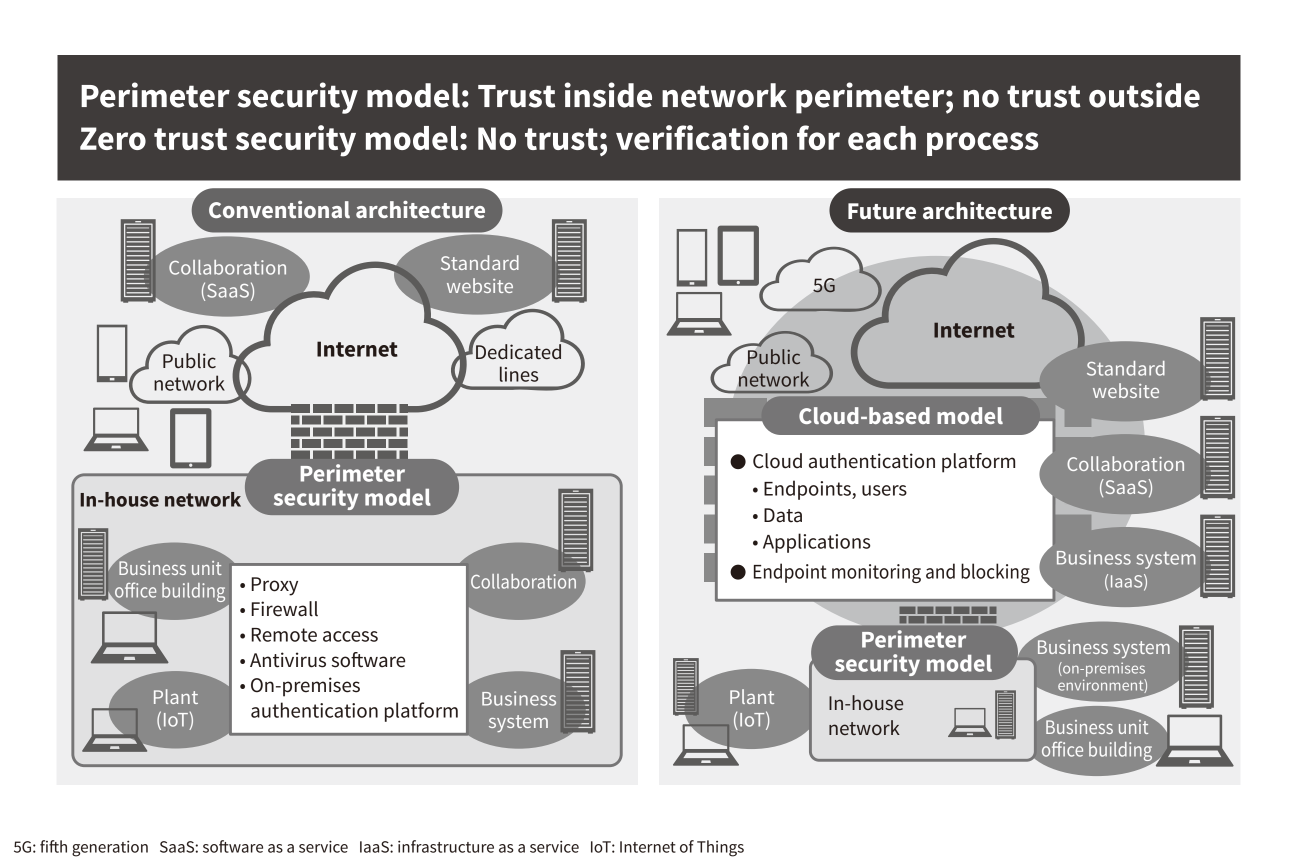
As shown in the figure, the aim is to provide optimum security by using a hybrid configuration that is based on the cloud (set to become the mainstream architecture in the years ahead) while also incorporating the conventional perimeter security model. The three key elements for implementing zero trust security using this cloud-based IT architecture are described below.

Authentication is the first element. Recent cloud use shows that cloud systems without multifactor authentication experience a very high likelihood of unauthorized access. Hitachi has responded by considering how best to implement cloud-based authentication and working on improving permissions management and individual user authentication.

The endpoints are the second element. The goal here is to improve endpoints as a total system that includes cloud systems and applications as well as PCs, servers, and smartphones. Work is also being done to study the security of network gateways and the data itself.

Figure 1 — Approach to Cloud-based IT Architecture

Cloud-based environments are going to become the mainstream architecture in the years ahead. Hitachi is working on creating cloud-based optimum zero trust security architecture with a hybrid configuration that also incorporates the conventional perimeter security model.


Perimeter security model: Trust inside network perimeter; no trust outside
Zero trust security model: No trust; verification for each process
Conventional architecture
Collaboration (SaaS)
Standard website
Internet
Public network
Dedicated lines
In-house network
Perimeter security model
Business unit office building
• Proxy
• Firewall
• Remote access
• Antivirus software
• On-premises authentication platform
Collaboration
Plant (IoT)
Business system
Future architecture
5G
Internet
Public network
Standard website
Cloud-based model
● Cloud authentication platform
• Endpoints, users
• Data
• Applications
● Endpoint monitoring and blocking
Collaboration (SaaS)
Business system (IaaS)
Perimeter security model
Business system (on-premises environment)
Plant (IoT)
In-house network
Business unit office building
5G: fifth generation SaaS: software as a service IaaS: infrastructure as a service IoT: Internet of Things

Cyber-integrated monitoring is the last of the three elements. The focus has traditionally been on analyzing and responding to logs in perimeter-based networks. However, the years ahead are going to see a need to respond to incidents by gathering and analyzing the correlation among a wide range of logs from the cloud, endpoints, and other components. So the company has started studying monitoring systems and organizations created as refinements of conventional cybersecurity monitoring.

3. Co-creating Security: Work on Building a Security Ecosystem

The overall concept here is to co-create a security ecosystem covering both in-house and outside areas. Hitachi believes that even departments with supposedly different operations can assist each other in working on security activities as a single shared objective, resulting in the maintenance and growth of business activities in the organization.

Security work is usually considered an area done together with IT departments. However, when incidents occur, they need to be handled through work done with a wide array of other departments in addition to IT. Examples include public relations, human resources and service, and legal affairs departments. Security measures are also being applied to a growing range of areas, so ensuring their effectiveness means they need to be done in close collaboration with departments such as manufacturing, quality assurance, and procurement. The WannaCry attack highlighted the importance of security ecosystems, leading Hitachi to begin creating an ecosystem designed to enable company-wide responses to cyberattack threats. A security ecosystem works by creating connections among its component elements—things, organizations or individuals, and the world at large. Each of these elements is described below.

3. 1 Connections between Things

DX creates various connections that generate new added value and provide solutions to issues of public concern. Creating these connections requires an environment that brings together objects such as the devices and systems that make up the IoT. Hitachi is responding by working to provide a comprehensive set of cybersecurity measures used in several different environments.

3. 2 Connections between Organizations or Individuals

Ensuring security in an environment that creates connections between things that were previously unconnected requires collaborative work on response measures among different organizations. Hitachi is working on activities that connect organizations and individuals by providing governance to enforce security measures, creating a community that extends across different professional and organizational lines, and reaffirming the company's role while creating closer ties to neighbors.

3. 3 Connections within Society

Hitachi feels that community-building extending across different structures is an essential requirement for security ecosystems, so the connections of Hitachi's security ecosystem extend beyond just the company itself. For example, this community-building can take the form of sharing threat information and issues encountered when mounting responses with countries, schools, and other companies working on cybersecurity measures. Hitachi is actively working on activities that create connections within society by helping outside companies or organizations to enhance the expertise they gain from their communities and use it in feedback to their security management cycles.

4. *Jibungoto*: Security Awareness-raising Work

The rise of the COVID-19 pandemic has forced many workers into new ways of working. Hitachi's use of remote work has rapidly gained momentum. Working from home is being treated as the standard as the company works on measures to promote the work styles of the future.

Meanwhile, the ongoing rise of cyberattack threats are making adequate security measures a crucial requirement when promoting remote work. Attackers have so far mainly targeted IT vulnerabilities among organizations, but vulnerabilities in security awareness are expected to become targets as remote work becomes mainstream. Working outside the office puts every worker at risk as they can let their guard down in unfamiliar environments, and have no coworkers nearby to ask for advice.

Security measures are supposed to require a balance of three elements—IT, processes, and people. While the measures needed for the IT and process elements are routinely provided, the people element (awareness-raising and education) tends to be neglected in practice. This failure to implement measures effective enough for the security needs of the modern world is a problem. To deal with today's radically changing environment and reduce the company's future security risks, Hitachi has come to understand the need for greater education and awareness-raising among employees to ensure more balanced security measures.

So the company has identified the need to raise every employee's level of security awareness as the final bulwark for the future of its cybersecurity strategies. Hitachi is enforcing existing governance measures, and has started work on a set of activities designed to raise security awareness by

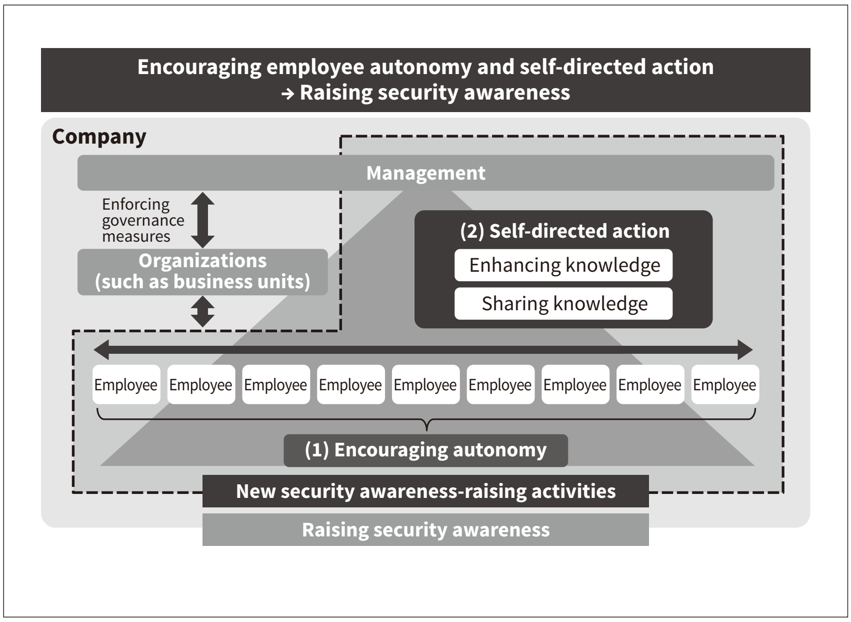

Encouraging employee autonomy and self-directed action
→ Raising security awareness
Company
Management
Enforcing governance measures
Organizations (such as business units)
(2) Self-directed action
Enhancing knowledge
Sharing knowledge
Employee
Employee
Employee
Employee
Employee
Employee
Employee
Employee
Employee
(1) Encouraging autonomy
New security awareness-raising activities
Raising security awareness

Figure 2 — Future Security Awareness-raising Aims

Hitachi is enforcing in-house governance measures while working on activities designed to raise security awareness by encouraging employee autonomy and self-directed action.

encouraging employee autonomy and self-directed action (see **Figure 2**).

These activities are designed to change employee mindsets about security measures. Instead of thinking of work on security measures as a duty, the aim is to encourage a personal interest in security that resonates on an emotional level and makes employees deal with security as "*jibungoto*," (taking ownership) something impacting them personally. Specifically, Hitachi is working to provide venues for collaborative awareness-raising among employees that will give employees hands-on experience of security and security practices in a self-directed manner as they share their newfound knowledge with other employees.

5. Conclusions

This article has described the work Hitachi is doing to enhance cyber resilience, divided thematically into the areas of governance, co-creating security, and "*jibungoto*" (taking ownership).

Hitachi is rigorously enforcing in-house governance measures while working on building a society-wide security ecosystem. By drawing on activities directed outside the company, this ecosystem will enable co-creation among industry, government, and academia.

To create a sturdy bulwark for protecting the organization, the company is working on raising employee awareness of the personal impact of security. The aim is to give every employee a proper understanding of security while fostering the awareness needed to work on properly designed measures.

By creating cybersecurity strategies in the areas of governance, co-creating security, and "*jibungoto*" (taking ownership) Hitachi is working on enhancing cyber resilience to enable a more safe, secure, pleasant, and risk-free experience in the world of the "new normal."

Authors

Atsushi Murayama
Information Security Strategy Office, Information Security Risk Management Division, Hitachi, Ltd.
Current work and research: Security governance strategic planning work.

Takeshi Nishimura
Information Security Planning Department, Information Security Strategy Office, Information Security Risk Management Division, Hitachi, Ltd.
Current work and research: Information security planning work and security awareness work.

Mari Watanabe
Information Security Planning Department, Information Security Strategy Office, Information Security Risk Management Division, Hitachi, Ltd.
Current work and research: Planning work for security awareness.