Hitachi's Work on Enhancing Zero Trust Security

Zero trust security is a new security model that has recently been attracting interest as an alternative to the perimeter-based security model now in mainstream use. Hitachi was an early adopter of the model, adding zero trust pilot systems to in-house IT environments before the technology's commercial release. Zero trust is now used by Hitachi Group members in 33 countries worldwide. This article presents the issues that Hitachi has faced when developing zero trust systems, along with the measures used to solve them. It also describes the zero trust architecture components Hitachi has devised, along with Hitachi's solutions business.

Tatsuya Hisanaga
Takeshi Akutsu
Yurika Kamimura
Kensuke Tamura

1. Introduction

The conventional security model has brought the perimeter-based defense model into widespread use. This model is premised on the assumption that in-house networks are secure and trusted. Perimeter-based defense provides in-house networks with multilayer defense using multiple security technologies such as firewalls and virtual private networks (VPNs). The security of the information assets to protect is ensured by placing them on in-house networks.

Meanwhile, remote work and other increasingly diverse work styles along with the rapid rise of cloud services have created sudden growth in the use of information assets on external networks and the cloud, creating a need for data protection outside perimeters. Information assets within perimeters are also no longer always safe since today's increasingly advanced cyberattacks have sometimes resulted in permission being mistakenly granted to infiltrators of in-house networks.

These issues are demonstrating that security assurance driven by the conventional perimeter-based defense model is approaching the end of its useful life, resulting in a growing shift toward the use of the zero trust security model as an alternative. Zero trust is premised on the notion that all access to information assets is untrustworthy.

Hitachi was an early in-house adopter of zero trust security, and has now added it to in-house IT environments at approximately 2,400 business hubs in 33 countries worldwide. This article describes the measures Hitachi has used to add zero trust to in-house systems, presents the priority areas for zero trust operations, and describes those operations.

2. Work on Bringing Zero Trust Security to In-house IT Systems

Hitachi has been working on enhancing its perimeter-based defense since becoming a victim of the WannaCry ransomware attack in May 2017. However, when using cloud services or working on collaborative or co-creation projects with other companies, the information assets to protect are not always to be found on in-house networks. Companies with different security policies also require time to be admitted inside Hitachi's network perimeters, which has revealed problems such as lost business opportunities when doing mergers and acquisitions (M&A) operations for business restructuring. Hitachi has responded by working to adopt zero trust security designed to enable IT infrastructure that can flexibly adapt to a changing business environment without relying on a network environment.

The security issues and operations issues encountered when installing zero trust systems were solved by using identity-as-a-service (IDaaS) and endpoint detection and response (EDR) solutions. IDaaS is a cloud-based system that is independent of network location. EDR is used to combat unknown malware (see **Figure 1**).

The main measures implemented by Hitachi's zero trust security systems are described below.

(1) Migrating network security to the cloud

Zero trust migrates web proxy and remote access functions from on-premises environments to the Internet. It uses web proxies to provide access control for communication with cloud services and with on-premises environments, while at the same time providing dynamic access control reflecting user or device safety. This approach is being used to ensure security at the session level. Handling these web proxies as communication-routing hubs lets Hitachi and newly merged or acquired enterprises with different security policies use each other's systems in a secure manner, enabling more rapid synergy between business operations.

(2) Enhancing endpoint security

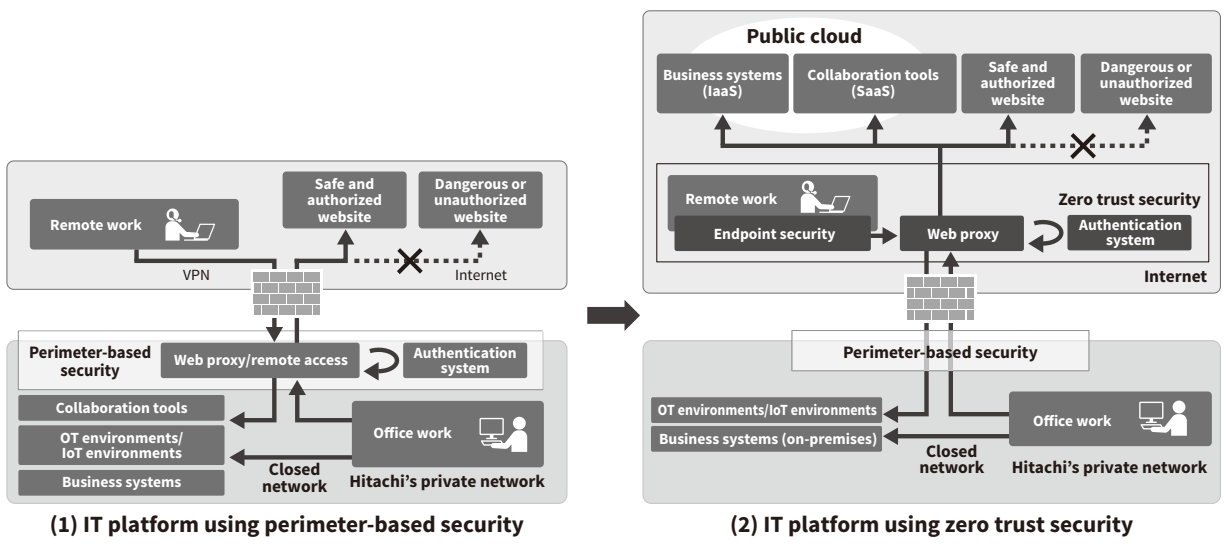
EDR measures to combat unknown malware (by behavior detection) have been installed in PC terminals alongside conventional endpoint protection platform (EPP) measures that combat known malware. Unified endpoint management (UEM) measures will be installed in the future to provide centralized management of PC terminals and smart devices, while patch installation and policy control will be enhanced and made more efficient. A fat client-based PC data volatile security service has also been developed as a further security enhancement. It erases the information assets in the PC terminal upon shutdown to deal with physical security risks (loss and theft), ensuring a remote work environment that makes working from home secure.

(3) Adopting cloud-based authentication infrastructure and using multifactor authentication to enhance authentication

Zero trust security requires authentication with multiple factors and control of dynamic risks. Hitachi has adopted

Figure 1 — Hitachi's Zero Trust Security-based IT Platform

Web proxies and authentication infrastructure have been migrated to the cloud alongside collaboration tools. Access is controlled dynamically using communication as well as user and device safety.



IaaS: infrastructure as a service SaaS: software as a service OT: operational technology IoT: Internet of Things VPN: virtual private network

IDaaS cloud services to create robust authentication systems that can authenticate users irrespective of network location using multiple factors such as devices or biometric identifiers. The authentication for software as a service (SaaS) processes are handled using IDaaS.

All the measures described above apply to zero trust added to Hitachi's in-house IT systems. Meanwhile, Hitachi also has manufacturing sites where zero trust security measures cannot be mounted in operational technology (OT) environments or Internet of Things (IoT) devices as they can for PC terminals. So the overall configuration of Hitachi's in-house IT systems is a hybrid configuration combining zero trust security with perimeter-based security protected by network perimeters. Hitachi will continue to work on creating optimum IT platforms to aid the company's business growth while speeding the rise of digital transformation (DX).

3. Three Key Points for Promoting Zero Trust

The NIST SP 800-207 Zero Trust Architecture released by the National Institute of Standards and Technology (NIST) defines seven basic principles for zero trust (see **Table 1**).

As component technologies for satisfying these basic principles, the three architectural elements of endpoint enhancement, dynamic access control, and visualization are what Hitachi considers to be the key component elements of zero trust (see **Figure 2**).

Endpoint enhancement provides unified endpoint control using measures such as EPPs and EDR to combat known and unknown malware, and UEM to control patch installation and block unauthorized applications. It protects the organization's mobile devices from outside threats while ensuring organizational cyber hygiene by preventing unauthorized internal operations by users and high security-risk operations.

Dynamic access control uses IDaaS to provide cloud-based ID management while enhancing authentication using multifactor- and risk-based authentication[*1]. The use of secure web gateways (SWGs) and software-defined perimeters (SDPs) also enables access control for web proxy control/remote access control in a seamless and secure manner that is independent of the local connected device's location or the network.

Visualization provides visual displays of security states by using various approaches to gather information from the entire system. For example, cloud access security brokers (CASBs) provide visual displays of user cloud service use while verifying its safety. Data loss prevention (DLP) measures detect and block processes such as unauthorized removal of confidential information. Security information and event management (SIEM) and user and entity behavior analytics (UEBA) systems gather and analyze log information from IT assets used for work processes to enable early detection of security incidents and unauthorized internal operations. Visualization measures are designed to prevent or minimize security damage by providing advance detection of security risks throughout the system, and enabling rapid responses when incidents occur.

4. Comprehensive Solution Package Provided by Hitachi

Hitachi provides a zero trust security solution that offers a comprehensive lineup of services ranging from consulting optimized to the customer's business vision, to installation (service integration) and operation. The solution has been created by drawing on a portfolio of expertise in integration and operation that Hitachi has acquired by satisfying a wide array of customer needs in many different industries

*1 An authentication method that uses patterns of behavior (such as the authentication request initiator's device type or the location or time of the request) and other information to detect suspicious access and dynamically change authentication request levels.

Table 1 — Basic Principles of Zero Trust as Defined by NIST

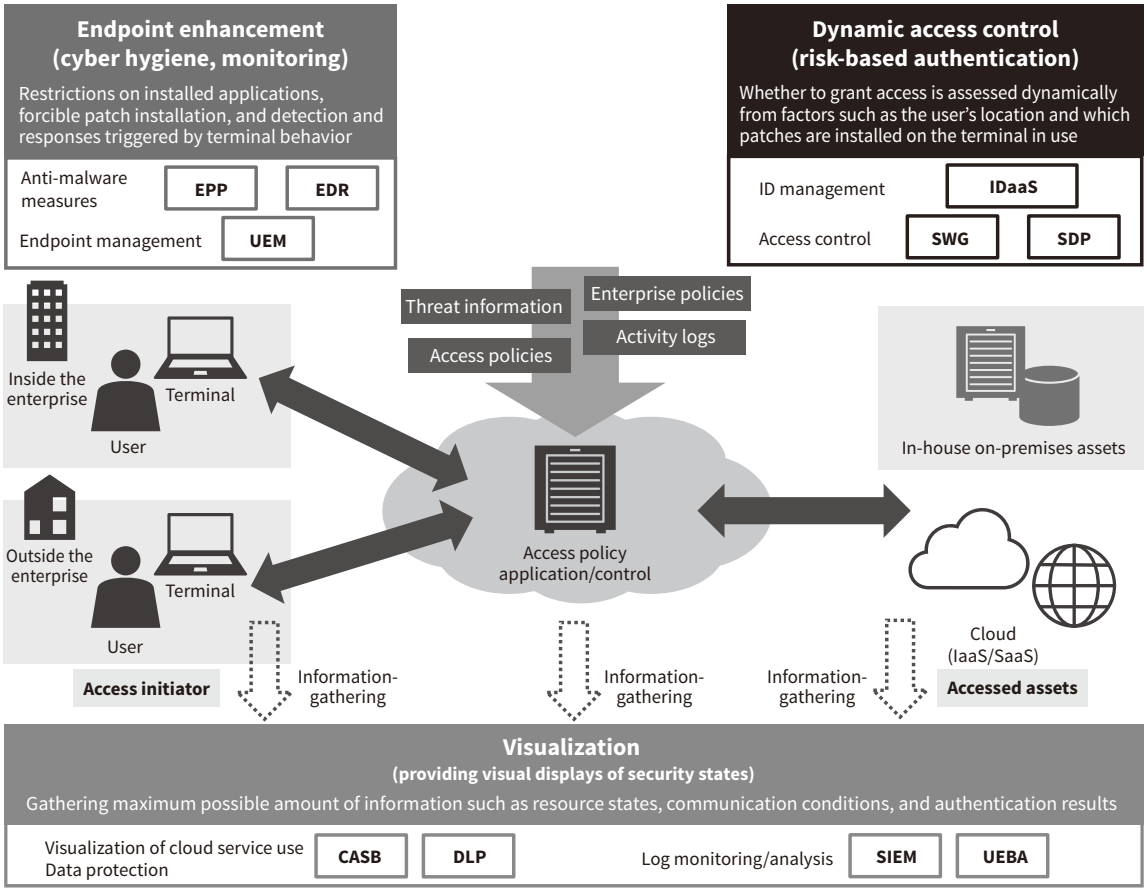
NIST has defined the ideal approach to implementing zero trust. Hitachi aims to implement all or a selected portion of these principles as dictated by the needs of the organization.

Basic principles of zero trust
(1) All data sources and computing services are considered resources
(2) All communication is secured regardless of network location
(3) Access to individual enterprise resources is granted on a per-session basis
(4) Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes
(5) The enterprise monitors and measures the integrity and security posture of all owned and associated assets
(6) All resource authentication and authorization are dynamic and strictly enforced before access is allowed
(7) The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture

Source: National Institute of Standards and Technology (NIST), "NIST Special Publication 800-207: Zero Trust Architecture"

Figure 2 — Basic Configuration of Zero Trust Architecture as Devised by Hitachi

Endpoints are enhanced and access is controlled dynamically to enable flexible security measures tailored to device and user states, while visual displays enable early detection of security risks.



EPP: endpoint protection platform EDR: endpoint detection and response UEM: unified endpoint management IDaaS: identity-as-a-service SWG: secure web gateway SDP: software-defined perimeter CASB: cloud access security broker DLP: data loss prevention SIEM: security information and event management UEBA: user and entity behavior analytics

centered around public infrastructure and financial institutions (see **Figure 3**).

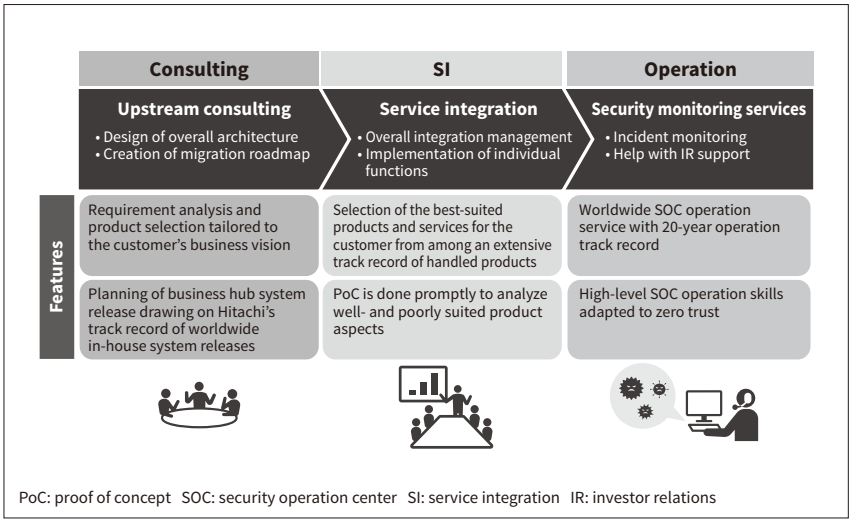
Hitachi's consulting work involves analyzing the requirements alongside the customer's future business vision by working closely with the customer starting from the system installation planning phase. When the requirements have been finalized, a combination of services matching the customer's requirements are selected. The gap between the customer's desired vision (To-Be) and current circumstances (As-Is) is then analyzed to create the grand design for the overall zero trust system. A secure and effective migration roadmap is also created and provided to the customer by drawing on Hitachi's experience in releasing IT systems to in-house business hubs worldwide. Covering large numbers of business hubs either inside or outside Japan, the roadmap includes elements such as planning for system installation and business hub release, planning for operation once services begin, and planning assistance for revising or discontinuing legacy systems.

Hitachi's service integration work involves having the customer select the best-suited products from among the diverse lineup of products and services in Hitachi's extensive product handling and installation track record. A proof of concept (PoC) trial is then promptly carried out to analyze which product aspects are well suited to the customer's desired vision and which fall short. When the products and services have been finalized, Hitachi teams with product vendors to promptly create a zero trust environment tailored to the customer's needs. Assuming an Internet breakout has been provided, the environment is then released to the customer's business hubs and the system handover is performed securely. This integration work is greatly assisted by Hitachi's expertise in implementing large-scale authentication infrastructure[*2], done as part of installing zero trust in the company's in-house IT systems.

*2 Hitachi has integrated in-house authentication infrastructure for about 340,000 Group employees worldwide (as of 2017).

Figure 3 — Overview of Hitachi's Zero Trust Security Solution

Hitachi provides zero trust aligned to customer needs by offering a comprehensive solution package covering everything from project proposals to installation and operation.



Hitachi's operation work centers around a security operation center (SOC)-based operation service provided worldwide by Hitachi 24×7, 365-days-a-year. Hitachi has provided security monitoring services to financial institutions and other customers in a wide array of industries for over 20 years. Hitachi's SOC operation service provides a wide range of high-level SOC operation skills to meet the latest needs. It has been made possible by working to acquire advanced techniques supporting zero trust architecture without clinging to legacy SOC operation for conventional perimeter-based security. By drawing on Hitachi's extensive track record and advanced techniques, the service provides high-level correlation analysis monitoring to the zero trust security systems installed by the customer. It helps enable prompt responses to incidents, and provides ongoing support for the customer's security operations.

5. Conclusions

Despite the advanced work Hitachi has done to install zero trust security in its in-house systems, zero trust is still a developing area. So the company is planning to further augment its in-house security as zero trust technology advances in the future.

The Hitachi Group will continue working as a team to propose and provide the best-suited zero trust security environments to customers in the years ahead. This work will be done by drawing on the work done on its own in-house IT systems to identify the latest security technology trends. The achievements and expertise gained in this area will then be used to transfer knowledge to solutions projects.

Reference

1) National Institute of Standards and Technology, "NIST Special Publication 800-207: Zero Trust Architecture" (Aug. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Authors

Tatsuya Hisanaga
Cyber Security Solution Business Department, Security Business Innovation Division, Service Platform Business Division, Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research:* SIEM/Zero trust-related service integration work in the cybersecurity business.

Takeshi Akutsu
Cyber Security Solution Business Department, Security Business Innovation Division, Service Platform Business Division, Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research:* Planning and project coordination for the cybersecurity business.

Yurika Kamimura
Strategy Promotion Department, Global Solution 2nd Office, IT Strategy & Digital Integration Division, Hitachi, Ltd. *Current work and research:* Strategy and planning of internal IT services (infrastructure area).

Kensuke Tamura
Strategy Promotion Department, Global Solution 2nd Office, IT Strategy & Digital Integration Division, Hitachi, Ltd. *Current work and research:* Strategy and planning of internal IT services (infrastructure area).