EQST insight

Zero Trust Era – Never Trust, Always Verify

■ Outline

Zero Trust, mentioned in the last May's headline 'Seven strategies for controlling access rights to respond to cybersecurity threats in the WFA (Work-From-Anywhere) era,' has recently emerged as a hot topic in the cybersecurity field. Accordingly, based on the NIST[1] Zero Trust Guideline (SP 800-207) and CISA[2] (Zero Trust Maturity Model, ZTMM), we would like to explain considerations in the review stage of Zero Trust introduction and reference points when establishing a plan.

As the use of cloud services increases and remote work becomes a daily routine due to the COVID-19 pandemic, the working environment in companies is undergoing major changes. The existing boundary that used firewalls to distinguish between a company's internal network and external network is blurring, and with the emergence of various types of devices, it is becoming increasingly difficult to tell 'which devices can be trusted'.

Now, for the sake of security, we must prepare for the Zero Trust era in which we must "Never Trust, Always Verify."

[1] NIST (National Institute of Standards and Technology)

[2] CISA (Cybersecurity and Infrastructure Security Agency)

■ The concept of Zero Trust and its expansion

In 2010, Forrester Research presented the first Zero Trust concept and model. It claimed that as all access entities cannot be trusted, access rights to a company's internal assets should be restricted. In other words, since implicit trust can cause security problems, access should be allowed only based on the result of trust verification. These days, the concept has been expanded in line with changes in technology, and the target has expanded from data to users, devices, networks, workloads, etc., and the scope has also expanded to include securing visibility, analysis, automation, and integrated operations.

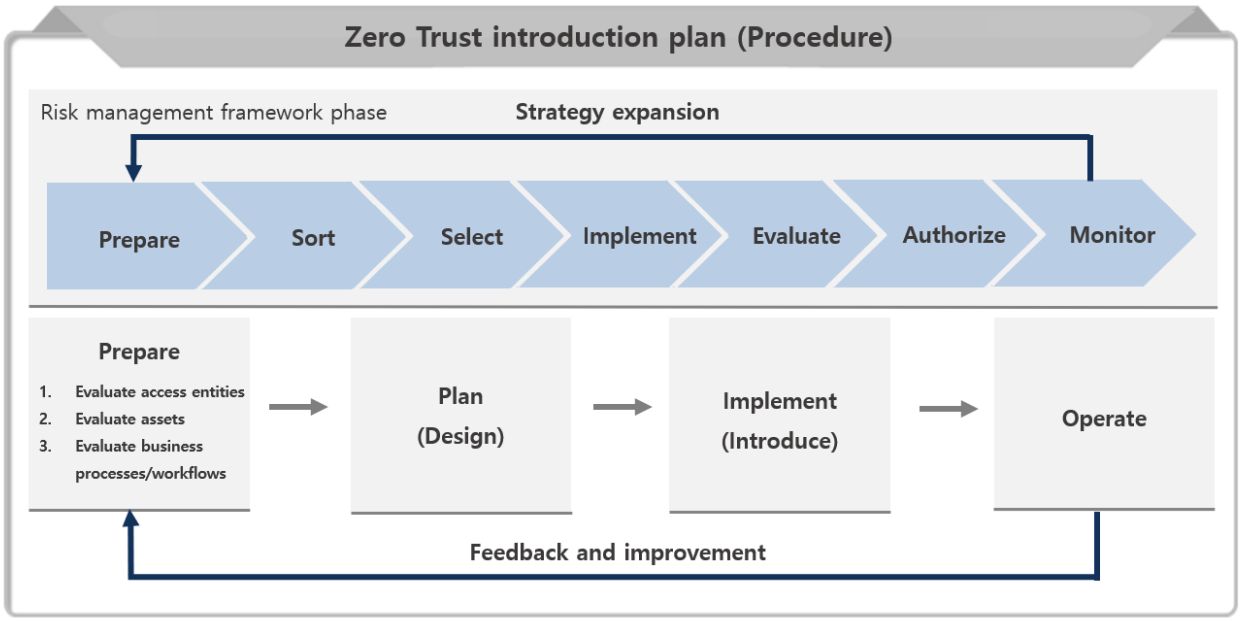
■ Zero Trust introduction plan

The first thing to consider when a company tries to apply Zero Trust is that Zero Trust is a set of all principles used in security policies, not a single technique or product, and there is no separate correct answer.

The US NIST Annual Report for 2020 introduces a detailed guideline for implementing the 'Zero Trust Guideline (NIST SP 800-207)'. In particular, it says that "there cannot be a single implementation plan because each company's use cases and data assets are unique," and emphasizes that sufficient review and systematic preparation are required because a lot of resources, time, and budget are required.

It is said that active support from the management should always be a priority in order to build a cybersecurity system. However, to implement Zero Trust, as the basic principle of constant evaluation and re-approval if necessary is required to suit the context rather than granting system access rights based on existing 'implicit trust', the existing infrastructure system must be changed. Therefore, active participation and cooperation of data and system operators and users is necessary.

Establishment of an introduction plan is a procedure for reducing security threats to resources, which is reviewed in connection with the NIST Risk Management Framework (NIST SP 800-37).



* Source: Reprocessed image of the Ministry of Science and ICT Zero Trust Guideline

[Figure 1] The detailed procedure for introducing Zero Trust

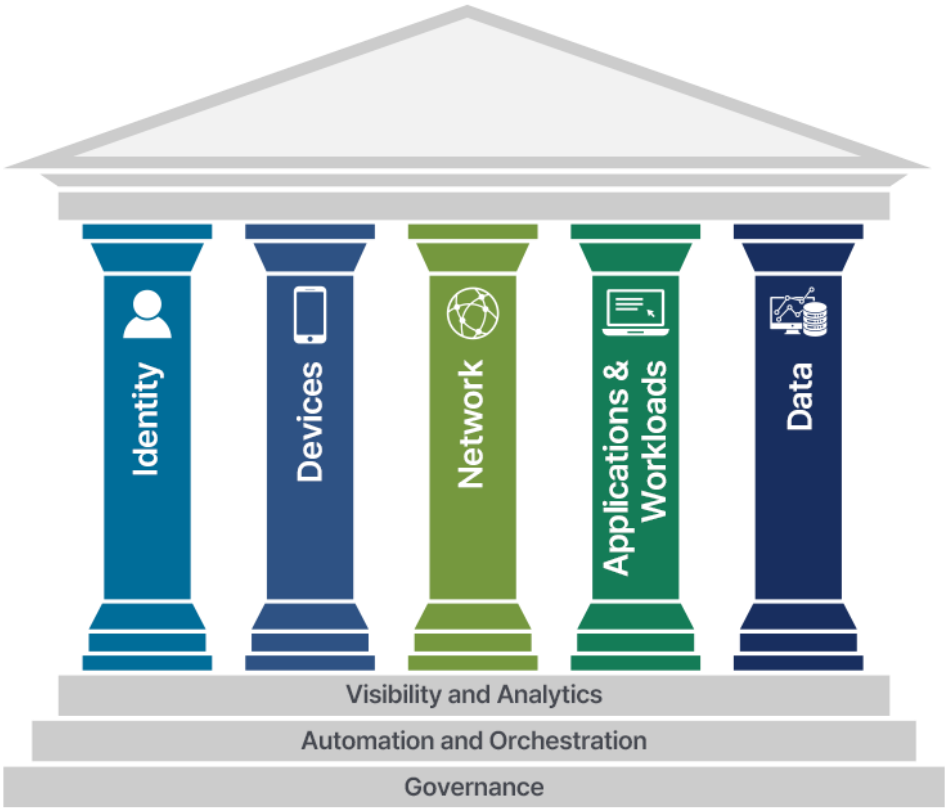
〈Table 1〉 Detailed procedures for introducing Zero Trust

Prepare	Before introducing Zero Trust, it is necessary to evaluate the company's **current security target/level**** focusing on **key elements*** * Identifiers, devices, networks, systems, applications and workloads, data ** Identify access entities, assets/devices, business processes/workflows and evaluate maturity
Plan	Review introduction design and budget to secure a **higher level** of security by **harmonizing** with the existing security system based on the **maturity model**
Implement	**Review and implement a solution** suitable for the company's ecosystem in consideration of the **location** of major resources, **protocols***, and various services * (Resource location) On-Premise, Cloud, (protocol) web, SSH, IPv4, IPv6, etc.
Operate	Set/manage it to ensure that the **core principles**** operate appropriately based on the **basic philosophy*** in the implemented Zero Trust architecture *Do not trust any type of access. *Consistent and centralized policy management and access control decision/implementation are required. *User, device management and strong authentication *Elaborate access control through resource classification and management (granting minimum privileges) *Create logical boundaries, allow access on a per-session basis, and apply communication protection technology *Continuously verify/control reliability through monitoring and log recording of all conditions **Strengthen the authentication system: Establish a reliability-based authentication policy **Micro segmentation: Deploy individual resource groups through security gateway **Software-defined boundary: Create channels for accessing resources after dynamic configuration of networks according to policy engine decision, and securing user trust
Feedback/ Improvement	Enhance the level through **repetitive management** of each stage, e.g. **comparison and monitoring of completion level** based on Zero Trust maturity, and **derivation of improvement measures**

* Source: Ministry of Science and ICT Zero Trust Guideline

■ Zero Trust Maturity Model (ZTMM)

The Zero Trust Maturity Model (ZTMM) is a model to objectively express whether the security concept based on the Zero Trust model is well applied and operated. 'Maturity' is not something that can be reached at a high level all at once, but develops to reach an optimal level through gradual changes. When explaining the Zero Trust architecture, the standard elements are schematically expressed as five pillars and cross-functions commonly applied to each pillar.

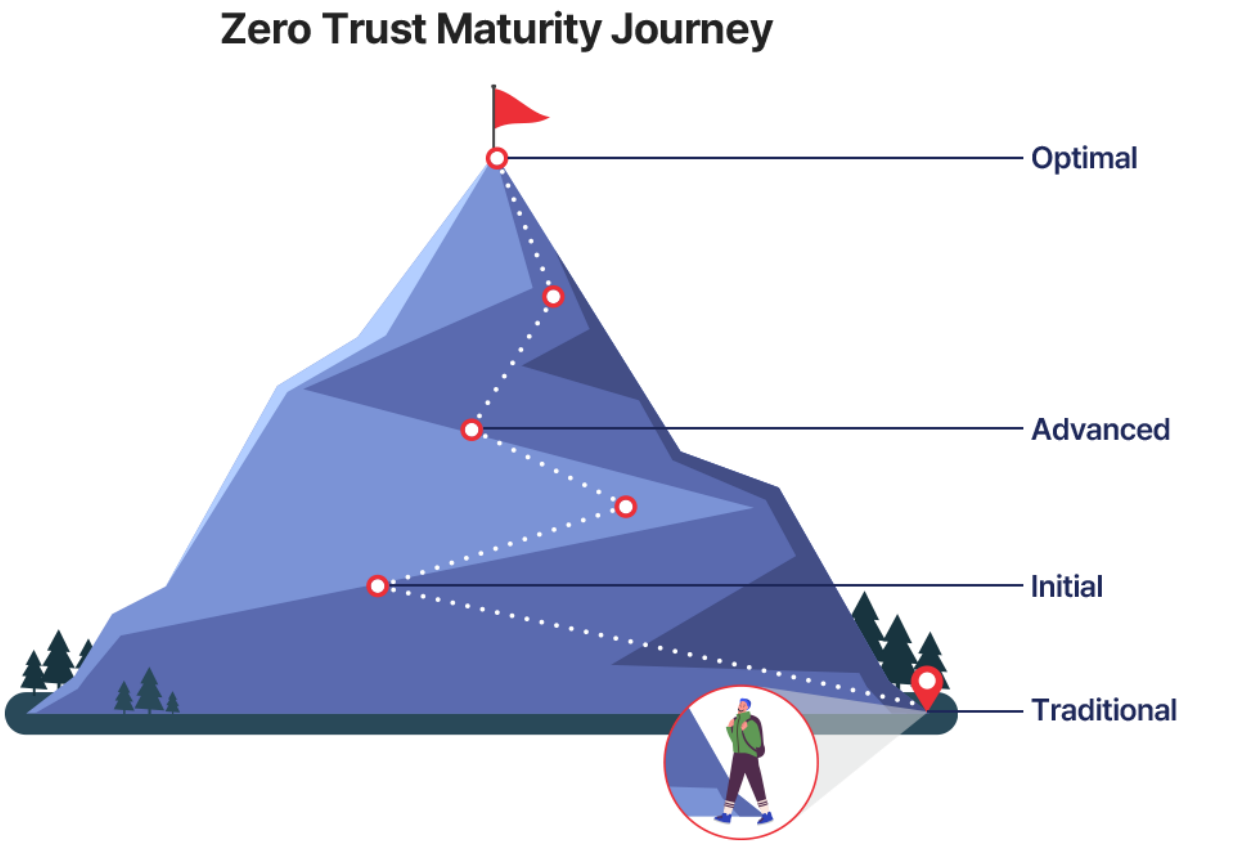


* Source: US CISA

[Figure 2] CISA Zero Trust Maturity Model (ZTMM)

According to CISA, in the initial stage of Zero Trust implementation and the organization must focus on building the "initial cross-functions by automating attribute assignment for the five pillars (identity, device, network, application & workload, data), configuring the life cycle, determining and implementing policies, and integrating external systems."

In ZTMM version 2, which was announced in April 2023, the maturity stage was divided into four stages: Traditional, Initial, Advanced, and Optimal, as shown in the figure below.



* Source: US CISA

[Figure 3] Zero Trust Maturity Journey

This means that starting from the traditional architecture and moving on to the initial, advanced, and optimal stage is not a simple process. It shows that in the initial stage, we must recognize that there are no shortcuts no matter what method we use, and that we must gradually move from the initial stage to the optimal stage through a measurable method.

〈Table 2〉 Zero Trust maturity level/definition by stage

Classification	Traditional	Advanced	Optimal
User/Identity	* Password or multi-factor authentication (MFA) * Limited risk assessment	* MFA * Partial ID combination with cloud and on-premise systems	* Continuous verification * Real-time machine learning analysis
Device	* Limited visibility of compliance * Simple inventory	* Compliance enforcement * Data access differs depending on device status at first access	* Continuous device security monitoring and verification * Data access differs depending on real-time risk analysis.
Network	* Large-scale macro segmentation * Minimal encryption of internal or external traffic	* Defined by incoming/outgoing micro boundaries * Basic analysis	* Fully distributed terminating/originating micro-boundary * Machine learning-based defense against threats * Encrypt all traffic
Application	* Access based on local authentication * Minimal integration with workflows * Some cloud accessibility	* Access based on centralized authentication * Basic integration with the application workflow	* Access is approved continuously. * Strong integration of application workflows.
Data	* Inadequate inventory (Not Well) * Static control * Not encrypted	* Minimal privilege control * Minimize data stored on the cloud or in a remote environment in idle state	* Dynamic support * All data is encrypted.

* Source: Canadian Centre for Cyber Security

■ Closing

Over the years, cybersecurity has responded sensitively to trends, and currently, the concept of Zero Trust has emerged as a new trend. Considering the speed at which technology develops, it is expected to lead the trend for a long time. Implementing Zero Trust is now a must, not an option.

Zero Trust will be of great help as a means of reducing security threats to companies at a time when network boundaries are disappearing and cyber threats are becoming more diverse and intelligent. We hope to create a seamless security environment under the principle of 'Never Trust, Always Verify'.

References

[1] NIST SP 800-207, “Zero Trust Architecture”, Aug. 2020

[2] CISA, “Zero Trust Maturity Model”, Apr. 2023

[3] Ministry of Science and ICT, “Zero Trust Guideline 1.0”, Jun. 2023