Cross-ministerial Strategic Innovation Promotion Program (SIP)

NTT

1-1 Protection of Critical Infrastructures by Continuous Monitoring of Unauthorized Changes to the Server Devices

Authenticity and Integrity Monitoring Technology

Continuous Monitoring of unauthorized changes to the systems prevents abnormal behavior, such as backdoor communications

Features

I. Continuous monitoring of unauthorized changes to the system and protection of records

Continuously monitoring the facts regarding changes in systems to prevent abnormal behavior resulting from such changes (real-time detection/prevention technology).

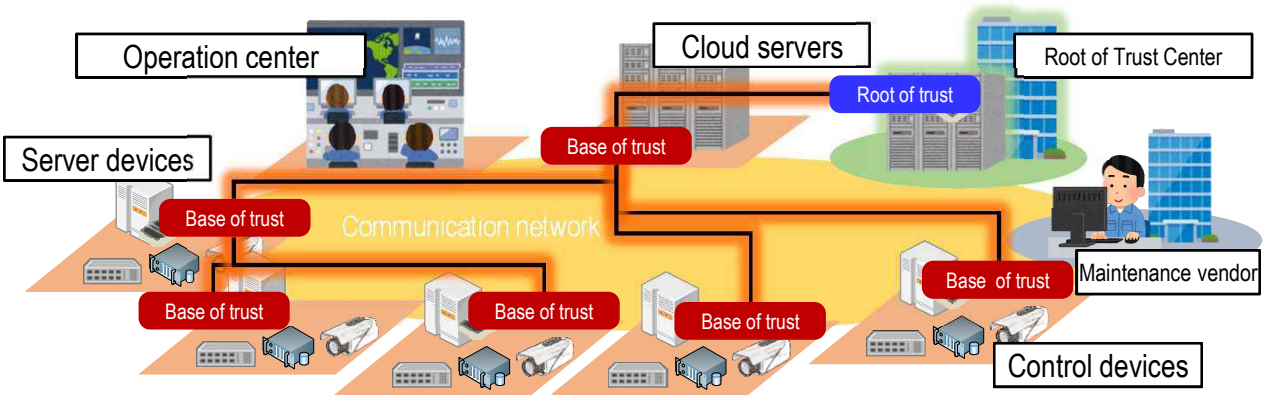
Inspecting operation of this technology and providing countermeasures against unauthorized change monitoring records enable secure and sound monitoring (secure recording technology).

II. Effective deployment and operation

The Configurations necessary for this technology can be safely shared among devices and also effectively introduced to a system consisting of many devices (secure configuration sharing technology).

The Configurations necessary for this technology can be). automatically adjusted according to the configuration of the software installed on devices (auto-configuration technology)

Introduction Image and Keys to Differentiation (Achieves *Meticulous Integrity Attestation Technology* Equipped with High Resistance to Cyberattacks)



Secure and sound detection of unauthorized changes

Make full use of the world standard latest security chip (TPM2.0) and cryptography technology to achieve secure and sound monitoring function.

Monitor over large-scale system

Construct「chain of *trust*」that enables the authenticity and integrity over facilities by supporting hundreds to thousands of server devices, and hundreds to thousands files per server device.

Monitor over life cycle

Monitor the integrity of software in real time from server devices startup to operation.

Plan for Practical Use and Commercialization

	FY2017	FY2018	FY2019	FY2020-
Spread of research results	Company's proposal → Technology verification → Trial implementation ⇒ Commercial implementation			
	Expand introduction while providing feedback about the preceding introduction result → Roll out to critical infrastructure fields (Individual SI type)			
Further measures for roll out	Roll out to other than critical infrastructure fields, such as OA fields → Implement solution by linking existing products			
			Introduction through sharing of facilities → Certification system/Root of trust center service	

Cross-ministerial Strategic Innovation Promotion Program (SIP)

NTT

1-1 Protection of Critical Infrastructures by Continuous Monitoring of Unauthorized Changes to the Server Devices

Background of the R&D Theme

There are growing risks of unauthorized devices with backdoors that come to be mixed in critical infrastructure through human-made modification or advanced malware incorporated at the time of delivery, introduction, or maintenance of devices. Especially in Japan, such threats are predicted to increase further toward the Tokyo 2020 Olympic and Paralympic Games. Therefore, in 2020, in addition to conventional demand-driven security measures, such as implementation of a firewall, new technologies should be necessary that radically enhance the security strength of critical infrastructure facilities themselves.

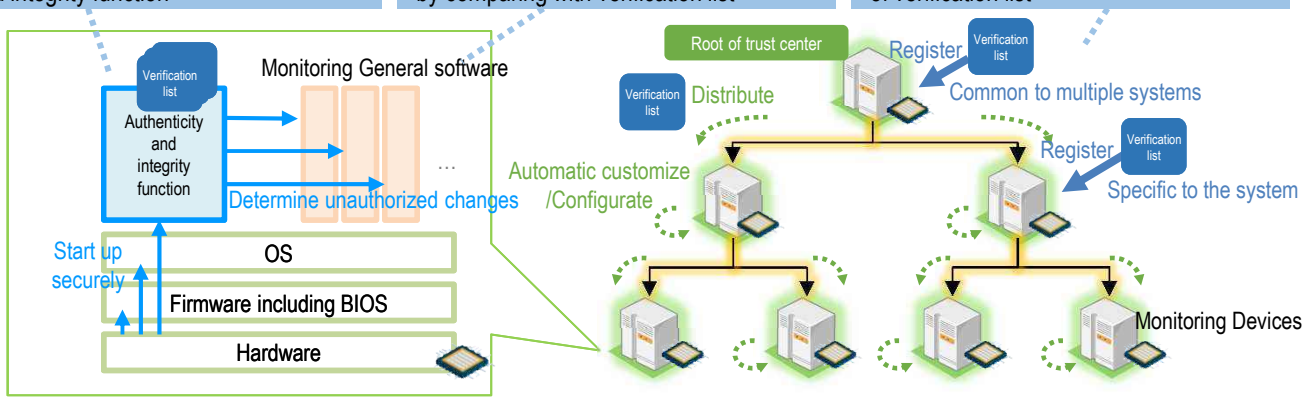
Operation Overview of the Technology

Three features

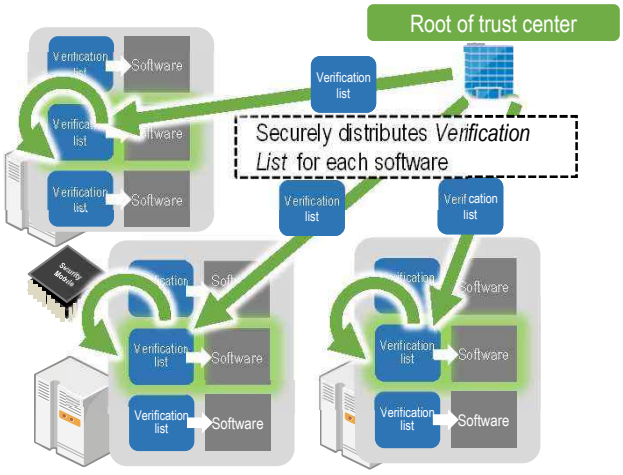
Secure startup of the authenticity and integrity function

Determination of unauthorized changes by comparing with verification list

Secure acquisition and auto configuration of verification list



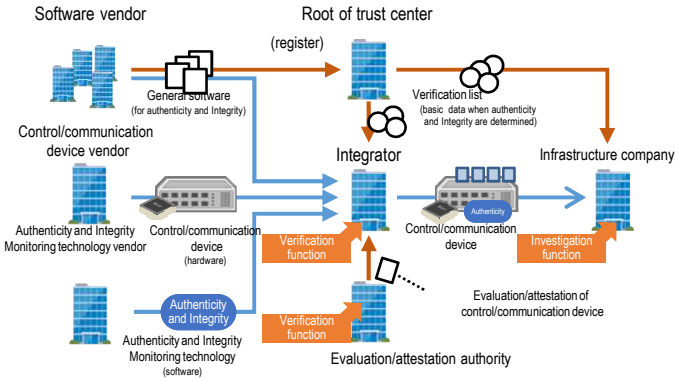
Enables secure update of a large-scale system



Automatic configuration based on the *rules* for each software

Verification list is shared through the chain of trust, and auto configuration is made according to the difference of each device.

Provides a verification function in a supply chain



Verification in the introduction process of control/communication device

In the supply chain of control/communication devices as shown above, each of *integrator*, *infrastructure company*, and *evaluation/attestation authority* can properly introduce authenticity and Integrity Monitoring technologies and verify that there is no unauthorized changes of control/communication devices.

Comparison with the Competitive Technologies

	This technology	A's product	B's product	C's product
Protection of monitoring records	○	×	×	×
Ease of introduction to a large-scale system	○	△	×	-
Real-time monitoring	○	△	△	×
Prevention of the execution of a unauthorized change file	○	×	×	×