4. Device Configuration Attestation in Supply Chain

A
Creation & Confirmation

NTT Corporation

Realizes a supply chain that is resistant to malware contamination by authenticity judgment that can support various OT / IoT devices

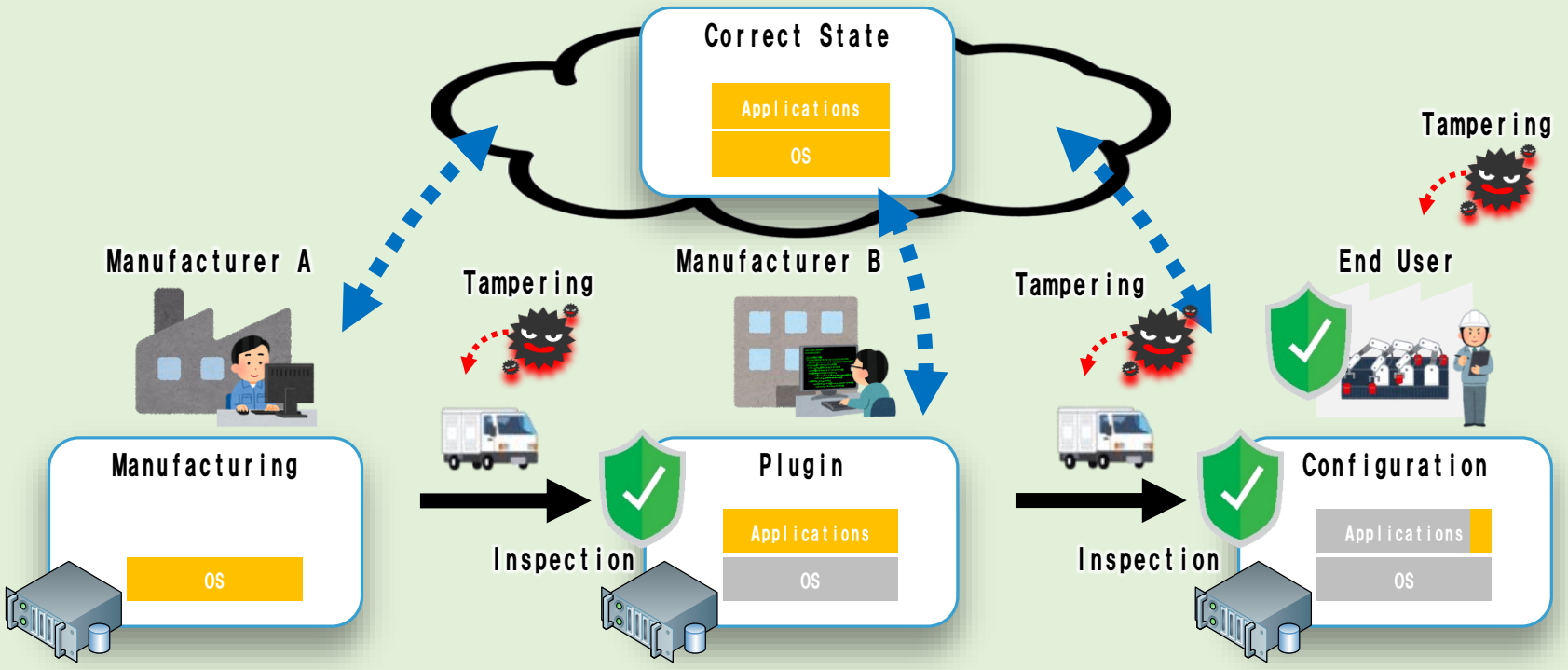
Technical Features

- **Smart Scan Technology**
  An efficient configuration verification function enables us to be applied to a wide variety of devices.
- **Configuration Change Management Technology**
  Track all configuration changes to the device in the supply chain.
- **Correct State Definition Technology**
  The configuration analysis function enables non-experts to define precise configurations.

Challenges and Proposed Technologies

- OT / IoT systems consist of a wide variety of devices. There is a risk that devices that do not have security measures will be violated and the damage will spread to the entire system.
- Open systems will be used on more and more devices. As a result, previously closed specifications become more open, and the risk of tampering will increase even in a supply chain.

Confirm the integrity of the various devices not only during operation but also throughout the supply chain.



Smart Scan Technology

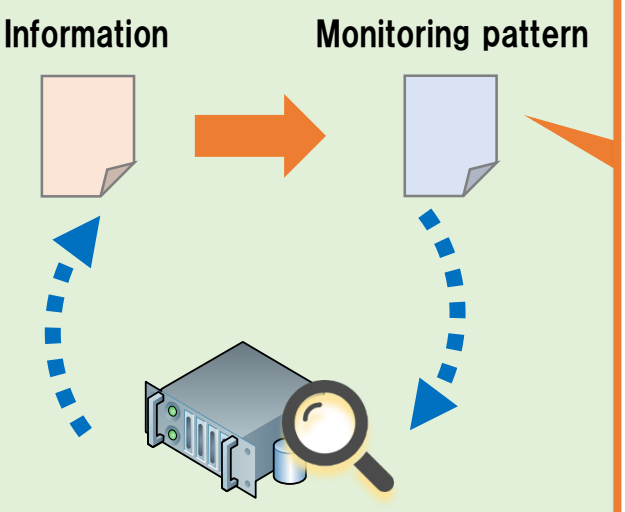
Smart scan technology can efficiently detect tamper of devise with small amount of resources. This means that it can be used in a wide variety of devices.

Configuration Change Management Technology

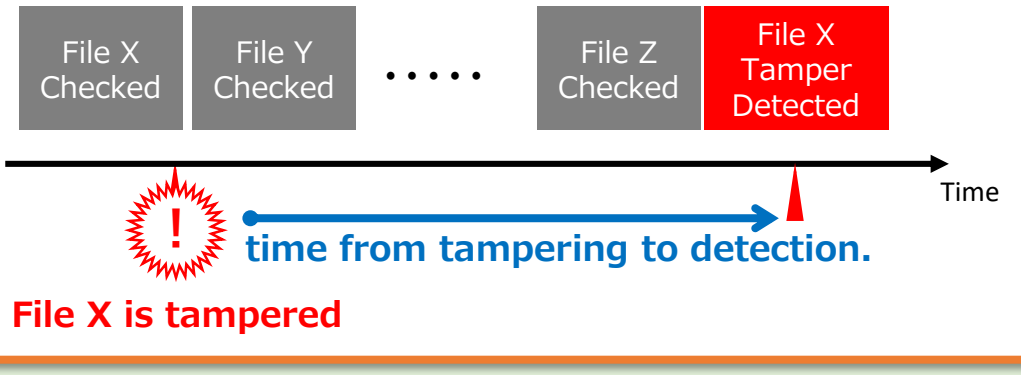
By having each business operator inspect the arrival of products, it is possible to detect tampering at an early stage and realize a secure supply chain.

Smart Scan Technology

By analyzing information about the operation of the device in advance and generating the optimum monitoring pattern, tampering can be detected efficiently even with a small amount of resources (smart scan technology), and the integrity of the system can be confirmed without impairing the original operation.

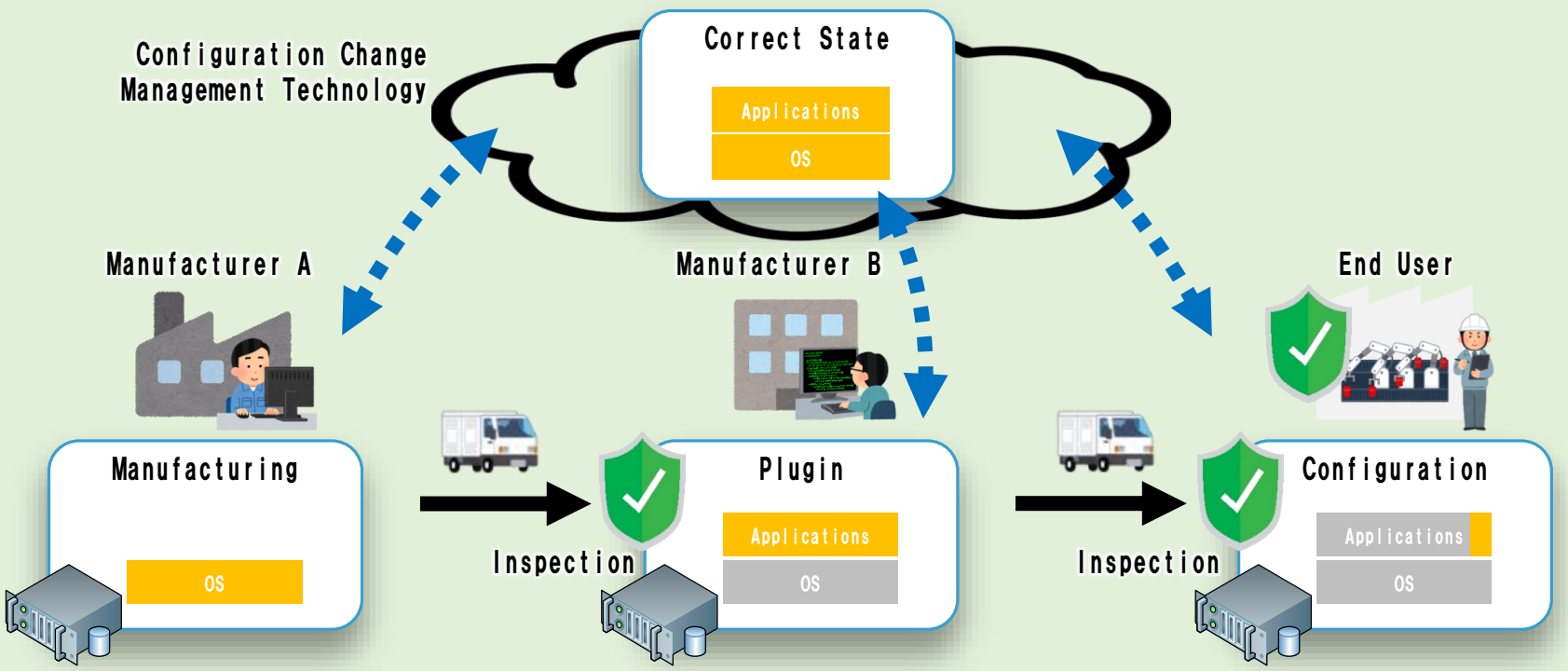


It analyzes information about the operation of the device and generates a monitoring pattern that minimizes the time from tampering to detection.



Configuration Change Management Technology

In order for each business operator to be able to confirm that the device that has arrived has not been tampered with, the business operators must share information on correct state of the device. By sharing information of correct state via configuration change management technology, tampering and misuse of information of correct state (manufacturing of counterfeit products, etc.) are prevented.



Schedule

2020	2021	2022	2023～
Experiment STEP1 →	Experiment STEP2 →	Experiment STEP3 →	
Research and Development →			Practical use / commercialization →

Contact：
Nippon Telegraph and Telephone Corporation
NTT Secure Platform Laboratories E-mail: scpflab@hco.ntt.co.jp