Authenticity and integrity monitoring technology for IoT device configuration

Nippon Telegraph and Telephone Corporation

Realization of supply chains that are not easily contaminated with unauthorized software through verification that can be applied to various IoT devices

Application Area

- Manufacturer
- Infrastructure
- ICT vendor
- Local Government
- IoT
- Building / Smart City

Technology Features

- **Applicable to a wide range of devices through a highly efficient scan mechanism**
  Efficiently monitor the software integrity of running devices with fewer resources.
- **Non-experts can define the configuration of the equipment in detail**
  Create verification criteria accurately and easily using tools.
- **Manage the configuration change history of devices in the supply chain**
  By securely sharing verification criteria that define the correct software configuration of devices, all companies in the supply chain can perform tamper detection at any time.

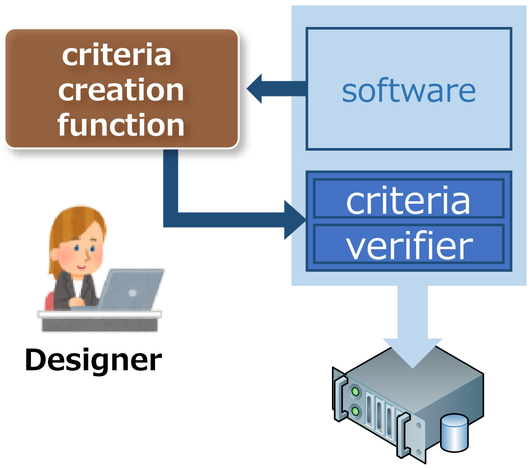
Effects

- **Reduce supply chain security risks by making the configuration of devices visible.**
  Ascertain changes in the configuration of devices throughout its life cycle, and reduce the risk by detecting elements of fraud not only in the operation phase but also in the supply chain phases.
- **Provide users with verification criteria that can be used for vulnerability management.**
  Verification criteria indicating the software configuration of a product can be used as input for vulnerability management tools, etc.

Use case

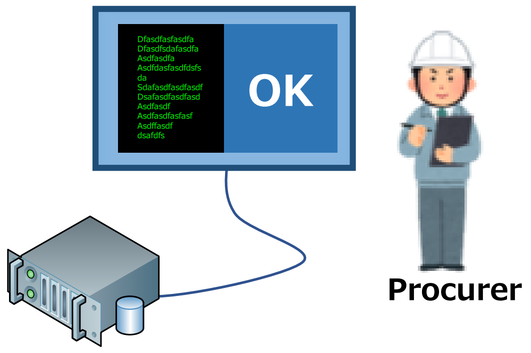
Manufacturer

Reduces the additional cost of implementation by automatically creating criteria for each product.



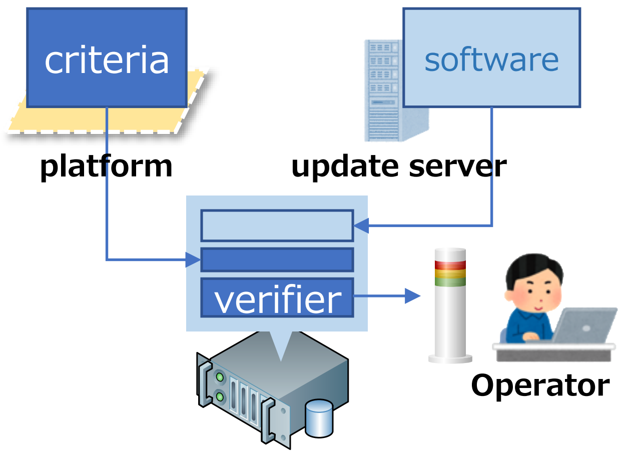
Integrator / User (procurer)

Reduce the risk of malicious code contamination by confirming the configuration, including software, at the time of procurement.



User (maintainer and operator)

Reduce the risk of malicious code contamination by checking the safety of software updates by means other than updates.



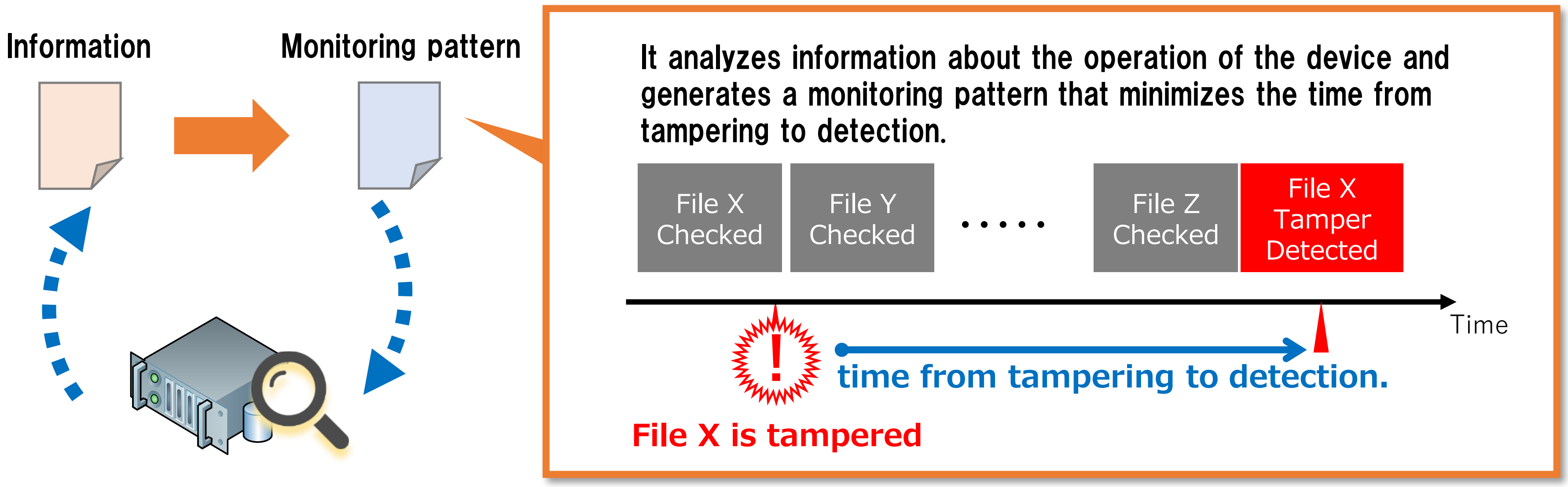
Authenticity and integrity monitoring technology for IoT device configuration

Nippon Telegraph and Telephone Corporation

Technology Description

A. Smart Scan Technology

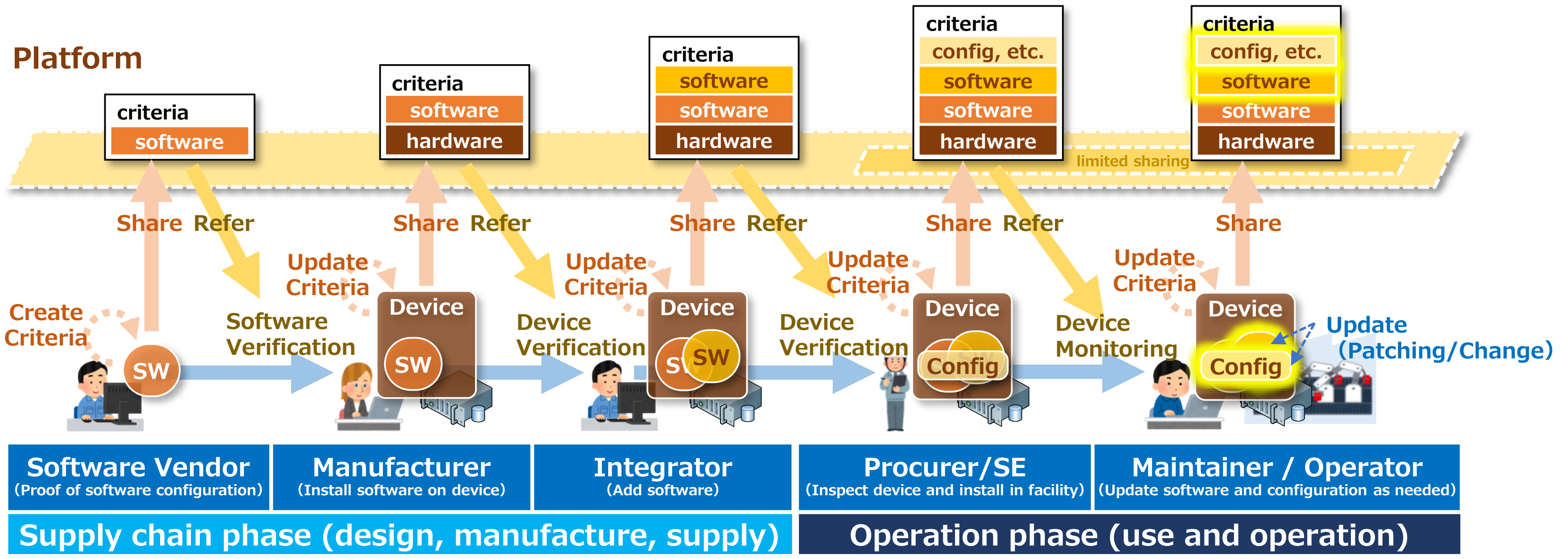
Theme	Compatibility of security performance and resource-saving required for low performance equipment.
Solution	Generates optimal monitoring patterns by analyzing information on device operation in advance. Efficient monitoring, even with low resources, to confirm the correctness without affecting the original function.



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

B. Configuration Change Management Technology

Theme	Realization of an environment in which all operators in the supply chain can perform tampering detection at any time.
Solution	Analyze the configuration of devices and automatically generate verification criteria that define the software configuration. The criteria are shared among the operators, and the correctness of the configuration is constantly assessed.



Contact

Nippon Telegraph and Telephone Corporation
NTT Social Informatics Laboratories
Email: solab@hco.ntt.co.jp