# 9. Detection and security measurement technology of invalid data between cyber and physical

C
Verification & Maintenance

Hitachi, Ltd.

Reduce the primary mitigation time for malicious data in IoT systems and reduces the impact of security incidents.

## Technical Features

### Abnormal data detection adapted to the characteristics of various IoT systems

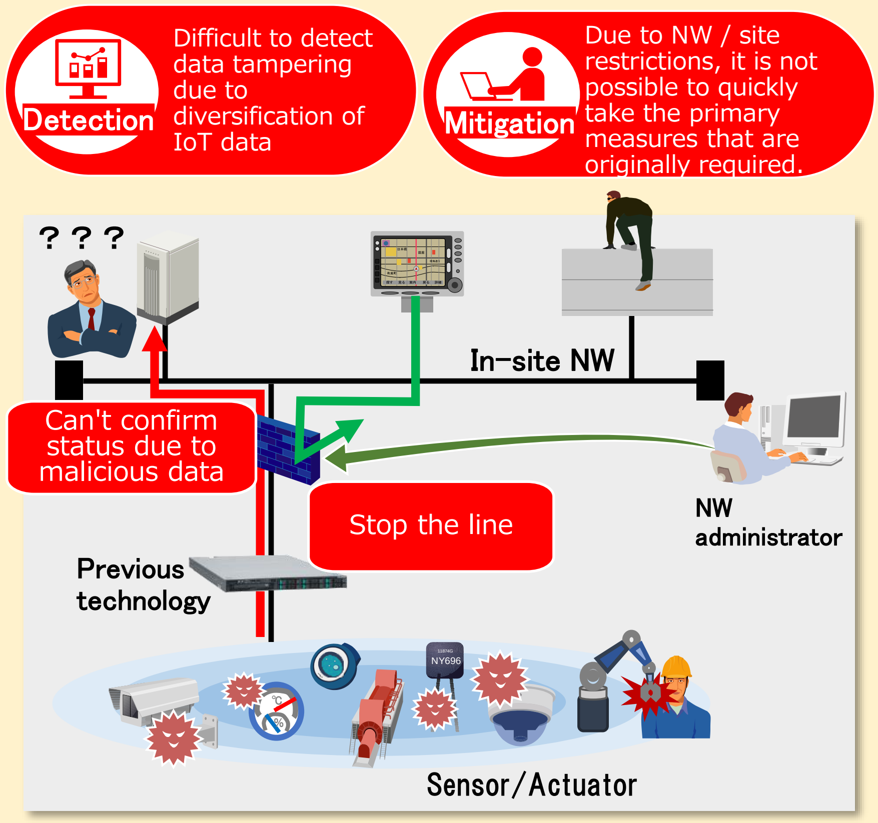
Realizes abnormal data detection with low risk of false positives / oversights using system characteristic data

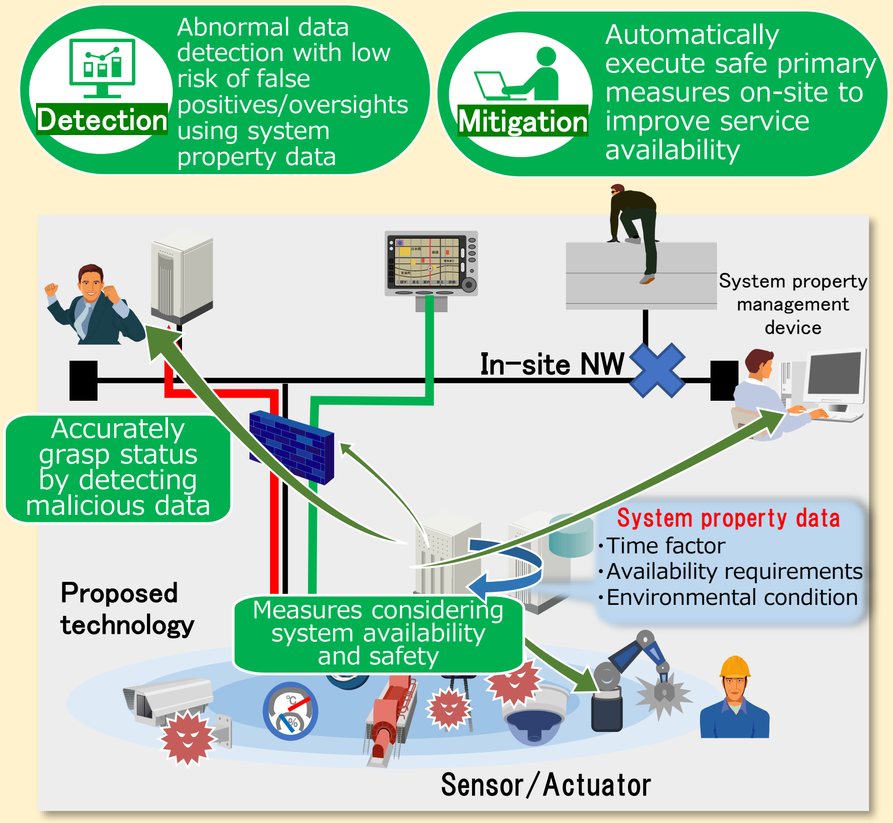
### Take appropriate primary mitigation automatically for service continuity

Improve service availability with abnormal data mitigation technology that automatically executes flexible and highly secure primary mitigations according to the system

IoT: Internet of Things

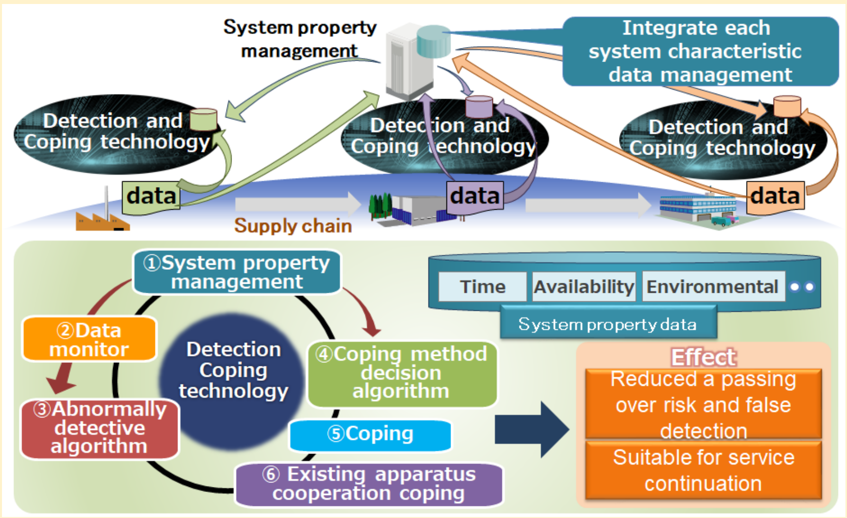
## Issues in IoT system and features of this technology


Detection
Difficult to detect data tampering due to diversification of IoT data
Mitigation
Due to NW / site restrictions, it is not possible to quickly take the primary measures that are originally required.
? ? ?
In-site NW
Can't confirm status due to malicious data
Stop the line
NW administrator
Previous technology
NY696
Sensor/Actuator


Detection
Abnormal data detection with low risk of false positives/oversights using system property data
Mitigation
Automatically execute safe primary measures on-site to improve service availability
System property management device
In-site NW
Accurately grasp status by detecting malicious data
System property data
・Time factor
・Availability requirements
・Environmental condition
Proposed technology
Measures considering system availability and safety
Sensor/Actuator

NW: NetWork

## R&D technology summary


System property management
Integrate each system characteristic data management
Detection and Coping technology
Detection and Coping technology
Detection and Coping technology
data
data
data
Supply chain
①System property management
②Data monitor
③Abnormally detective algorithm
Detection Coping technology
④Coping method decision algorithm
⑤Coping
⑥ Existing apparatus cooperation coping
Time
Availability
Environmental
System property data
Effect
Reduced a passing over risk and false detection
Suitable for service continuation

## Inflection of system properties

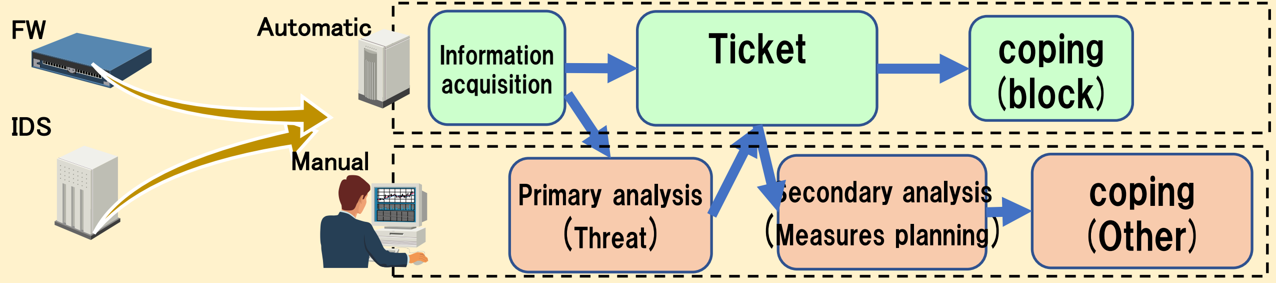
(1) Gather and manage IoT system property information

(2) Utilize system property information in abnormal detective algorithm

(3) Utilize system property information in coping method decision algorithm

## Comparison with existing technology

### ■Previous technology:SIEM/SOAR

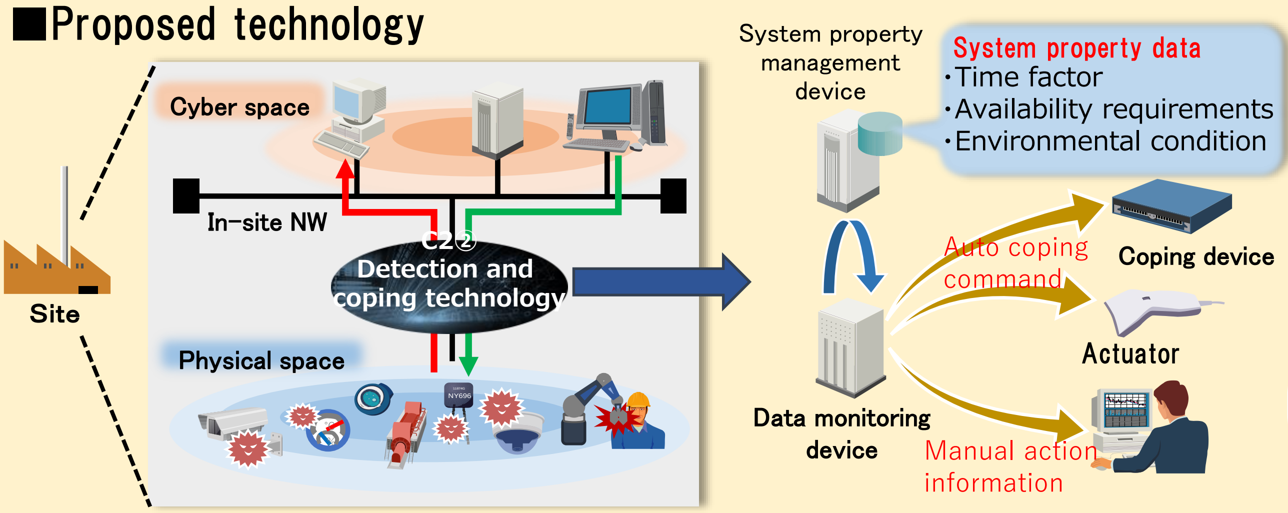


Security detection depends on FW / IDS / various sensors, detection that does not consider the characteristics of each site

Automate ticket / email issuance at SIRT. On-site automatic response is almost only shut off (isolated)

Operation
- MTTR as a whole will be reduced, but the primary action will be limited.

### ■Proposed technology



**System property data**
- ・Time factor
- ・Availability requirements
- ・Environmental condition

Abnormal data detection with low risk of false positives/oversights using system property data

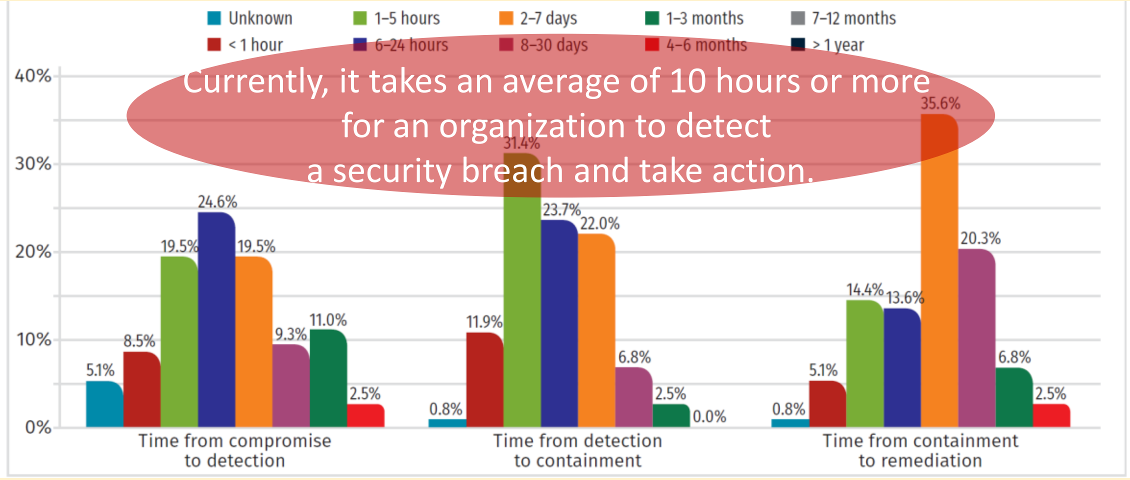
Automatically execute safe primary measures on-site to improve service availability

Operation
- The downtime of the system is greatly reduced by speeding up the first response.

SIEM: Security Information and Event Management SOAR: Security Orchestration, Automation and Response
SIRT: security incident response team FW: FireWall IDS: Intrusion Detection System MTTR: Mean Time To Repairs

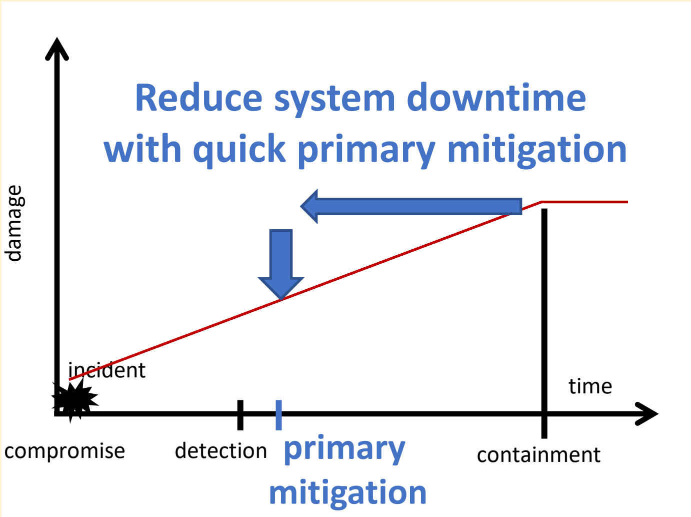
## Benchmark

### Aim to reduce response time by increasing the primary mitigation ratio at the site and significantly improve system downtime due to security breaches



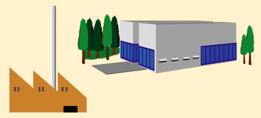
Currently, it takes an average of 10 hours or more for an organization to detect a security breach and take action.

Source: SANS 2019 Incident Response (IR) Survey: It's Time for a Change
Figure 2. Compromise to Remediation Times1

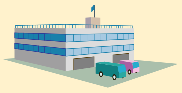


SANS: SysAdmin, Audit, Network, Security

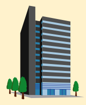
## Segment/Use cases



Production(factory)



Circulation



Building

This technology is applicable to security monitoring without adding a hand to an existing system in IoT system operating in various segments such as production (factory), the circulation, the building

## Expected effect

Keep the safe operation

Availability improvement of IoT systems

Early application of security measures

Maintenance of reliability of supply chain