Cross-Ministerial
Strategic Innovation Promotion Program (SIP)
Research and Development Plan for Cyber Physical Security (CPS)
for IoT Society
SIP-CPS Symposium 2019

～The goal is to realize a secure IoT supply chain for Society 5.0～

October 31, 2019（Thursday）　13：30～17：00

Bellesalle KANDA 2F HALL　SUMITOMO Fudousan　Kanda Bldg.
Kandamitoshiro-chou 7. chiyoda-ku Tokyo

Cabinet Office
New Energy and Industrial Technology Development Organization (NEDO)

内閣府
Cabinet Office, Government of Japan

NEDO
新エネルギー・産業技術総合開発機構
New Energy and Industrial Technology Development Organization

SIP 戦略的イノベーション創造プログラム
Cross-ministerial Strategic Innovation Promotion Program

ー Table of Contents ー

【Overall & Combination】

【Creation & Confirmation of Trustworthiness】

【Construction & Distribution of Trustworthy Chain】

【Verification & Maintenance of Trustworthy Chain】

Cross-Ministerial Strategic Innovation Promotion Program（SIP）
Research and Development Plan for Cyber Physical Security for IoT Society

Program Director, Dr. Atsuhiro GOTO（President, Institute of Information Security ）
Management Corporation: the National Research and Development Agency New Energy and Industrial Technology Development Organization（NEDO） Implementation Period:2018～2022

Cyber Physical Security Infrastructure, which can be utilized to protect IoT systems, services and large-scale supply chains including SMEs, should be developed and verified for the purpose of protecting various IoT devices, and ensuring safety and security in society as a whole, towards the secure Society 5.0.

Research & Development Items

A Creation & Confirmation of Trustworthiness

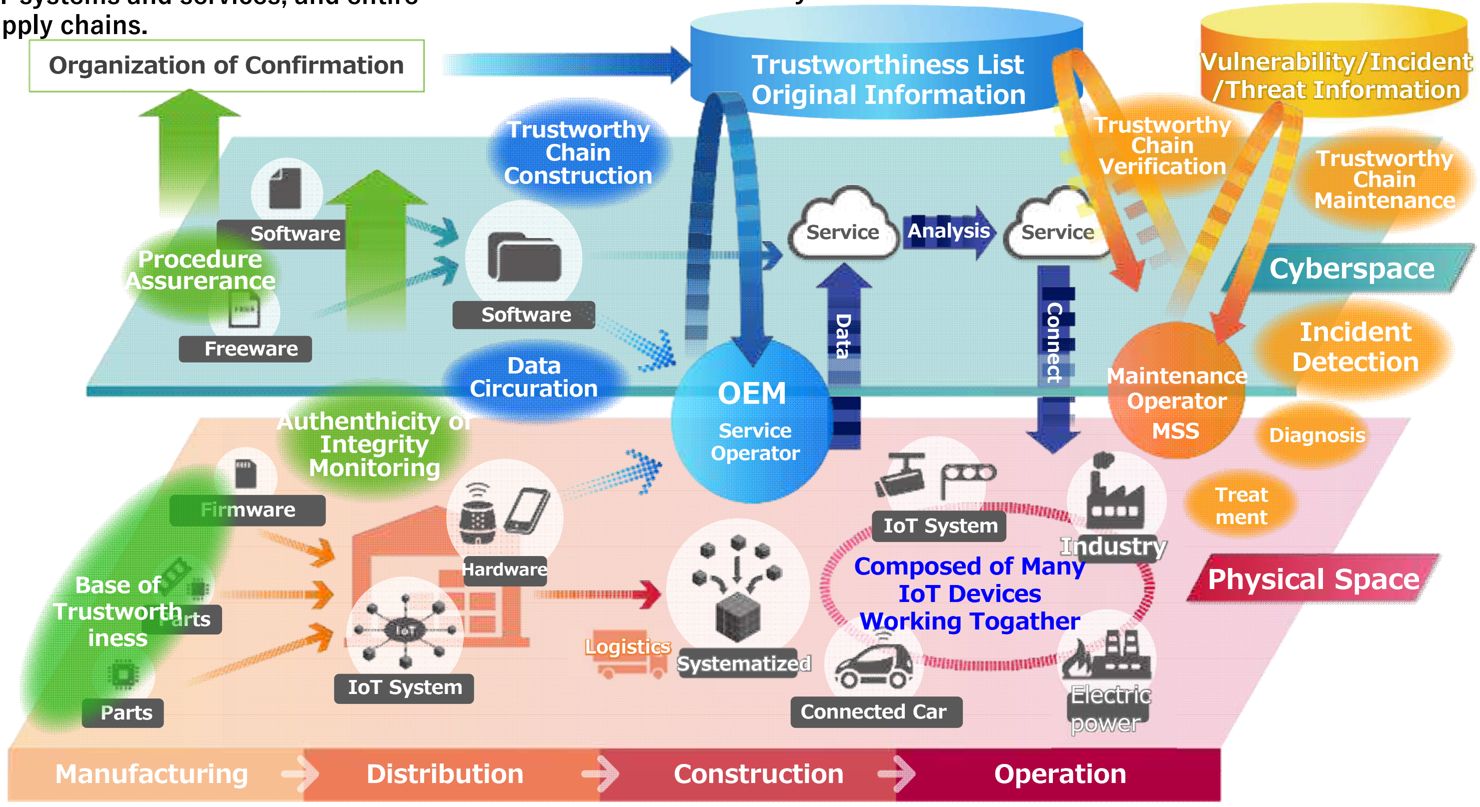
Technology for creation and confirmation of trustworthiness, which is necessary to achieve assurance of security for various IoT systems and services, and entire supply chains.

B Construction & Distribution of Trustworthy Chain

Technology for constructing a "trustworthy chain" and construction, and for ensuring the secure distribution of necessary information

C Verification & Maintenance of Trustworthy Chain

Technology to enable verification of safe operation, and maintenance of a "trustworthy chain"



Background of R&D

IoT risks：
Cyber attack threats lurk in all industrial activities

Global economic losses from cybercrime are $ 600 billion（Equivalent to 0.8% of global GDP⇒About 3 trillion yen in Japan）

Risk that cyber attack will reach physical space and economic loss will further increase due to fusion of physical and cyber by IoT

Supply chain risks：
The trend of the cybersecurity framework, which is required by supply chains for procurement

In the United States, NIST SP800-171 is established as a standard for cybersecurity measures for controlling Controlled Unclassified Information (CUI) and required by supply chains for defense procurement.

In Europe, the policy package published in September 2017 states that the EU Cybersecurity Certification Framework will be improved in the future.

Dealing with IoT risks and supply chain risks is an urgent issue.

【Hitachi, Ltd. / NEC Corporation / KDDI Research, Inc.】

Challenge to recover the trust of the supply chain

CREATION & CONFIRMATION

CONSTRUCTION & DISTRIBUTION

VERIFICATION & MAINTENANCE

Society connected by trust with avoiding fraud of product and service

Introduction of the concept

The shape of future security that we consider is:
creating “Trust” in Society 5.0 that is smart society of cyber-physical integration.

Future figure of Society 5.0

1 Creation of Trust

- Conforming of “Value Creation Process” with defined standards or rules
- Creating “Trust” proved by “Digital Evidence”

Booth No

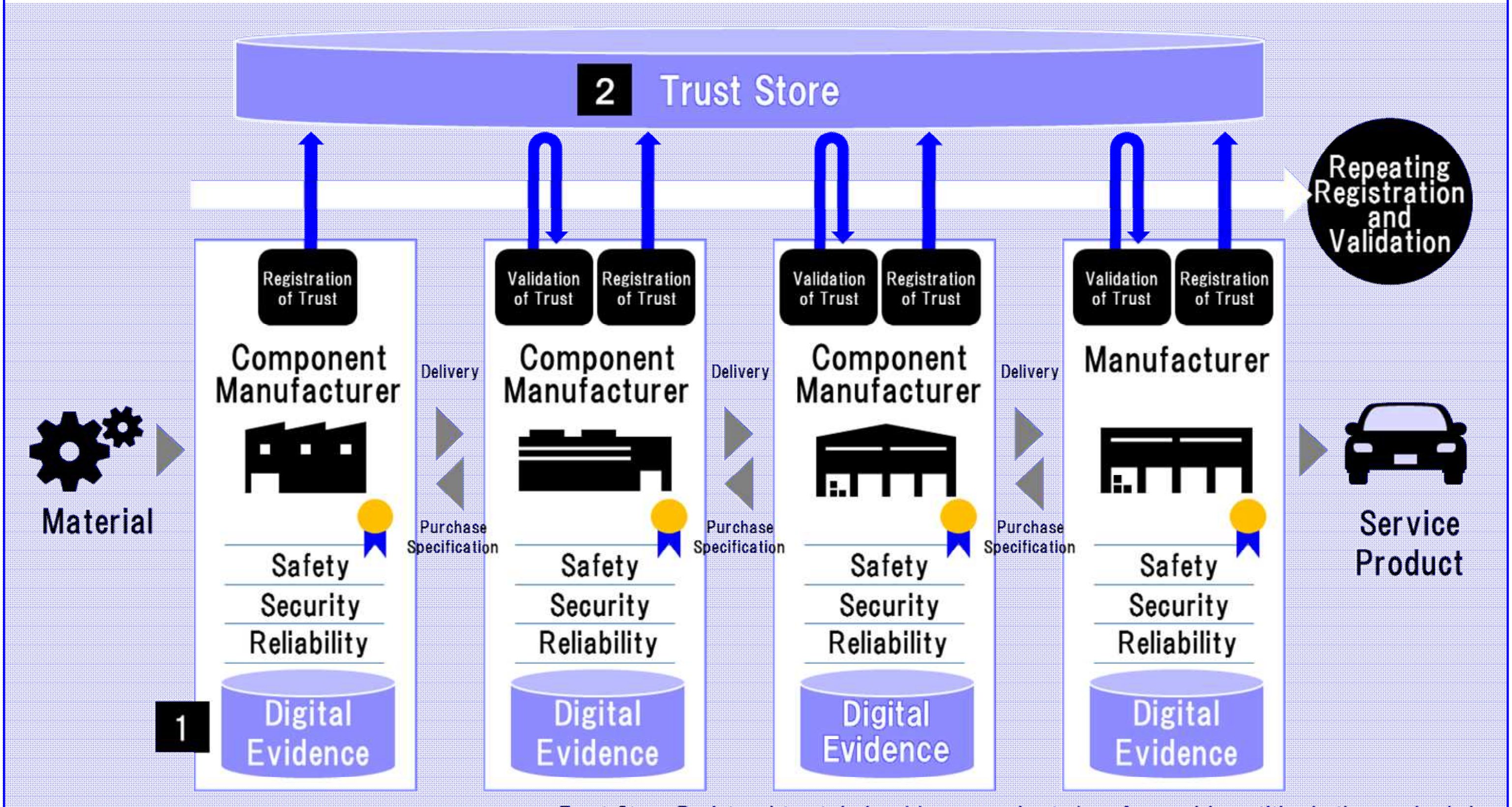
confirming trust through certification of the eligibility of ⑪People, ⑫Data, ⑬Procedures

2 Trust Chain

- Connecting each safety, security and reliability by mutual linkage in the Trust Store ＊
- Validness of “Trustworthiness” in the whole of the supply chain

Booth No

⑭Visualized of Trust Chain



＊Trust Store: Registered trust declared by companies to be referenced by entities in the supply chain

【Hitachi, Ltd.】

Visualization of the Trust Chain across the organization in the Supply Chain

CONSTRUCTION & DISTRIBUTION

VERIFICATION & MAINTENANCE

Structuring and validation of Trust Chain by registration and linkage of trust information

Our Features

- **Construction of a Trust Chain**
  Trust Chains structured by Certificates, Linkage Information and Capability Lists
- **Interface for Trust Store**
  Providing I/F to utilize Trust Store for suppliers
- **Management on whole lifecycle**
  Adaptable for lifecycles of products
- **Design for Trust Chain in the society**
  Roadmap and future image of the system

Our Solution

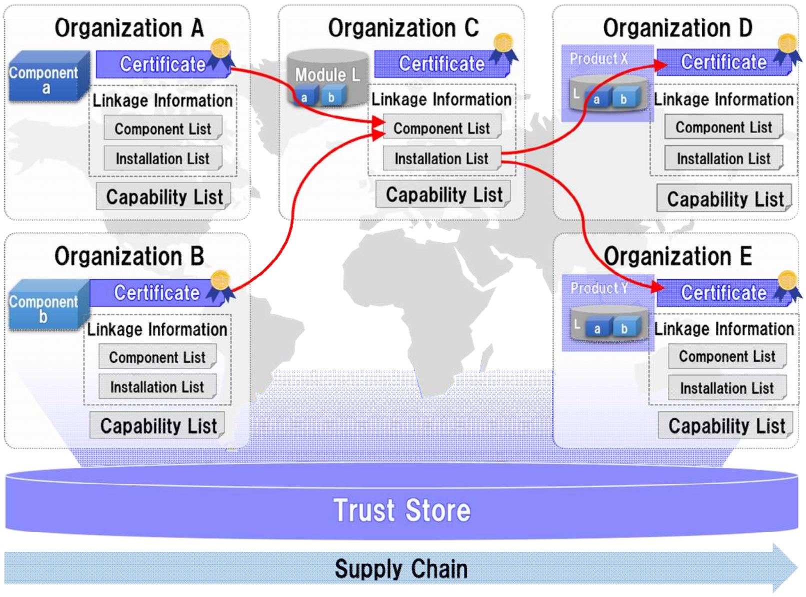
①Enable to confirm the trustworthiness on whole of the supply chain

②Easy adaption for suppliers

③Long term usability for various suppliers

④Enable to confirm the trustworthiness on different sectors and nations

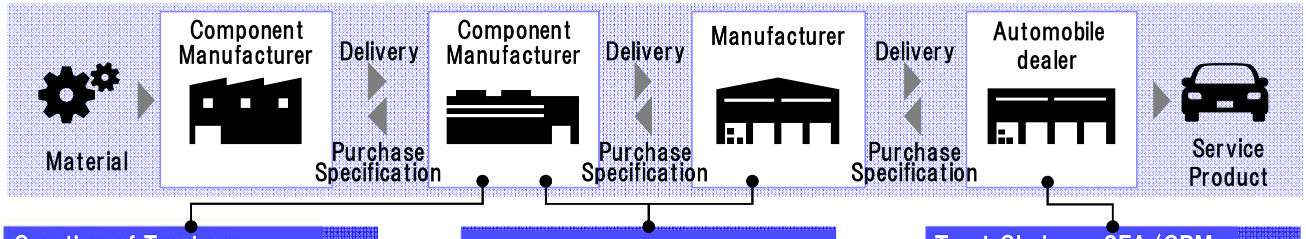
Outline of confirming trustworthiness in supply-chain



Certificate	： document to show the component, module, product and service are good
Linkage Information	： information of the connection of organizations
Capability List	： information of conformed capability (qualification, capability, regulation, standard, etc.)
Trust Store	： storing Certificates, Linkage Information, Capability Lists to enable confirmation of trustworthiness on whole of the supply chain

Demonstration : introduction of one of use case

Introduction of the world where the trust of the entire supply chain can be confirmed in an environment that simulates the system of parts vendors, finished product vendors, and sales offices.



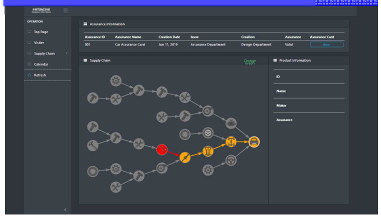
Creation of Trust on production support system

Adaption image on a production management system used in Japanese shared factory

Digital Evidence on PLM system

Adaption image on a PLM which have many experience in global manufacturing fields
PLM: Product Lifecycle Management

Trust Chain on SFA/CRM system



Development of usage image on a future sales support system
SFA: Sales force automation
CRM: Customer relationship management

【ECSEC, AIST, etc.】

Trust Creation in the IoT Supply Chain

CREATION & CONFIRMATION

"Chain of Trust"
Security and Trust for the Foundation of Society 5.0: the IoT system / Service / Supply Chain

Technical Features

■ Root of Trust Implementation

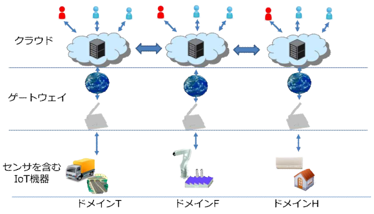
Research and development for implementing Root of Trust applicable to a wide variety of small IoT devices to build a chain of trust

■ Security Assurance Scheme

Promoting practical application through research and development of security assurance schemes for Root of Trust

Assumption: Open IoT Deployment

1 Until around 2020

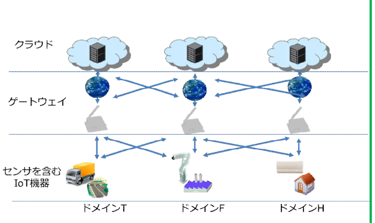


Slightly closed IoT

■ IoT architecture is currently configured by vertical integration for each domain or business owner.

■ Information is partially exchanged between domains or business owners via the cloud.

2 Around 2030



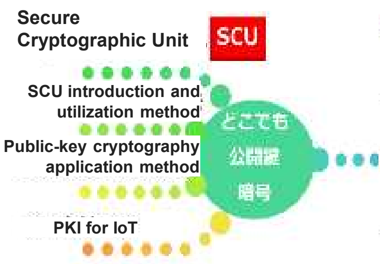
Open IoT

■ Regardless of domain or business owner, data will be processing in various layers for distribution meshing, service diversification, and virtualization.

■ Develop toward the ultimate IoT environment where multiple stakeholders are connected.

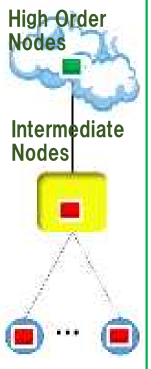
Ideal: Widely Available Public-key Cryptography

Public-key cryptography can be widely available, even at the end nodes in large-scale IoT system, .

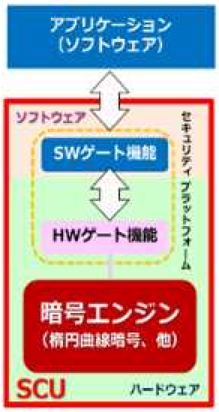

Secure Cryptographic Unit
SCU
SCU introduction and utilization method
Public-key cryptography application method
PKI for IoT
どこでも
公開鍵
暗号

SCU Utilities

A	Stronger security than when only common key cryptography is available
B	Reduction of key management and security management costs for end nodes
C	Contributing to the convenience and security of large-scale IoT



SCU（Secure Cryptographic Unit）


アプリケーション（ソフトウェア）
ソフトウェア
SWゲート機能
HWゲート機能
セキュリティプラットフォーム
暗号エンジン（楕円曲線暗号、他）
SCU
ハードウェア

Hardware Crypto Engine

256-bit elliptic curve cryptography processing

・For end nodes: Achieved ultra-low power of 1mW class and small area and low cost of 10k gate class

・For intermediate nodes: Ultra-high speed operation of 10,000times/sec or more

Physical random number generator, Common key cryptography, etc.

Security Platform

Even if the application is tampered with and attempts to gain unauthorized access to the cryptographic engine, the security platform with the SWG/HWG function detects the malicious access.

Useful for System Security

Data encryption/decryption, digital signature generation/verification, storage/communication data/program protection, system secure boot, etc.

Electronic Commerce Security Technology Research Association(ECSEC), National Institute of Advanced Industrial Science and Technology(AIST), Yokohama National University, The University of Tokyo, Tohoku University, Kobe University, Nara Institute of Science and Technology, Mitsubishi Electric Corporation

【ECSEC, AIST, etc.】

SCU Application Systems Leading to Social Implementation

CREATION & CONFIRMATION

Model System Establishment Promoting Social Implementation of SCU with Public-key Crypto Engine

POINT

- Implements mutual authentication of cryptographic devices suitable for various model systems with high-speed engines
- Build the model system, Establish SCU application system, and demonstrate practical technology
- Promoting social implementation of SCU equipped with public key encryption engine

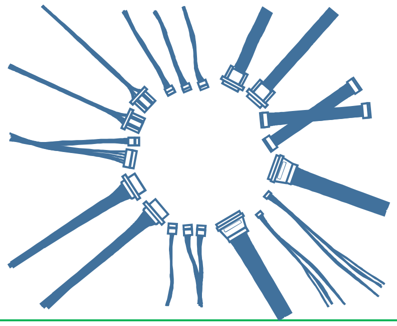
Model System 1

SCU application model system for general embedded devices

中～大規模監視をサポート—最大1000台のカメラを統合管理
最大接続管理数
※カメラ　1,000台
※操作PC　100台
※レコーダ　500台
※センサ　4,000台
P
監視センター

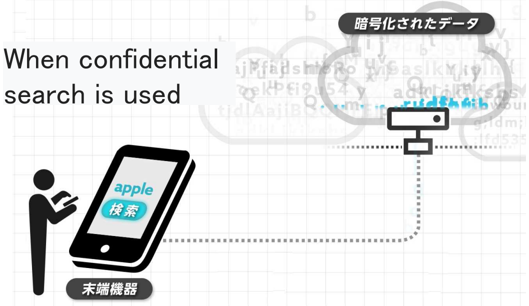
Model System 2

SCU application model system for ultra-small embedded devices



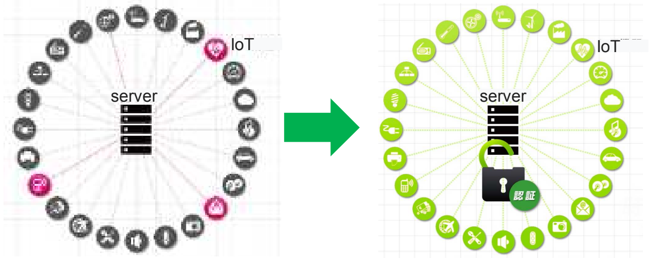
Model System 3

SCU application model system for Searchable Encryption



Model System 4

SCU application model system for aggregate signature



Electronic Commerce Security Technology Research Association(ECSEC)、National Institute of Advanced Industrial Science and Technology(AIST)、YOKOHAMA National University、The University of Tokyo、TOHOKU UNIVERSITY、Kobe University

【NAIST･Kobe Univ.･Tohoku Univ.･YNU･ECSEC】

Countermeasure Technologies against Hardware Trojan

CREATION & CONFIRMATION

We keep hardware security as the root of trust in information systems and dramatically improve the reliability of information systems supporting social infrastructure.

Technical Features

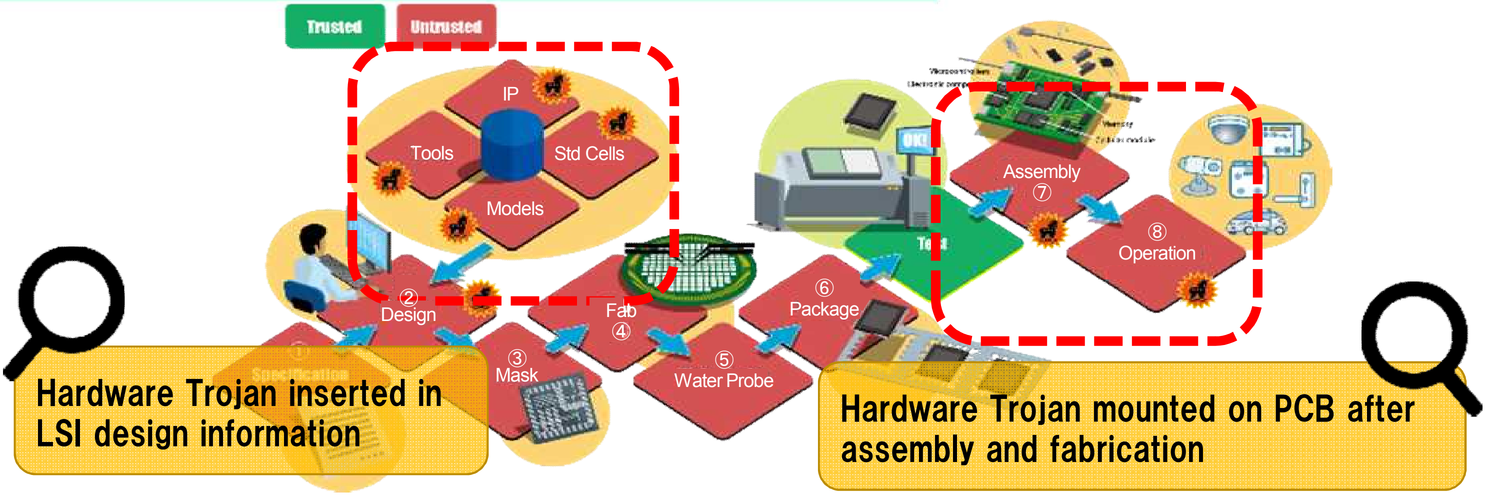
■ Hardware Trojan detection methods

We are developing detection methods of hardware Trojan mounted on the PCB board after the manufacturing process and fabrication. Based on this, we will secure hardware security as the root of trust.

■ Formal verification methods for hardware Trojan-free IC design

We are integrating hardware logical description verification methods for IP cores and formal verification used for software security. Based on this, we will build fundamental theories that guarantee hardware Trojan-free IC design.

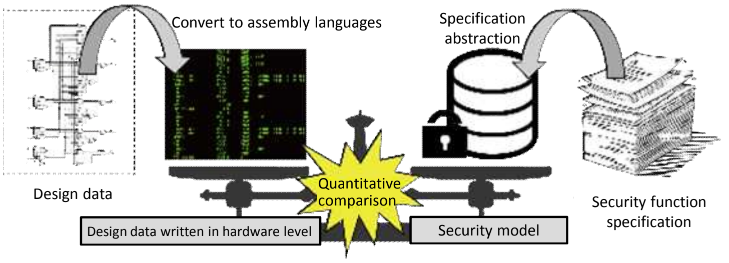
Hardware Trojan threats in supply chains



Hardware Trojan inserted in LSI design information

Hardware Trojan mounted on PCB after assembly and fabrication

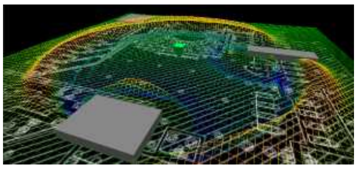
Formal verification methods


Convert to assembly languages
Specification abstraction
Design data
Quantitative comparison
Security function specification
Design data written in hardware level
Security model

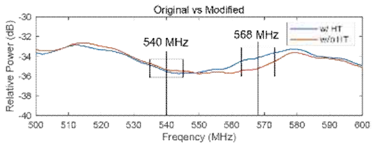
Assuming that HT is installed in IP purchased from a third party when designing a semiconductor chip, we are developing a theory to detect HT inserted into IP using formal verification methods.

Electrical detection methods

Time-domain detection



Frequency-domain detection



We are developing methods of measuring the electrical variations in the ICs and PCBs using the active sensor inside the SCU and detecting the mounted position of HTs based on the measurement information.

Nara Institute of Science and Technology, Kobe University, Tohoku University, Yokohama National University, Electronic Commerce Security Technology Research Association(ECSEC),

【National Institute of Advanced Industrial Science and Technology（AIST）】

Building security assurance schemes for SCUs used in low-cost IoT devices

CREATION & CONFIRMATION

Ensuring a balance between rigorous security evaluation and development man-hours by means of threat analysis and security requirement clarification

Technical Features

■ Security level classification

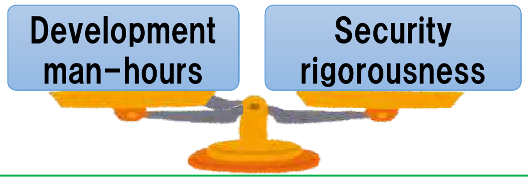
Ensuring the validity of how to classify the level of certainty of security implementation and of how to show security for the low-cost IoT nodes

■ Security assurance schemes

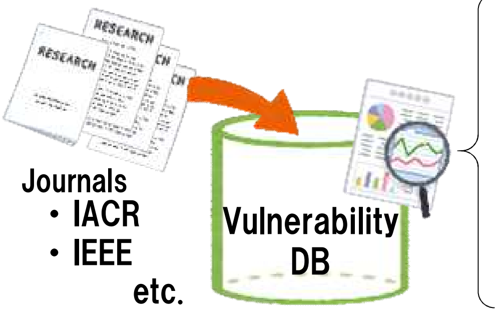
Building security assurance schemes（security evaluation technology and certification framework）optimal for devices using hardware roots of trust

Security assurance of SCU-used IoT devices

Based on cryptographic hardware roots of trust, develop highly reliable devices at reasonable cost



Systematic aggregation of attack methods for IoT devices



Journals
- IACR
- IEEE

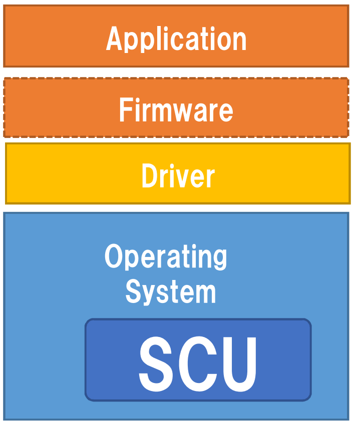
etc.

Vulnerability DB

- Physical Attacks
- Overcoming sensors and filters
- Perturbation Attacks
- Retrieving keys with DFA
- Side-channel Attacks
- Exploitation of Test features
- Attacks on RNG
- Java Card applications
- Software Attacks

Building security assurance schemes for roots of trust

Ensuring security of an IoT device by using an SCU as root of trust



Application

Firmware

Driver

Operating System

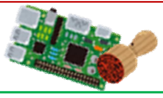
SCU

= IC chip

User oriented Approach
- ･Guideline
- ･Checklist

Reliable use of cryptography achieving low power consumption and high security

Rigorous Assurance



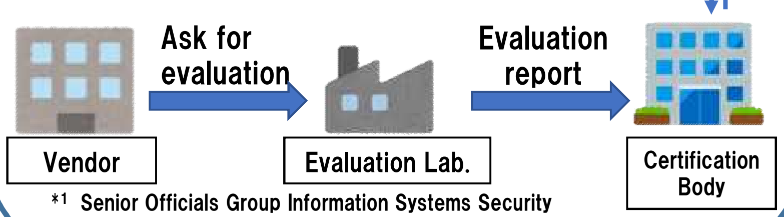
Building security assurance schemes for SCUs

- SOGIS
- JEDS
- JHAS

Certify SCUs used in the target IoT devices as cryptographic modules

Oversea Organization

Consider how security assurance for SCU-used devices should be, based on discussion trends such as vulnerability rating in SOGIS[*1] and evaluation assurance level EAL[*2],



Ask for evaluation

Evaluation report

Vendor

Evaluation Lab.

Certification Body

[*1] Senior Officials Group Information Systems Security

[*2] (Evaluation Assurance Level)

National Institute of Advanced Industrial Science and Technology（AIST）

【Nippon Telegraph and Telephone Corporation】

Authenticity and Integrity Monitoring System for OT/IoT devices

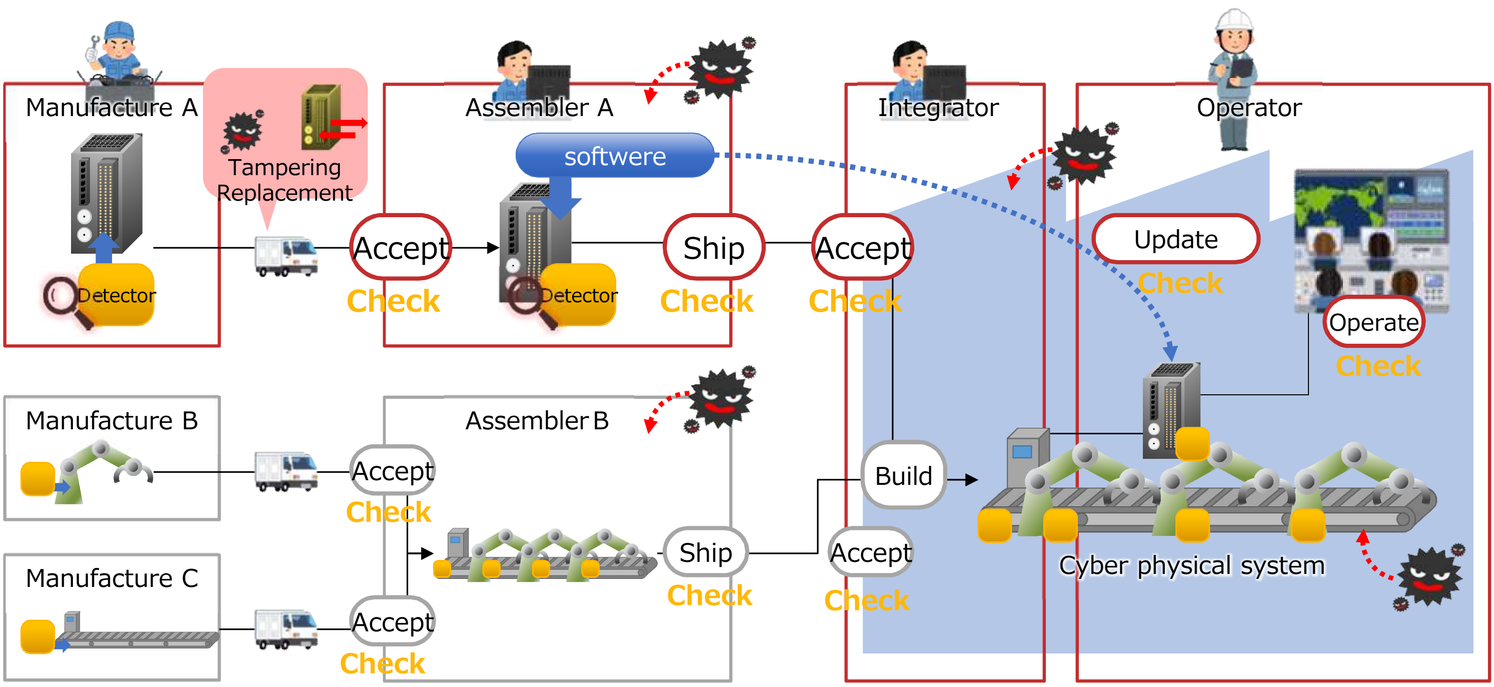
CREATION & CONFIRMATION

Achieve a supply chain that is resistant to the introduction of unauthorized software by monitoring the authenticity and Integrity of various OT/IoT devices

Technical Features

- **Integrity monitoring at any step of the distribution process**
  Automate a software integrity monitoring securely and reliably various OT/IoT devices.
- **Secure verification list sharing and updating**
  Multiple suppliers can update and share a verification list when authorized changes are applied to the devices. Segregation of authority realize secure integrity monitoring.
- **Verification list generator for non-security professionals**
  Automatic generator provides accurate verification list for various devices.

Any supplier in supply chain can easily confirm the integrity of devices at any time



Integrity monitoring even after shipment

The verification function implemented on the devices allows the user to check the integrity of the devices after shipment, and securely perform security updates.

Detect tampering and replacement

Each company verifies the authenticity of devices at the time of acceptance and shipment, thereby realizing a secure supply chain that prevents unauthorized software from mixing in.

Ensure system integrity In operation

Enables the detection of falsification of the entire cyber physical system, which is composed of a variety of devices, by determining each device.

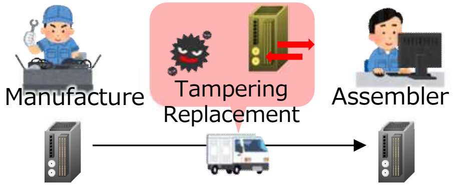
Background of this research

Toward the realization of Society 5.0, smarter factories and the spread of IoT devices are increasing the risk of "incorporation of illegal functions" throughout the devices lifecycle. To supply safe products and operate devices safely, it is necessary to verify the integrity of devices not only during the manufacturing and operation of devices, but also throughout the supply chain.

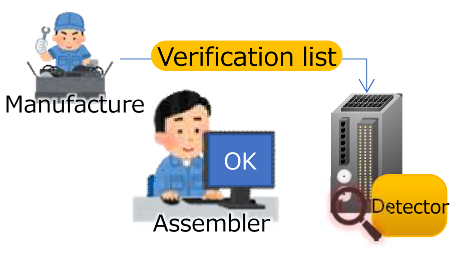
Usage of the technology

Monitoring upon arrival

There is a risk that unauthorized software may be installed or devices may be replaced during the delivery of devices.

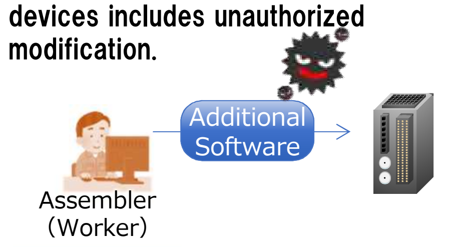


Enables monitoring that the correct software is installed on the correct devices based on the criteria.

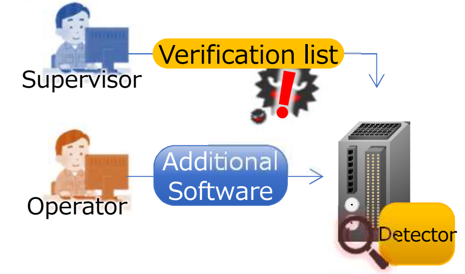


Monitoring before shipment

When a function is added to a devices, there is a risk that the devices includes unauthorized modification.

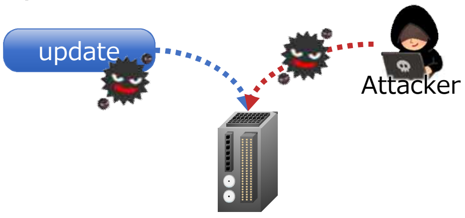


Enables monitoring that the work has done correctly based on verification list defined by the supervisor.

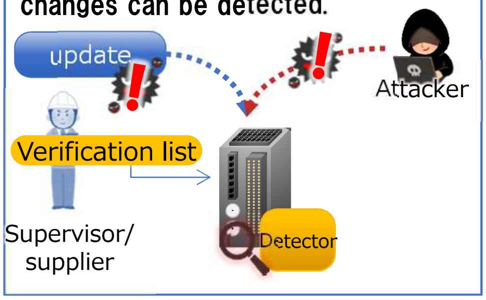


Monitoring during the operation

There is a risk of external attack and modification of update when operating the devices.

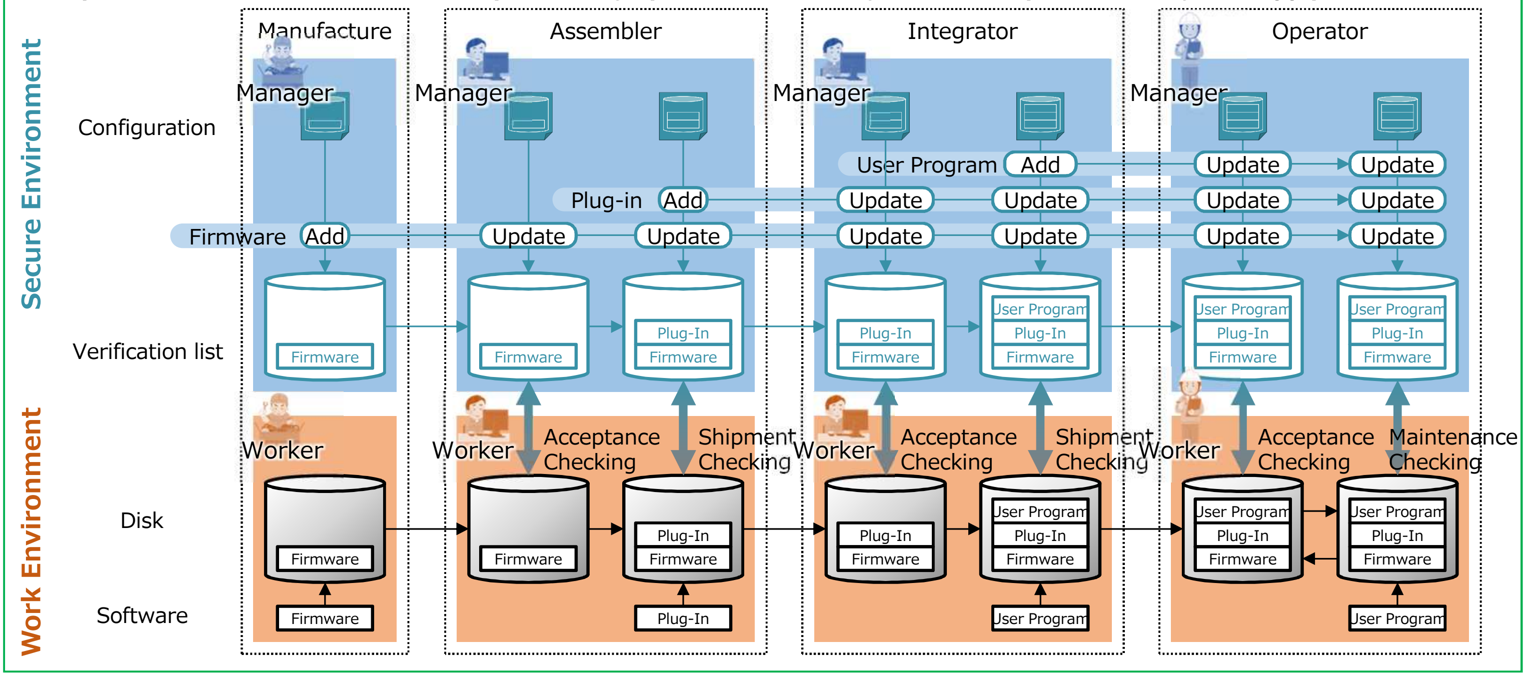


Using verification list with third party certification, unintended software changes can be detected.



Technical Essentials

In accordance with changes in the software configuration at the time of distribution and at each stage after the start of operation, the state of the correct devices is managed in a secure environment, and the latest evaluation criteria are always shared. This ensures authenticity and integrity of devices throughout its lifecycle, including the supply chain.



【NEC Corporation】

Lightweight Authenticity and Integrity Monitoring of Devices in Operation

CREATION & CONFIRMATION

Ensuring safety via "tamper detection" of software in operation implemented on IoT devices with limited performance and memory capacity

Technical Features

- **Continuous monitoring of IoT devices (not limited to booting)**
  Improving the safety of IoT devices in continuous operation by monitoring authenticity and integrity of the software codes of IoT devices
- **Supporting operation via automated implementation and recovery**
  Minimizing the cost of development/recovery (when tampering is detected) even when there is device or software update using automated tools

Problems

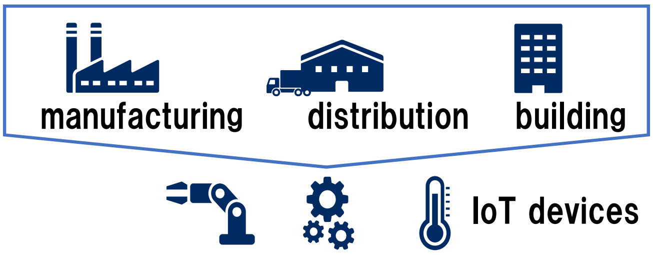
There are existing authenticity and integrity monitoring technologies comparing the software hash values using a whitelist;

① Cost of whitelist preparation for each software version is high

② Execution order has to be monitored in addition to code integrity

③ Cost of recovery from tampering is high

Target Domain and Use Cases



Applicable to IoT devices used in IoT systems of manufacturing, distribution, smart building, etc. to monitor devices' integrity

Overview of R&D Technologies toward Solving Problems

① Development phase

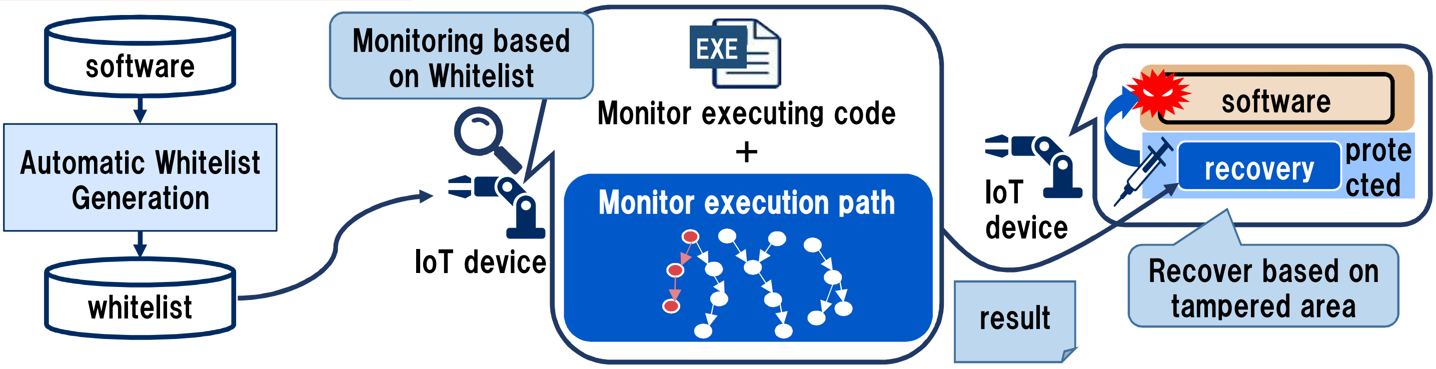
Whitelist Generation
Generating whitelist automatically to reduce monitoring overhead

② Detection phase

Accuracy Improvement
Improving the safety by monitoring both the execution path and code

③ Recovery phase

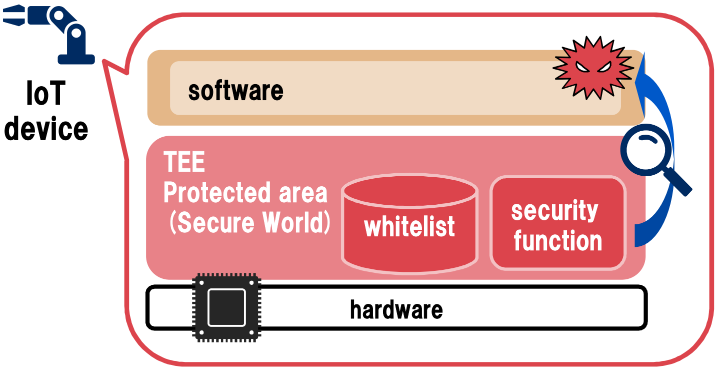
Automated Recovery
Recovery of devices from tampered state to normal state



Realizing Authenticity and Integrity Monitoring of Operating IoT devices

■ Lightweight

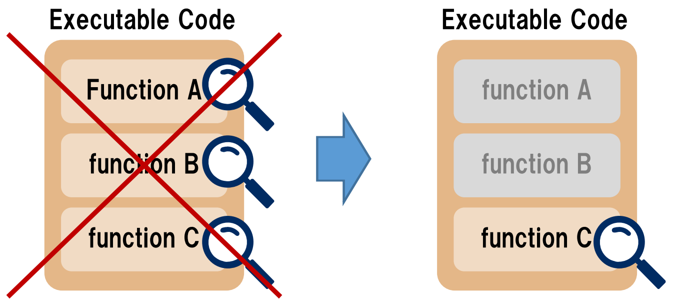
Monitoring only the executing code instead of the complicated software behavior. Using protected memory of TEE(*) to achieve lightweight implementation without additional software protection.



(*) TEE: Trusted Execution Environment

■ High speed

By understanding the software structure and the memory region of functions to be inspected, monitoring only the specific region. High-speed monitoring is achievable without affecting the operation.



Monitoring all regions causes high overhead

Reduce overhead by monitoring specific region

Usage Image of the Technology

Equipment manufacturer

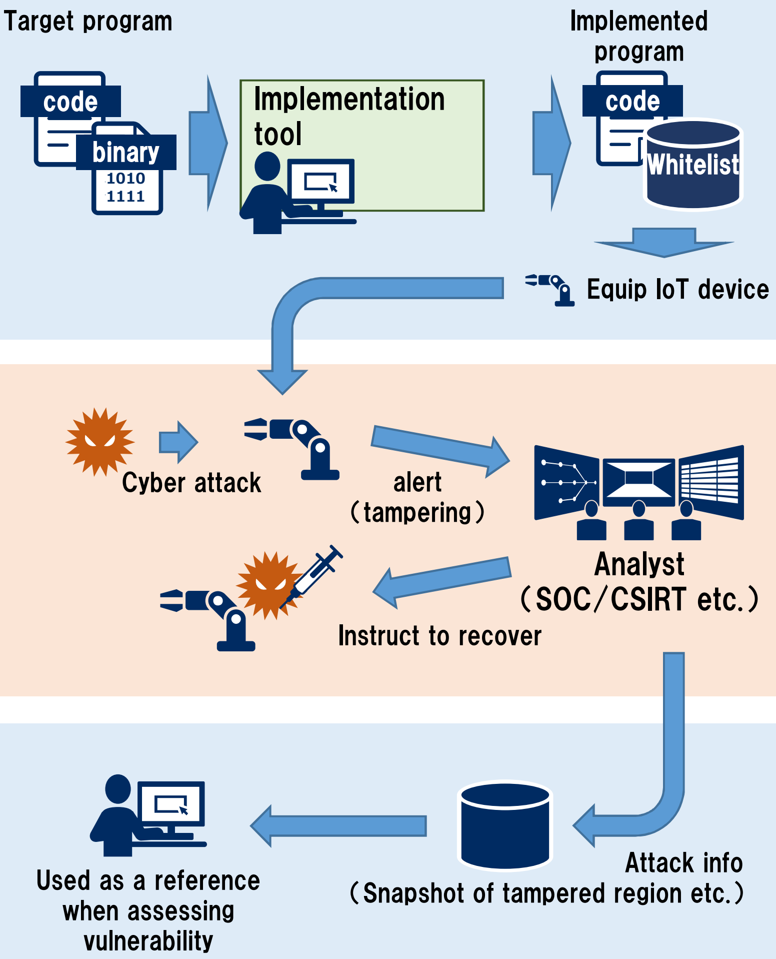
- Implement the authenticity and integrity monitoring functions automatically via a development tool which incorporates source code and binary
- Equip the IoT device with the implemented programs

User company

- Raise an alert on a remote console when tampering occurs due to cyber attacks
- When recovery is performed from the console, the device resumes normal operation

Equipment manufacturer

- Fix vulnerabilities based on information collected from attacked IoT devices



[MEMO]

【Hitachi, Ltd. 】

VCP Conformance Validation for Supply Chain

CREATION & CONFIRMATION

Creation/Confirmation of trust based on conformance of people, data, and procedures

Technical Features

- **Conformance Validation**
  Define VCP* model as a standard of validation and validate conformance with field results
- **Digital Evidence**
  Store digital evidence being a root of trust

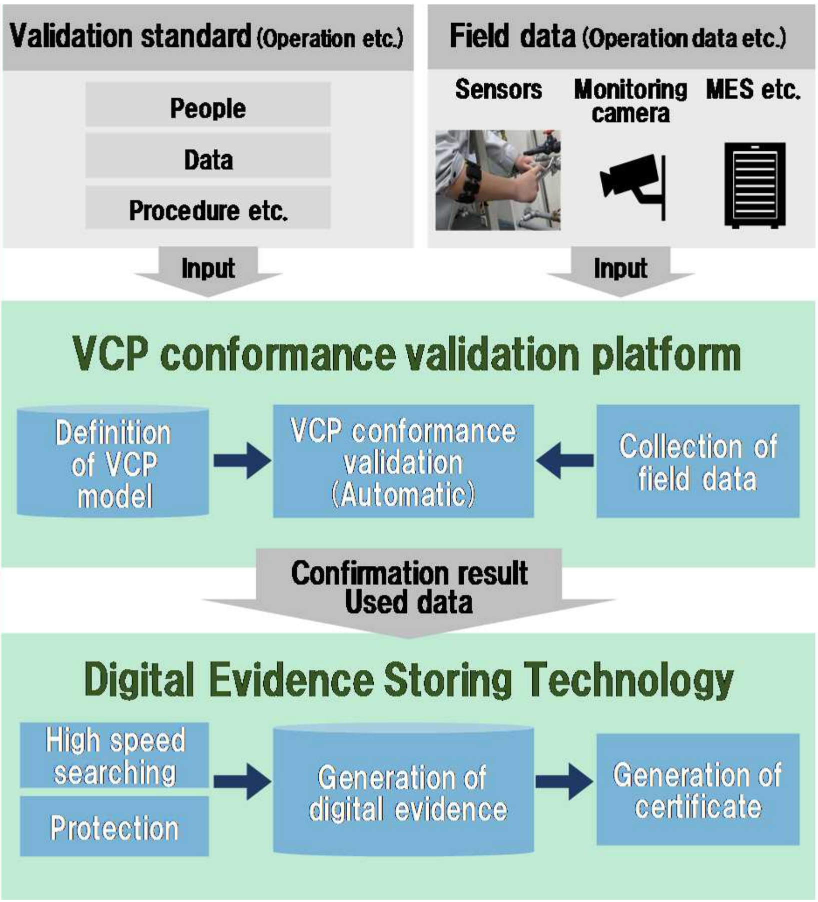
*VCP:Value Creation Process

Effects

Conformance validation of VCP in supply chain by using this technology

- Increase company values and CSR
  ① Contribution for company compliance by detection of illegal operation
  ② Contribution for increasing company value and CSR by indicating accountability for others as rationales
- Use cases
  Validate conformance of people, data, and procedures in supply chain and store evidence

Outline of Creation and Confirmation of Trust


Validation standard (Operation etc.)

People

Data

Procedure etc.

Field data (Operation data etc.)

Sensors

Monitoring camera

MES etc.

Input

Input

VCP conformance validation platform

Definition of VCP model

VCP conformance validation (Automatic)

Collection of field data

Confirmation result

Used data

Digital Evidence Storing Technology

High speed searching

Protection

Generation of digital evidence

Generation of certificate

Demonstration of VCP Conformance Validation

In this demonstration, we show example system with VCP conformance validation. We introduce a sequential flow of conformance validation in each process, VCP conformance validation by using each result and output of digital evidence with used data.

Display field movie at conformance validation in each VCP process ▶ Operation (Myogenic potential signal) | Position

Display status of each VCP process ▶ VCP conformance validation

Conformance of data management in supply chain

CREATION & CONFIRMATION

Confirming the “Correctness” of data management

Technical Features

- **Make rules of correct data management**
  Set conditions to prevent falsification and leak as profile
- **Acquire and store log and environmental information of terminal securely**
  Acquire and store as Digital Evidence in data
- **Conformance**
  Automatic conformance by comparing profile and DE

Effect

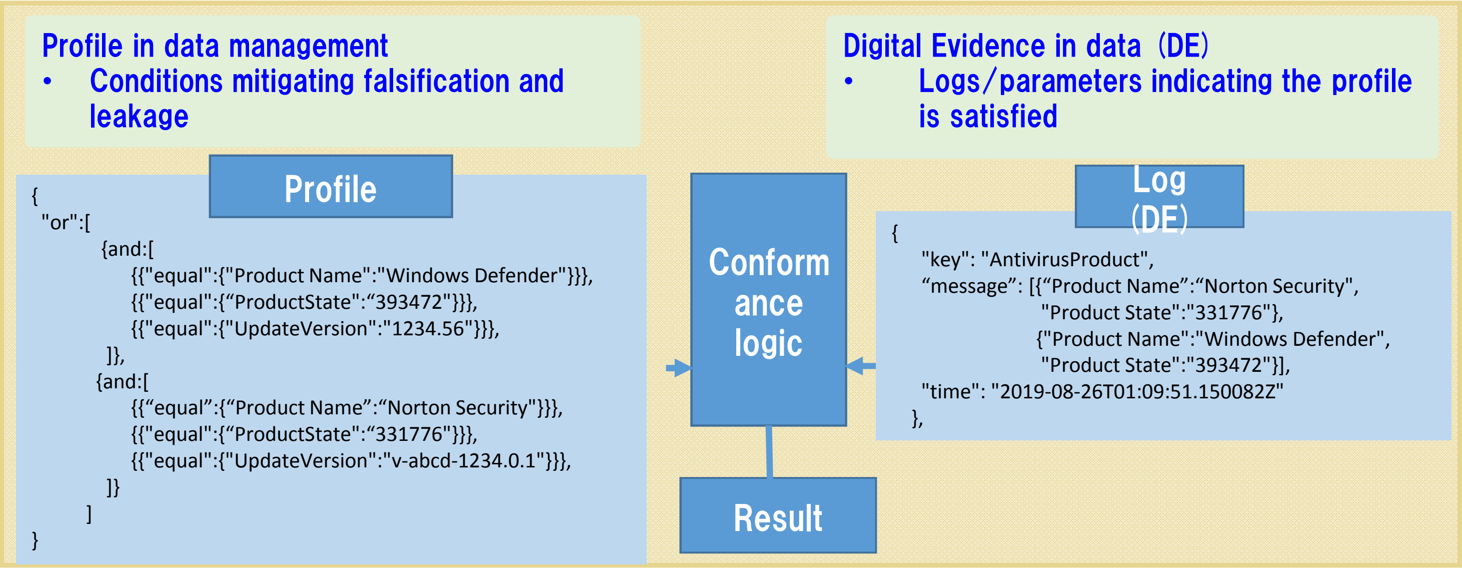
Object：Creation of trust by ensuring data management
Usecase：Data exchange on supply chain
Threat：Falsification, leak and theft

Overview of conforming data management

Profile example:
 Security software is installed and updated to the latest version

Conforming data management logic

1. Extract conditions specified in profile
2. Search the target log and compare with conditions



Profile in data management
- Conditions mitigating falsification and leakage

Digital Evidence in data（DE）
- Logs/parameters indicating the profile is satisfied

```
{
 "or":[
          {and:[
               {{"equal":{"Product Name":"Windows Defender"}}},
               {{"equal":{“ProductState":“393472"}}},
               {{"equal":{"UpdateVersion":"1234.56"}}},
           ]},
         {and:[
               {{“equal”:{“Product Name”:“Norton Security"}}},
               {{"equal":{“ProductState":“331776"}}},
               {{"equal":{"UpdateVersion":"v-abcd-1234.0.1"}}},
           ]}
        ]
}
```

```
{
    "key": "AntivirusProduct",
    “message”: [{“Product Name”:“Norton Security",
                    "Product State":"331776"},
                   {"Product Name":"Windows Defender",
                    "Product State":"393472"}],
    "time": "2019-08-26T01:09:51.150082Z"
   },
```

Conformance of data management in supply chain

CREATION & CONFIRMATION

Confirming the “Correctness” of data management

Implementation image of confirming the correctness

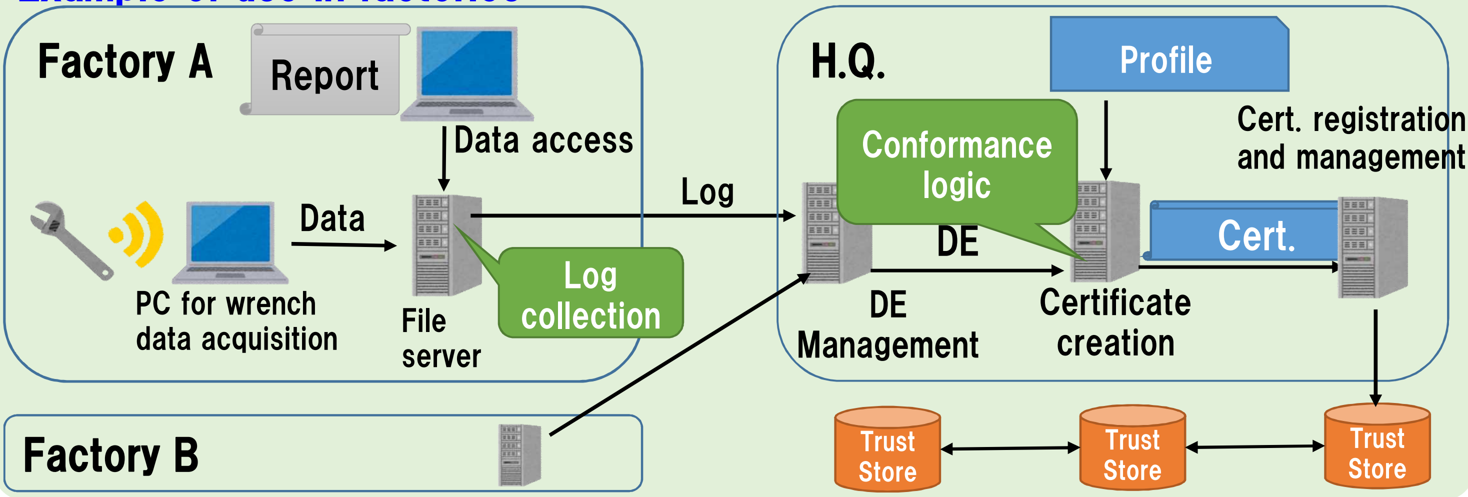
◆Data management includes data access, data acquisition, data transmission and data storage. Confirmation of “correctness” is required for all process

◆Certificate proves the correctness in each organization

◆Digital Evidence as the basis of “correctness”

◆Trust Store connects the correctness of each organization and proves overall correctness

Example of use in factories



Application to building management

Organization	Role	Targeted data
Elevator manufacture	Manufacturing, remote monitoring	Specification, Monitoring data
CCTV manufacture	Manufacturing	Specification, Maintenance record
Air conditioning equipment manufacture	Manufacturing	Specification, Maintenance record
Contractor	Construction	Specification
Maintenance worker	Maintenance	Maintenance record
Security service provider	Surveillance	CCTV data, Entry/exit record

Contact : https://www.kddi-research.jp/inquiry.html

【NEC Corporation】

Conformance validation of people in supply chains

CREATION & CONFIRMATION

Ensuring trustworthiness of service delivery and manufacturing enabled by employees

Technical Features

Conformance validation of people and issuance of certificates

■Retrieval of attributes with different characteristics

Acquiring latest, valid values of attributes to validate employee conformance

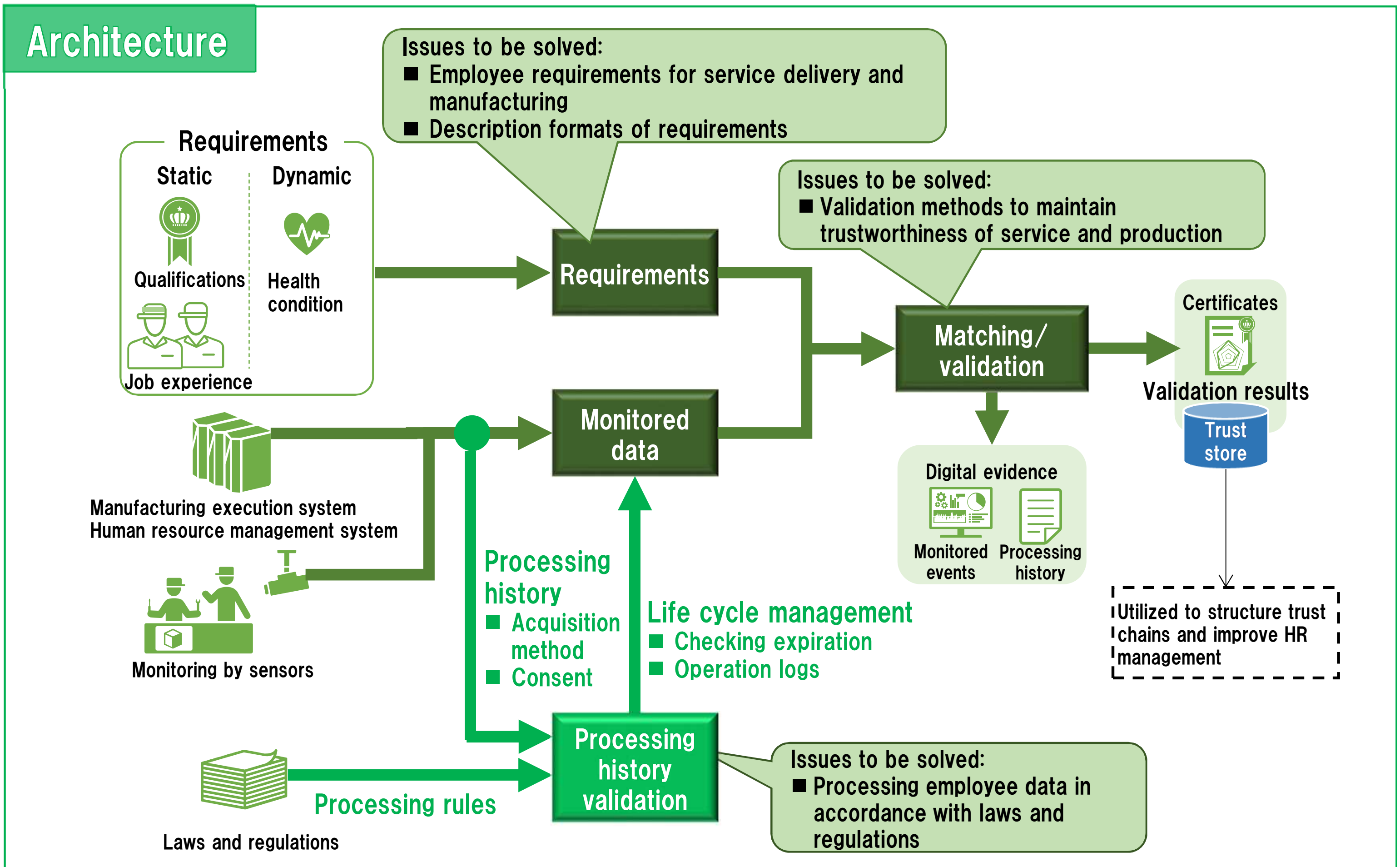
■Regulation-compliance in processing employee data

Disclosure of employee data to third parties in accordance with laws and regulations

Value

1. Detecting non-conforming operations to help maintain the safety of services and products
2. Structuring trust chains to accelerate problem discovery in supply chains
3. Utilizing certificates in a trust store to improve human resource management

Architecture



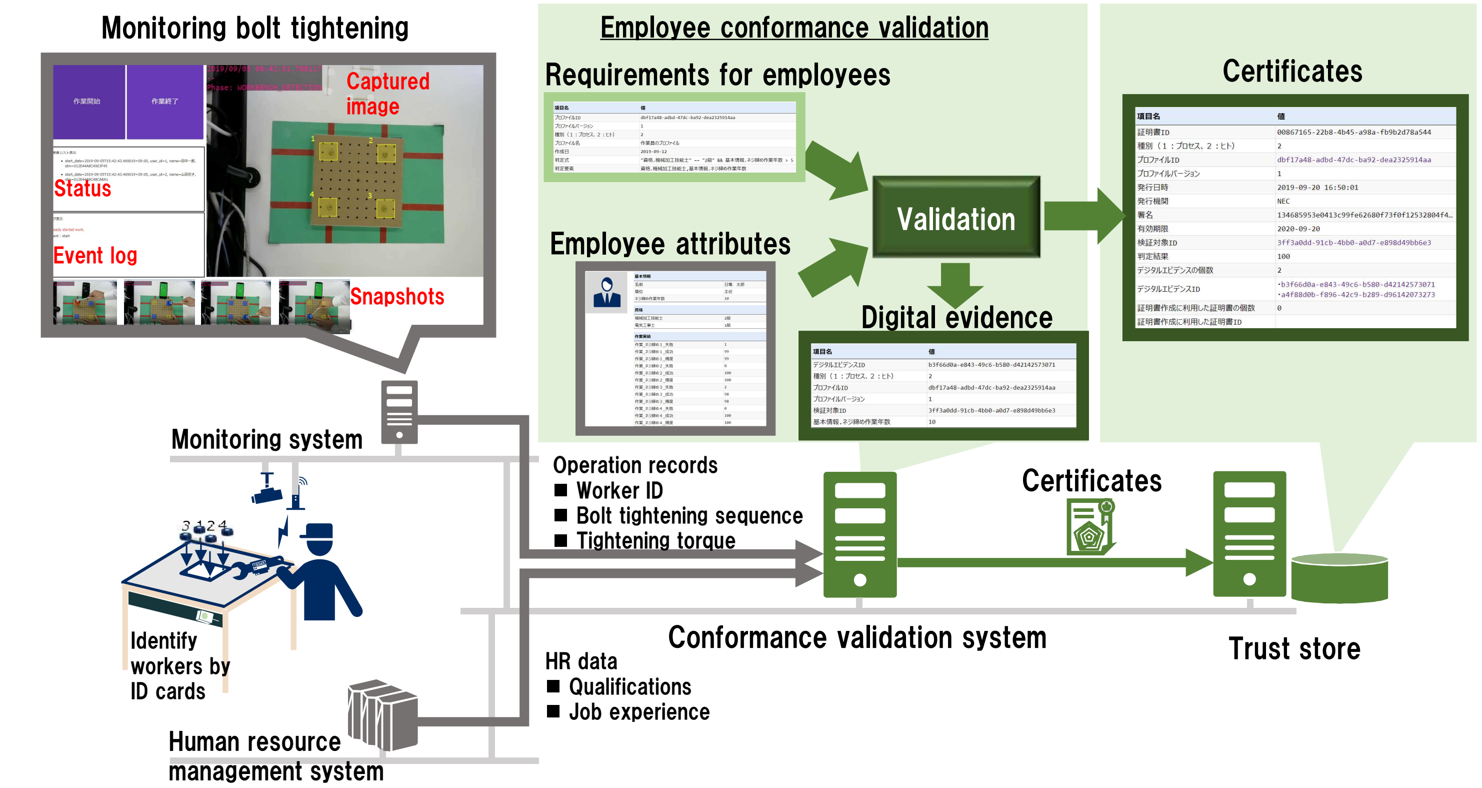
Issues to be solved:
- ■ Employee requirements for service delivery and manufacturing
- ■ Description formats of requirements

Issues to be solved:
- ■ Validation methods to maintain trustworthiness of service and production

Issues to be solved:
- ■ Processing employee data in accordance with laws and regulations

Utilized to structure trust chains and improve HR management

Employee Conformance validation in bolt tightening


Monitoring bolt tightening
作業開始
作業終了
Captured image
Status
Event log
Snapshots
Monitoring system
3 1 2 4
Identify workers by ID cards
Human resource management system
Validation
Conformance validation system
Trust store

Employee conformance validation

Requirements for employees

項目名	値
プロファイルID	dbf17a48-adbd-47dc-ba92-dea2325914aa
プロファイルバージョン	1
種別（１：プロセス、２：ヒト）	2
プロファイル名	作業員のプロファイル
作成日	2019-09-12
判定式	"資格.機械加工技能士" -- "2級" && 基本情報.ネジ締め作業年数 > 5
判定要素	資格.機械加工技能士,基本情報.ネジ締め作業年数

Employee attributes

基本情報	
名前	日電　太郎
職位	主任
ネジ締め作業年数	10
資格	
機械加工技能士	2級
電気工事士	1級
作業実績	
作業_ネジ締め１_失敗	1
作業_ネジ締め１_成功	99
作業_ネジ締め１_精度	99
作業_ネジ締め２_失敗	0
作業_ネジ締め２_成功	100
作業_ネジ締め２_精度	100
作業_ネジ締め３_失敗	2
作業_ネジ締め３_成功	98
作業_ネジ締め３_精度	98
作業_ネジ締め４_失敗	0
作業_ネジ締め４_成功	100
作業_ネジ締め４_精度	100

Digital evidence

項目名	値
デジタルエビデンスID	b3f66d0a-e843-49c6-b580-d42142573071
種別（１：プロセス、２：ヒト）	2
プロファイルID	dbf17a48-adbd-47dc-ba92-dea2325914aa
プロファイルバージョン	1
検証対象ID	3ff3a0dd-91cb-4bb0-a0d7-e898d49bb6e3
基本情報.ネジ締め作業年数	10

Certificates

項目名	値
証明書ID	00867165-22b8-4b45-a98a-fb9b2d78a544
種別（１：プロセス、２：ヒト）	2
プロファイルID	dbf17a48-adbd-47dc-ba92-dea2325914aa
プロファイルバージョン	1
発行日時	2019-09-20 16:50:01
発行機関	NEC
署名	134685953e0413c99fe62680f73f0f12532804f4…
有効期限	2020-09-20
検証対象ID	3ff3a0dd-91cb-4bb0-a0d7-e898d49bb6e3
判定結果	100
デジタルエビデンスの個数	2
デジタルエビデンスID	・b3f66d0a-e843-49c6-b580-d42142573071 ・a4f88d0b-f896-42c9-b289-d96142073273
証明書作成に利用した証明書の個数	0
証明書作成に利用した証明書ID	

Operation records
- ■ Worker ID
- ■ Bolt tightening sequence
- ■ Tightening torque

Certificates

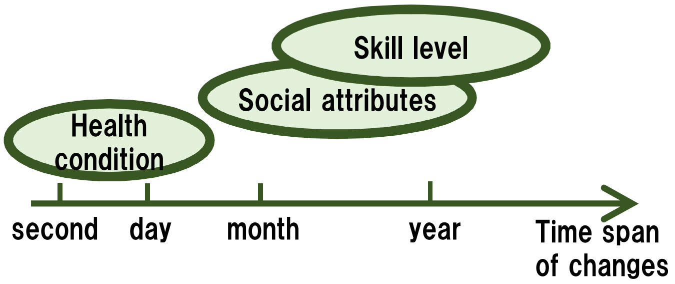
HR data
- ■ Qualifications
- ■ Job experience

Issues in conformance validation of people

Issues in confirmation of attributes

- Identifying relevant attributes, defining their description formats, and acquiring their values.

- Methods to acquire latest values of attributes with different speeds of change



Issues in processing employee data

- Laws and regulations stipulate different conditions in processing employee data and in processing consumer data
  - In handling consumer data, obtaining consent is usually most important
  - In handling employee data, consent is insufficient because it may not be voluntary due to power imbalance between the employer and employees.
- The opinion of the European Commission* on data processing at work states that employers must show that processing employee data is necessary either to:
  - perform employment contracts,
  - comply with legal obligations, or
  - further the legitimate interests of the employer

*Opinion2/2017, Article 29 working party, European Commission

【Fujitsu Limited】

Guarantee of Data Distribution in Cyberspace

CONSTRUCTION & DISTRIBUTION

Secure Data Distribution Technology for Next Generation Supply Chain

Technical Features

■ **Building Consensus Between Participants in Cyberspace**

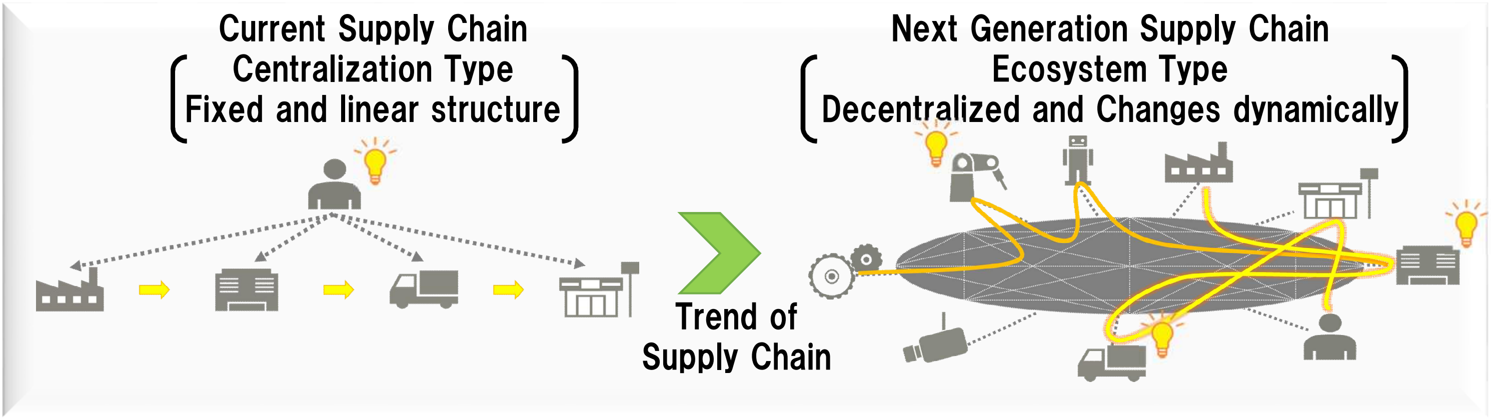
Build consensus between participants for connecting participants, and then achieve dynamic construction/re-construction of secure supply chain in cyberspace

■ **Unification of Threat Countermeasures**

Deal sharing and autonomous cooperating by deploying unified threat measures

Background

Next generation supply chain is required for achieving Society 5.0
It is decentralized and dynamically changes structure for new value proposition


Current Supply Chain
(Centralization Type
Fixed and linear structure)
Trend of Supply Chain
Next Generation Supply Chain
(Ecosystem Type
Decentralized and Changes dynamically)

Problem and Solution

Secure Data Distribution that supports Next Generation Supply Chain

■ **Limit of fixed form and linear structure of centralization type**

- No mechanism of reconstruction of supply chain by each participants
- Maintain of unified security level in supply chain is difficult, because Its construction is originated each company

■ **Solving with Distributed and Dynamically changeable structure**

- Provide a mechanism “Trustworthy Field Constructor” to form a “Trustworthy Field” by building consensus between participating companies
- Provide a mechanism to maintain security levels by sharing threat countermeasures and applying countermeasures to the entire supply chain autonomously

【Fujitsu Limited】

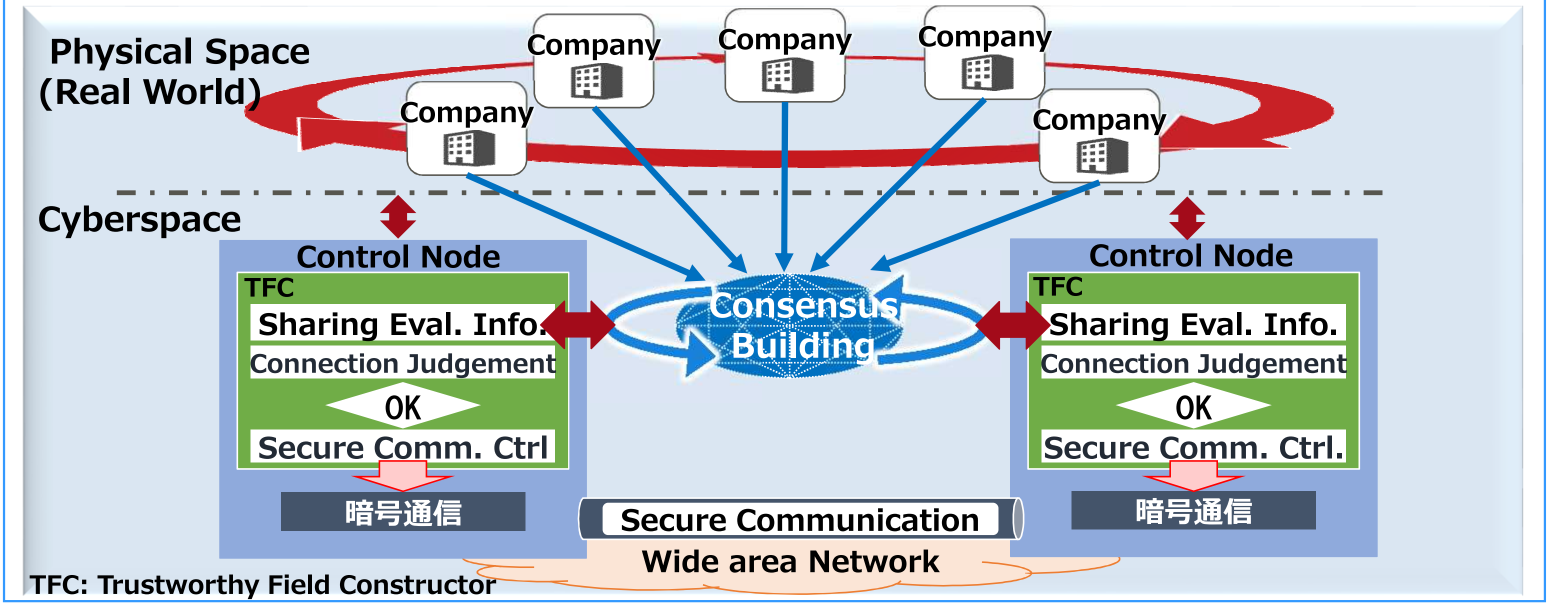
Guarantee of Data Distribution in Cyberspace

Secure Data Distribution based on consensus building in Cyberspace

All participants can form consensus building for create dynamic "Trustworthy Field"

◆Technical Features

- •Participating companies form a consensus by evaluation of disclose information
- •Automatically configures "Trustworthy Field" using published comm. parameters



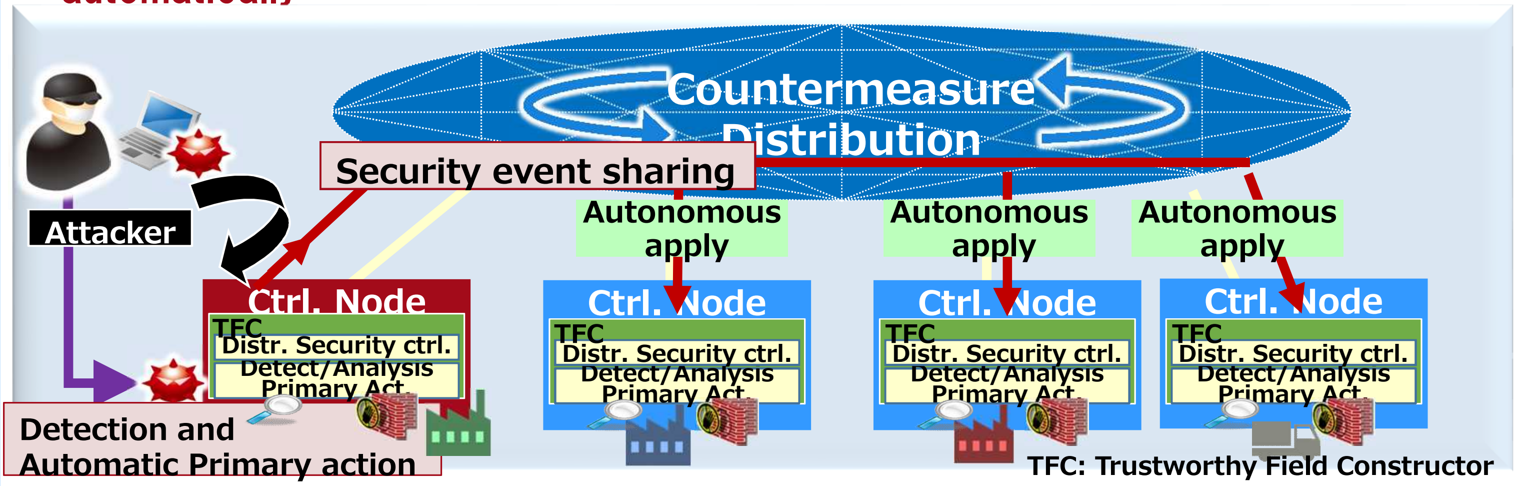
TFC: Trustworthy Field Constructor

Technology of maintaining Security Level

Maintaining security levels by sharing threat countermeasures and applying countermeasures to the entire supply chain autonomously

◆Technical Features

- •Applying primary countermeasures such as changing defense settings autonomously based on damage detection analysis within control node
- •Countermeasures are shared to other control nodes and they apply measures automatically



TFC: Trustworthy Field Constructor

【Nippon Telegraph and Telephone, Mitsubishi Electric】

Anomaly Detection for Cyber-Physical Systems

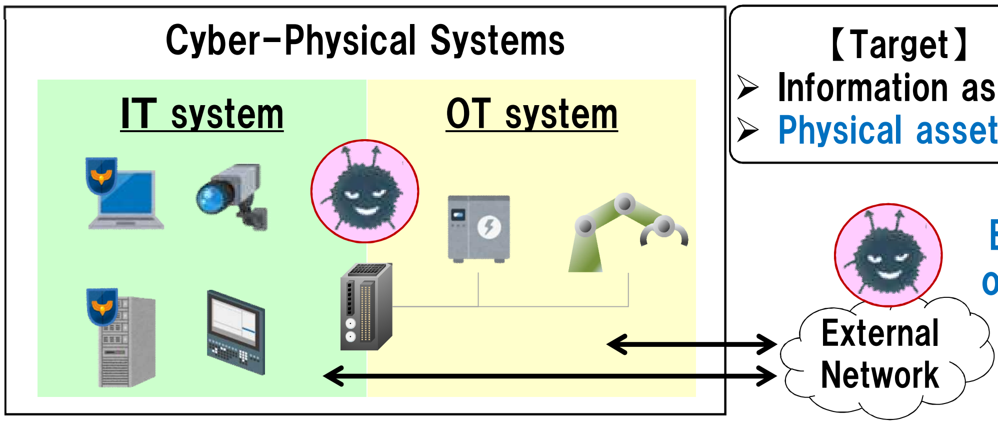
VERIFICATION & MAINTENANCE

Immediate monitoring, anomaly detection and incident handling support

Technical Features

- **Immediate monitoring from just after installation**
  By improving the learning efficiency using sensing information focusing on device characteristics, the monitoring blank period due to the learning period of ML is avoided.
- **Early stage anomaly detection to prevent damage**
  By capturing even subtle signs of anomaly resulting from cyber-attack preparations, hard-to-recover situations are avoided.
- **Root cause analysis to accelerate incident handling**
  By utilizing information including the management layer such as system operation plan, the root cause assumption is provided to achieve smooth incident handling.

Security issues for cyber-physical systems



【Target】
- Information assets
- Physical assets

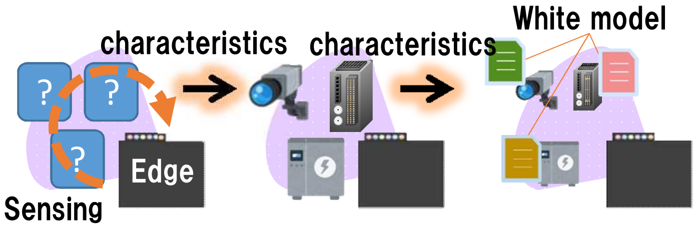
【Damage】
- Infringement of CIA triad
- Physical/Human damage

Business impact due to system outages and quality degradation

Requires anomaly detection at an early stage

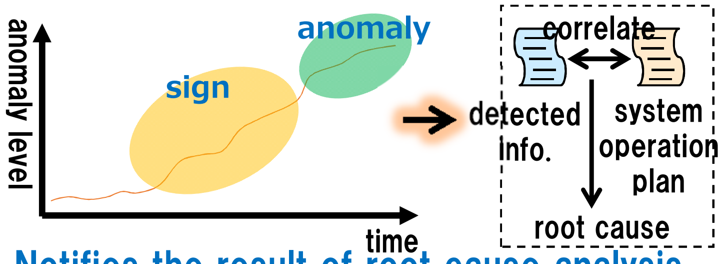
R&D Technologies

Immediate monitoring technology



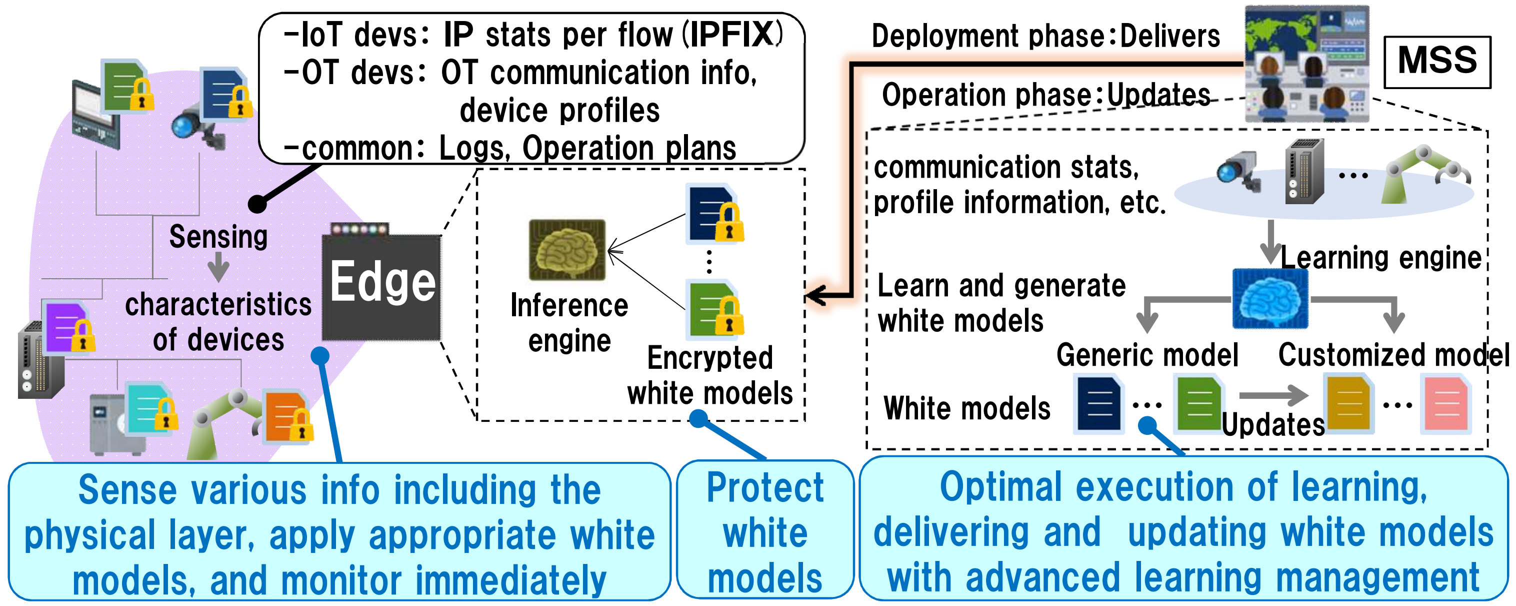
Starts monitoring immediately by selecting and applying white models based on sensed device characteristics

Anomaly sign detection/Root cause analysis



Notifies the result of root cause analysis obtained by correlating the detected anomaly sign with the system operation plan

Immediate monitoring realized by cooperation of the Edge and MSS



-IoT devs: IP stats per flow (IPFIX)
-OT devs: OT communication info, device profiles
-common: Logs, Operation plans

Sensing

characteristics of devices

Edge

Inference engine

Encrypted white models

Deployment phase: Delivers

Operation phase: Updates

MSS

communication stats, profile information, etc.

Learning engine

Learn and generate white models

Generic model

Customized model

White models

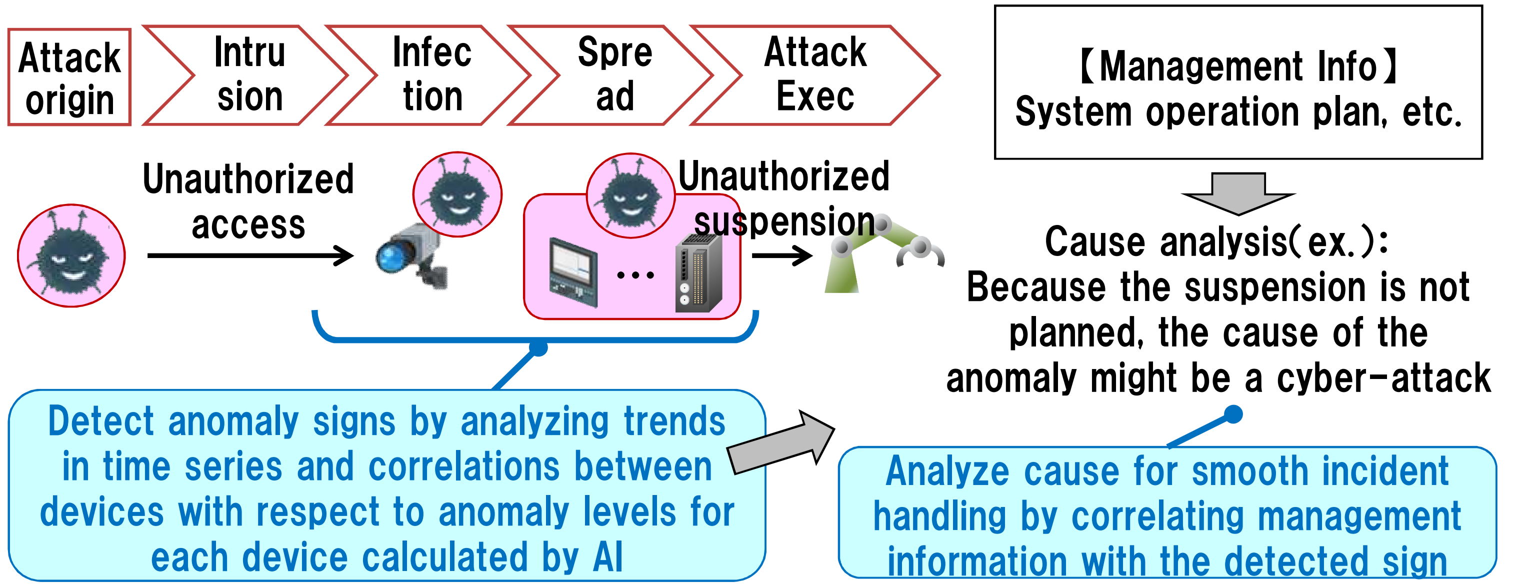
Updates

Sense various info including the physical layer, apply appropriate white models, and monitor immediately

Protect white models

Optimal execution of learning, delivering and updating white models with advanced learning management

Incident handling support with anomaly detection & cause analysis



Attack origin

Intrusion

Infection

Spread

Attack Exec

【Management Info】
System operation plan, etc.

Unauthorized access

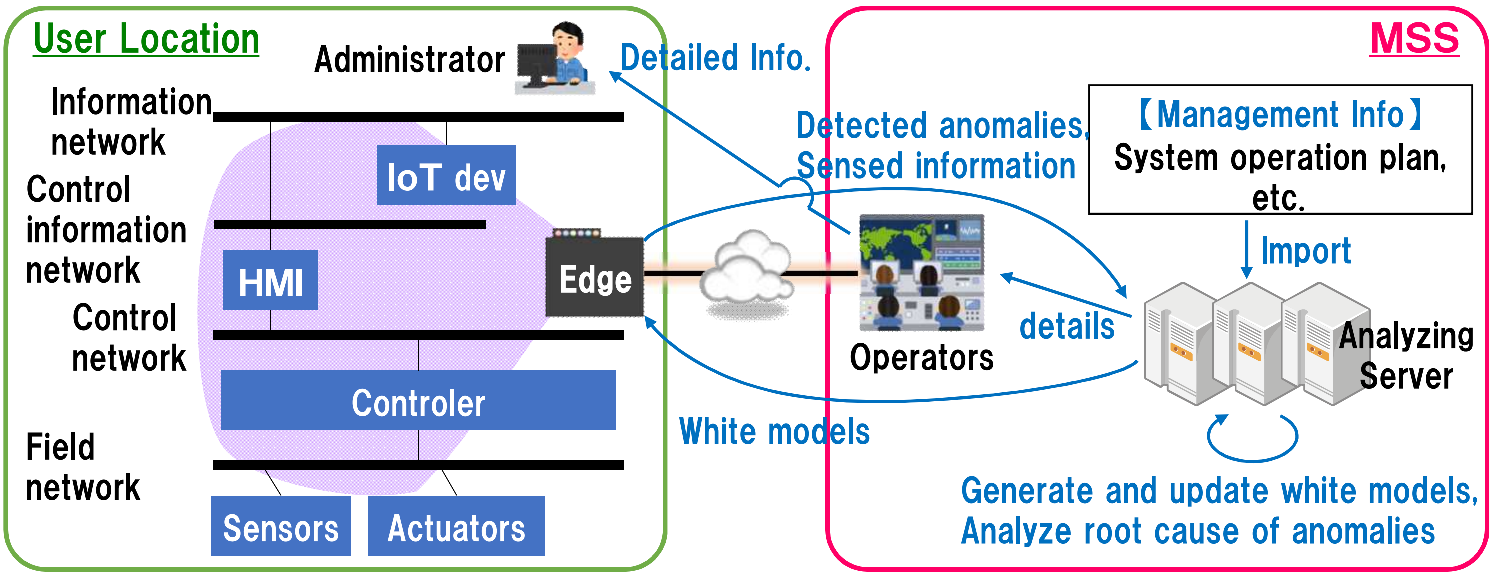
Unauthorized suspension

Cause analysis(ex.):
Because the suspension is not planned, the cause of the anomaly might be a cyber-attack

Detect anomaly signs by analyzing trends in time series and correlations between devices with respect to anomaly levels for each device calculated by AI

Analyze cause for smooth incident handling by correlating management information with the detected sign

System configuration example



User Location

Administrator

Information network

Control information network

Control network

Field network

IoT dev

HMI

Edge

Controler

Sensors

Actuators

Detailed Info.

Detected anomalies, Sensed information

White models

MSS

【Management Info】
System operation plan, etc.

Import

Operators

details

Analyzing Server

Generate and update white models, Analyze root cause of anomalies

【Hitachi Ltd.】

Detection and security measurement technology of invalid data between cyber and physical

VERIFICATION & MAINTENANCE

This technology perform invalid data detection in consideration of an IoT system characteristic and decide an appropriate measurement method depending on system availability.

Technical Features

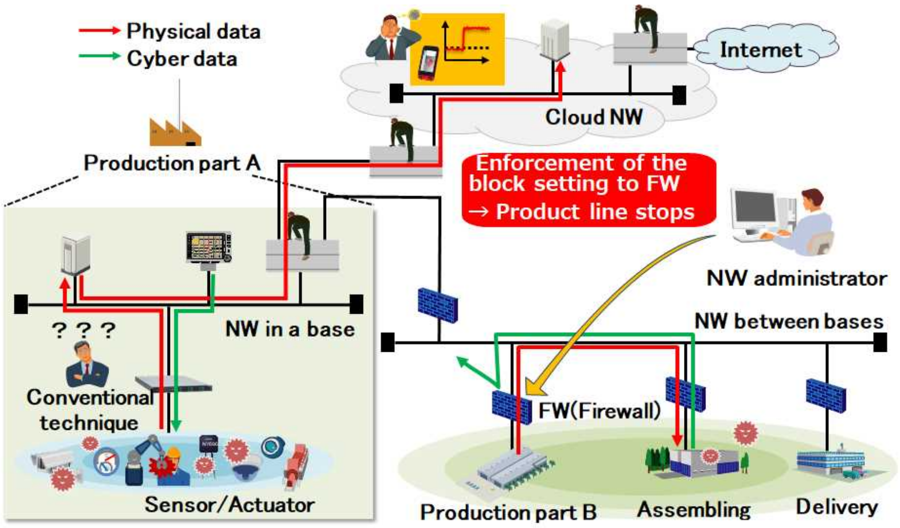
- **Reduce false detection and overlooking**

  Detect unjust data which is hard to detect in an existing technique by collating data with system properties information

- **Decide a coping method suitable for service continuation**

  Decide a coping method suitable for service continuation of a monitored IoT system by making use of system properties information

The present problem in an IoT system



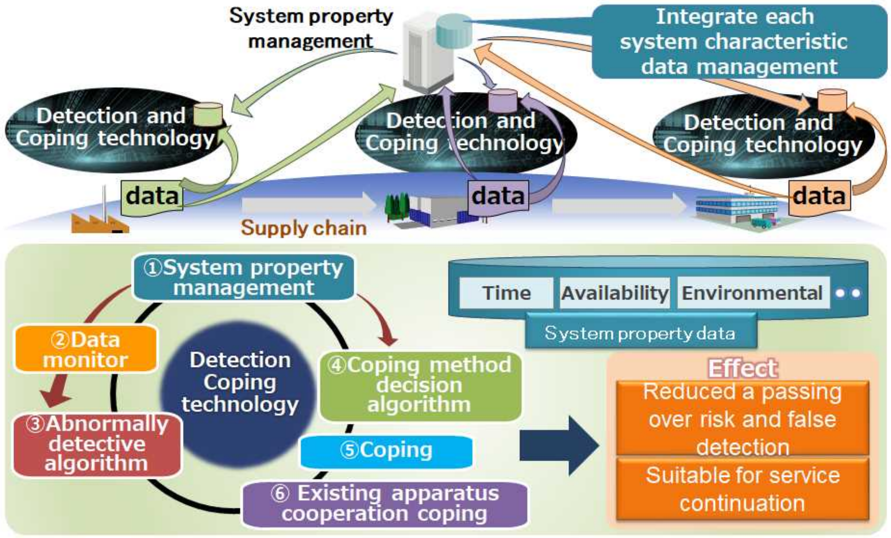
For manipulation data detection

- The tracking to a wide variety of equipment is difficult
- The detection of a data abnormality is difficult

For manual security measurement

- Damage increases due to delay of judgement
- Secondary disaster due to human error

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

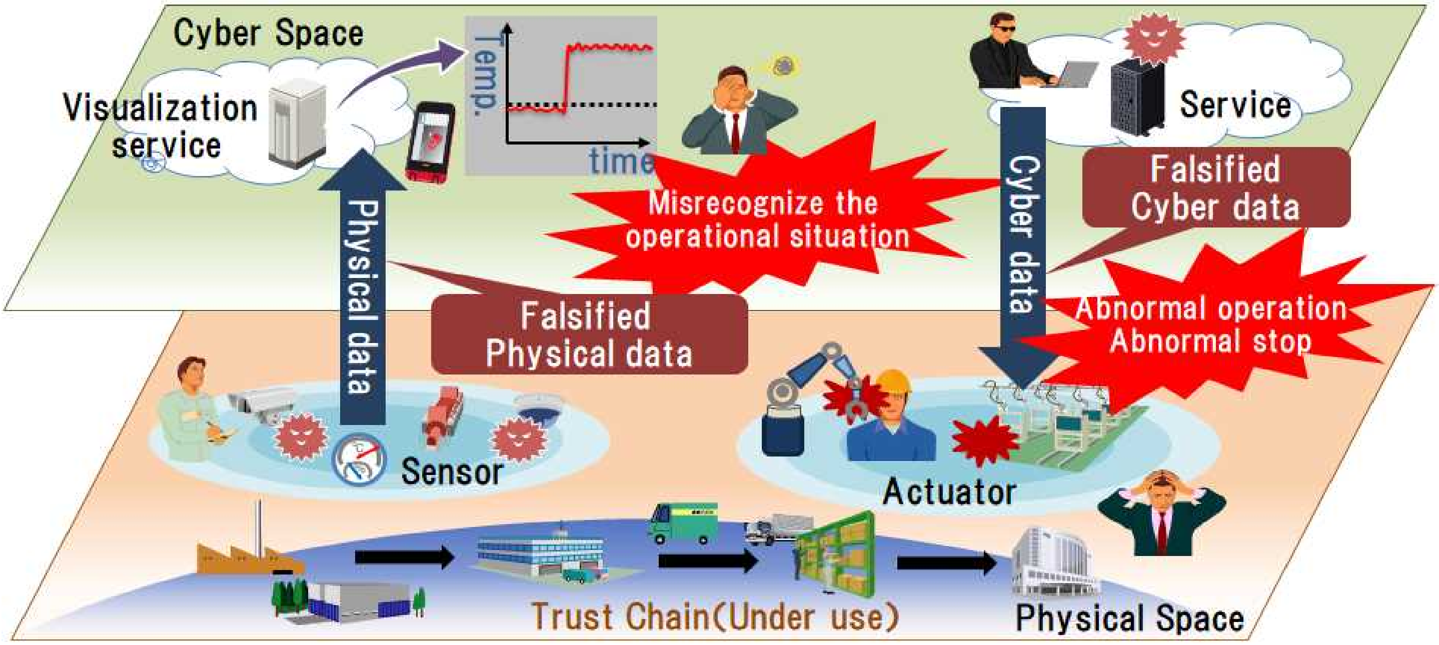
Inflection of system properties

(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

Background of a research and development theme



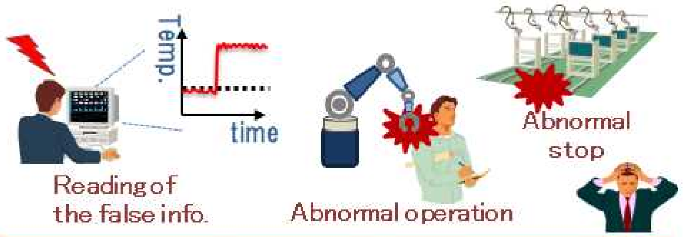
Menace on the heels of IoT system

- In late years, risks of cyber attack to OT/IoT systems are increasing.
- A wide variety of IoT equipment leading to the Internet may have been already invaded an assailant
- Cyber attack using cyber/physical data is in danger of giving serious damage to IoT service beyond traditional defense.

Needs of IoT data monitoring

Impossible to completely prevent invasions

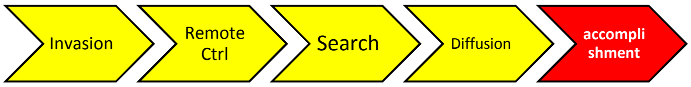
Cyber/physical data falsification cause



Serious damage of IoT system

As a characteristic after invasion

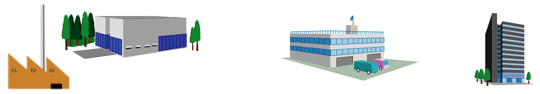
Attack preparations are carried out before invasion leads to attack. Traffic shows minute change.



Detect movement of attack preliminary stage, and coping in consideration of service continuity is more important

👉 We are researching and developing.

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

【NEC Corporation】

Impact Assessment and Countermeasure Execution Support Technology

VERIFICATION & MAINTENANCE

Automatic cyber-attack risks analysis of OT/IoT systems
Support for risk visualization and countermeasure execution

Technical Features

■ Visualize effects of the cyber attack

Analyze both system impacts and affected devices automatically in case of a cyber-attack. Operator understands potential cyber-attack risks without security knowledge.

■ Provide countermeasure plans against the cyber attack

Evaluate countermeasure plans automatically and support operator to execute them.

Problems of Cyber Attack Countermeasure

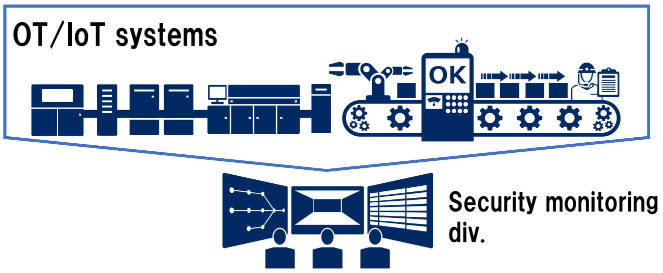
■ Comprehension of cyber attack effects

Require enough security knowledge to understand both system impacts and affected devices from cyber attacks.

■ Pre-evaluation of countermeasure efficacy

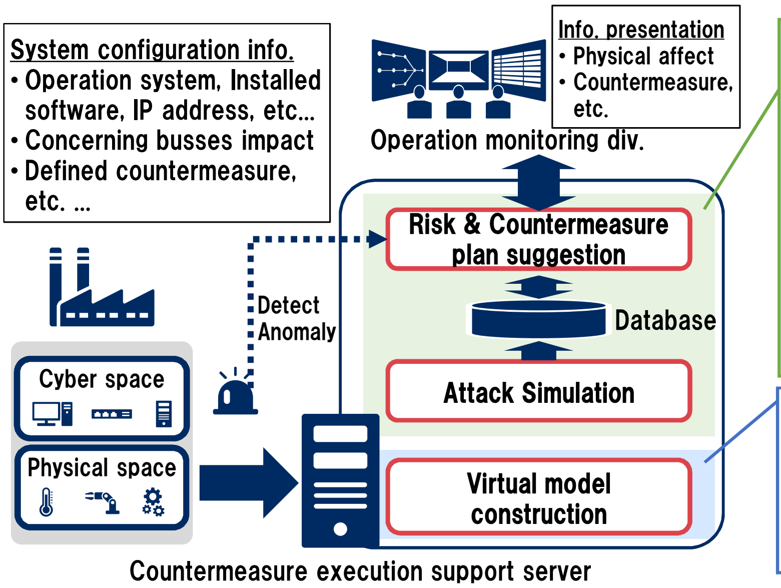
Difficulty to evaluate a lots of countermeasure plans comprehensively without disturbing the system operation.

Target Domain and Use Cases



Daily security operations (risk analysis, etc.) and incident operations on OT/IoT systems of manufacturing (plants), distribution, smart building and so on.

Overview of R&D Technologies toward Solving Problems


System configuration info.
• Operation system, Installed software, IP address, etc...
• Concerning busses impact
• Defined countermeasure, etc. ...
Info. presentation
• Physical affect
• Countermeasure, etc.
Operation monitoring div.
Risk & Countermeasure plan suggestion
Database
Attack Simulation
Virtual model construction
Detect Anomaly
Cyber space
Physical space
Countermeasure execution support server

■ Countermeasure execution support technology

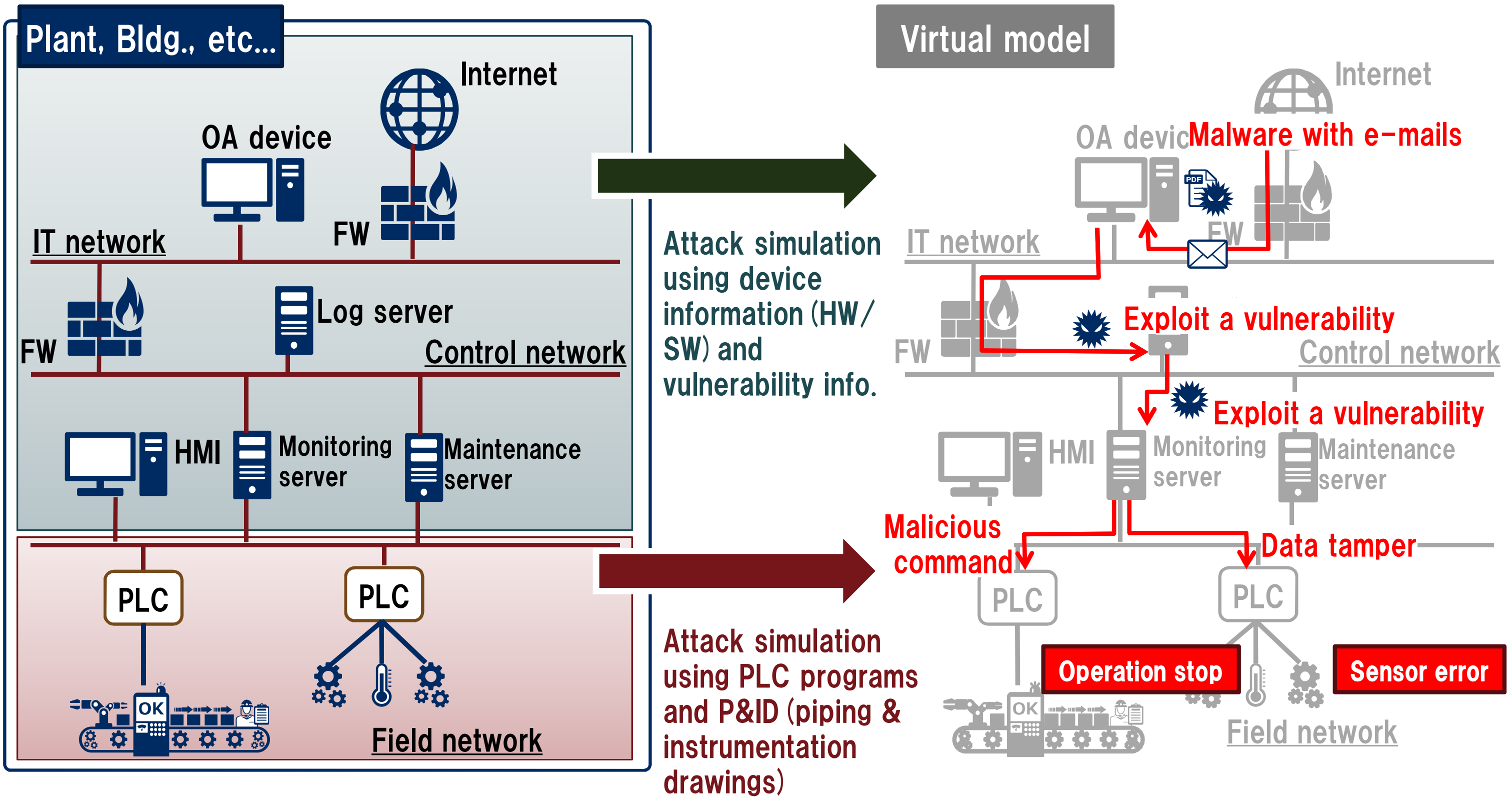
Perform attack simulations and evaluate effectiveness of countermeasure plans on the virtual model. When an anomaly is detected, the technology suggests applicable countermeasure from evaluated plans.

■ Virtual model construction technology

Create the model which is used to analyze cyber-attack risk without using actual systems.

Attack Simulation on Virtual Model

Search both concrete attack paths (steps, attack methods) and impacts on the system using the virtual model which consists of information required for analyzing the cyber-attack risks.



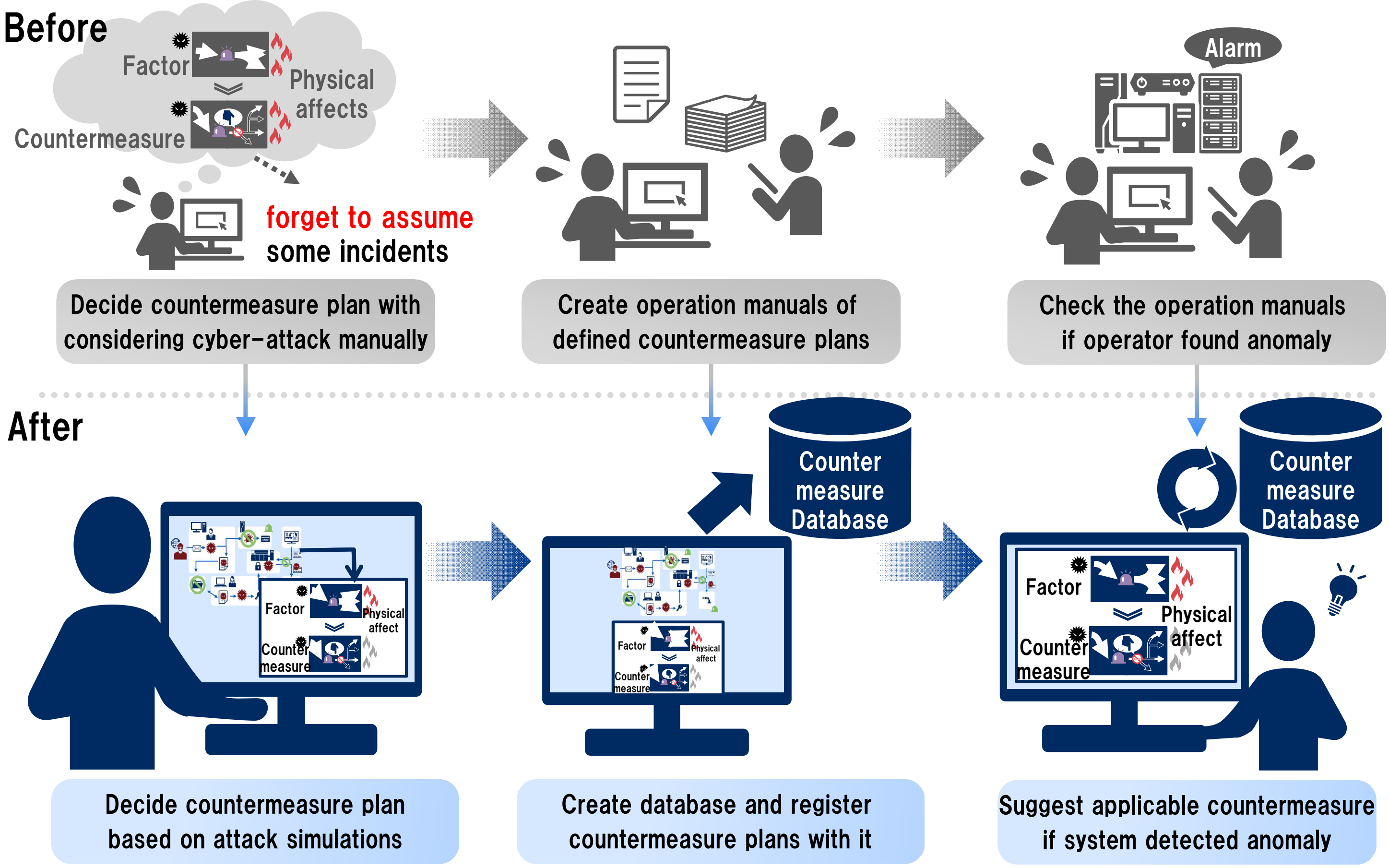
Plant, Bldg., etc…

Virtual model

Attack simulation using device information (HW/SW) and vulnerability info.

Attack simulation using PLC programs and P&ID (piping & instrumentation drawings)

Image of Countermeasure Execution Support



Before

Decide countermeasure plan with considering cyber-attack manually

Create operation manuals of defined countermeasure plans

Check the operation manuals if operator found anomaly

After

Decide countermeasure plan based on attack simulations

Create database and register countermeasure plans with it

Suggest applicable countermeasure if system detected anomaly

SIP「Research and Development Plan for Cyber Physical Security」
Symposium 2019