Mitsubishi Electric, NTT

2-1 Security Monitoring Equipment for IoT Systems

Technologies for IoT

Automatic adjustment to a variety of IoT devices to monitor and analyze operations of them for detecting security anomalies

Features

I. Operation monitoring and analysis of IoT systems supporting a variety of IoT devices including unknown devices

The monitoring equipment automatically adapts itself to monitor and analyze IoT systems even in the case of the addition of new IoT devices or the diversification of the use (IoT device characteristics learning technology).

There is no need for an IoT device itself to be equipped with any specific function (IoT device behavior monitoring technology).

II. Operation monitoring and analysis of IoT systems consisting of a huge number of IoT devices

A huge number of IoT devices can be automatically detected and efficiently covered regardless of the connection method (Monitoring target automatic setting technology).

Results from multiple IoT systems are securely aggregated and analyzed in order to presume and classify anomalies (IoT system integrated analysis technology).

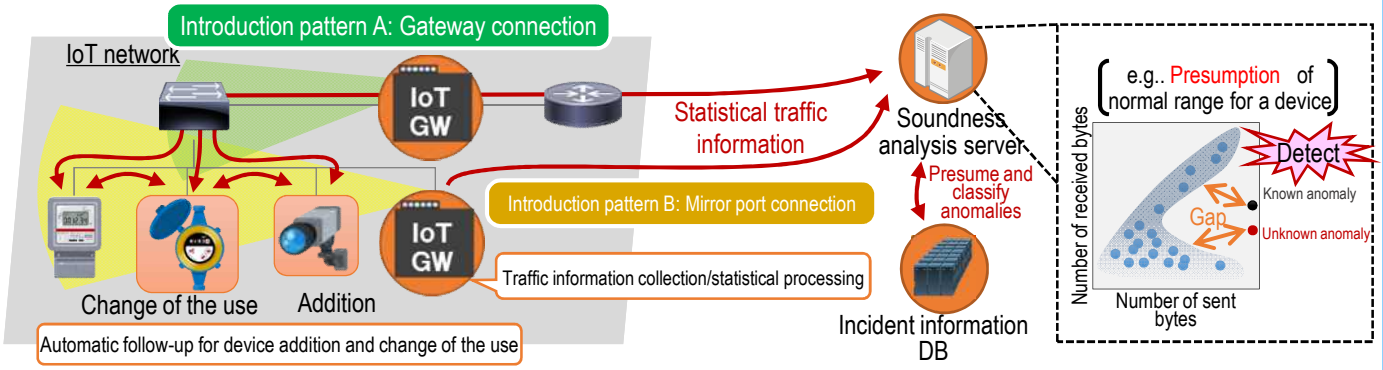
III. Introduction and operation of security monitoring service for critical infrastructure companies

Mitsubishi Electric, NTT provide flexible IoT security monitoring service suitable for 2020 era in line with the use utilization of each company and existing management systems (IoT security monitoring service).

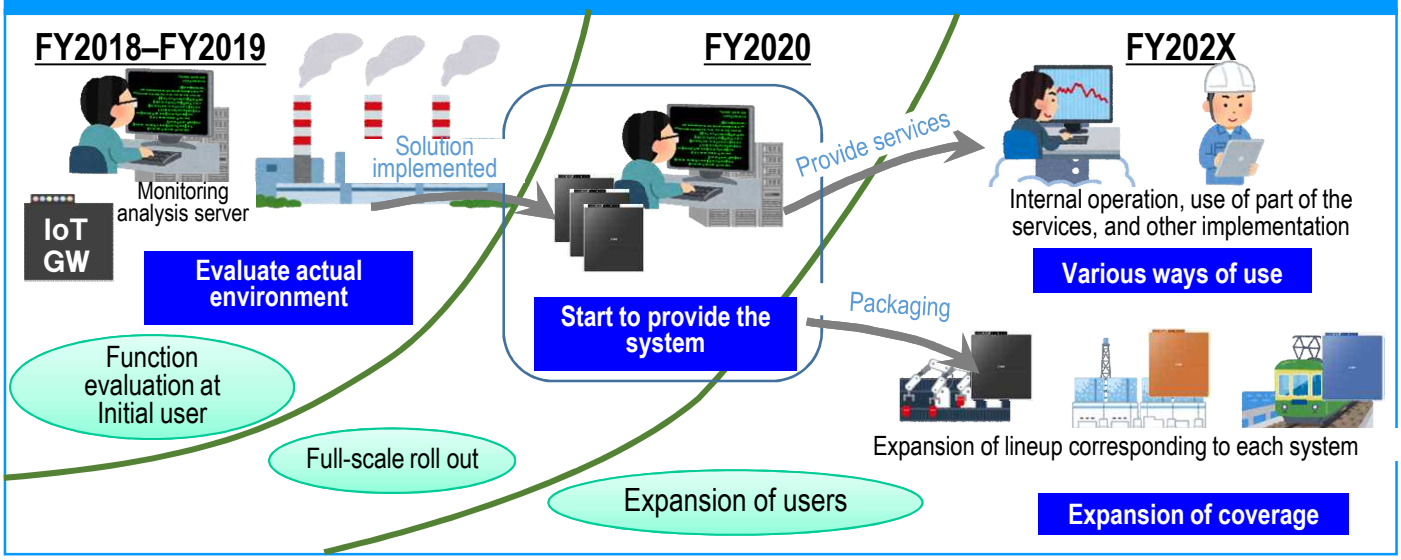
Expansion of threats with rapid growth of IoT requires preparation for security accidents caused by IoT.

The monitoring equipment can be introduced without any modification to the IoT devices and system configuration, enabling immediate response to new threats to a variety of IoT devices.

The soundness analysis server and incident information DB can be provided as MSS according to the customer's system environment, where IoT GW needs to be placed.



Social implementation and business roll out security technologies using IoT GW

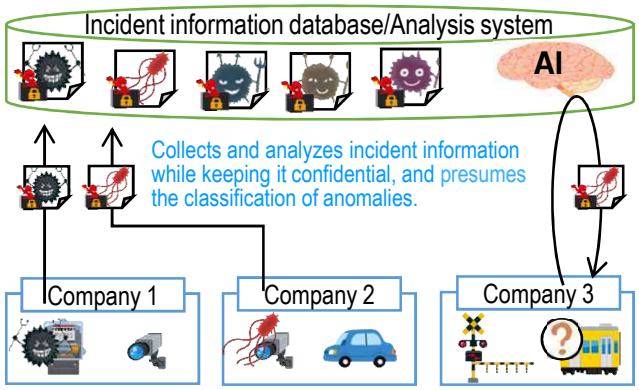


Cross-ministerial Strategic Innovation Promotion Program (SIP)

Mitsubishi Electric, NTT

2-1 Security Monitoring Equipment for IoT Systems

Securely collect incident information and presume classification



Collect information in real time from a large amount of IoT devices

To detect an attack, every communication that occurs from a large amount of IoT devices needs to be processed into statistical information without exception.

Example of target system: For visual surveillance
256 cameras x 4 types of communication flows = 1024 communication flows

		Requirements	This technology
Collect statistical info.	(i) Flow count (ii) Item count	(i) 1024 flows or more (ii) 9 items or more (5 tuples + communication traffic volume)	(i) 5000 (ii) 17 items (+ flag information)
Communication transfer performance		1 Gbps wire rate	

Development of technology enabling both anomaly detection and presumption of anomaly classification (comparison with the existing technologies)

With an expanded white list method using AI, a white list can be automatically generated and the classification of anomalies can be presumed.

	Black list method	White list method	This technology (expanded white list method)
Detection of anomalies caused by known attacks	○	○	○ (automatic)
Detection of anomalies caused by unknown attacks	×	○	○ (automatic)
Presumption of the classification of anomalies	○	×	○

[Black list method]

- Defines known anomalies.
  ⇒ Possible to classify anomalies.
- Cannot respond to unknown attacks that are not defined.

[White list method]

- Defines normal operation.
- Possible to detect anomalies but not possible to presume the classification of anomalies.

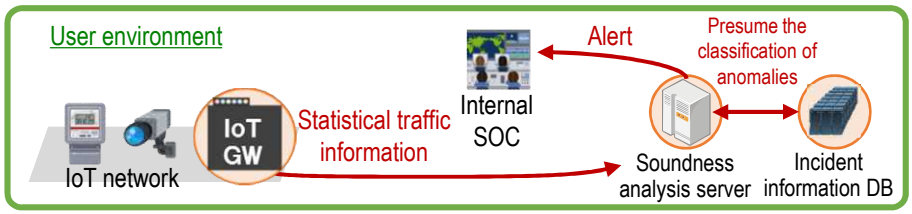
[This technology]

- Automatically defines normal operation.
- Possible to presume the classification of anomalies.
- Automatic response to addition and change of IoT devices.

Introduction configuration

(i) Provided by SI (on-premises)

- Provide a full set on premises for companies that who can conduct security operations on their own.



(ii) Provide the package and services

- Provide as a remote security monitoring service that requires users only to install IoT GW; no need of special knowledge.
- Provide the incident information DB service, as an added value, that enables highly accurate presumption of anomaly classification.