## Behavior Monitoring/Analysis Technologies by Means of Gateways for IoT Devices

Automatically adapts to a variety of IoT devices, and performs monitoring and analysis to detect unauthorized behavior

### Characteristics

1. **Monitors and analyzes IoT system behavior of a variety of IoT devices, even those that are unknown**
   - Although a variety of IoT devices are being introduced one after another and the uses of IoT devices have diversified greatly, these technologies can automatically adapt to monitor and analyze behavior (IoT device feature learning technologies). No special functions need to be installed onto IoT devices (network-attached IoT monitoring technologies).

2. **Monitors and analyzes behavior of IoT systems consisting of a large number of IoT devices**
   - Can automatically detect IoT devices connected using a variety of methods to enable efficient introduction, monitoring, and analysis, even in configurations consisting of a large number of devices (automatic IoT asset tracking technologies). Aggregating information from multiple IoT systems while protecting confidentiality (the creation of big data) makes it possible for local monitoring to perform previously impossible high-precision analysis and effectively cope with anomalies (IoT big data analysis technologies).

### Necessity to Prepare for Security Accidents Caused by IoT

- **Insufficient security countermeasures**
  - As devices not connected to the Internet have successively been converted to the IoT, sufficient security countermeasures for each device have become difficult to anticipate.

- **Unique difficulties of IoT monitoring**
  - Because of the various methods of using IoT devices, it may become difficult to define the normal state, monitor behavior, and detect abnormalities.

### Can Automatically Adapt to a Variety of IoT Devices and Perform Monitoring

- **Automatically learns features**
  - Devices do not need to be configured in advance

- **Monitors communication and device status**
  - Functions do not need to be added to devices

- **Detects anomalies**
  - Also tracks the addition of assets

- **Automatically adapts to unknown IoT devices**
  - Even for new IoT devices, the feature is automatically analyzed by AI technologies to make it possible to monitor IoT devices in a variety of fields.

- **Does not require IoT device modification**
  - IoT devices targeted for monitoring do not need updating, so even old devices that are already running can easily be monitored.

### Can Also Handle Systems Consisting of Many IoT Devices

- **Automatic configuration of monitoring targets**
  - Because IoT devices connected by a variety of methods can be automatically detected, this technology can be efficiently deployed, even in systems consisting of many devices.

- **Integrated analysis of multiple IoT systems**
  - Aggregating information from multiple systems while protecting confidentiality (the creation of big data) enables high-precision analysis by means of AI technologies.

### Schedule

Systems able to be introduced for commercial applications are scheduled to be developed by the end of FY2018. By 2020, the aim is to expand the locations and fields in which this technology will be introduced while utilizing the TOP plan in accordance with the spread and expansion of IoT and to support security for facilities in leading fields of critical infrastructure.

---

**Copyright © 2016 Mitsubishi Electric Corporation and NTT Corporation. All Rights Reserved.**
Behavior Monitoring/Analysis Technologies by Means of Gateways for IoT Devices

Background of the Topic of This R&D

The IoT, including current devices, is progressing quickly. According to a FY2015 white paper on telecommunications, the size of the IoT market will be US$1.7 trillion in 2020, and the number of IoT devices, such as sensors and the like, will reach 53 billion. Also, broad increases in IoT devices in every field are anticipated (from 2014 to 2020, an approximate six-fold increase in fields for general consumers and manufacturing fields and an approximate 20-fold increase in automotive fields), so it is thought this trend will continue even beyond 2020. This explosive popularization means that many IoT devices, which have insufficient security, will begin to quickly expand into critical infrastructure and user environments, which means that security incidents caused by IoT devices may occur sooner than later.

On the other hand, the most recent survey by Gartner predicts that the scale of the IoT security market will rapidly expand from the current figure of US$350 million to US$840 million in 2020. Based on the aforementioned security concept, responding to this rapid expansion of needs by creating IoT security countermeasure technology that can be deployed quickly and simply and used for longer will lead to a massive creation of business.

Image of Countermeasures Prepared for Societal Permeation of IoT Devices

1. Gathers information from each monitoring company to implement cross-sectional monitoring by providers
2. Supports in advance the necessary minimum standard specifications (related to monitoring)
3. Installs IoT gateways at user companies to provide security monitoring services of IoT device companies
4. Expands the utilization of a variety of IoT devices by simplifying the assurance of monitoring

Supports Diversification for IoT Devices with Machine Learning

- Supervised learning
  - Normal
  - Anomalies
  - Unknown anomalies
  - Judgment by comparison between normal and anomaly (Learns normal status and anomaly status in advance)
  - In a state in which a variety of IoT devices will explosively spread, instructor-less learning that does not require anomalies to be learned in advance is effective. The goal is technology that can also detect unknown attacks in accordance with these characteristics.

- Unsupervised learning
  - Normal
  - Judgment with deviations from trends in the normal status (Learns the trends of a normal status in advance)
  - Automatic abstraction of the amount of all For IoT devices, the goal is to be able to also support unknown devices by automatically extracting the amount of characteristics (the axis in the above graph), with a focus on making it easy to acquire the trends of a normal status when the types of devices are established.

Support for Many IoT Devices

- Execution of IoT system monitoring
  - In a society in which the utilization of IoT devices will explosively expand, IoT device agency monitoring services will be required for user companies who have problems investing in security and have no choice but to use IoT devices.

- Cross-sectional monitoring by providers
  - As security countermeasures for each device become more difficult and a single user company cannot sufficiently handle security by itself, a social mechanism will be necessary to share knowhow and monitoring information to increase the precision of monitoring.

Software/hardware behavior

- For IoT-GWs to be achieved in a compact form and at a low cost, coordinated behavior technology that uses software processing by CPU and a packet transfer engine will be established to make signal monitoring and transmission processing compatible.

Policy for R&D Based on Technological Trends

As cloud computing and computer performance have improved, data analysis technologies based on big data and AI have reached a practical level.

This R&D aims to use these technologies to establish behavior monitoring/analysis technology that corresponds to the characteristics of IoT devices. Also, this R&D is attempting to produce technology that protects the confidentiality of secret data in the processing stages of data aggregation, storage, and analysis.