IoT and OT security protected by AI
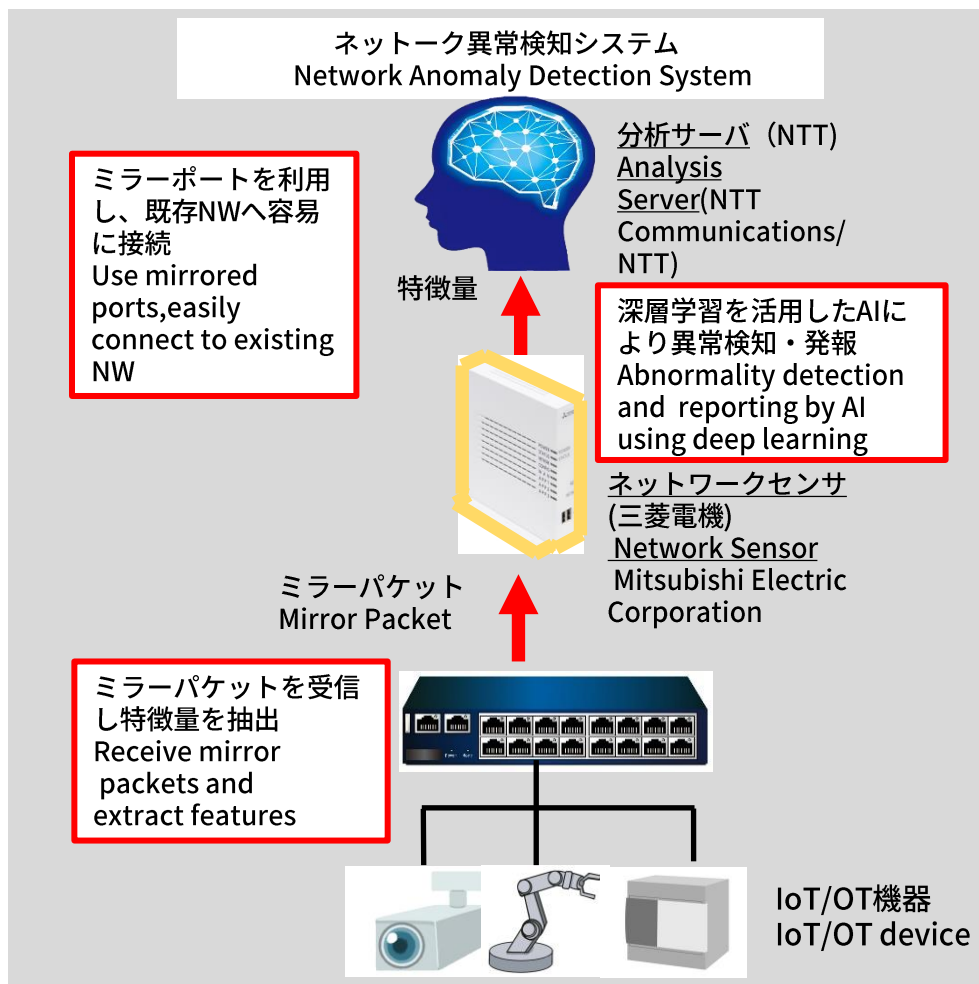
Detect unknown cyber-attacks by utilizing AI-based anomaly detection to enhance IoT/OT security

#Business Resilience

ネットーク異常検知システム
Network Anomaly Detection System

分析サーバ（NTT)
Analysis Server(NTT Communications/ NTT)

ミラーポートを利用し、既存NWへ容易に接続
Use mirrored ports,easily connect to existing NW

特徴量

深層学習を活用したAIにより異常検知・発報
Abnormality detection and reporting by AI using deep learning

ネットワークセンサ (三菱電機)
Network Sensor Mitsubishi Electric Corporation

ミラーパケット
Mirror Packet

ミラーパケットを受信し特徴量を抽出
Receive mirror packets and extract features

IoT/OT機器
IoT/OT device

///Technical Issue

The detection method of existing security devices/software is pattern matching, which makes it difficult to detect unknown attacks.

///Research Goal

Predicting and defending against unknown cyber-attacks reduces corporate economic losses, increases client confidence, and enhances corporate value.

---Technology

Equipped with AI (deep learning) models developed independently by NTT Service Innovation Laboratory Group.

---Novelty

By using AI to learn communication status without relying on signatures, anomalies can be detected without relying on protocols, making it easy to deploy even in OT environments where external communication is restricted, such as critical infrastructure.

---Applicable Business

Early detection of system anomalies in critical infrastructure (power, gas, water, telecommunications, transportation, finance, medical, etc.) and manufacturing industries (service available).