R&D phase | Research **Expected Commercialization** | FY28-

Mehr Licht!
More Photonics for Intelligence

#E03

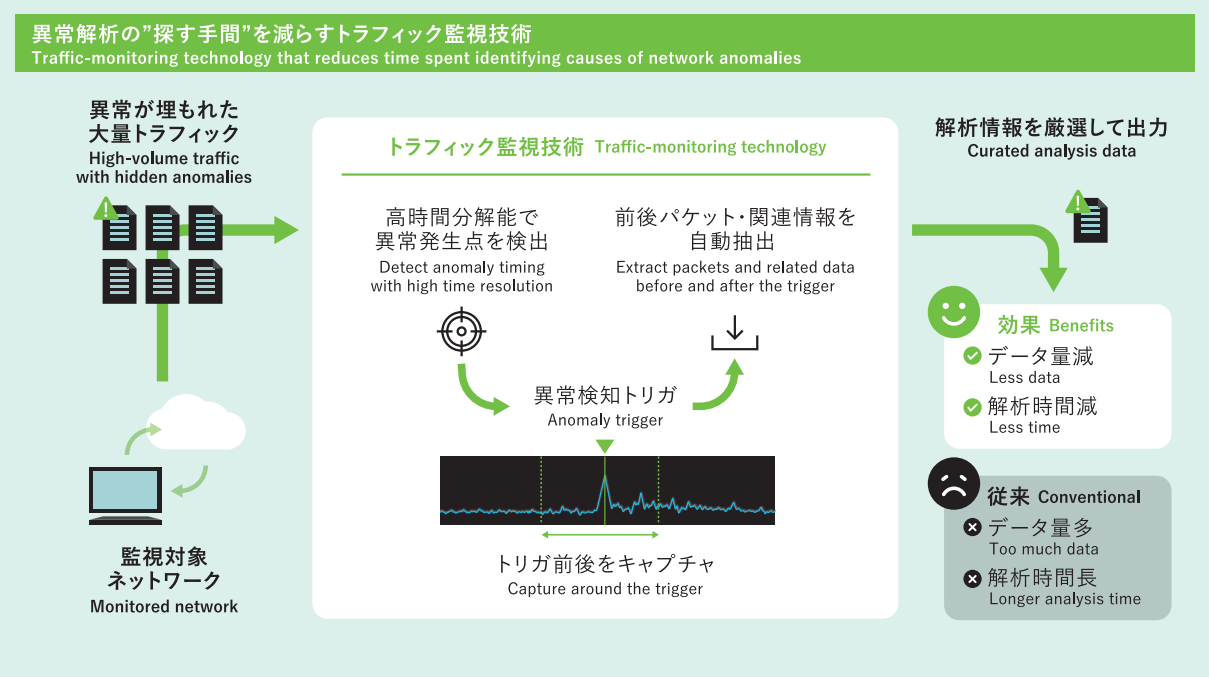
#Operational Efficiency#Digital & AI Transformation

Anomaly Evidence Extraction

Detects anomalies and extracts data for faster root-cause analysis

Technical Challenges & Goals

During network failures, transient anomalies can be buried in massive monitoring data, making it time-consuming to identify information required for root-cause analysis. This technology pinpoints anomaly timing from transient traffic changes and captures only surrounding traffic data to reduce root-cause analysis time.



Key Technologies

Core Technologies

- 1 Gbps-capable full-packet monitoring detects anomaly timing from transient traffic changes
- Combines multiple anomaly detection results and auto-extracts pre/post traffic evidence and metadata

Key Differentiators

- Captures transient traffic changes missed by aggregated monitoring and pinpoints anomaly timing
- Narrows analysis to traffic around anomalies, reducing PCAP data to about one-third in initial tests

Use Cases

Communication Services

During network failures, this technology automatically extracts pre/post traffic evidence and analysis metadata then provides them to LLMs, AI agents, or operators, enabling faster root-cause analysis and reducing operational workload.

Exhibitors

IOWN Integrated Innovation Center, NTT, Inc.