Network Infrastructure in OKI's IoT Business Platform

Kei Kato

The spread of IoT (Internet of Things) is progressing worldwide, and it is expected that IoT applications will be developed for various business domains. Together with the advancement in AI technology, the analysis of large-scale data obtained from IoT infrastructure will lead to full-fledged offerings of such services as detecting failure signs of machine tools and predicting disasters. In order to provide these services, transmitting large volumes of data via the Internet is indispensable, and the effect of traffic on existing networks will become extremely large. As a result, unanticipated congestion may occur and raises concern that situations may arise in which services and applications cannot perform the expected behavior. OKI's IoT business platform is aimed at solving these issues and minimizes impact on service quality to customers. This article introduces the concepts, features of the platform and gives the direction of future efforts.

Background

With its explosive spread, the Internet has a strong foothold in the daily lives of individuals/corporate entities and even deemed important as a lifeline. In recent years, deployment of services is proceeding to connect "things" to the Internet, collect data from those "things" and analyzing the data utilizing IoT. This means the Internet, which until now connected people with people or people with "things" (such as servers), will be used to connect numerous "things" with each other and cause a new paradigm shift to occur. In other words, the Internet traffic will remarkably increase in the upstream direction regardless of whether the access network is fixed or mobile and redesign of the current network will be inevitable.

However, the spread of IoT differs from one business domain to other. This makes it extremely difficult for providers of network infrastructures controlling all the traffic to predict the spread and economically plan investments. In order to spread IoT, introduction of LPWA (Low Power Wide Area) is being promoted as an interface for IoT, but fundamental overhaul of the infrastructure including the core network is not progressing. Furthermore, standardization of the future 5G mobile network that includes IoT is underway, but service provisioning is said to take place after the year 2020.

Meanwhile, with present IoT, a sensor network (FAN: Field Area Network) is used to gather information from sensors installed at manufacturing, social infrastructure and transport/distribution sites (Field). The acquired information goes through a gateway and makes its way across the network infrastructure via 3G/LTE and optical fiber to a data center with an IoT service platform where accumulated data is analyzed. In this case, there will be an explosive spread of sensors in a certain business domain and when upstream data increases, the volume of data arriving at a data center will become large causing congestion at the entry connection to the data center. In addition, if the service is provided on a daily basis, the reliability of the applications running in the data center becomes very important.

Operationally, when setting up an IoT business platform at a data center that is not highly reliable, measures against severe disasters may be inadequate resulting in loss of valuable user data. Moreover, if security measures are not implemented in the gateways, intrusion into the data center may occur and lead to information leakage. These issues are summarized in **Figure 1**.

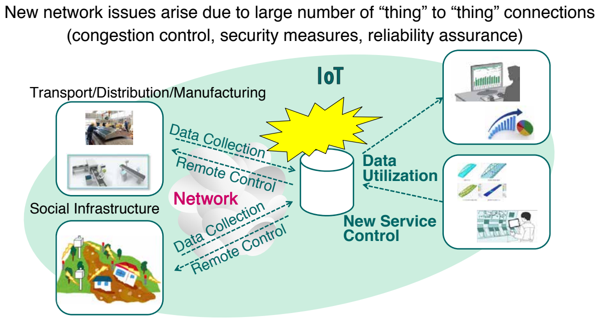
New network issues arise due to large number of "thing" to "thing" connections
(congestion control, security measures, reliability assurance)
IoT
Transport/Distribution/Manufacturing
Social Infrastructure
Data Collection
Remote Control
Network
Data Collection
Remote Control
Data Utilization
New Service Control

Figure 1. Issues Associated with Spread of IoT

IoT Business Platform

Currently, under the premise of these Internet environments, users of IoT applications that tie directly to lifelines such as social infrastructure tend to use leased lines. However, a leased line is very expensive, and it is not designed to enhance IoT services. Meanwhile,rrent Internet with very cheap SIM cards, but security issues and communication quality problems arise. Therefore, OKI is developing an IoT business platform to solve these problems. The platform will provide a highly reliable infrastructure that is as close to a leased line as possible at a price that is low as possible (**Figure 2**).

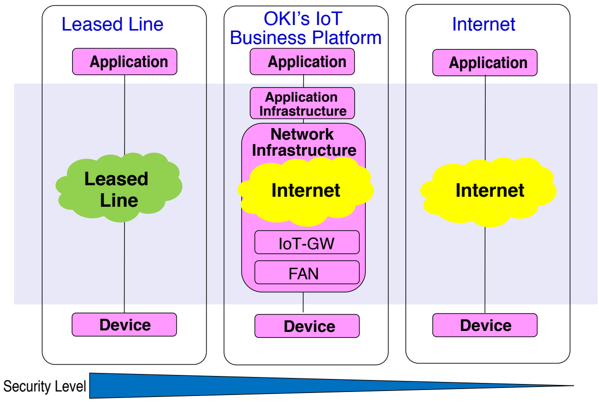

Figure 2. Positioning of IoT Business Platform

The network infrastructure of the IoT business platform is under development based on the four concepts of "connect," "reliable," "low delay" and "secure" (**Figure 3**). This consists of "connect" technology that contributes to the convenience of IoT users as well as the above-mentioned topics of "reliable" technology to assure "reliability," "low delay" technology to cope with "congestion" and "secure" technology as a measure against information leaks.

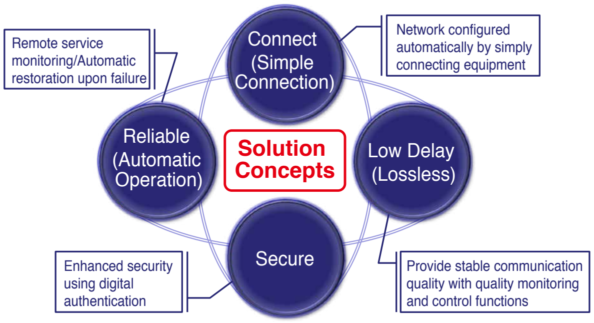
Remote service monitoring/Automatic restoration upon failure
Connect (Simple Connection)
Network configured automatically by simply connecting equipment
Reliable (Automatic Operation)
Solution Concepts
Low Delay (Lossless)
Secure
Enhanced security using digital authentication
Provide stable communication quality with quality monitoring and control functions

Figure 3. Network Infrastructure Concept

(1) Connect

Installing numerous sensors in each business domain and easily connecting them to the network will be the key factor in the spread of IoT. OKI has developed "Zero configuration" software that easily connects with the IoT business platform. The software is deployed in a gateway, and when the gateway is powered up, it automatically contacts with the IoT business platform in the cloud enabling data to be collected, visualized and analyzed. With regard to FAN, OKI has already deployed varieties of 920MHz multi-hop products. FAN can be installed in various domains using those products. Additionally, all sensors that comply with Modbus*1) RTU can be connected.

(2) Reliable

A highly reliable middleware (HA-MW (High Availability Middleware)) was developed for the IoT platform to ensure reliability of the IoT service does not affect the reliability of the data center itself. The middleware is OKI's proprietary product that was developed and improved since the telephone exchange era. It has been in long use with call processing systems to provide highly reliable voice communication assuring 99.999% availability. With the use of this middleware, it is possible to provide a stable IoT service without being affected by the difference of the data center.

In addition, the IoT business platform constantly monitors the state of the connected gateways, and if a problem occurs, the gateway for example can be remotely restarted thus improving the reliability of the gateway.

(3) Low Delay

To cope with the congestion problem at the entrance connection to the data center caused by increase in sensor data, the IoT business platform has a function to monitor the communication quality. This makes it possible to monitor congestion and control the gateway as necessary to avoid congestion. For example, if the cause of congestion is a temporary increase in the volume of sensor data, the congestion can be suppressed by compressing the data at the gateway before it is sent to the data center or by controlling the order in which the data is sent.

(4) Secure

Solving security problems is vital for connecting gateways to the IoT service. Normally with gateways, password authentication is performed in which an administrator inputs a password that is authenticated

*1) Modbus is a registered trademark of Modicon Inc. (AEG Schneider Automation International S.A.S.).

by the server. However, information leakage due to spoofing is recognized as a major problem in operation when password authentication is performed at factories or outdoors. Therefore, digital authentication has been adopted in OKI's IoT business platform. In this method, a digital certificate is embedded in the gateway at the time of shipment and when the gateway is started up at the site, the certificate is automatically authenticated with the authentication server using OMA-DM. As a result, the user can perform secure operation without managing passwords. Additionally, issues that threaten availability such as DDoS attacks on gateways may arise, thus a security incident monitoring system is being developed to ensure secure operation.

Future Direction

While development and deployment of the IoT business platform will proceed according to the aforementioned concepts, application development in various business domains will accelerate on the platform. Therefore, OKI plans to develop application packages that can be used laterally for many business opportunities within this IoT business platform (**Figure 4**).

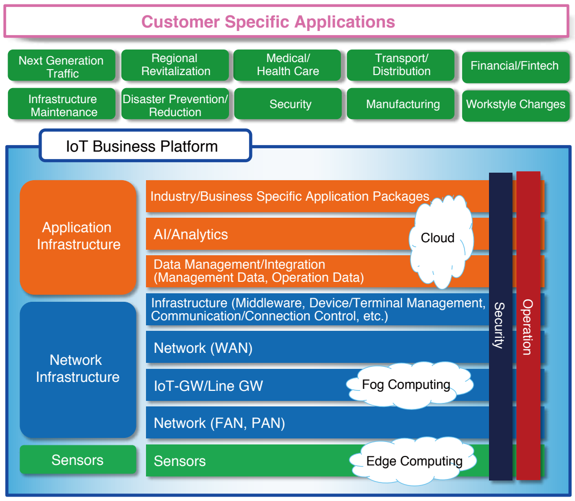
Customer Specific Applications
Next Generation Traffic
Regional Revitalization
Medical/ Health Care
Transport/ Distribution
Financial/Fintech
Infrastructure Maintenance
Disaster Prevention/ Reduction
Security
Manufacturing
Workstyle Changes
IoT Business Platform
Application Infrastructure
Industry/Business Specific Application Packages
AI/Analytics
Cloud
Data Management/Integration (Management Data, Operation Data)
Infrastructure (Middleware, Device/Terminal Management, Communication/Connection Control, etc.)
Network Infrastructure
Network (WAN)
IoT-GW/Line GW
Fog Computing
Network (FAN, PAN)
Sensors
Sensors
Edge Computing
Security
Operation

Figure 4. Layered Structure of IoT Business Platform

Hence, common functions will be available across multiple business domains, which contribute to reducing implementation cost. The flexible configuration of the application package allows it to interwork easily with other analysis engines in other clouds. Additionally, in the process of collecting data from various domains, substantial knowledge can be obtained through the accumulated data. In order to enable service deployment in multiple business domains, the IoT business platform is already implemented with a mechanism to facilitate multi-tenant management. As a result, while maintaining closed management of information for each business domain, it is possible to perform tenant management such as operation management in each business domain without touching confidential information and facilitate horizontal deployment.

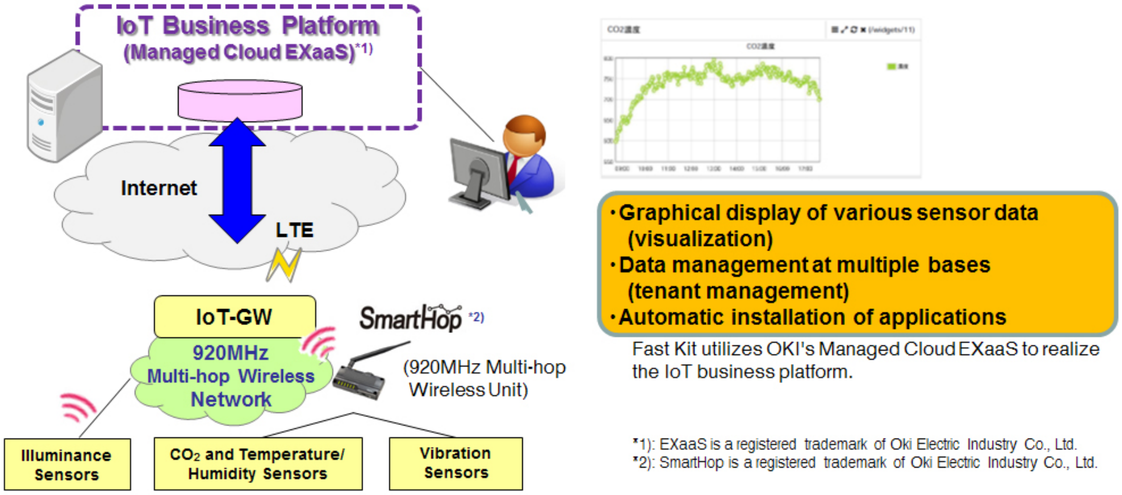
IoT Business Platform
(Managed Cloud EXaaS)*1)
Internet
LTE
IoT-GW
920MHz Multi-hop Wireless Network
SmartHop *2)
(920MHz Multi-hop Wireless Unit)
Illuminance Sensors
CO2 and Temperature/ Humidity Sensors
Vibration Sensors
CO2濃度
·Graphical display of various sensor data (visualization)
·Data management at multiple bases (tenant management)
·Automatic installation of applications
Fast Kit utilizes OKI's Managed Cloud EXaaS to realize the IoT business platform.
*1): EXaaS is a registered trademark of Oki Electric Industry Co., Ltd.
*2): SmartHop is a registered trademark of Oki Electric Industry Co., Ltd.

Figure 5. IoT Fast Kit

To accelerate the spread of future IoT, OKI is deploying the “IoT Fast Kit,” which is a startup kit for customers to utilize the IoT business platform easily (**Figure 5**). The kit is packaged with typical sensors (temperature/humidity, illuminance, vibration, CO_2 sensors, etc.), 920MHz multi-hop wireless units and gateway. Visualization becomes possible for the customer by simply assembling and turning on the power. Through the implementation of this kit, actual sensor data can be acquired to extract issues and appropriate application can be developed within the platform. Thus, an application matching the customer can be provided inexpensively in a high-quality IoT environment.

Conclusion

Assuming the impact the IoT’s current spread will have on network infrastructure, an IoT business platform was introduced, which will encourage the future spread of IoT while at the same time solve the various challenges on network infrastructure. OKI will now focus on building new application packages within the IoT business platform and promote deployment to various business domains. ◆◆

Authors

Kei Kato, Business Development Division, ICT Business Division

TIPS 【Glossary】

LPWA (Low Power Wide Area)
A communication specification undergoing development both as a de facto and official standard for IoT. Data obtained from sensors are generally very small packets and require transmission over long distances to a base station. Considering the sensors may be used outdoors, low power consumption is also a requirement. A communication standard that satisfies these requirements is called LPWA.

LTE (Long Term Evolution)
Specification standardized by 3GPP (Third Generation Partnership Project), a standards organization for mobile networks, and put into service in 2010. Standard for streaming voice in LTE called VoLTE (Voice over LTE) was also standardized by 3GPP and started service in 2012.

Upstream
In communication via a network, communication that flows from a person or a “thing” to the server is normally called upstream. On the contrary, communication that flows from server to a person or a “thing” is called downstream.

OMA-DM (Open Mobile Alliance Device Management)
A device management function standardized by the Open Mobile Alliance, a standardization organization for mobile terminal applications. It defines a protocol to configure a terminal from the server before service startup.

Zero Configuration
A function that enables a terminal or communication device to connect only by turning on the power and without configuration from the user. Term was initially used by the IETF (Internet Engineering Task Force), an Internet standards organization, during the standardization of communication equipment.

DDoS (Distributed Denial of Service) Attack
Denial of Service occurs when a malicious user sends an extreme volume of traffic to a communication facility, terminal, or server on the network and renders the facility unusable. When this malicious attack comes simultaneously from multiple unspecified sources, it is referred to as a DDoS attack.

Security Incident Monitoring System
Situations such as a DDoS attack that affect facilities are referred to as security incidents. A system for monitoring such incidents is called a security incident monitoring system.

920MHz multi-hip wireless unit
Product utilizing the high radio reachability of the 920 MHz band and OKI’s own multi-hop wireless technology. A communication system that transmits data via multiple wireless devices similar to a bucket relay. Even if signals do not directly reach from the base unit, connection to the network is possible via a neighboring slave unit. Therefore, a wide area wireless network can be constructed at low cost. In addition, it automatically selects the communication path with best signal, thus it is strong against temporary signal interference and excellent in reliability.