Security Technology for Remote Monitoring Service Systems Using Edge Computing

KENJI TAKAO[*1] OSAMU KIMURA[*2]
TOSHIMICHI NISHIMURA[*2] FUTOSHI YOSHIKAI[*3]

Services utilizing cloud systems to perform condition analysis and predictive detection have been widely used, but constant connection of a monitoring target such as a plant to an external network has security concerns. For this reason, remote monitoring service systems using edge computing to monitor conditions without transmitting data externally have been attracting attention in recent years. However, even when using such edge computing-based state monitoring of a plant, there was the problem of how to efficiently and securely share the current plant state with remote maintenance personnel to determine the cause of a detected abnormality.

Therefore, we have developed a technology that enables a relatively easy and inexpensive secure connection between an edge computing system and an external network only when necessary. This makes it possible to provide a remote monitoring service while maintaining a high level of security.

1. Introduction

With the background where machine learning and AI technologies have been improving in recent years, there are an increasing number of examples of the introduction of remote monitoring services that perform abnormality detection and prediction based on plant data collected daily. In addition, as the reliability of cloud servers increases and their cost decreases, remote monitoring systems are constructed on the cloud in many cases. However, it is necessary for remote monitoring using a cloud server to constantly connect to an external network and upload operational data to the cloud server. Such constant connection increases the risk of cyberattacks on the control devices and the leakage of operational data, so many plant owners are reluctant to introduce remote monitoring systems and services. One solution is a data analysis service based on edge computing. Edge computing uses a computer that includes monitoring and analysis logic installed in the plant to process data on site to detect and predict abnormalities, thus making state monitoring of the plant without transmitting data externally possible. However, monitoring services using edge computing have the following problems:

(1) Sharing data collected by the edge computer and analysis results with remote maintenance personnel
(2) Updating the data analysis program installed on the edge computer

As a measure for the above, a VPN (virtual private network) is often used in general, but the equipment and service is expensive and setting it up is troublesome. Therefore, we developed a system for remote monitoring services that establishes a secure connection with an external network only when needed and allows only necessary operations using security technologies that are relatively cheap and can be set up relatively easily without complicated configuration.

*1 Chief Staff Manager, ICT Solution Headquarters, CIS Department
*2 Manager, MHPS Engineering Co., Ltd.
*3 MHPS Engineering Co., Ltd.

2. Secure communication technology - NAT traversal + original encrypted communication

2.1 Characteristic of secure communication technology

The developed system uses secure communication technology provided by remot3.it of the United States. This technology is based on NAT traversal and encrypted communication unique to remot3.it, and is characteristically small, light and simple. In particular, a high level of security is ensured by the following functions:

(1) No public IP (Internet Protocol) required for a secure connection. No need to disclose the private IP to the connection destination (**Figure 1**).

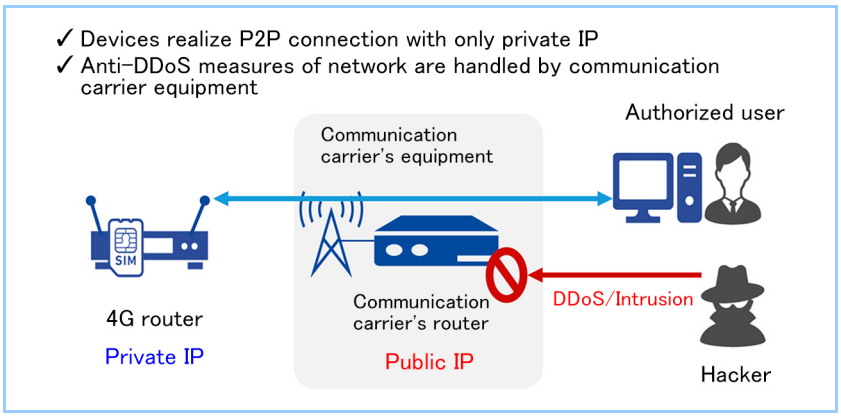

Figure 1 Feature of secure communication technology (1): No public IP used for P2P (Pier-to-Pier) connection

(2) Secure communication is possible with all ports of inbound (outside to inside) communication destination machines closed (**Figure 2**)

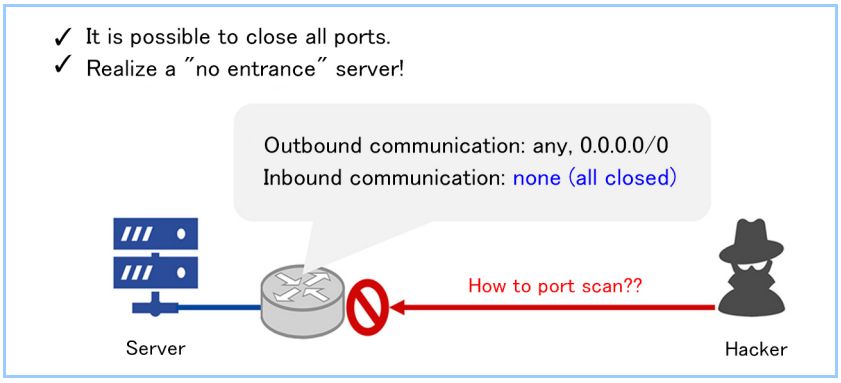

Figure 2 Feature of secure communication technology (2): All inbound communication ports of connection destination machines can be closed

In addition, this technology is a package technology that allows secure communication technology to be easily used without knowledge of encrypted communication and NAT traversal, and can be introduced relatively smoothly.

2.2 Details of secure communication technology

Figure 3 shows the mechanism of secure communication technology combining remot3.it's unique NAT traversal and encryption. In this figure, "Management server" is located in the cloud, and that server manages all connections. Each terminal encrypts its own location (its own local IP and the public IP of the connected router) and periodically transmits the information to the management server using UDP. Thereby, even when the terminal is connected to another router, the management server can always determine the location of the terminal by appropriately updating the terminal information based on the information transmitted from the terminal.

When starting a connection between terminals, the connection request source sends the connection request destination service name (machine name + service name) to the management server (1). The server authenticates the request source (2, 3, 4), interprets the request information, encrypts the information necessary for connection, and sends it to the connection request source (5-1) and the information of the connection request source to the connection request destination at the same time (5-2). During this process, information exchange (5-1, 2) using the principle of Stateful Inspection is performed based on the UDP port numbers of the connection request source and the connection request destination, and an original encryption tunnel is established between the terminals (6, 7). For the established original encrypted tunnel, when using SSH for example, the IP address and port number of the SSH connection destination can be completely hidden by using the local host (loopback address 127.0.0.1), without the host information of the SSH connection destination. The preparation for using this technology is just to install a dedicated application on the machine to be connected and register the machine name and the service name, so a high level of security can be ensured with simple settings and operations.

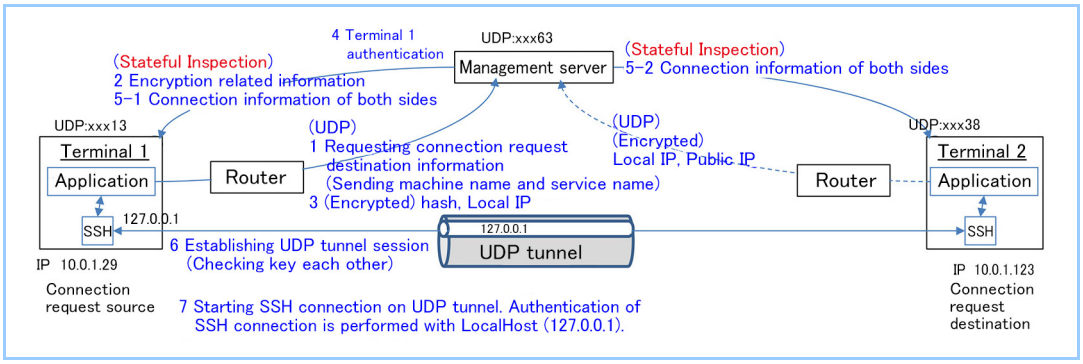

Figure 3 Secure communication mechanism combining NAT traversal and unique encryption technology

3. Secure remote monitoring service system

3.1 System configuration

This chapter describes a remote monitoring service system developed using the secure communication technology described in Chapter 2. **Figure 4** depicts the configuration of this system. It is not necessary to install remot3.it software on the remote monitoring PC that is the connection source and the customer's monitoring PC if the remote monitoring function (3.2 (1)) by the web application is only used. (Note: It is necessary to install remot3.it software if the functions of 3.2(2) or 3.2 (3) are used.).

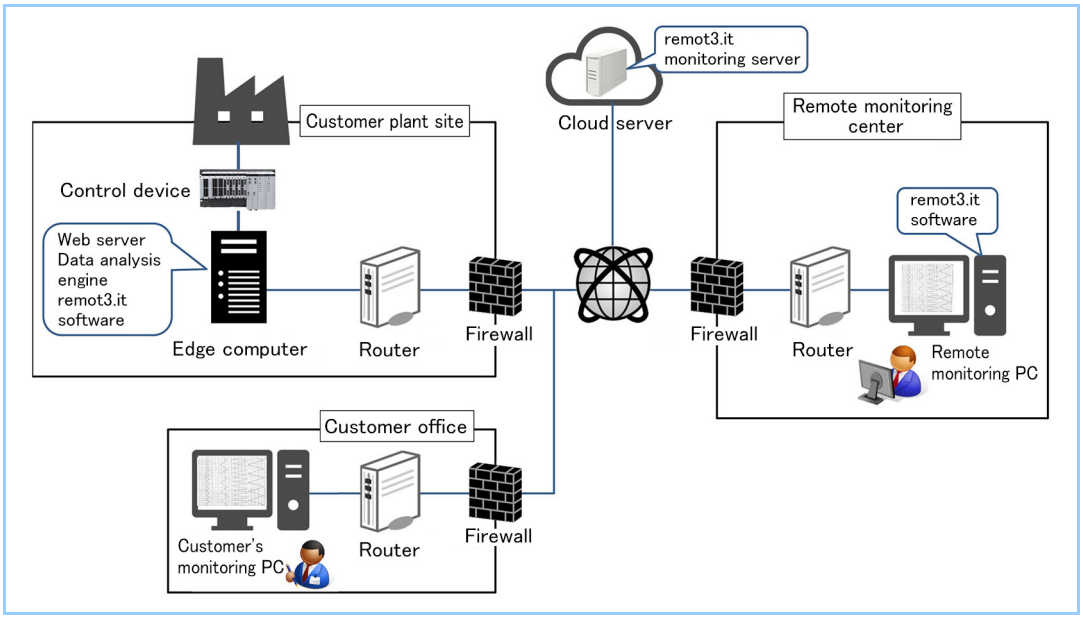

Figure 4 Remote monitoring service system using edge computing

3.2 Function

The remote monitoring service provides the following functions. The use of these functions enables the introduction of a secure remote monitoring service, which leads to the expectation that the availability will improve through early detection and recovery in the case of abnormalities.

(1) Web application screen browsing using http/https

This function can increase the security level by restricting the use of the web services to specific users. Users of this function can browse the corresponding web application screen simply by entering the local host address (127.0.0.1) in the browser after establishing a connection to the machine containing the web server. No actual IP address is used, so a high level of security is ensured.

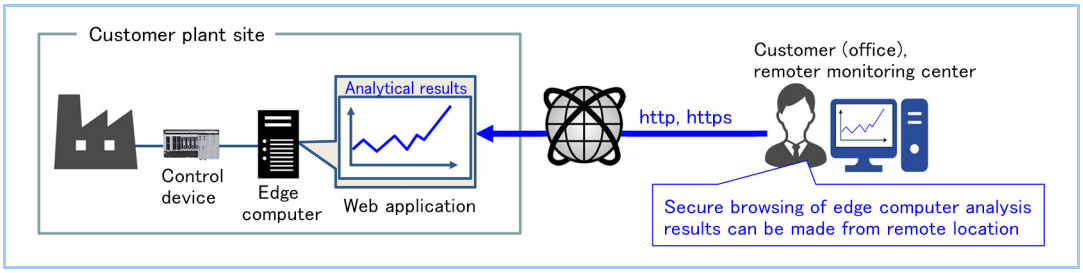

Figure 5 Web application screen browsing function using http/https

(2) Access to remote machines using remote desktop

Remote maintenance is required to operate a computer (edge computer) containing the data analysis engine and the web server located at the customer plant site. By giving the authority of remote access to the customer, it is possible for the customer to easily control external access by themselves. Similarly to (1) above, the IP address for remote access uses the local host address (127.0.0.1) (**Figure 6**).

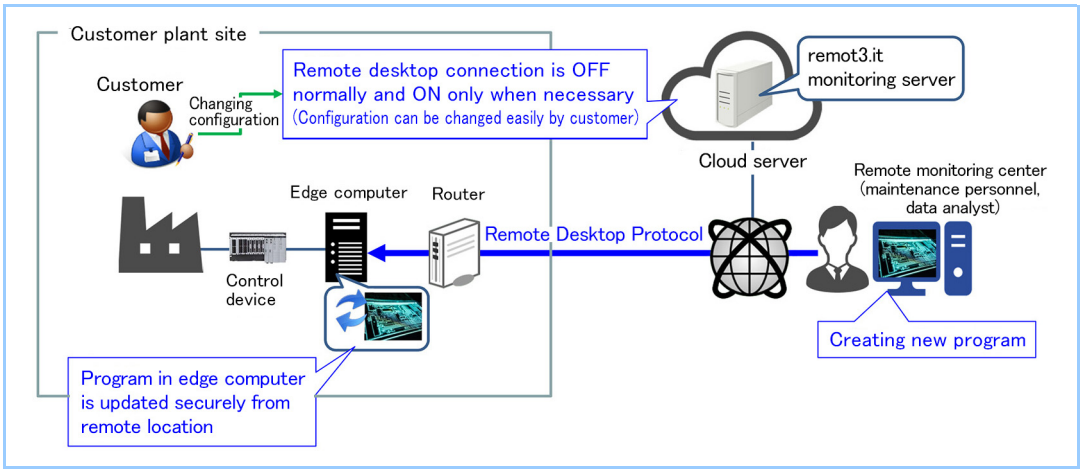

Figure 6 Access to remote machines using remote desktop

(3) Automatic secure transmission of data

Even when a monitoring service using edge computing is used, detailed analysis of data by a remote data analyst may be required in the event of an abnormality, etc. In such a case, this function can be utilized to transmit and receive data securely. For example, in the case of the prediction of a measurement value using edge computing, when a decrease in the prediction accuracy is detected, the data required for cause analysis is transmitted to the corresponding machine (remote location) using secure data transfer protocol (sFTP), and the secure connection will be automatically disconnected after the transmission is completed. This enables automatic data sharing without human intervention and quick cause identification. In addition, for example, in the case of sending security patches to an edge computer, files can be transmitted securely from a remote location to the edge computer in a similar manner (**Figure 7**).

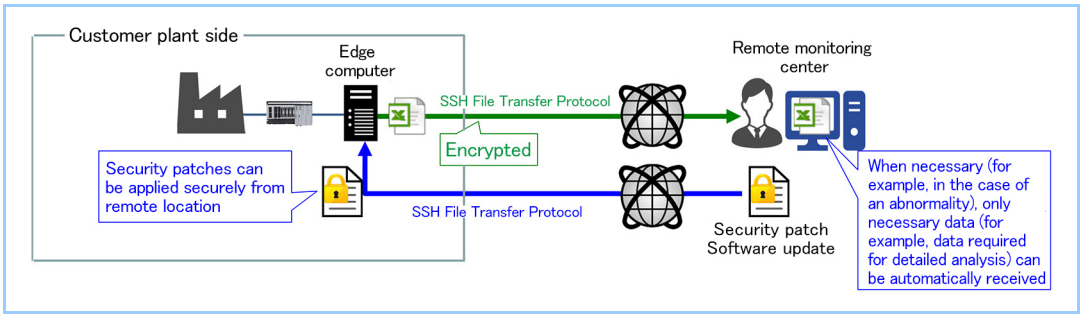

Figure 7 Secure file transmission (including automatic connection, transmission and disconnection functions in the case of an event)

4. Application examples

Some functions of the system described in this paper were verification-tested with after-sales service of the VPSA (Vacuum Pressure Swing Adsorption) oxygen generator carried out in Nagasaki Division of MHPS Engineering Co., Ltd.

Conventionally, when an alarm occurred at a customer plant, MHPS Engineering requested that the customer emails the data necessary to investigate the cause and then performed detailed analysis (**Figure 8**). In this process, it took a lot of time to recover, resulting in a decrease in the availability of the customer's plant.

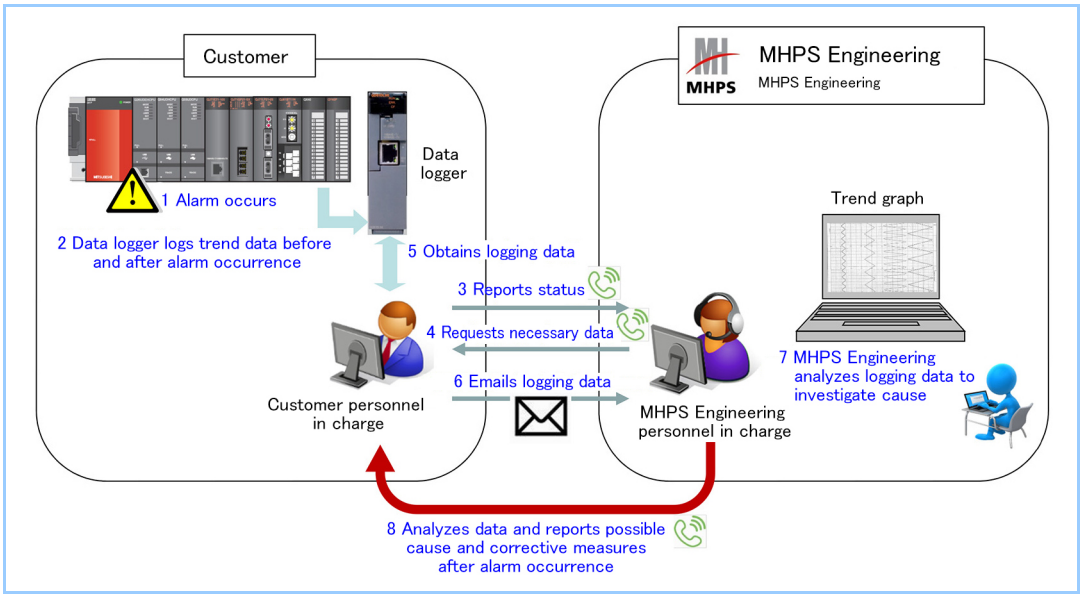

Figure 8 Conventional handling process of MHPS Engineering for alarm event

The developed secure communication system was applied to this remote monitoring service. **Figure 9** is the schematic diagram and the secure connection process. This service system was provided with the following functions:

(1) Operation support using graphic operation terminal
(2) Display of ladder program of controller (PLC) and improvement of program
(3) Trend graph monitoring of data obtained from control device in customer's plant
(4) Secure transmission function of operation log file for detailed data analysis

The developed system was applied to a customer plant and verification-tested. As a result of the verification test, it was confirmed that all of the above functions could be executed remotely from MHPS Engineering, satisfying the desired requirements.

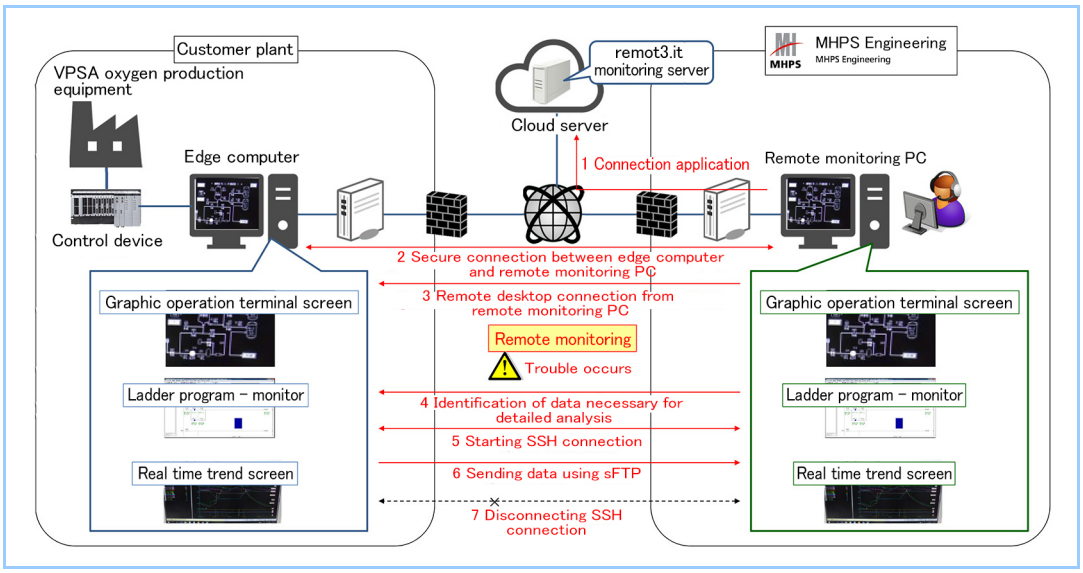

Figure 9 Outline of VPSA remote monitoring service system and secure connection process

Furthermore, this system is being verification-tested by MHPS Engineering at several customer plants. After these verification tests, the service is scheduled to start in fiscal 2020.

5. Conclusion

This paper presented our developed remote monitoring system using secure communication that combines NAT traversal and original encryption technology.

The use of secure communication combining NAT traversal and unique encryption technology made it possible to solve the problems of conventional edge computing such as the data sharing method, etc., and to provide a remote monitoring service to a wide range of customers.

The developed system was applied to a remote monitoring service planned by MHPS Engineering and its effectiveness was verified. In the future, we plan to expand this to other plants and develop functions that can further contribute to improving customer value.

In developing this system, we received technical support from remot3.it. We would like to express our appreciation.

References

(1) remot3.it website,https://remote.it/