Azbil's cloud operation infrastructure for providing safe and secure services

Takashi Noma
Tadakazu Suzuki
Masaru Kishi
Hidenobu Seki

Keywords
SaaS, cyber security, ISMS, ITIL, DevSecOps, DX

As the provision of value in the form of cloud-based software as a service (SaaS) increases, cyber security risks are also increasing day by day, and they are assuming new forms. Commensurate measures to maintain secure operation are indispensable. However, it is not easy to build an individual cloud service that adequately addresses security. For that reason we have built a common platform for cloud service development and implementation that is equipped with security measures and is constantly updated. In addition, by establishing a specialized organization in charge of cloud operational security, by utilizing IT service management frameworks, and by acquiring information security management system certifications, we are constantly striving to improve operational security. Additionally, a specialized organization has been set up to ensure security in the overall product development process and to monitor its progress. Through these efforts to enhance our cloud operation infrastructure, we have been able to provide the safety and security of Azbil's services, which we continue to strengthen.

1. Introduction

The nature of society and industry and their needs are significantly changing, as can be seen by the fact that they are described with phases like the Fourth Industrial Revolution and Society 5.0. In addition, the spread of the novel coronavirus has revealed various problems requiring solution and has created new ones. The role of the azbil Group is expanding along with the increasing opportunities to create value. The azbil Group aims to make contributions that stand "in series" with a sustainable society using the SDGs as guidelines.

The Group is striving to offer cloud-based value in order to quickly provide services with high added value that leverage advanced IoT and AI technology, that are appropriate for the life cycle of customers' facilities, and that reduce the operating and maintenance costs of customers' systems. However, cyber security risks in the cloud increase day by day and constantly change. Therefore, risk-appropriate security measures and operational security measures are required.

This article describes Azbil's cloud operation infrastructure for safe and secure services and the cloud solutions that are built on the infrastructure.

2. Azbil's efforts

First and foremost, a development and implementation platform with sufficient security is required to provide cloud services safely and securely. In addition, operational security measures and a function to ensure and review the security of the product development process in general are also extremely important. This article describes our efforts for these challenges.

2.1 Common platform for cloud service development and implementation

The three principles of information security are availability, confidentiality, and integrity. Designing and building a system configuration that satisfies these requirements for every application development project separately would not only pose a large burden on application developers, but also risk problems such as missing something in the design or deficiencies in the structure. In addition, designing and building such a system configuration in a cloud environment requires expertise, leading to a significant bottleneck in application development. In this context, Azbil has designed a common application platform and made it available to limit the range of necessary considerations during application development, reduce the needed man-hours for application development, and shorten the development period while guaranteeing availability, confidentiality, and integrity. The use of this common platform also improves operational efficiency through standardization of operation design and actual operation.

The functionality provided on the common platform is roughly divided into the engineering platform and the runtime platform. This article describes the runtime platform, which directly contributes to the provision of safe and secure cloud services. The runtime platform provides the container orchestration environment Docker, which guarantees safety and high availability. When a container created as an application service is run on this platform, a structure for stable operation and container management functions are available.

Next, regarding the security risk countermeasures on the platform, which are essential to stable operation, we have implemented thorough entry and exit measures at the service provision boundary with the outside world as part of the common platform, in addition to monitoring and management during operation. These entry and exit measures are difficult to design and build, and also require large initial costs and operation costs in order to make the security measures thorough. If these measures were implemented separately for each application, their cost would be directly reflected in the cost of providing the application service and could weigh on the business. Therefore, we provide them as part of the common platform so that the burden is shared across multiple applications, thereby satisfying the two contradictory requirements of security and cost.

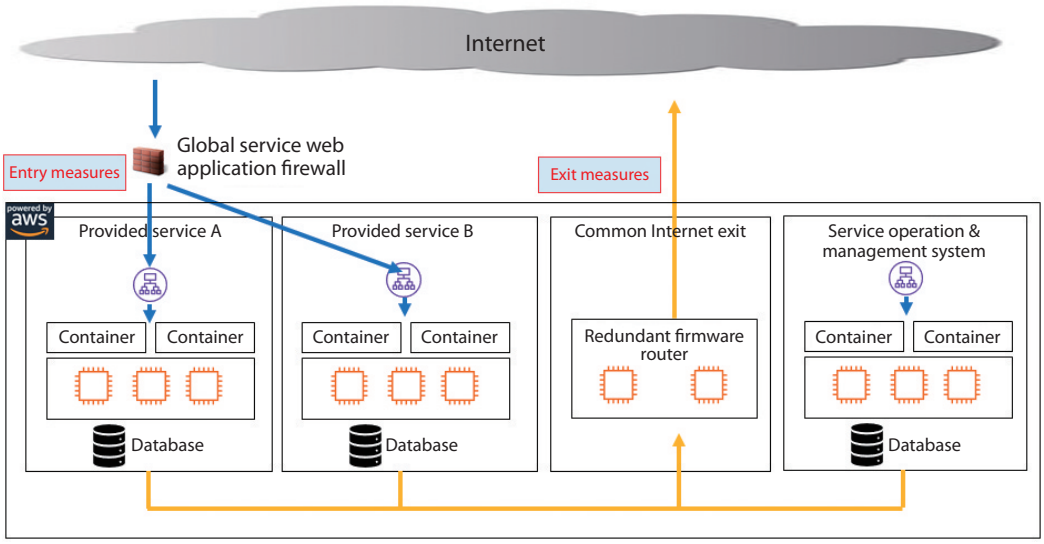

Fig. 1. Overall configuration

2.2 Cloud Operation Center

Unlike the case with conventional one-off sales, a cloud service must be maintained even after delivery so that customers can continue to use it safely and with peace of mind. In the past at Azbil, each department operated its cloud services, and the related expertise stayed in each department. Although this situation was working well from the viewpoint of individual optimization, there would have been problems in terms of provision of standardized services as Azbil looked to enhance its cloud services. In April 2019, the azbil Group set up the Cloud Operation Center as a specialized organization to address this issue and provide our cloud services more safely and reliably.

An example of efforts to provide standardized services is the presentation of functional requirements related to operation at the project planning phase. In the past, functional requirements related to operation were not clear in the planning phase, resulting in different implementations of operation-related functions in each service. Because differences in operation between individual services must be manually addressed, they increase operation costs and raise the risk of incidents due to operational errors. Standardization of the operation functions unifies the quality of operation of each service, and as a result, services can be provided safely and securely from the beginning. Also, because the importance of operation tasks is conveyed to related parties through these activities, the operation department receives the information it needs. As a result, the company can consolidate inquiries from customers, promptly react to incidents, and perform other activities.

In addition, we guarantee reliable operation by taking a variety of security measures and operational measures. Figures 2 and 3 give an overview.

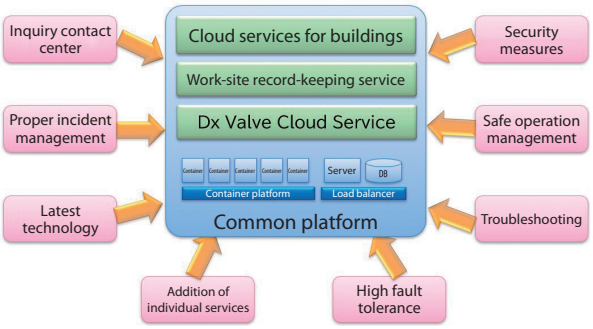

Fig. 2. Operation diagram of the common platform

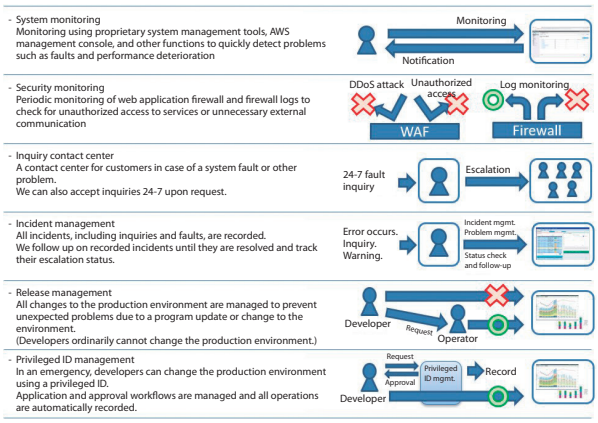

Fig. 3. Main operation tasks

2.3 ITIL (IT service management framework)

A variety of operation tasks must be reliably carried out for customers to use services with peace of mind. Therefore, the Cloud Operation Center makes reference to the IT Infrastructure Library (ITIL) as it designs a variety of operation tasks. ITIL provides systematic guidelines for best practices for IT service management. By referencing ITIL, it is possible to build an operation framework and system more rapidly and efficiently.

Because ITIL addresses the whole life cycle of IT services, including strategies, design, migration, operation, and continuous improvement, it cannot be fully utilized by applying it only to operations. Therefore, the Cloud Operation Center strives to convey insights from ITIL to personnel working in planning, development, and other departments so that it is used across our IT services. Although ITIL was initially unfamiliar to us, we are now carrying out specific activities such as creating service catalogs. We believe that making everyone aware of insights from ITIL will make it possible to enhance customer satisfaction about our IT services.

2.4 Information security management system (ISMS)

The largest concern of cloud service users is information security. It is important for the service provider to make efforts to address their concerns in an understandable way. For this purpose, the Cloud Operation Center has obtained certification for compliance with the ISO 27001 international standard for information security management systems (ISMS) and the ISO 27017 international standard for cloud security. We needed to spend many hours confirming conformity with these standards, enhancing a variety of security measures, creating relevant documents, and modifying the terms of use to obtain these certifications. However, we believe that these efforts resulted in more secure operation.

Because information security incidents must never occur, providers cannot lower their guard even after obtaining certifications. Operations to guarantee information security may lose their effectiveness over time and become unable to prevent incidents. Therefore, the Cloud Operation Center provides ISMS training and implements periodic improvement activity to maintain a high level of awareness about information security and achieve more secure operation.

CLOUD 722670
IS 722669

Fig. 4. ISMS 27001 and 27017 certification

2.5 Cyber Security Office

Azbil set up its Cyber Security Office in April 2019 as a specialized organization to reliably ensure the cyber security of our current and future products (including products and cloud services). Ensuring product cyber security has been defined by Azbil as protecting and maintaining the availability, integrity, confidentiality, authenticity, accountability, non-repudiation, reliability, and other properties of products in cyberspace.

This organization takes the lead in ensuring the cyber security of products mainly through the following activities:

1. Establishing rules and policies to ensure cyber security throughout the product life cycle
2. Steps to ensure cyber security in the product development process and reviews of their implementation status
3. Collection of information on vulnerabilities in products sold and taking countermeasures

To properly and efficiently ensure the cyber security of products, everyone engaged in the long life cycle from product planning and development through to maintenance must recognize the importance of cyber security, consider and implement steps to ensure cyber security in their business tasks, and work on this matter as a team.

First, in the product development process, in addition to the conventional development process standards and practice activities, we continuously review the process with an eye to ensuring cyber security. We review a wide range of items based on a cyber security risk assessment, taking into consideration cyber security requirements, more secure design and implementation, validation, handling of information on the vulnerabilities of third-party components, and other items. We created our process standards by referring to many different standards and guidelines. These policies and standards are conveyed as needed at periodic company-wide product cyber security enhancement meetings.

In reviewing cyber security throughout the entire product life cycle, we begin by reviewing the cloud services that Azbil develops and sells. With cloud services, operational security after the service begins is especially important.

Regarding information on vulnerabilities in third-party components in our products, Azbil has created vulnerability information handling standards and periodically implements activity according to the standards.

We reliably repeat the PDCA cycle to make improvements on the following points that were revealed through past efforts.

- Implementation and verification of measures to ensure cyber security were not efficiently incorporated into the development process.
- Steps to raise the awareness of product planning developers about ensuring cyber security are still insufficient.
- Awareness of measures to maintain and improve cyber security after product release is low.

To accelerate product development and improvement while making these improvements, we have introduced the DevSecOps approach, which considers security beginning in the product development or operation planning design phase, incorporates cyber security diagnostics tools into the development process, further promotes automation, develops personnel who consciously ensure cyber security, and encourages more employees to obtain Registered Information Security Specialist certification, among others, as shown in the conceptual diagram in figure 2. We will continue to make improvements so that our customers can use our products with peace of mind.

3. Azbil's cloud services

This section describes the cloud services provided on Azbil's cloud operation infrastructure. Azbil has obtained the ISMS 27017 cloud security certification for its cloud services for monitoring and managing energy, equipment, and quality.

3.1 Cloud Services for Buildings

The features of cloud services allow not only the building owner but everyone involved in the building, including workers in offices and the building manager, to use the services in line with their purposes, regardless of the time and their location, thereby promoting information sharing among related parties.

The building owner and building manager can streamline building energy management and equipment management operations and reduce management costs. Occupants can easily turn on and off, configure, and otherwise operate air conditioning and lighting from a PC, tablet, or smartphone. These services also help to improve the office environment because occupants can change the set temperature depending on whether they feel hot or cold. In addition, these services visualize energy use to promote energy-saving measures and raise awareness.

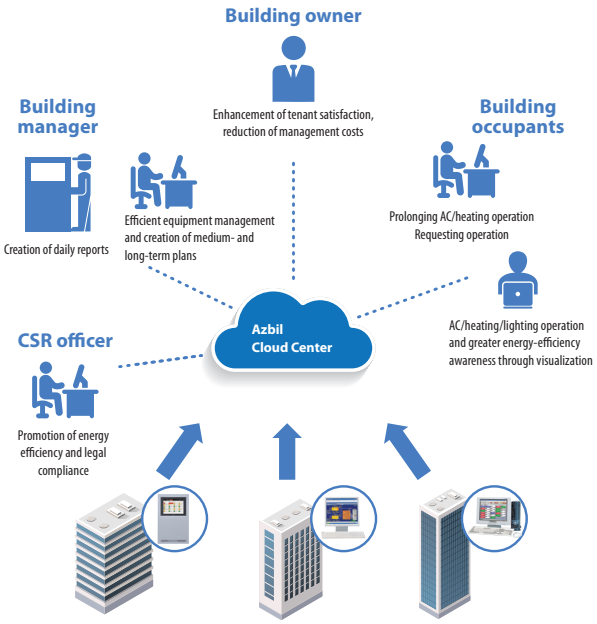

Fig. 5. Use cases for cloud services for buildings

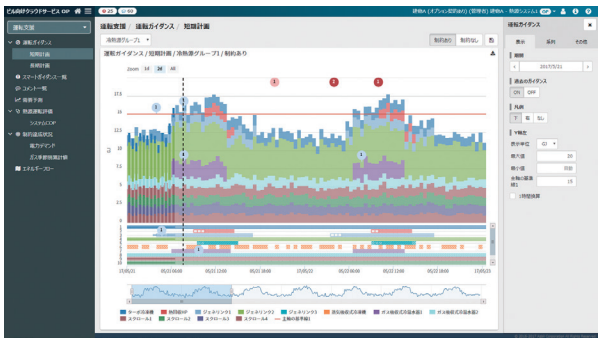

Fig. 6. Sample energy management screen (for heat source optimum operation)

3.2 Work-site record-keeping service

This cloud service easily and smartly digitizes handwritten paper records still used at many sites. The service takes advantage of the features of cloud services in that it requires no hardware assets or customer-employed operators and has the flexibility for a quick launch of operations whenever needed.

Handwritten records for a wide variety of operations at manufacturing, maintenance, and other sites can be digitized with a PC, smartphone, or tablet on the spot and saved in the cloud. Photos can also be taken on the spot and saved as images in addition to data such as text, numerical values, or dates and times.

Fig. 7. Digitization of handwritten records

A records screen suitable for the type of business can be created with simple operations such as drag-and-drop and text entry. In addition, there is an information collection function that supports diverse entry formats, including data acquisition from QR codes or barcodes and image recording, which cannot be done with paper records, by taking advantage of the features of mobile devices.

Intuitive record operations lead to a reduction in errors and working hours. Because paper records are converted into digital data and saved in the cloud on the spot, information can be shared in real time for understanding the status of the site, etc. Using this data to accurately understand the status on the site facilitates operational improvements and progression toward digital transformation.

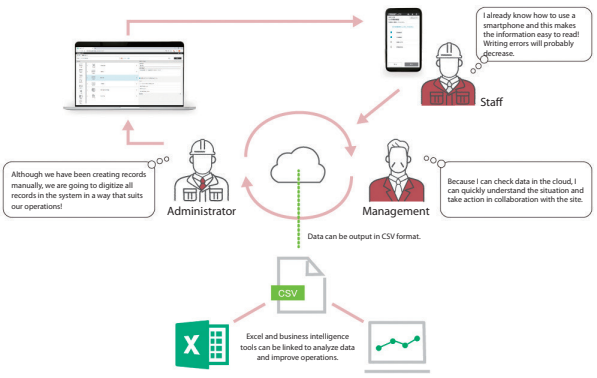

Fig. 8. Use cases for the work record service

3.3 Valve Cloud Service

Operating data from valves that is collected by the PLUG-IN Valstaff control valve maintenance support system is automatically sent to the cloud and analyzed. Customers can see diagnostic results when needed, in the form needed, and in the situation needed by leveraging the features of the cloud service. In the past, customers had to check and evaluate operating data accumulated in Valstaff day by day to check that valves were functioning well. Because the valve cloud service detects valve abnormalities at an early stage and shows the predicted progress of abnormalities based on diagnostic data, customers do not have to check or evaluate the operating data. This service contributes to the stabilization of production equipment and the enhancement of safety. Figure 9 provides an overview.

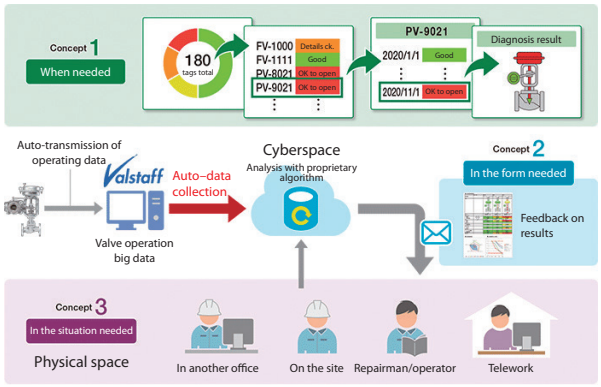

Fig. 9. Use cases for the valve cloud service

4. Conclusions

Each company in the azbil Group is accelerating the provision of value by leveraging cloud services. The Group will continue to further enhance its vital cloud operation infrastructure.

We trust that more customers will use Azbil's cloud services safely and with peace of mind, knowing that we are their partners in promoting digital transformation (DX) and quickly addressing changes in the business environment.

Authors

Takashi Noma — Cloud Operation Center, Azbil Corporation

Tadakazu Suzuki — Cloud Operation Center, Azbil Corporation

Masaru Kishi — IT Development Department 1, IT Development Headquarters, Azbil Corporation

Hidenobu Seki — Cyber Security Office, Azbil Corporation