Technology Reports (Special Articles) Public Clouds CCoE Serverless
Special Articles on Use of Public Clouds

NTT DOCOMO's Use of Public Clouds and Role of CCoE

Innovation Management Department Hiroki Moriya Takeshi Mori
DOCOMO Innovations, Inc. Yasuhiro Naoi

NTT DOCOMO has been providing a multitude of services using public clouds for over ten years. Today, activities continue toward more efficient and optimal use of public clouds centered about NTT DOCOMO's Cloud Center of Excellence (CCoE). This article describes those activities and the public cloud usage system at NTT DOCOMO and introduces recent development trends on the cloud.

1. Introduction

The use of public clouds[*1] in companies and organizations has been increasing rapidly in recent years, and business expansion using public clouds has practically become the norm as reflected by the catchphrase "cloud first." At the same time, the need has arisen for many companies and organizations to expand or reform their business operations by leveraging the swiftness and flexibility of public clouds that are not on-premise[*2]. On the other hand, using a public cloud often requires an approach different from that of constructing and operating a conventional on-premise IT system, and for this reason, there are not a few companies and organizations that cannot introduce and efficiently use public clouds without problems.

In general, a number of issues must be given attention when using a public cloud. These include service testing on introduction, implementation of security measures, drafting of usage policies, establishment of a usage system within the company, acquisition of skills, personnel training, collection of fast-changing cloud information, and know-how development. To make good use of a public cloud, it is important to recognize how its use differs from that of conventional on-premise IT systems and to proactively keep up with changes that can frequently

*1 Public clouds: Cloud computing services that anyone can use over the Internet.

occur on a public cloud.

NTT DOCOMO has also been using public clouds for many of its services for over ten years. As a result, it has faced the issues described above and continues to this day with activities that aim to achieve more efficient and appropriate use of public clouds. In this article, we describe those activities and the public cloud usage system at NTT DOCOMO.

2. Use of Public Clouds at NTT DOCOMO

This section describes the use of public clouds at NTT DOCOMO as of December 2020.

2.1 Scale of Public Cloud Use

At NTT DOCOMO, the use of public clouds began in 2009 for research-and-development and testing purposes. Following this, the range of use began to expand leading to the adoption of public clouds for large-scale commercial services in 2012. The volume of use continued to increase on a yearly basis, and as of December 2020, total use came to more than 900 accounts on Amazon Web Services (AWS)*3, more than 250 accounts on Google Cloud Platform (GCP)*4, and more than 50 subscriptions on Microsoft Azure*5 (hereinafter referred to as "Azure").

2.2 Range of Public Cloud Use

NTT DOCOMO uses public clouds in a wide range of fields. These include Web services, back end system*6 for mobile applications, data analysis platforms, machine learning, and internal company systems.

2.3 Public Cloud Usage System

NTT DOCOMO has set up a usage system to facilitate the efficient use of public clouds (**Figure 1**). The most outstanding feature in the use of public clouds at NTT DOCOMO is the existence of a definitive Cloud Center of Excellence (CCoE)*7. This is a team having a wide range of specialized knowledge related to public clouds, and at NTT DOCOMO, the use of public clouds has been centered on this CCoE.

3. NTT DOCOMO CCoE Activities

This section describes in detail the activities of the CCoE that plays a core role in NTT DOCOMO's public cloud usage system.

3.1 Consultation

Providing support when using public clouds is an important role of the CCoE. Given a certain in-house project, the CCoE provides support for system design when constructing a system on a public cloud, conducts reviews, and presents methods for efficiently satisfying security requirements. Initial system design is particularly important when using a public cloud since it can greatly affect subsequent costs and system operation. The CCoE often provides support at the time of system design for this reason.

In addition, a sudden increase in the number of system users when beginning system operation will inevitably lead to an escalation of costs, so to optimize costs in such a situation, the CCoE will provide support for grasping cost factors, reviewing design, etc.

3.2 Coordination and Optimization of Cloud Costs

In general, a public cloud provides much flexibility in the way that it is used, but at the same time, an expanding number of services and purchasing

*2 On-premise: An environment in which a company owns, maintains, and operates the hardware making up its system.
*3 AWS: A cloud computing service provided by Amazon Web Services, Inc.
*4 GCP: A cloud computing service provided by Google LLC.
*5 Microsoft Azure: A cloud computing service provided by Microsoft Corporation.
*6 Back end system: The system that is centrally operated on servers or other hardware as opposed to operation on user mobile terminals or computers.

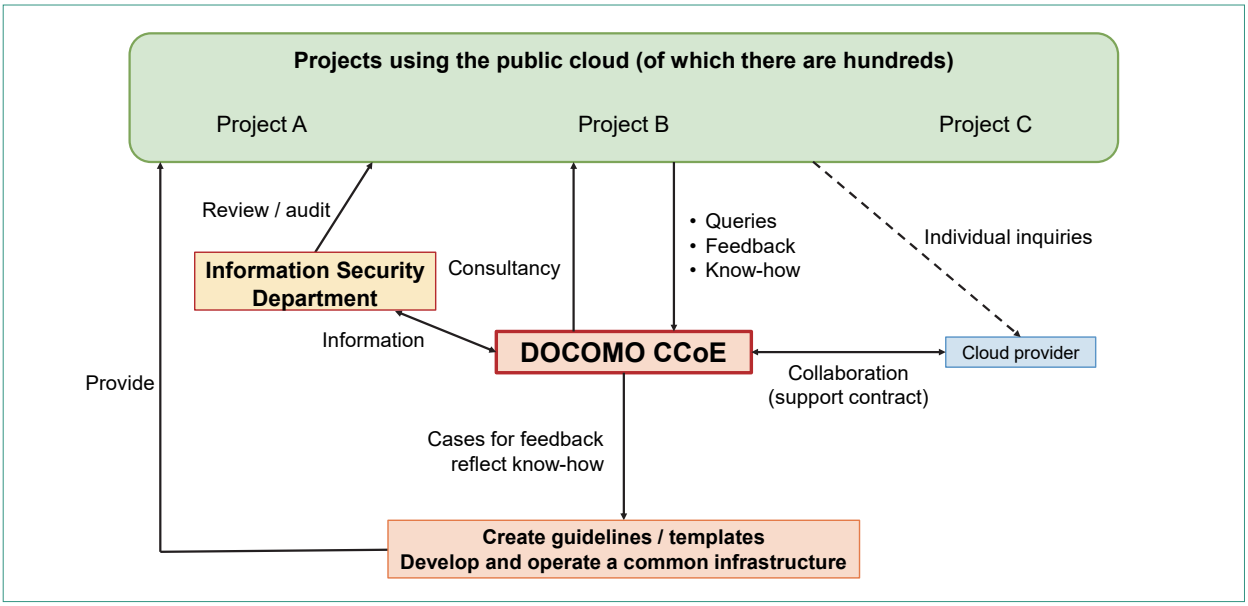


Figure 1 NTT DOCOMO public cloud usage system

options can easily make the payment of expenses and account processing overly complicated. An increase in the number of cloud-based projects can therefore increase the labor involved in these tasks. For these reasons, the CCoE centrally concludes contracts with cloud operators and coordinates and processes payments for each project in a lump-sum manner thereby reducing the workload of each project.

There is another advantage to making lump-sum payments in addition to reducing the load of business processing. Public cloud operators offer a volume discount option as the amount of use increases, so lumping payments together can ensure a certain volume and minimize usage fees over the entire company.

3.3 Collection and Dissemination of Up-to-date Information

Public clouds are evolving rapidly and keeping up with the latest information about clouds can be difficult for project members burdened with project tasks. The CCoE has therefore taken the initiative in keeping up to date on the state of public clouds. For example, the CCoE actively participates in technical events related to public clouds to gather information and give presentations. It also reflects gathered information in guidelines as know-how, performs verification tests on its own, and disseminates information to project members within the company.

3.4 Creation and Dissemination of Cloud Business Support Tools

The CCoE prepares a variety of support tools and disseminates them within the company so that each project can efficiently use public clouds.

Although the cloud offers many and varied functions for accelerating business development, using them incorrectly may lead to a fault on the cloud and service interruption and making erroneous settings may cause a security accident to occur. It is therefore necessary that users have the technical

*7 CCoE: An exclusive team within an enterprise that establishes best practices and creates essential systems and governance to make cloud usage successful.

knowledge for using the cloud correctly, but the knowledge level of users varies, so from a company perspective, how to raise the level of technical knowledge of all employees is an issue of concern.

With the above in mind, the CCoE prepares guidelines that feature cloud usage methods from the NTT DOCOMO point of view. These guidelines make it possible to acquire the minimally required amount of knowledge on the use of public clouds in a short time even for users with little knowledge of clouds. These guidelines cover the use of AWS, GCP, and Azure. Here, we present the list of guidelines prepared for AWS in **Table 1** and an excerpt from those guidelines in **Figure 2**.

Table 1 List of guidelines (AWS)

No	Type	Description
1	Cloud development guidelines	Describes mindset and manners when using the cloud and guidelines that should be considered and implemented in each phase of development flow. Covers important points such as design and security and minimizes mistakes in usage.
2	Security design patterns	Minimizes omissions in security considerations when using the cloud and constructing a system. Prepares requirements in line with ISO/IEC27017 beforehand to enhance compliance with ISO management measures. Lists essential security requirements when constructing a system using AWS.
3	Security templates	Provides AWS CloudFormation templates for generating instance groups that provide network configurations, network filtering functions, and basic functions that take security design patterns into account. Simplifies the implementation of security measures.
4	IAM design patterns	Lists best practices in the design of IAM policies within NTT DOCOMO in line with AWS account usage patterns.
5	Incident response guidelines	Lists responses to incidents such as cyber attacks in in-house systems and service-providing systems on the Internet using AWS combined with actual case studies.
6	Cost optimization guidelines	Describes cost determination/analysis methods and cost reduction/optimization methods for personnel managing AWS costs.
7	System migration guidelines	Lists key points and matters deserving attention during a system migration based on knowledge gained in past migration examples to facilitate a smooth migration from an on-premise system to AWS.
8	Common platform guidelines	When beginning to put multiple accounts and multiple systems into operation, raising efficiency by unifying operations and standardizing operation systems can be an effective approach. These guidelines list methods for smoothly achieving greater efficiencies in operations by leveraging the characteristics of cloud computing.
9	Container guidelines	Describes which tools to use and how to use them to achieve effective and safe use of containers in each project. Targets personnel who wish to incorporate containers in service development/operation.
10	Serverless guidelines	Lists methods for efficiently and effectively using serverless computing in each project when developing and operating serverless systems on AWS. Answers questions like "What is the best way to implement a serverless system?" and "In what way and in what kind of services can serverless computing be used?"
11	DevOps guidelines	Describes which tools to use and how to use them to achieve efficient and effective practice of DevOps in each project. Targets personnel who wish to incorporate a DevOps mindset in service development/operation.

IAM: Identity and Access Management
IEC: International Electrotechnical Commission
ISO: International Organization for Standardization

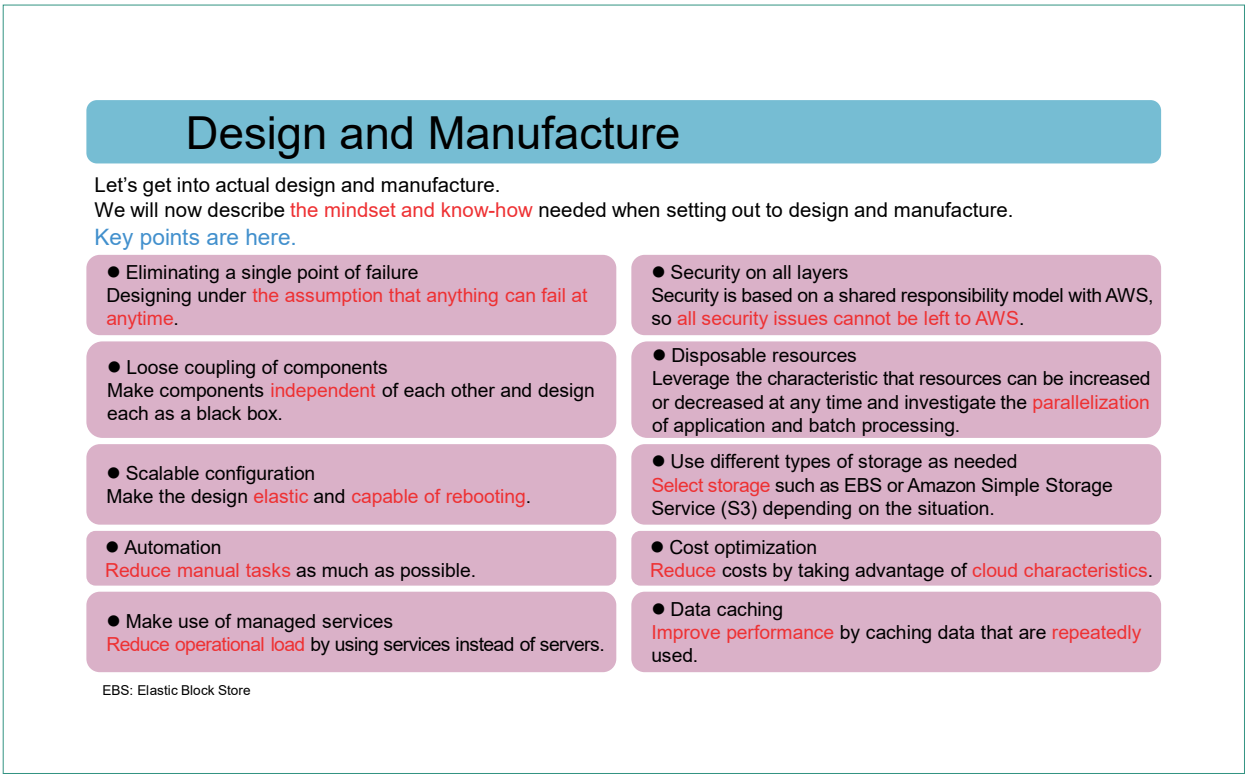


Figure 2 Guideline example (excerpt from cloud development guidelines)

As one of these guidelines, security design patterns[*8] aim to minimize omissions in security considerations when constructing a system using a cloud. They do this by listing requirements in accordance with the security check items (ISO/IEC27017, JISQ27002, etc.) of the NTT DOCOMO Information Security Department plus requirements in a cloud environment and requirements and specifications when constructing a system using AWS alongside the functions and services provided by AWS. These patterns facilitate compliance with security check items. The person in charge of system construction need not test each and every security check item to satisfy requirements. Constructing the system while referring to these security design patterns according to use will satisfy the security check items in due course. An excerpt from these security design patterns is shown in **Figure 3**.

The speed at which public clouds add functions and release updates requires that these support tools be updated just as frequently. The CCoE incorporates agile development[*9] in these support tools and is actively involved in keeping up with frequent function additions and system updates.

4. Latest Development Trends at NTT DOCOMO

This section describes a recent case study on applying serverless technology at a new NTT DOCOMO development site.

*8 Security design patterns: Guidelines that describe methods for satisfying security requirements when using public clouds.

*9 Agile development: Generic name for a group of lightweight application development methods for quick and adaptive software development.

ISO/IEC27017 or JISQ27002		AWS Security Design Patterns		
Section No.	Management Measure	Requirements in a cloud environment	Requirements and specifications when constructing a system using AWS and the functions and services provided by AWS	
12.1.4	The development environment, test environment, and operation environment should be separated to reduce unauthorized access or risk of change to the operation environment.	・A system constructed in a cloud environment shall be divided into commercial, development, test, and backup environments. —Separate contracts if possible —Separate networks, etc. ・Although the cloud has a configuration exposed to the Internet, it shall be possible to logically separate a network by firewalls, routings, etc. and to configure network segments according to roles. ・Given a service in a multitenant environment, the ability to separate use should be verified so that other users and environments (commercial, development, etc.) are not affected. —Physically separable —Logically separable	**【Requirements and specifications】** ・Make AWS accounts separate when separating commercial, development, test, and backup environments. If difficult, separate using the VPC function. ・Separate network segments according to role (DMZ, remote-connection network segment, internal-server network segment, etc.) using the VPC function or subnet function.	**【Functions and services provided by AWS】** ・Environments can be logically divided among tenants by allocating AWS accounts by application, and network environments can be logically divided using the VPC function. If physical division of environments is required, either of the following can be used: —Hardware-exclusive instance —Dedicated hosts ・Multiple virtual subnets can be created within a VPC by the subnet function, which means that subnets can be configured according to role in this way. ・"VPC peering" enables two VPCs to be treated as if they exist within the same network. **【Note】** ・Availability can be improved by a Multi-AZ configuration.
13.1.3	Information services, users, and information systems should be separated into different groups on the network.			
14.1.2	Information included in application services provided over the public network should be protected from malicious behavior, contract disputes, and unauthorized release or alteration.	Function requirements		
14.1.3	Information included in transactions of application services should be protected to prevent the following items from occurring: —Incomplete communications —Erroneous communication-path settings —Unauthorized message alteration —Unauthorized release —Unauthorized message duplication or regeneration	Function requirements		

AZ: Availability Zone
DMZ: DeMilitarized Zone
JIS: Japanese Industrial Standards
VPC: Virtual Private Cloud

Figure 3 Example of security design patterns (listed with reference to the ISO27017 standard in the version for external use)

4.1 Appearance of Serverless Technology

In the world of cloud computing, so-called DevOps, which increases productivity by integrating development and operations that had previously been done separately, and architecture design, which assumes a transition from the use of conventional virtual machines[*10] to containers[*11], have found widespread use. The use of containers has been successful in accelerating the development and release cycle, but operation monitoring and maintenance operations for security purposes are still needed the same as with virtual machines. Despite this trend in containerization, public cloud operators including AWS have already begun to provide a series of managed services[*12] as "serverless" technology that includes server operation management via middleware[*13]. This is technology for using a cloud infrastructure that revolves around a different axis than that of containerization. It enables developers and operation managers to rely on the cloud operator for all infrastructure operations and management without having to worry about the existence of servers. It also enables more resources to be concentrated in the design of business logic.

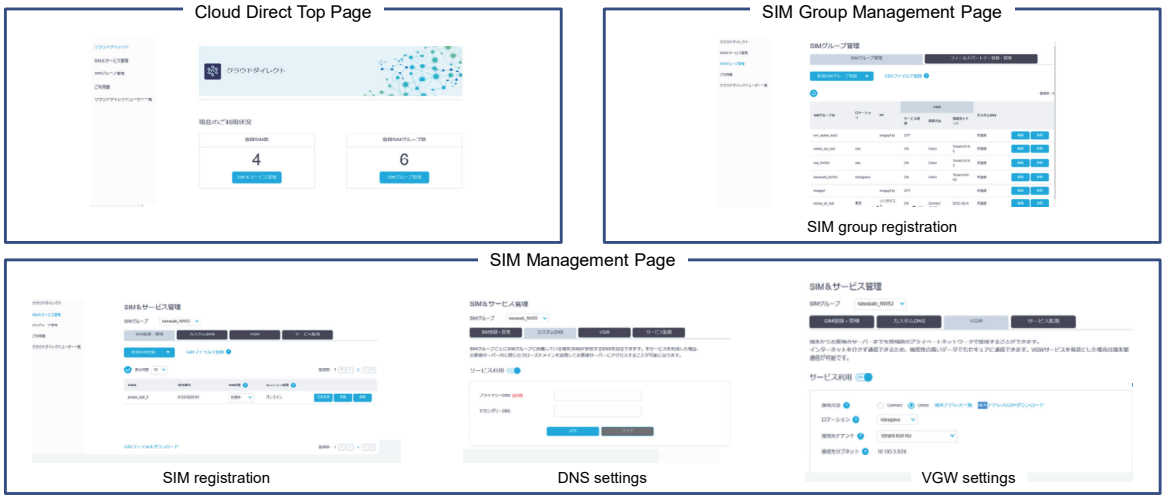
4.2 Case Study of Serverless Application Development at NTT DOCOMO

The Web portal for the DOCOMO Open Innovation Cloud released in June 2020 by NTT DOCOMO is a general Web application system based on React[*14]

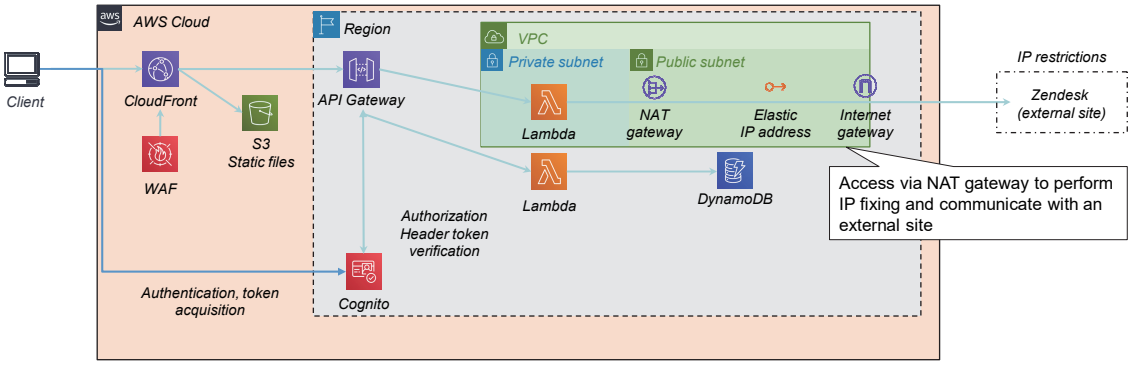
*10 Virtual machines: Computers such as servers constructed in a virtual manner by software.
*11 Containers: As one type of computer virtualization technology, a method for creating a dedicated area called a container on one host OS and running necessary application software within that container.
*12 Managed services: Cloud services whose resource provisioning, operation, etc. are mostly the responsibility of the cloud operator. Among cloud computing services, these are referred to as PaaS and SaaS, for example.
*13 Middleware: Software providing functions for common use by multiple applications.

as described below (**Figure 4** (a)).

In the development of the DOCOMO Open Innovation Cloud, the time taken until its first release was four months and operation and maintenance personnel was limited to the minimum number needed. Here, to offload*15 server management to



(a) Screenshot of each Web page



(1) In the Client's initial access, Cognito issues an authentication token at the time of user authentication. Then, from this point on, the Client can use this authentication token issued by Cognito to gain access again.
(2) A request from Client is received at CloudFront linked to WAF. CloudFront passes a static content request to S3 and an API request to API Gateway.
(3) A static content request treats S3 as a Web server that directly returns that content to the client.
(4) An API request is processed by back-end Lambda via API Gateway.
(5) Lambda uses DynamoDB as persistent storage for reading/writing user data and returns API processing results to Client.

API Gateway: API proxy service managed by AWS
CloudFront: CDN service managed by AWS
Cognito: User management service managed by AWS
DynamoDB: A managed service providing key-value data stores
Lambda: A managed service in which a function is the unit of processing
S3: An object storage service managed by AWS
WAF: A Web application firewall managed by AWS

(b) System configuration around the Web

Figure 4 DOCOMO Open Innovation Cloud

*14 **React:** A JavaScript library for creating user interfaces.

*15 **Offload:** The transfer of system, service, or network processing to separate but similar services to reduce the processing load of the original service.

AWS as much as possible, we adopted serverless architecture overall using, for example, AWS Lambda*16 (Fig. 4 (b)). As a result, we shortened development time considerably and succeeded in releasing the Web site in a relatively short period.

At the time of this writing, the DOCOMO Open Innovation Cloud has been in operation for one year. There have been zero problems due to infrastructure such as the network or servers. In terms of availability, we have benefited from the fact that redundancy and fault tolerance*17 are built into this serverless architecture beforehand. We also achieved our initial goal of keeping the number of operation and maintenance personnel to two or three people. In addition, this serverless service can automatically deal with situations in which an increase in user access requires scalability. As for charges, you only pay for what you use, so we were able to significantly reduce costs in this project.

5. Conclusion

This article described the use of public clouds at NTT DOCOMO and the role played by the CCoE. Amid expectations that the use of public clouds will expand from here on, using them wisely in a way that leads to business success will become increasingly important. For this reason, we would like to see the support provided by the CCoE expand even further so that each and every project can make full use of public clouds.

Innovation in prompt deployment and practical use of new serverless technology in commercial services is a next-generation challenge. With this in mind, we will promote efficient development practices within NTT DOCOMO with a view to increasing the number of successful case studies.

*16 AWS Lambda: A type of FaaS provided by AWS that provides an execution environment for application code so that the user need only register created source code to run the application.

*17 Fault tolerance: The ability of a function to continue operation as usual even in the event of a system fault.