翻訳トライアル実践講座　第 12 回

＜問題 1＞　全文を訳して提出してください。

What Does A Real Cloud Platform Look Like?

Cloud washing is a — more or less deceptive — attempt to rebrand old hosting services as cloud to take advantage of the huge interest in cloud technology. To take just one example, many hosting companies have rebranded traditional virtual private server hosting plans as cloud servers. In fact, they're nothing of the sort. Both use virtualization, but it takes more than that to be a true cloud platform.

How can businesses determine whether a vendor's offering is a true cloud or the result of cloud washing? I use this simple heuristic: true clouds are elastic, on-demand, and programmable.

Elastic

To be elastic, a platform has to be able to scale both up and down quickly. The servers that make up the cloud platform can be deployed in minutes and discarded in minutes. Scaling can be achieved via a web interface or an API, but the important point is that launching a new server onto a cloud platform should be as easy as choosing the server you want, deploying it, and waiting a few minutes for it to be ready. When you're finished with the server, discarding it should be just as simple.

Cloud washed services can't do this. You might be able to deploy a new VPS relatively quickly, but most of these pseudo-cloud services have a monthly billing cycle which means there's no scaling advantage in the other direction.

On-Demand

Public cloud platforms offer on-demand access to compute and storage resources with metered billing. Cloud users pay for the resources they use, billed by the minute or the hour.

Traditional platforms can't do this, and the difference in cost efficiency is stark. Consider the case of an eCommerce store in the run up to the holiday season. With a cloud platform, the store could bring up new web servers behind the load balancer to handle peak traffic, and then reduce the deployment as traffic wanes — paying only for the resources they consume.

＜問題 2＞　全文を訳して提出してください。

Mitigating insider threats - a technical perspective

Insiders are tricky because they represent a demographic that is largely trusted; employees have presumably been vetted and gone through the HR process; they have been interviewed by managers and potential colleagues to assess their knowledge and capabilities; and if to be engaged in work in support of the government, have obtained some level of clearance for access to classified information, networks, and systems. The incidents with Chelsea Manning and Edward Snowden have revealed just how damaging an insider can be in obtaining and making public highly sensitive information.

Data leakage is but one possible consequence resulting from the efforts of these individuals. Data and network destruction, disruption, and data manipulation are all possible alternatives depending on the level of malicious intent. Given the recent events involving the use of ransomware to encrypt hospital networks, it's easy to see how direct access to networks could enable hostile insiders to inserting this type of malware into a network and holding it for considerable ransom.

According to a 2014 presentation by Carnegie Mellon's Computer Emergency Response Team, out of 557 respondents polled, insider threats were the cause of approximately one-third of security incidents experienced, with 46 percent believing that they were far more damaging than external events. The majority of these insider incidents resulted in private information unintentionally exposed; confidential records compromised or stolen; customer records compromised or stolen; and employee records compromised or stolen. These findings are echoed in the Verizon Data Breach Investigations Report that found that 50 percent of all security incidents were caused by individuals inside the organization.

以上