Contribution ID: **58** Type: **Oral Presentation**

Toward Single Sign-on Establishment for Inter-Cloud Environment

Wednesday, 3 April 2019 17:00 (30 minutes)

As diversification of cloud services is making progress, a service-oriented approach is more important, in which services are chosen from multiple cloud vendors according to the demands of users. The purpose of this paper is to investigate a mechanism that establishes single sign-on for inter-cloud computing environment built as the optimized result of the needs of users.

Single sign-on mechanism is indispensable for inter-cloud computing environment that is composed of various services – each service is provided by different cloud vendor. In general a single sign-on mechanism works within cloud environment provided by a cloud vendor, however, a single sign-on mechanism that extends across multiple clouds is not established at the beginning of use. For example, an academic researcher who can obtain a SAML assertion from the home organization should be enabled to access a public cloud with the assertion. Since cloud vendors, of course, already supports major authentication technologies such as SAML and OAuth, technically the credential issued by the home organization will be usable for access to public clouds. However, it is often hard for the identity provider operated by the home organization to manage the user attributes that the cloud vendor requires, because the operating department of the IdP is responsible only for attributes that are assigned naturally in terms of the constitute member of organization. Therefore, establishment of single sign-on to public clouds is being hampered. Based on the credential issued by the home organization, a mechanism for handling necessary attributes information is needed, which should not impose a burden on administrators of the identity provider.

GakuNin Cloud Gateway Service (CGS) is a service portal that enables users to manage services available in academic research or education based on the user authentication information. It is developed and maintained by National Institute of Informatics in Japan. In cooperation with identity providers and service providers that participate in the GakuNin, an academic access management federation, the GakuNin CGS checks service providers that the identity provider allows of sending SAML assertions to based on user's SAML assertion provided by the identity provider. Thus it displays users the list of available services.

In this paper, we design a single sign-on mechanism for the inter-cloud environment. The basic idea is to delegate responsibility for suitable attribute assignment to trusted third party. The trusted third party assumes a role of sender that sends necessary attributes for the service combined with fundamental authentication information. For various services we consider requirements to the attribute assignment system. Thus, we discuss a model that realizes single sign-on in the inter-cloud environment by designing such functions on the GakuNin CGS.

Primary author: Dr SAKANE, Eisaku (National Institute of Informatics)

Co-authors: Prof. AIDA, Kento (National Institute of Informatics); Dr NAKAMURA, Motonori (National Institute of Informatics); Mr NISHIMURA, Takeshi (National Institute of Informatics)

Presenter: Dr SAKANE, Eisaku (National Institute of Informatics)

Session Classification: Infrastructure Clouds and Virtualisation

Track Classification: Infrastructure Clouds and Virtualisation