New software that configures access policy automatically developed by NEC

January 12 2011

NEC Corporation announced today the development of technology that collectively distributes and configures access policy to a variety of computing resources in a cloud computing environment. The newly developed technology helps to significantly reduce operation costs and to improve security.

Access policy is the information that determines the computing resources that are accessible to each user as part of protecting against unauthorized use. All software with access control functions, including virtual machines, operating software, data base and application software, require access policy to be set individually. This manual configuration becomes a heavy burden for system administrators within cloud environments, which feature a variety of software that run on a broad range of virtual machines.

NEC developed a management software model based on the Distributed Management Task Force Common Information Model that enables the distribution and centralized configuration of access policy.

The company also developed "Integrated Access Control Management Software" and "Policy Provisioning Agent Software" based on this newly established software model.

These new developments enable automatic configuration of access policy, which reduces the work load of system administrators, while at the same time lessening vulnerability.

Furthermore, the flexibly of these developments accommodate changes and additions to servers and software.

NEC is promoting this CIM based model as an international standard specification in 2011 through a proposal to DMTF. As a part of this activity, NEC and the Electronics and Telecommunications Research Institute of Korea jointly demonstrated the model's effectiveness through "Integrated Access Control Management Software" loaded on an NEC server that successfully distributed access policy to "Policy Provisioning Agent Software" on a Linux server at ETRI.

The "Policy Provisioning Agent Software" used in this demonstration is available to the public as open source software by ETRI (opendrim.sourceforge.net).

The main features of these new developments are as follows:

1. CIM based management model

The model enables a common method to distribute and configure access policy that is independent from vendor specifications in an integrated server environment, where it is necessary for different virtual machine software, operating systems and middleware to co-exist.

NEC modeled access control behavior and control information as an extension of CIM. Adoption of policy distribution and configuration functions based on this model enable system administrators to distribute and configure access policy collectively, regardless of vendor and software.

2. Development of "Integrated Access Control Management Software" and "Policy Provisioning Agent Software" based on a new software model

"Integrated Access Control Management Software" enables centralized control and collective distribution of access policy, while "Policy Provisioning Agent Software" configures access policy for individual software on the receiving side.

This software is in compliance with international standards of message distribution protocol for system operation management. System administrators can automatically set policy configuration for existing virtual machines, operating systems and middleware by simply installing "Policy Provisioning Agent Software."

Looking forward, NEC will continue to promote research and development in order to establish commonly usable IT security measures for the coming cloud computing era.

Source: NEC