# Concept of the QOS Control Method Based On the Data Mining in the VDACS Scheme for the Common Use between Plural Organizations

**Kazuya Odagiri†, Shogo Shimizu††, Naohiro Ishii†††**
†Sugiyama Jogakuen University, 464-8662, 17-3Hosigaokamotomachi Chiksa-ku,Nagoya, Aichi, Japan
††Gakushuin Women's College, Tokyo, Japan
†††Aichi Institute of Technology, Aichi, Japan

**Summary**
In the current Internet system, there are many problems using anonymity of the network communication such as personal information leaks and crimes using the Internet system. As the study for solving this problem, there is the study of Policy Based Network Management (PBNM). This is the scheme for managing a whole Local Area Network (LAN) through communication control for every user. As one scheme of the PBNM, we have studied theoretically about the Destination Addressing Control System (DACS) Scheme and the Virtual DACS (vDACS) Scheme. By applying these schemes to Internet system management, we will realize the policy-based Internet system management. In this paper, to add the QOS control function for the DACS Scheme, we propose the concept of the QOS control method based on the data mining in the VDACS Scheme for the common use between plural organizations.

***Key words:***
*Policy-based network management; DACS Scheme; QOS*

## 1. Introduction

In the current Internet system, there are many problems using anonymity of the network communication such as personal information leaks and crimes using the Internet system. The news of the information leak in the big company is sometimes reported through the mass media. Because TCP/IP protocol used in Internet system does not have the user identification information on the communication data, it is difficult to supervise the user performing the above acts immediately. As studies and technologies for managing Internet system realized on TCP/IP protocol, those such as Domain Name System (DNS), Routing protocol, Fire Wall (F/W) and Network address port translation (NAPT)/network address translation (NAT) are listed. Except these studies, various studies are performed elsewhere. However, they are the studies for managing the specific part of the Internet system, and have no purpose of solving the above problems.

As a study for solving the problems, Policy Based Network Management (PBNM) [2] exists. The PBNM is a scheme for managing a whole Local Area Network (LAN) through communication control every user, and cannot be applied to the Internet system. This PBNM is often used in a scene of campus network management. In a campus network, network management is quite complicated. Because a computer management section manages only a small portion of the wide needs of the campus network, there are some user support problems. For example, when mail boxes on one server are divided and relocated to some different server machines, it is necessary for some users to update a client machine's setups. Most of computer network users in a campus are students. Because students do not check frequently their e-mail, it is hard work to make them aware of the settings update. This administrative operation is executed by means of web pages and/or posters. For the system administrator, individual technical support is a stiff part of the network management. Because the PBNM manages a whole LAN, it is easy to solve this kind of problem. In addition, for the problem such as personal information leak, the PBNM can manage a whole LAN by making anonymous communication non-anonymous. As the result, it becomes possible to identify the user who steals personal information and commits a crime swiftly and easily. Therefore, by applying the PBNM, we will study about the policy-based Internet system management.

In the existing PBNM, there are two types of schemes. The first is the scheme of managing the whole LAN by locating the communication control mechanisms on the path between network servers and clients. The second is the scheme of managing the whole LAN by locating the communication control mechanisms on clients. It is difficult to apply the first scheme to Internet system management practically, because the communication control mechanism needs to be located on the path between network servers and clients without exception. Because the second scheme locates the communication control mechanisms as the software on each client, it becomes possible to apply the second scheme to Internet

Manuscript received August 5, 2017
Manuscript revised August 20, 2017

system management by devising the installing mechanism so that users can install the software to the client easily.
As the second scheme, we have studied theoretically about the Destination Addressing Control System (DACS) Scheme. As the works on the DACS Scheme, we showed the basic principle of the DACS Scheme, and security function [14]. After that, we implemented a DACS System to realize a concept of the DACS Scheme. By applying this DACS Scheme to Internet system, we will realize the policy-based Internet system management. Then, the Wide Area DACS system (wDACS system) [15] to use it in one organization was showed as the second phase for the last goal. As the first step of the second phase, we showed the concept of the cloud type virtual PBNM, which could be used by plural organizations [16]. In this paper, we describe the concept of the QOS control method based on the data mining in the VDACS Scheme for the Common Use between Plural Organizations. In Section 2, motivation and related research for this study are described. In Section 3, the existing DACS Scheme and wDACS Scheme is described. In section 4, the proposed QOS control method is described.

## 2. Motivation and Related Research

In the current Internet system, problems using anonymity of the network communication such as personal information leak and crimes using the Internet system occur. Because TCP/IP protocol used in Internet system does not have the user identification information on the communication data, it is difficult to supervise the user performing the above acts immediately.
As studies and technologies for Internet system management to be comprises of TCP/IP [1], many technologies are studied. For examples, Domain name system (DNS), Routing protocol such as Interior gateway protocol (IGP) such as Routing information protocol (RIP) and Open shortest path first (OSPF) , Fire Wall (F/W), Network address translation (NAT) / Network address port translation (NAPT) , Load balancing, Virtual private network (VPN), Public key infrastructure (PKI), Server virtualization. Except these studies, various studies are performed elsewhere. However, they are for managing the specific part of the Internet system, and have no purpose of solving the above problems.
As a study for solving the above problem, the study area about PBNM exists. This is a scheme of managing a whole LAN through communication control every user. Because this PBNM manages a whole LAN by making anonymous communication non-anonymous, it becomes possible to identify the user who steals personal information and commits a crime swiftly and easily. Therefore, by applying this policy- based thinking, we study about the policy-based Internet system management.

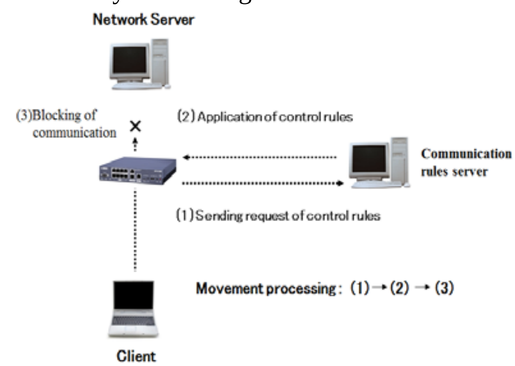


Figure 1. Principle in First Scheme

In policy-based network management, there are two types of schemes. The first scheme is the scheme described in Figure 1. The standardization of this scheme is performed in various organizations. In IETF, a framework of PBNM [2] was established. Standards about each element constituting this framework are as follows. As a model of control information stored in the server called Policy Repository, Policy Core Information model (PCIM) [3] was established. After it, PCMIe [4] was established by extending the PCIM. To describe them in the form of Lightweight Directory Access Protocol (LDAP), Policy Core LDAP Schema (PCLS) [5] was established. As a protocol to distribute the control information stored in Policy Repository or decision result from the PDP to the PEP, Common Open Policy Service (COPS) [6] was established. Based on the difference in distribution method, COPS usage for RSVP (COPS-RSVP) [7] and COPS usage for Provisioning (COPS-PR) [8] were established. RSVP is an abbreviation for Resource Reservation Protocol. The COPS-RSVP is the method as follows. After the PEP having detected the communication from a user or a client application, the PDP makes a judgmental decision for it. The decision is sent and applied to the PEP, and the PEP adds the control to it. The COPS-PR is the method of distributing the control information or decision result to the PEP before accepting the communication.
Next, in DMTF, a framework of PBNM called Directory-enabled Network (DEN) was established. Like the IETF framework, control information is stored in the server storing control information called Policy Server, which is built by using the directory service such as LDAP [9], and is distributed to network servers and networking equipment such as switch and router. As the result, the whole LAN is managed. The model of control information used in DEN is called Common Information Model (CIM), the schema of the CIM（CIM Schema Version 2.30.0）[11] was

opened. The CIM was extended to support the DEN [10], and was incorporated in the framework of DEN.

In addition, Resource and Admission Control Subsystem (RACS) [12] was established in Telecoms and Internet converged Services and protocols for Advanced Network (TISPAN) of European Telecommunications Standards Institute (ETSI), and Resource and Admission Control Functions (RACF) was established in International Telecommunication Union Telecommunication Standardization Sector (ITU-T) [13].

However, all the frameworks explained above are based on the principle shown in Figure 1. As problems of these frameworks, two points are presented as follows. Essential principle is described in Figure 2. To be concrete, in the point called PDP (Policy Decision Point), judgment such as permission and non-permission for communication pass is performed based on policy information. The judgment is notified and transmitted to the point called the PEP, which is the mechanism such as VPN mechanism, router and Fire Wall located on the network path among hosts such as servers and clients. Based on that judgment, the control is added for the communication that is going to pass by.

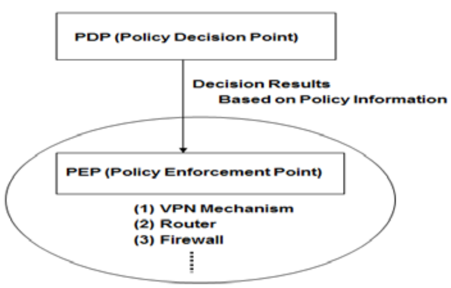


Figure 2. Essential Principle

The principle of the second scheme is described in Figure 3.By locating the communication control mechanisms on the clients, the whole LAN is managed. Because this scheme controls the network communications on each client, the processing load is low. However, because the communication control mechanisms need to be located on each client, the work load becomes heavy.

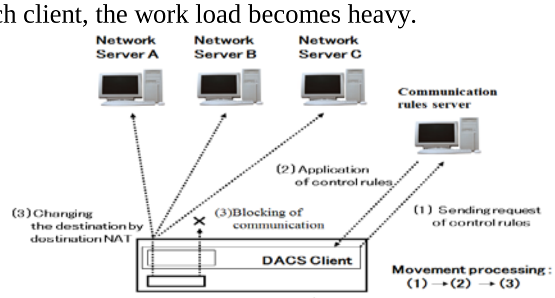


Figure 3. Principle in Second Scheme

When it is thought that Internet system is managed by using these two schemes, it is difficult to apply the first scheme to Internet system management practically. This is why the communication control mechanism needs to be located on the path between network servers and clients without exception. On the other hand, the second scheme locates the communication controls mechanisms on each client. That is, the software for communication control is installed on each client. So, by devising the installing mechanism letting users install software to the client easily, it becomes possible to apply the second scheme to Internet system management. As a first step for the last goal, we showed the Wide Area DACS system (wDACS) system [15]. This system manages a wide area network, which one organization manages. Therefore, it is impossible for plural organizations to use this system.Then, as the first step of the second phase, we showed the concept of the cloud type virtual PBNM, which could be used by plural organizations in this paper.

## 3. Existing DACS SCHEME and wDACS System

In this section, the content of the DACS Scheme is described.

### 3.1 Basic Principle of the DACS Scheme

Figure 4 shows the basic principle of the network services by the DACS Scheme. At the timing of the (a) or (b) as shown in the following, the DACS rules (rules defined by the user unit) are distributed from the DACS Server to the DACS Client.

(a) At the time of a user logging in the client.

(b) At the time of a delivery indication from the system administrator.

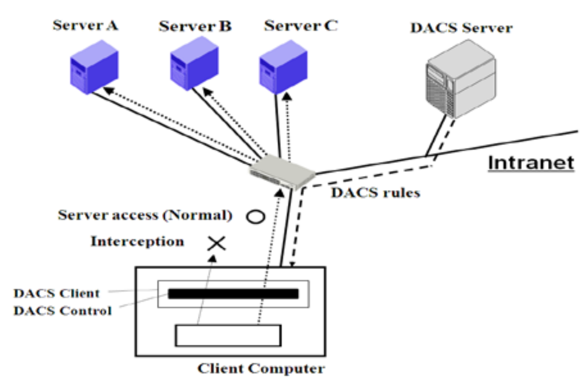


Figure 4. Basic Principle of the DACS Scheme

According to the distributed DACS rules, the DACS Client performs (1) or (2) operation as shown in the following.

Then, communication control of the client is performed for every login user.

(1) Destination information on IP Packet, which is sent from application program, is changed.

(2) IP Packet from the client, which is sent from the application program to the outside of the client, is blocked.

An example of the case (1) is shown in Figure 4. In Figure 4, the system administrator can distribute a communication of the login user to the specified server among servers A, B or C. Moreover, the case (2) is described. For example, when the system administrator wants to forbid an user to use MUA (Mail User Agent), it will be performed by blocking IP Packet with the specific destination information.

In order to realize the DACS Scheme, the operation is done by a DACS Protocol as shown in Figure 5. As shown by (1) in Figure 5, the distribution of the DACS rules is performed on communication between the DACS Server and the DACS Client, which is arranged at the application layer. The application of the DACS rules to the DACS Control is shown by (2) in Figure 5.

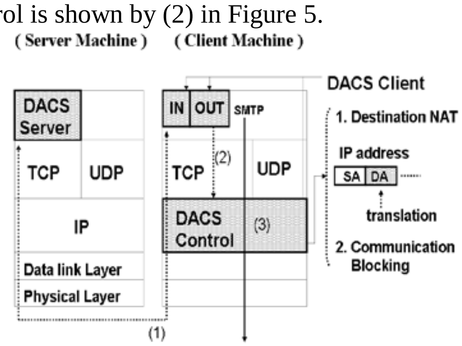


Figure 5. Layer Setting of the DACS Scheme

The steady communication control, such as a modification of the destination information or the communication blocking is performed at the network layer as shown by (3) in Figure 5.

## 3.2 Communication Control on Client

The communication control on every user was given. However, it may be better to perform communication control on every client instead of every user. For example, it is the case where many and unspecified users use a computer room, which is controlled. In this section, the method of communication control on every client is described, and the coexistence method with the communication control on every user is considered.

When a user logs in to a client, the IP address of the client is transmitted to the DACS Server from the DACS Client. Then, if the DACS rules corresponding to IP address, is registered into the DACS Server side, it is transmitted to the DACS Client. Then, communication control for every client can be realized by applying to the DACS Control. In this case, it is a premise that a client uses a fixed IP address. However, when using DHCP service, it is possible to carry out the same control to all the clients linked to the whole network or its subnetwork for example.

When using communication control on every user and every client, communication control may conflict. In that case, a priority needs to be given. The judgment is performed in the DACS Server side as shown in Figure 6. Although not necessarily stipulated, the network policy or security policy exists in the organization such as a university (1). The priority is decided according to the policy (2). In (a), priority is given for the user's rule to control communication by the user unit. In (b), priority is given for the client's rule to control communication by the client unit. In (c), the user's rule is the same as the client's rule. As the result of comparing the conflict rules, one rule is determined respectively. Those rules and other rules not overlapping are gathered, and the DACS rules are created (3). The DACS rules are transmitted to the DACS Client. In the DACS Client side, the DACS rules are applied to the DACS Control. The difference between the user's rule and the client's rule is not distinguished.

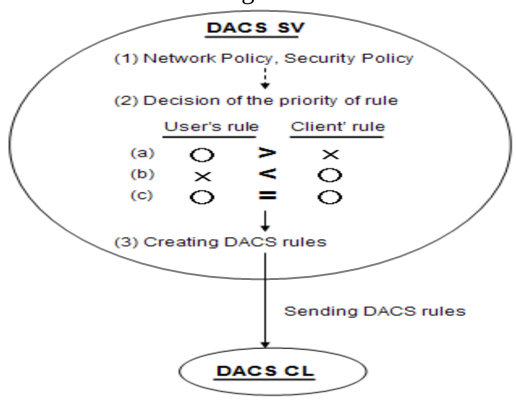


Figure 6. Creating the DACS rules on the DACS Server

## 3.3 Security Mechanism of the DACS Scheme

In this section, the security function of the DACS Scheme is described. The communication is tunneled and encrypted by use of SSH. By using the function of port forwarding of SSH, it is realized to tunnel and encrypt the communication between the network server and the, which DACS Client is installed in. Normally, to communicate from a client application to a network server by using the function of port forwarding of SSH, local host (127.0.0.1) needs to be indicated on that client application as a communicating server. The transparent use of a client, which is a characteristic of the DACS Scheme, is failed. The transparent use of a client means that a client can be used continuously without changing setups when the network system is updated. The function that doesn't fail the transparent use of a client is needed. The mechanism of that function is shown in Figure 7.

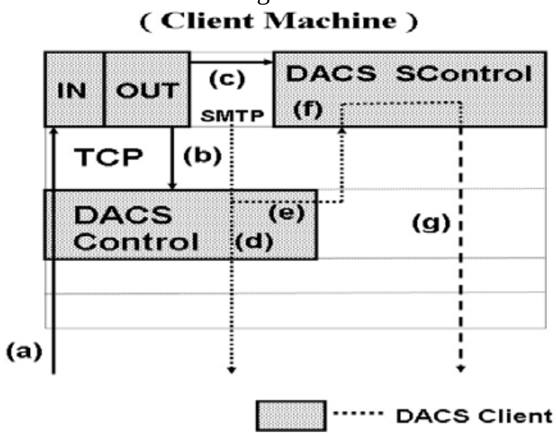


Figure 7. Extend Security Function

## 3.4 Application to cloud environment

In this section, the contents of wDACS system are explained in Figure 8.

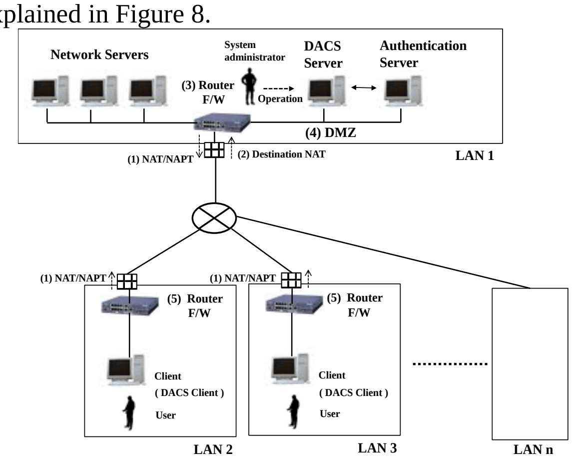


Figure 8. Basic System Configuration of wDACS system

First, as preconditions, because private IP addresses are assigned to all servers and clients existing in from LAN1 to LAN n, mechanisms of NAT/NAPT are necessary for the communication from each LAN to the outside. In this case, NAT/NAPT is located on the entrance of the LAN such as (1), and the private IP address is converted to the global IP address towards the direction of the arrow. Next, because the private IP addresses are set on the servers and clients in the LAN, other communications except those converted by Destination NAT cannot enter into the LAN. But, responses for the communications sent form the inside of the LAN can enter into the inside of the LAN because of the reverse conversion process by the NAT/NAPT. In addition, communications from the outside of the LAN1 to the inside are performed through the conversion of the destination IP address by Destination NAT. To be concrete, the global IP address at the same of the outside interface of the router is changed to the private IP address of each server. From here, system configuration of each LAN is described. First, the DACS Server and the authentication server are located on the DMZ on the LAN1 such as (4). On the entrance of the LAN1, NAT/NAPT and destination NAT exists such as (1) and (2). Because only the DACS Server and network servers are set as the target destination, the authentication server cannot be accessed from the outside of the LAN1. In the LANs form LAN 2 to LAN n, clients managed by the wDACS system exist, and NAT/NAPT is located on the entrance of each LAN such as (1). Then, F/W such as (3) or (5) exists behind or with NAT/NAPT in all LANs.

## 3.5 Concept of the Cloud Type Virtual PBNM for the Common Use between Plural Organizations

In Figure 9, the proposed concept is shown [16]. Because the existing wDACS Scheme realized the PBNM control with the software called the DACS Server and the DACS client, other mechanism was not needed. By this point, application to the cloud environment was easy.

The proposed scheme in this paper realizes the common usage by plural organizations by adding the following elements to realize the common usage by plural organizations. (user identification of the plural organizations, management of the policy information of the plural organizations, application of the PKI for code communication in the Internet, Redundant configuration of the DACS Server (policy information server), load balancing configuration of the DACS Server, installation function of DACS Client by way of the Internet )

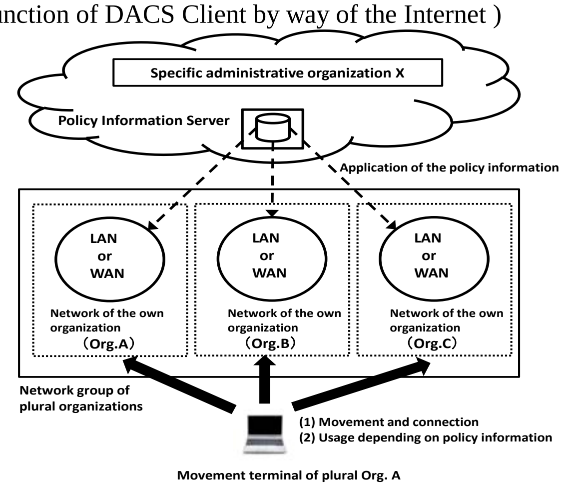


Figure 9. Concept of the proposed scheme

## 4. Concept of the proposed QOS control method based on the data mining

In this section, the proposed QOS control method is described in the Figure 10. To be concrete, the QOS for the Web Server on the cloud environment is described. At first, it is described about the system configuration for it. On the LAN1, the Web Server for which is targeted for the QOS control, the virtual router which is located in front of the Web Server and the DACS Server are located. Then, the clients which have the DACS Client as the virtual clients are distributed and located on the LANs for each organization. The accesses from each client go by way of the virtual router in front of the Web Server by all means.

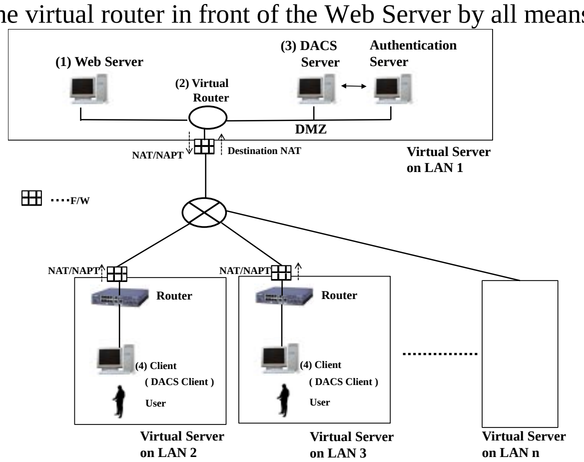


Figure 10. System Configuration for the proposed QOS control method

From here, it is described about the movement of this system. Processes from the DACS Server and the DACS Client are the same movement as described in Section Ⅲ. As the additional processes, some processes are added as follows.

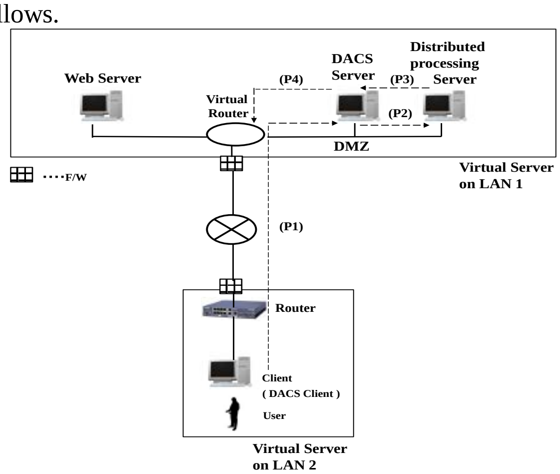


Figure 11. Processes for the proposed QOS control method

(P1) Sending the communication log on the Client

At first, after the processing by the destination change and packet filtering which are caused by the DACS Control in the DACS Client is performed, communication logs are stored on the client. The DACS Server sends them the DACS Server as described in (P1).

(P2)Sending the communication log the distributed processing server

After the DACS Server received the communication logs from the client that has the DACS Client, it sends them the distributed processing server. On the side of the distributed server like “Hadoop”, the count processing is carried out.

(P3) Sending the processing results the DACS Server

The distributed processing server sends the processing results the DACS Server, after the processing was finished.

(P4) Setting the control rules for QOS control

## 5. Conclusion

In this paper, we proposed the concept of the QOS control method based on the data mining in the VDACS Scheme for the common use between plural organizations. This is the study for adding the QOS function of this scheme. As the first stage, we suggested it about a function summary.

As a future work, we are going to examine the detailed function and perform the implementation to confirm the possibility and the evaluation.

**Acknowledgement**

This work was supported by JSPS KAKENHI Grant Number 26730037. We express our gratitude

## References

[1] V.CERF and E.KAHN,"A V. CERF and E. KAHN, "A Protocol for Packet Network Interconnection," IEEE Trans. on Commn, vol.COM-22, May 1974, pp.637-648.

[2] R. Yavatkar, D. Pendarakis and R. Guerin, "A Framework for Policy-based Admission Control," IETF RFC 2753, 2000.

[3] B. Moore at el., "Policy Core Information Model -- Version 1 Specification", IETF RFC 3060, 2001.

[4] B. Moore.,"Policy Core Information Model (PCIM) Extensions", IETF 3460, 2003.

[5] J. Strassner, B. Moore, R. Moats, E. Ellesson, " Policy Core Lightweight Directory Access Protocol (LDAP) Schema", IETF RFC 3703, 2004.

[6] D. Durham at el.,"The COPS (Common Open Policy Service) Protocol", IETF RFC 2748, 2000.

[7] S. Herzog at el.,"COPS usage for RSVP", IETF RFC 2749, 2000.

[8] K. Chan et al.,"COPS Usage for Policy Provisioning (COPS-PR)", IETF RFC 3084, 2001.

[9] CIM Core Model V2.5 LDAP Mapping Specification, 2002.

[10] M. Wahl, T. Howes, S.Kille, "Lightweight Directory Access Protocol (v3)", IETF RFC 2251, 1997.
[11] CIM Schema: Version 2.30.0, 2011.
[12] ETSI ES 282 003: Telecoms and Internet converged Services and protocols for Advanced Network (TISPAN); Resource and Admission Control Subsystem (RACS); Functional Architecture, June 2006.
[13] ETSI ETSI ES 283 026: Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control; Protocol for QoS reservation information exchange between the Service Policy Decision Function (SPDF) and the Access-Resource and Admission Control Function (A-RACF) in the Resource and Protocol specifica-tion", April 2006.
[14] K. Odagiri , R. Yaegashi , M. Tadauchi, and N. Ishii,"Secure DACS Scheme, "Journal of Network and Computer Applications," Elsevier, Vol.31, Issue 4, 2008, pp.851-861, November.
[15] K. Odagiri, S. Shimizu,M. Takizawa and N. Ishii,"Theoretical Suggestion of Policy-Based Wide Area Network Management System (wDACS system part-I)," International Journal of Networked and Distributed Computing (IJNDC), Vol.1, No.4, November 2013, pp.260-269.
[16] [16] K. Odagiri,S. Shimizu, N. Ishii, M. Takizawa, "Suggestion of the Cloud Type Virtual Policy Based Network Management Scheme for the Common Use between Plural Organizations," Proc of Int. Conf. on International Conference on Network-Based Information Systems (NBiS-2015),pp.180-186,Septmber, 2015

**Kazuya Odagiri** received the degree of B.S in 1998 from Waseda University. He is an Associate Professor in Sugiyama Jogakuen University now. In addition, he got his Ph.D. in Aichi Institute of Technology. He engages in a study of network management.

**Shyogo Shimizu** received the degree of B.S in 1996 from Osaka University and the degree of M.S in 1998 from Nara Institute of Science and Technology, Nara. He got his Ph.D. in Nara Institute of Science and Technology in March 2001. He is now Associate Professor in Gakushuin Women's College.

**Naohiro Ishii** received the B.E., M.E. and Dr. of Engineering degree from Tohoku University, Japan in 1963, 1965 and 1968, respectively. He was a professor in Department of Intelligence and Computer Science at Nagoya Institute of Technology. From 2003, he is a professor in Department of Information Science at Aichi Institute of Technology. His research interest includes computer engineering, artificial intelligence, and human interface.