Efficient Network Management System with DACS Scheme Management with communication control

Kazuya Odagiri,[†] *Rihito Yaegashi*[††], *Masaharu Tadauchi*[††], *and Naohiro Ishii*[†]

[†] Aichi Institute of Technology, Higashiyamadouri, Chikusa-ku, Nagoya-city, Aichi, Japan
[††]Toyota Technological Institute, Hisakata, Tenpaku-ku, Nagoya-city, Aichi, Japan

Summary

Where customers with different membership and position, use computers as in the university network systems, it often takes much time and efforts for them to cope with the change of the system management. This is because the requirements for the respective computer usage are different in the network and security policies. In this paper, a new destination addressing control system (DACS) scheme for the university network services is proposed. The DACS Scheme performs the network services efficiently through the communication management of a client. As the characteristic of DACS Scheme, only the setup modification is required by a system administrator, when the configuration change is needed in the network server. Then, the setup modification is unnecessary by a customer, which shows a merit for both a system administrator and a customer. This paper describes the instruction and the prototype for DACS Protocol as the implementation of DACS Scheme. Then, the simplicity of the system management in DACS Scheme, is examined from the customer and the system administrator viewpoints.

Key words:
destination nat, packet filtering, name resolution

1. Introduction

The characteristic of the operation and management in the university network systems, is that people with different membership and position as students, faculties, external persons, et al., use the network services comparatively freely. In the business corporations, it is comparatively easy to spread the information of the network usage based on a network policy or a security policy. However, in the university, it is often difficult to spread the information of the network usage, since the computer management section does not perform all operation and management for the respective needs. Although the system administrator of the computer section, carries out management and operation of the most network infrastructure and servers, the customer mainly performs the management of their clients[1]. Operation and management of the network system, are conventionally focused on the control in the infrastructure or server side [2] [3]. For example, DNS round robin [4], the control using the load balancer and the load distribution of the server [5] [6] [7], are performed at the infrastructure or server side. When the configuration change of a server is carried out, it is necessary to make a setup change at the client side. For example, the case that the communication of a specific user is distinguished from that of other user, is assumed. Where a specific group such as a laboratory connects an outside telecommunication line by their fund and only the group member uses a PROXY Server connected to the line, it is necessary for the communication of the group member to be made up by way of the PROXY server. At the same time, it is necessary for other user except the group member not to be connected by way of the PROXY server. Only in the case of the former, it can come true by using conventional name solution service. As for the case including the latter, it is difficult to realize it by conventional name solution service. In any case, if the system administrator is able to control the communication freely by the user unit, it is not necessary to make setup change at the client side to change the configuration of a server.

In this paper, a new DACS (destination addressing control system) scheme for the university network services, is proposed. The DACS Scheme performs the network services efficiently through the communication management. As the characteristic of DACS Scheme, only the setup modification is required by the system administrator, when the configuration change is needed in the network server. Then, the setup modification is unnecessary for the customer, which shows a merit for both a system administrator and a customer. This paper proposes the design of the DACS Scheme. The experimental evaluation is performed in the DACS Protocol.

2. Synopsis of DACS Scheme

2.1 Basic Principle of DACS Scheme

Fig.1 shows the basic principle of the network services by DACS Scheme. At the timing of the (a) or (b) as shown in

the following, DACS rules (rules defined by the user unit) are distributed from DACS Server to 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

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

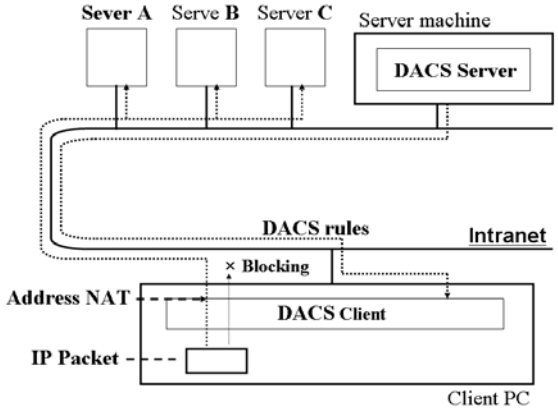

Fig.1 DACS Scheme

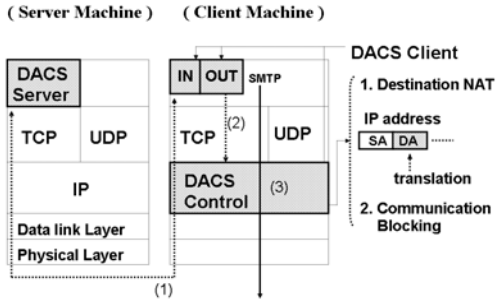

Fig. 2 Layer setting of DACS Scheme

2.2 Comparison with Existing Technology

Here, the difference between DACS Scheme and the existing technology is explained. Specifically, the difference from the technology of name resolution service (ex, WINS,DNS) and server load balancing is discussed. First, the difference from the name resolution service is explained. Although the mapping of a host name and an IP address is performed in the existing name resolution service, the mapping of the group of a host name, a user name and an IP address can be performed altogether by DACS Scheme. As the result, the IP address to be different for every user can be determined for the same host name. Next, the difference from server load balancing technology is explained. To realize server load balancing, there are methods by DNS round robin, and by the load balancer.

Then, the difference from how to use the load balancer using Destination NAT is explained. The large difference from DACS Scheme is the place which arranges Destination NAT. Although the load balancer arranges Destination NAT on the network course, it is arranged on the client in DACS Scheme. When Destination NAT is arranged on the network course, it cannot be specified whether IP Packet was sent by which user. For the reason, it is difficult to control communication per user. However, it can be guaranteed in DACS Scheme by arranging on the client that all IP Packet at the time of Destination Nat conversion is sent by the login user. But, when the client is multi-user system, the mechanism in the no login from remoteness is required. It is confirmed that the communication is sent by the user who sits down before a client and logs in directly, by the method of intercepting the unnecessary communication from the client outside.

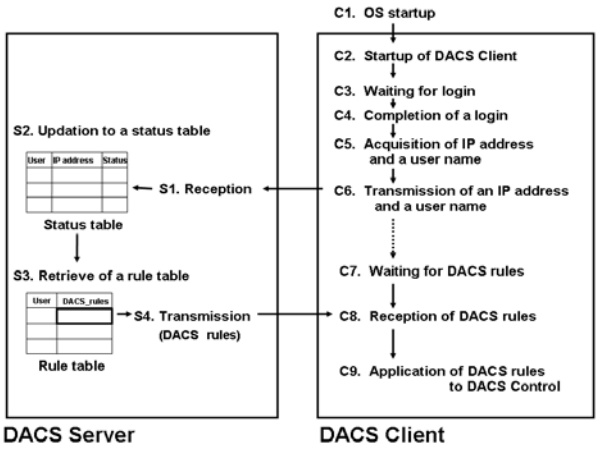

Fig. 3 .Phase 1 (DACS Protocol)

3. DACS Protocol Phases

DACS Protocol is a communication protocol required by DACS Scheme, and can be realized by Phase1 and Phase2 which is separated in the state of DACS Client.

Phase1: Initializing process of DACS Client

Phase2: Steady state process of DACS Client

a. When DACS rules is applied to DACS Control.

b. When DACS Server checks whether DACS Client has started.

The possibility of realization was checked by experiment as shown in chapter IV.

3.1 DACS Protocol

3.1.1 Phase 1

First, when OS starts (C1), DACS Client starts (C2). Then, DACS client is in the status of waiting for user login (C3). When user login is completed (C4), DACS Client acquires the IP address and login user name of the client (C5). Then, DACS Client transmits them to DACS Server (C6). Usually, how to set the IP address to the client has either to set up automatically using DHCP service, or other way in which the customer and the system administrator do manual setting. When a network interface starts, the IP address is set up by a method of either. Therefore, if DACS Client acquires the IP address of the client at the time of user login, there are no problems to acquire the IP address. Although it is how to acquire the IP address and login user name, in the experiment explained later, the IP address is extracted from the practice result message of a command to display network setting information. Moreover, since the user name is set to the environment variable when logged in OS, the user name is acquired through the environment variable. By DACS Scheme, since it is premised on the scheme which performs the user authentication of the client, the checks to the user name is not performed in DACS Server. Incidentally, the LDAP Server (Open LDAP) is adopted as an authentication server in this experiment. After transmitting the user name and the IP address to DACS Server, processing is performed in DACS Server. The DACS Server registers newly or updates the IP address and DACS Client presence of the client into the status table ,in which a user name is the main key (S2).

Status=0: DACS Client stops.

Status=1: DACS Client starts.

In the next processing, DACS rules of the login user registered into the rule table is extracted (S3), and it transmits to DACS Client (S4). Although DACS Client applies DACS rules to DACS Control (C9) after the reception (C8), it performs actually controlling the communication in DACS Control. In addition, at the time of the end of DACS Client, status is updated to 0.

3.1.2 Protocol in Phase 2-a

Next, the protocol in Phase2-a is shown in Fig.4. (S1-S5 shows the processing sequence performed in the server side, and C1-C3 shows the processing sequence in the client side.)

The system administrator gives DACS Server the indication of distributing DACS rules (S1). The DACS rules are applicable to DACS Client of the client to which the specific user logs in. As the sequence, the system administrator registers new DACS rules into a rule table first.

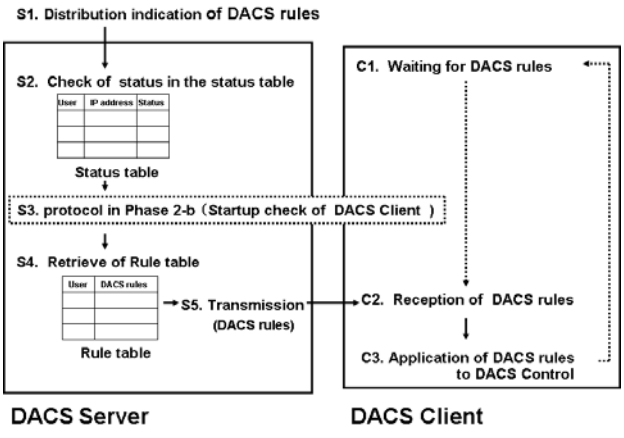

Fig. 4 Protocol in Phase 2-a (DACS Protocol)

Then, the user name used as the candidate for application is given to DACS Server. DACS Server checks the IP address of the client and the startup presence or absence of

the client in the status table (S2). When the status is 1, the seizing acknowledgment of DACS Client is performed. When the data in the status table shows an outage (i.e., when status is 0), the startup check of DACS Client is done (S3). When the client is in the status of seizing the presence of DACS Client, DACS rules are transmitted to DACS Client (S5). Then, DACS rules are applied to DACS Control (C3). DACS Client is in the status of awaiting after the application of DACS rules (C1).

3.1.3 Protocol in Phase 2-b

Protocol in Phase2-b is shown in Fig.5. DACS Server checks whether DACS Client has started. The timing which seizes the presence of DACS Client is as follows.

- When carrying out with the fixed interval periodically.
- When carrying out in Phase2-a before a transmission of DACS rules.(When Status is 0 in the status table.)

DACS Client is in the status that the receiving process from DACS Server is awaited. Therefore, when DACS Server asks, there is a response if DACS Client has started and an error occurs if it has stopped. When the error occurs, status is updated from 1 to 0 in the status table. The reason for checking whether DACS Client has started periodically is to improve the system efficiently by the minimum startup check of DACS Client in the sequence (S3) of Phase2-a. Here, the status description of DACS Server and DACS Client is shown in Fig.6. The directional arrow of the dotted line shows the flow of the state transition of DACS Server and DACS Client. The state changes in order as follows; to Active (steady state) from Initializing (initializing status), Off (idle state), and Initializing. Non-Active (transient status) in DACS Client shows all the statuses that it is not Active, when it does not reach to a steady state after the Off, or Initializing.

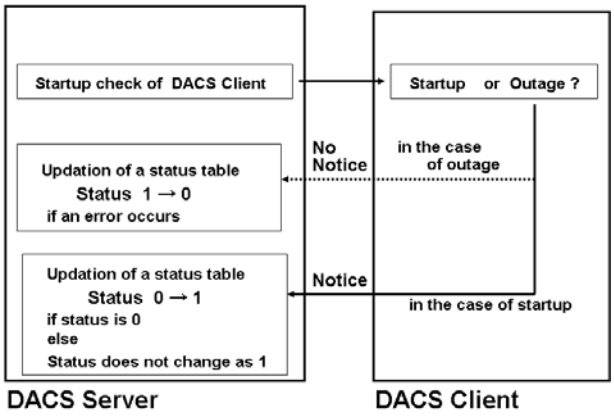

Fig.5 Protocol in Phase 2-b (DACS Protocol)

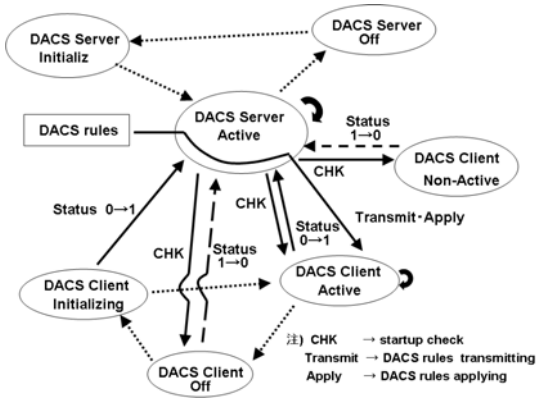

Fig..6 State transition in DACS Scheme

When DACS Client is in the status of Initializing, status is changed into 1 from 0. Under a steady state (Active), status is not changed from 1 in response to the notice from DACS Client for the startup check. However, when judged with Non-Active as a result of the startup check of DACS Client, status is changed into 0 by DACS Server from 1. Moreover, explanation about the directional arrow (solid line) of DACS Server (Active) and DACS Client (Active, Off, Non-Active) is given. First, there is a directional arrow between DACS Server (Active) and DACS Client (Active) as follows.

- The inquiry to DACS Client from DACS Server
- The response from DACS Client to the above-mentioned inquiry
- The transmission of DACS rules from DACS Server to DACS Client

In the opposite arrow of a dashed line for the directional arrows of solid line from DACS Server (Active) to DACS Client (Off, Non-Active), it is shown that there is no response from DACS Client to the inquiry from DACS Server to DACS Client.

4. Experimental Results by Prototype Construction

In order to prove the possibility of realization of the network services by DACS Scheme, the prototype was built. Then, the functional test was actually carried out under the operation. The prototype developed here, is shown in Fig.7. Further description of the system configuration is shown below.

(1) Server Machine
CPU: Celeron M Processor 340 (1.5GHz)
OS: FedoraCore3
Development language: JAVA (DACS Server)

(2)Client Machine

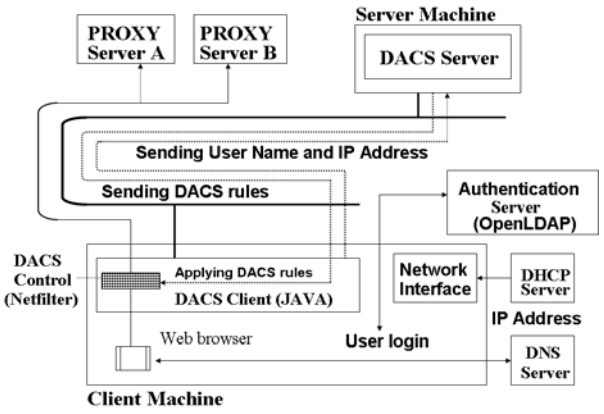

Fig.7 Diagram of prototype

CPU: Celeron M Processor 340 (1.5GHz)
OS: FedoraCore3
Development language: J AVA (DACS Client)
Others: Netfilter (DACS Control)

As the result of prototype construction, the function of changing a communicating PROXY server by a system administrator is realized as shown in Fig.7. When a PROXY Server A is set as reference PROXY server of the Web browser on a client, communication is done via PROXY Server B by the control of DACS Control. The confirmation by the way of PROXY Server B is identified in the access log of squid. The confirmation of no communication via PROXY Server A was also identified in the access log of squid.

4.1 Displayed Results of Status Table

Here, the window results of the status table are shown in Fig.8. In Phase1, the user name and the IP address of the login client are first transmitted from DACS Client. The IP address and the status flag are changed into the record of each user unit beforehand registered by the system administrator (status 0→1). Moreover, in phase 2-a, before transmitting DACS rules to DACS Client, the startup check is carried out to DACS Client.

```
dacs_db=# select * from status_table;
 user_name |   ip_address   | status
-----------+----------------+--------
 user1     | 192.168.10.1   | 0
 user2     | 192.168.10.2   | 0
 user3     | 192.168.10.3   | 1
 user4     | 192.168.10.4   | 0
 user5     | 192.168.10.5   | 0
 user6     | 192.168.10.6   | 0
 user7     | 192.168.10.7   | 0
 user8     | 192.168.10.8   | 0
 user9     | 192.168.10.9   | 0
```

Fig. 8 Window results of the status table

```
dacs_db=# select * from rule_table;
 user1     | tcp:192.168.1.1:3128-192.168.1.2:3128
 user2     | tcp:192.168.1.1:3128-192.168.1.2:3128
 user3     | tcp:192.168.1.1:3128-192.168.1.2:3128
 user4     | tcp:192.168.1.1:3128-192.168.1.2:3128
 user5     | tcp:192.168.1.1:3128-192.168.1.2:3128
 user6     | tcp:192.168.1.1:3128-192.168.1.2:3128
 user7     | tcp:192.168.1.1:3128-192.168.1.2:3128
 user8     | tcp:192.168.1.1:3128-192.168.1.2:3128
 user9     | tcp:192.168.1.1:3128-192.168.1.2:3128
```

Fig. 9 Window results of the rule table

4.2 Displayed Results of Displayed Results of Rule Table

Next, the result of a rule table used by Phase1 and Phase2 of DACS Protocol is shown in Fig.9. In every phase, DACS rules which are registered to the user name transmitted from DACS Client are extracted. Then, they are transmitted to DACS client.

4.3.3 Displayed Results after Application of DACS Rules

The result after the application of DACS rules from DACS Server to DACS Client (DACS Control) by Phase1 and Phase2 is shown in Fig.10. In this prototype, the functionality of Netfilter is used for DACS Control, and the iptables command is used for the application of DACS rules. The list of the rules is presented.

5. Discussion of Effectiveness

In this chapter, a discussion is performed from the viewpoint of a customer and a system administrator about the effectiveness by DACS Scheme, which works well in the operation and management of network services. In DACS Scheme, the centralized management of communication by a system administrator is possible. Then, the effectiveness is evaluated from both sides of a customer and a system administrator as shown in the following.

5.1 Effectiveness from Customer ’s Viewpoint

By the communication control of a system administrator, the subsequent modification of setups is not needed. As the result, the user can use network services continuously without being conscious of a configuration change of the network server. In these days, university gives student a notebook-sized personal computer. At such a university, the time taken for a student to maintain a notebook-sized personal computer, becomes longer. If the network services by DACS Scheme is performed, the time and effort for students is saved, and the burden on student is reduced.

```
Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  anywhere             192.168.1.1         tcp dpt:squid to:192.168.1.2:3128
DNAT       tcp  --  anywhere             192.168.2.1         tcp dpt:http to:192.168.2.2:80
DNAT       tcp  --  anywhere             192.168.3.1         tcp dpt:smtp to:192.168.3.2:25
```

Fig.10 Window results after the application of DACS rules

5.2 Effectiveness from System Administrator's Viewpoint

5.2.1 Affinity with Existing System

A modification of the existing system is unnecessary except building DACS Server on the server, and building DACS Client on each client. Furthermore, since a communication of the client can be performed by applying DACS rules and the existing system is continued without an outage of a server or a client, which shows affinity with the existing system.

5.2.2 Safety Network Environment Change

Because the customer does not need to change the setups of network in DACS Scheme, the system administrator can realize system change easily. For example, the case where the network server software is changed, is assumed. When introducing new network server software, both verification of its function and verification to the load are required. By the conventional method, it is difficult to do a load examination besides using special verification software etc, after performing functional verification. By the DACS Scheme, it becomes possible to divide all the users into five equally, and to shift a user gradually every 1/5 for example. Since the number of users is increased one by one gradually as a load examination in an actual environment, it can be checked whether it can bear to the number of users.

5.2.3 Reduction of Customers Support

The support about the setups of network services is frequently taken place. When performing a update and configuration change of the server by conventional method, the change notice of network application may be needed to the customer, but it is not needed in DACS Scheme. Moreover, except for the initial installation and setups in the client, it is not needed that the customer changes the setups of the communication server of network. For this reason, the mistake of the setups by the customer is not made after the initial introduction. As long as there are no mistakes by the system administrator, the inquiry from the customer about the setups of the communication server will be few. Then, the burden for the system administrator is reduced.

5.2.4 System Management Faithful to Policy

Although not necessarily stipulated, the policy on the network system management and the security policy, exist in the organization. Since the leaks of personal data, become to be an important problem, it becomes more important to protect their policies. The management by DACS Scheme developed here, can perform the system processing faithful to the policy.

6. Conclusion

As a way for making the efficiency of the operation and management for network services, DACS Scheme is proposed here. The characteristic of the operation and management by DACS Scheme is that the centralized management by the administrator is done after once the customer performs the initial setups. For this reason, it is not necessary to change the setups on the client. Moreover, communication server is determined, and available services can be set for every user by performing the management of the user and DACS rules. DACS Protocol required for the DACS Scheme was described, and the prototype was actually built. Then, experimental result was shown. Further, the study was discussed from the viewpoint of the customer and the system administrator about the effectiveness of the operation and management for the network services. For the customer, the burden of the management is reduced, such as changing the setups of the client, which shows as an advantage of the proposed DACS Scheme. Since the affinity with the existing system is good for the administrator, the utility is highly valuable at the following points.

- The initial introduction of DACS is very easy.
- The operation and management after an initial introduction of DACS Scheme are very easy.
- After starting the operation and management by DACS Scheme, a change of servers can be made freely and safely.
- There is an effect which reduces customer supports.

A construction of the whole system for the real operation, and implementation, will be done as a future project.

References

[1] S. Heilbronner, and R. Wies, ”Managing PC networks ”, IEEE Commun.Mag.,vol.35,No.10,pp.112-117,Oct.,1997.

[2] J.Chauki,M. and M.Shahsavari, ”Component-based distributed network management ”,Proc. Southeastcon 2000,pp.460-466,IEEE Pub.,2000.

[3] L.Raman, ”OSI systems and network management ”,IEEE Commun.Mag.,vol36,No.3,pp46-53, Mar.,1998.

[4] T.Shimokawa, Y.Koba, I.Nakagawa, B.Yamamoto, and N.Yoshida,” Server Selection Mechanism using DNS and Routing Information in Widely Distributed Environment ” , IEICE Tran. on Communications,vol.J86-B,No.8,pp.1454-1462,Aug.2003.

[5] S.K.Das, D.J.Harvey, and R.Biswas, ” Parallel processing of adaptive meshes with load balancing ”, IEEE Tran.on Parallel and Distributed Systems, vol.12,No.12,pp.1269-1280,Dec.,2002.

[6] M.E.Soklic,“ Simulation of load balancing algorithms: a comparative study ”,ACM SIGCSE Bulletin,vol.34,No.4,pp.138-141,Dec.,2002.

[7] J.Aweya, M.Ouellette, D.Y.Montuno, B.Doray, and K.Felske, ”An adaptive load balancing scheme for web servers, ” Int. ,J. of Network Management.,vol.12,No.1,pp.3-39,Jan/Feb.2002.

[8] A.Konno, T.Yoshimura, H.Hashima, Y.Iwatani, T.Abe, and T.Kinoshita,: ”Network Management Support System Based on the Activated Status Information ”,IPSJ Journal,vol.46,No.2,pp.493-505,Feb.,2005.

[9] M.Kawashima, and M.Matsushita, ”Application of HTTP Protocol for Enterprise Network Management ”,IEICE Tran. on Communications, vol.J82-B,No.3,pp.339-346,Mar.,1999.

Kazuya Odagiri He graduated from school of human sciences of Waseda University in 1998. He works in Information Processing Center of Toyota Technological Institute now. In addition, he is in Graduate School of Business Administration and Computer Sciences at Aichi Institute of Technology. He engages in a study of network management.

Rihito Yaegashi received the degree of B.S in 1999 and The degree of M.S in 2001 from Shibaura Institute of Technology, Tokyo. He is now Postdoctoral Fellow in Toyota Technological Institute, Information Processing Center. He is a member of Information Processing Society of Japan(IPSJ), The Institute of Electronics Information and Communication Engineering(IEICE), and The Society of Project Management. He got his Ph.D. in engineering from Shibaura Institute of Technology in March 2005.

Masaharu Tadauchi received the B.A., M.A. and Dr.-eng degree from Waseda University, Japan in 1943, 1945 and 1990, respectively. He joined Hitachi Reserch Laboratry of Hitachi, Ltd. in 1945. He was a professor in Infomation Processing Center of Toyota Tecnological Institute form 2003.

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.