Studies on New Network Management Scheme in University Network

Aichi Institute of Technology

Graduate Course of Business Administration and Computer Science

Matriculation Number	B05801
Name	Kazuya Odagiri
Regents Professor	Naohiro Ishii

Contents

1. Motivation

In the university network, there are some characteristics about management and operation. As a characteristic, it is pointed out that people with different membership and position as students, faculties, external persons, et al., use the network services comparatively freely. Moreover, as another characteristic, it is pointed out that there is not always a section for managing and operating a whole network system. A client computer for respective user is managed by each user. For example, a student manages a notebook-sized personal computer for using in a classroom. Moreover, management and operation of a laboratory network system is often done in each laboratory, and a computer management section manages and operates the part of them. Because a computer management section does not perform all operation and management for the respective needs, it is often difficult to spread the information for the network usage. In such environments, various problems occur from the view point of user supports. As a problem of user support, it is described as follows. When some different network services such as SMTP (Simple Mail Transfer Protocol) service and POP3 (Post Office Protocol Version 3) service on the same server machine are divided into different server machines, that is, when system configuration of a network system is changed, a user often must change host name on a client computer application by oneself. When it is necessary to support the respective individual user who cannot change setups of a client computer by oneself, it becomes a burden for a network administrator. As another problem of user support, it is pointed out that much time and effort are spent to cope with annoying communication from the virus infection client computer under the management by DHCP (Dynamic Host Configuration Protocol). This is because there is not any clear evidence which client computer uses which IP address. In the conventional network scheme, it is difficult to solve these problems well without complicated works by the person.

To solve these problems, new form of user support is proposed and examined. That user support can be realized on the network introducing DACS (Destination Addressing Control System) Scheme. DACS Scheme is a network operation and management scheme for managing a whole network system by communication control of a client computer which has been proposed by Odagiri at el. The realization and effectiveness is described. In the network by DACS scheme, it becomes possible to determine a communication server or to block the communication by the user or client computer unit for the same host name. It is difficult to realize the function in the network using the conventional name resolution services such as DNS (Domain Name System) and WINS (Windows Internet Name Service). By using theses functions, new form of user support is realized.

2. Introduction

The times of the ubiquitous network are coming in earnest, and anyone can almost connect to the network and use the network service anywhere anytime. It is very convenient. But, on the other hand, because a client (a client computer) is connected to the network without being known to the network administrator, network management becomes complicated. Generally, Network management means different things to different people. In some cases, it involves a solitary network consultant monitoring network activity with a protocol analyzer. In other cases, network management involves a distributed database, automatic polling of network devices and high-end workstations generating real-time graphical views of network topology changes and traffic. In general, Network Management is a service that employs a variety of tools, applications, and devices to assist human network managers in monitoring and maintaining networks. IS0 Network Management Model consists of five conceptual areas.

Fault Management - The goal of fault management is to detect, log, notify users of, and (to the extent possible) automatically fix network problems to keep the network running effectively because faults can cause downtime or unacceptable network degradation.

Configuration Management - The goal of configuration management is to monitor network and system configuration information so that the effects on network operation of various versions of hardware and software elements can be tracked and managed.

Accounting Management - The goal of accounting management is to measure network utilization parameters so that individual or group uses on the network can be regulated appropriately. Such regulation minimizes network problems (because network resources can be apportioned based on resource capacities) and maximizes the fairness of network access across all users.

Performance Management - The goal of performance management is to measure and make available various aspects of network performance so that network performance can be maintained at an acceptable level. Examples of performance variables that might be provided include network throughput, user response times, and line utilization.

Security Management - The goal of security management is to control access to network resources according to local guidelines so that the network cannot be sabotaged (intentionally or unintentionally) and sensitive information cannot be accessed by those without appropriate authorization. A security management subsystem, for example, can monitor users logging on to a network resource and can refuse access to those who enter inappropriate access.

If the network becomes easy to be managed, a network administrator can save the labor and time for maintaining the network. As the result, the system administrator can concentrate on the value-added high work such as the plan or construction of a new system. In the companies competition between companies based on a market mechanism is a commonplace. Similarly, in the universities, competition for survival adds to intensity year by year. For fighting successfully through competition, it is important that the environment for concentrating on the high value-added work is prepared.

A current network framework is constructed based on TCP/IP (Transmission Control Protocol/Internet Protocol) protocol assuming the anonymity communication. Because that network does not have the mechanism for managing the whole network by a user unit and by a client unit, there are some inconvenient points. For example, the network administrator often spend the labor and time for measures such as identification of the user who uses the streaming of the moving and sound, and troubles other users. In that case, the network administrator cannot also identify that user. In addition, when the configuration of the network system is changed, for example, when the mail boxes located on one network server are relocated on the different network servers, some users must change setups of the client software. When the user can not change it by oneself, the network administrator must support that user. As much as it is a large-scale network with many users, the network administrator must spend the much labor and time for user support. The anonymity communication is one of the factors that spread the Internet generally widely. However, there is a limit for close network management because of the anonymity. In this research, a new network management scheme for realizing the close network management on the network based on TCP/IP protocol is considered.

In this paper, first, it is explained about the researches of existing network management technology in section 3. From section 4 to section 6, the explanation about the scheme itself of DACS Scheme is done. In section 4, the basic content of DACS Scheme, that is, a new network management scheme is explained [1] [2] [3] [4], and the content of the security function [5][6][7] is explained in section 5. In section 6, evaluation of the processing workload for applying DACS Scheme to practical network is done. Then, as the researches to exemplify the effectiveness of DACS Scheme, the new user support which is realized on the network introducing DACS Scheme [8][9] is explained in section 7. Moreover, in section 8, the new portal system which is realized on the network introducing DACS Scheme [10]11] is explained.

3. Researches of Existing Network Management Technology

As the researches of the existing network management, there are some researches about communication control of changing the destination of communication such as load balancing, and about access control which is needed as the technology of security.

Communication controls in these researches are performed at the spot of either between a client and a network server. To be concreted, there are some methods for controlling in either of the place from (1) to (3) as follows.

(1) The method of communication control on the network server side.

(2) The method of communication control on the mechanism located on the network course

(3) The method of communication control on the client

In the method of (1), there are some methods as follows from (a) to (c). Only the access control is performed. It is impossible to perform communication control of changing the destination of the communication on the network server.

(a) The method of access control by the packet filtering mechanism which is located on the network server side when the communication from a client reaches a network server.

(b) The method of access control by use of authentication.

(c) The method of access control by supporting or not supporting VPN for the communication from a client to a network server.

In the method of (a), it is possible to perform access control only by an IP address and communication port unit. That is, it is impossible to perform access control by a user unit. The method of (b) can not applied to the unspecified number of network services, because authentication is performed by a network service unit individually. The method of (c) performs access permission control by supporting VPN for the communication from a client to a network server and permitting that communication. Then, access non-permission control is performed by denying the communication which is not supported by VPN. However, in this method, there is the problem that processing load at the server side becomes heavy because all access controls are performed in the server side. In the method of (2), there are some methods such as follows from (d) to (e).

(d) The method of access control for the communication between LAN (Local Area Network) and external network by SSL-VPN [12] and Opengate [13][14].

(e) The method of access control for the communication from a client to a network server in the different network via Communication Control Service such as quarantine network with gateway [15] or authentication switch [16].

In the method of (2), it is possible to perform access control for the communication from a client to a network server by a user unit. Moreover, it is possible to perform communication control of the destination of communication. For example, there is the load distribution technology of the server [17] [18] [19] by the control using the load balancer. However, because the mechanism for communication control needs to be located on the network course in these methods, the system configuration of existing network must be changed physically. Then, because communications from many clients concentrates, processing load on the Communication Control Service becomes heavy.

In the method of (3), there is a method to use the personal firewall of quarantine network [20][21]. The system configuration of the network does not need to be changed. But, because access control is performed by packet filtering mechanism on the client, it is impossible to perform access control for the communication from the client without that packet filtering mechanism. Moreover, it is possible to perform communication control of the destination of communication. For example, there is DNS round robin technology [22]. Because the different IP addresses are assigned to each client-software as the result of name solution and the communicating server is changed, it is understood that the destination of communication is changed on a client.

Each research explained in the above has each different purpose, and do not have the purpose of managing the network system.

In addition, there has been considerable interest in both policy-based management and autonomic distributed systems management [23- 28]. Policies are a crucial factor that may affect the autonomic manager, which self-controls the distributed application services at runtime over a network. The dynamic interconnectivity and the unpredictable environment of distributed systems makes it difficult to either predict the required control resolution strategy in case of conflict/failure, or embed static control policies in management process. Though these network management have a purpose of managing a whole network. However, the mechanism for communication control needs to be located on the network course in these methods in the same way as (2). The system configuration of existing network must be changed physically, and communications from many clients concentrates, processing load on the Communication Control Service becomes heavy.

4. Mechanism of DACS Scheme

4.1 Introduction

The characteristic of the operation and management in the university network system, 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 network management section carries out management and operation of the most network infrastructure and servers, the customer mainly performs the management of their clients [29]. Operation and management of the network system are conventionally focused on the control in the infrastructure or server side [30] [31]. For example, DNS round robin [22], the control using the load balancer and the load distribution of the server [17] [18] [19], 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 environment where student uses a notebook-sized personal computer, is assumed. When comfortable internet environment is needed for exclusive use of a classroom, it is necessary to reconnect to the PROXY Server by setting change of the Web browser. In such a case, if the system administrator is able to control the communication freely between the server and client, it is not necessary to make setup change at the client side.

In this section, 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.

4.2 The Summary of DACS Scheme

4.2.1 The Basic Principle of DACS Scheme

Figure 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.

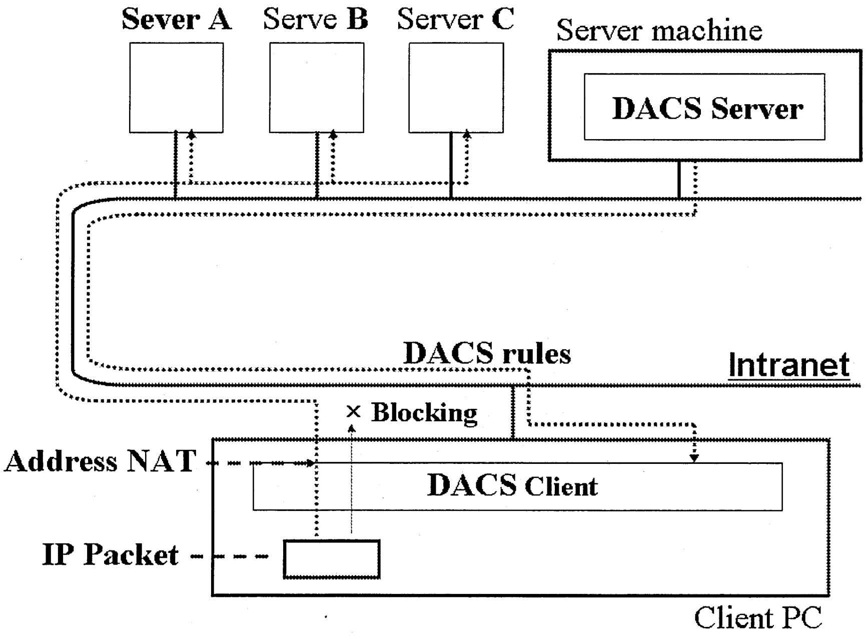


Figure 1. Basic Principle of DACS Scheme

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 Figure 1. In Figure 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 Figure 2. As shown by (1) in Figure 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 Figure 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 Figure 2.

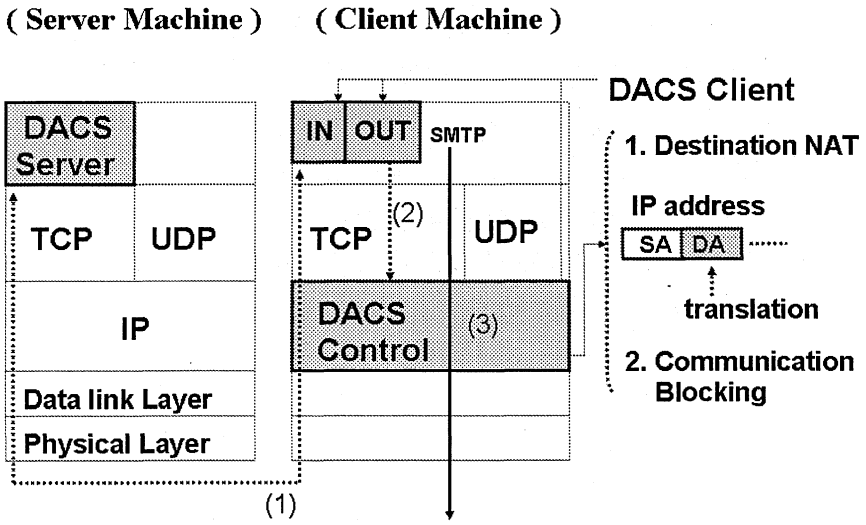


Figure 2. Layer Setting of DACS Scheme

4.2.2 Characteristic of DACS Scheme

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.

4.3 DACS Protocol

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 section 4.5.

4.3.1 Initializing Process in DACS Protocol (Phase1)

The protocol of Phase1 is shown in Figure3. (S1-S4 indicates the processing sequence by the server side, and C1-C9 indicate the processing sequence of the client side.)

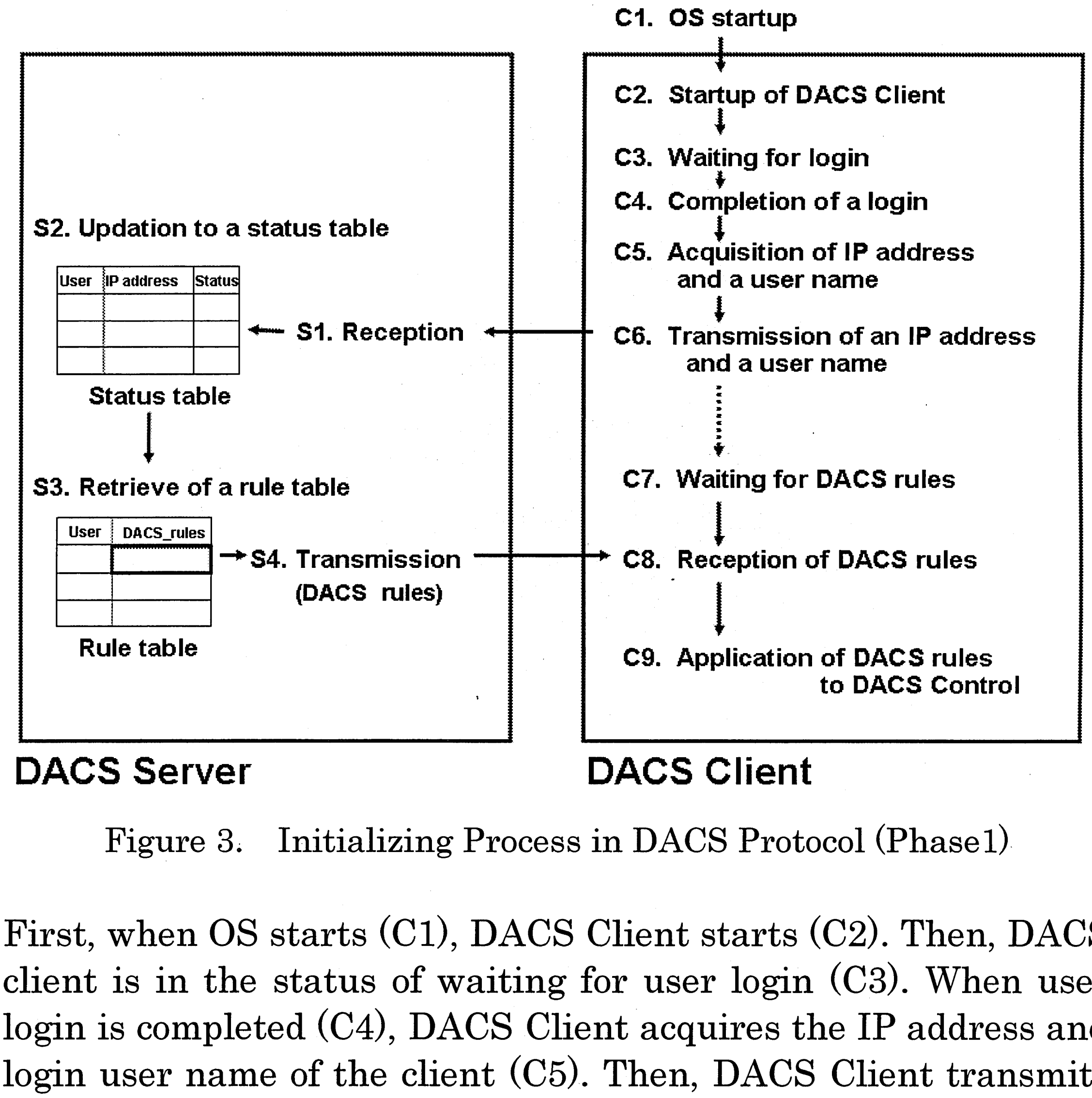

C1. OS startup
C2. Startup of DACS Client
C3. Waiting for login
C4. Completion of a login
C5. Acquisition of IP address and a user name
C6. Transmission of an IP address and a user name
C7. Waiting for DACS rules
C8. Reception of DACS rules
C9. Application of DACS rules to DACS Control
S2. Updation to a status table
User
IP address
Status
S1. Reception
Status table
S3. Retrieve of a rule table
User
DACS_rules
S4. Transmission (DACS rules)
Rule table
DACS Server
DACS Client

Figure 3. Initializing Process in DACS Protocol (Phase1)

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 (OpenLDAP) 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.

4.3.2 Distribution Process of DACS rules by System Administrator in DACS Protocol (Phase 2-a)

Next, the protocol in Phase2-a is shown in Figure4. (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. 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).

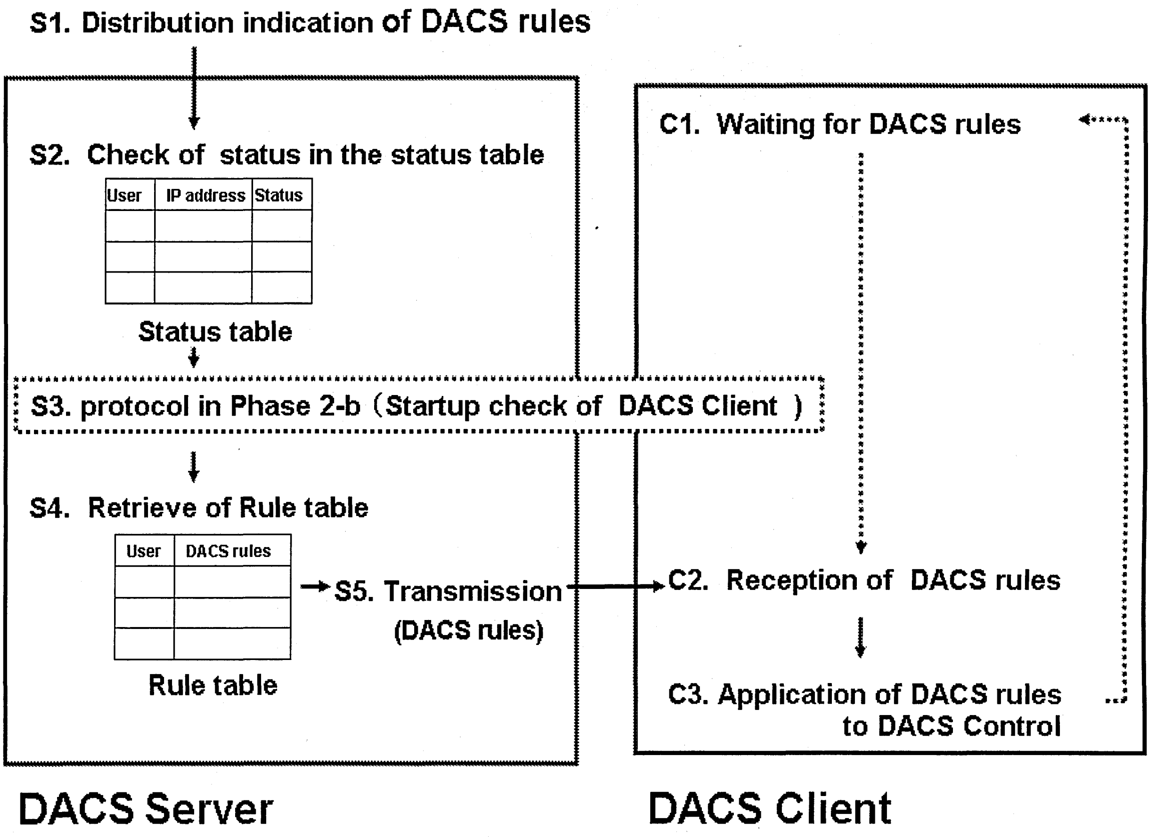

S1. Distribution indication of DACS rules
S2. Check of status in the status table
User
IP address
Status
Status table
S3. protocol in Phase 2-b (Startup check of DACS Client)
S4. Retrieve of Rule table
User
DACS rules
Rule table
S5. Transmission
(DACS rules)
C1. Waiting for DACS rules
C2. Reception of DACS rules
C3. Application of DACS rules to DACS Control
DACS Server
DACS Client

Figure 4. Distribution Process of DACS rules by System Administrator in DACS Protocol (Phase 2-a)

4.3.3 Checking Process of DACS Client startup in DACS Protocol (Phase 2-b)

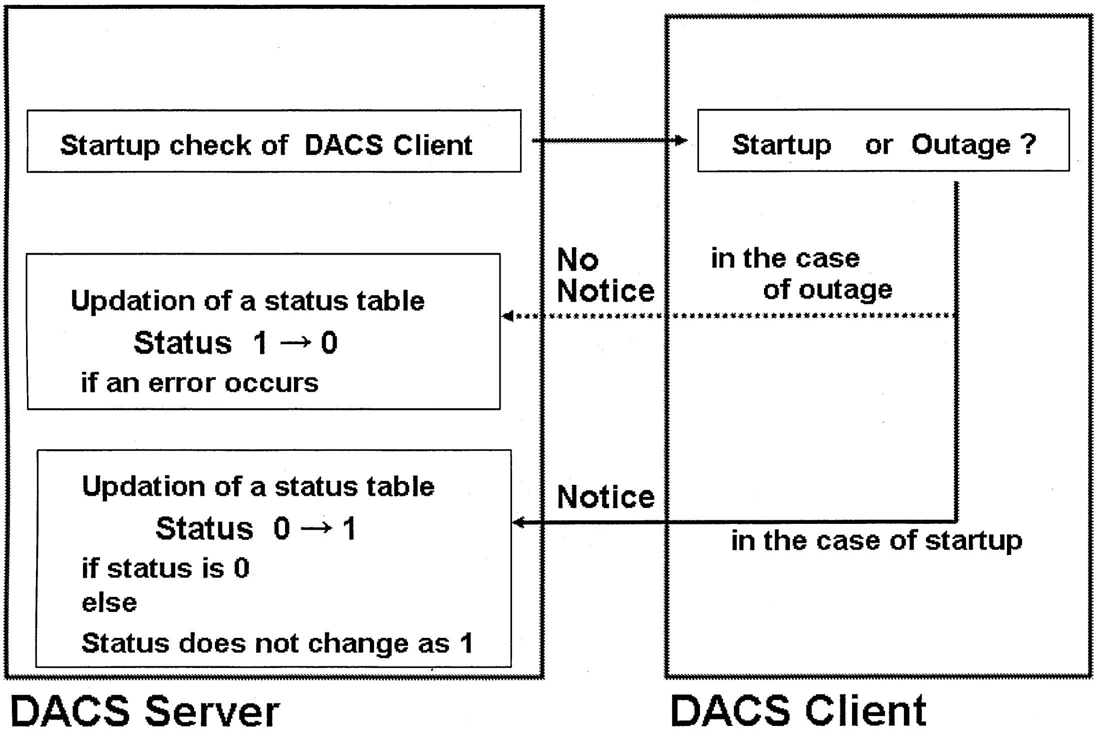


Figure 5. Checking Process of DACS Client startup in DACS Protocol (Phase 2-b)

Protocol in Phase2-b is shown in Figure5.. 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 Figure6. 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. 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.

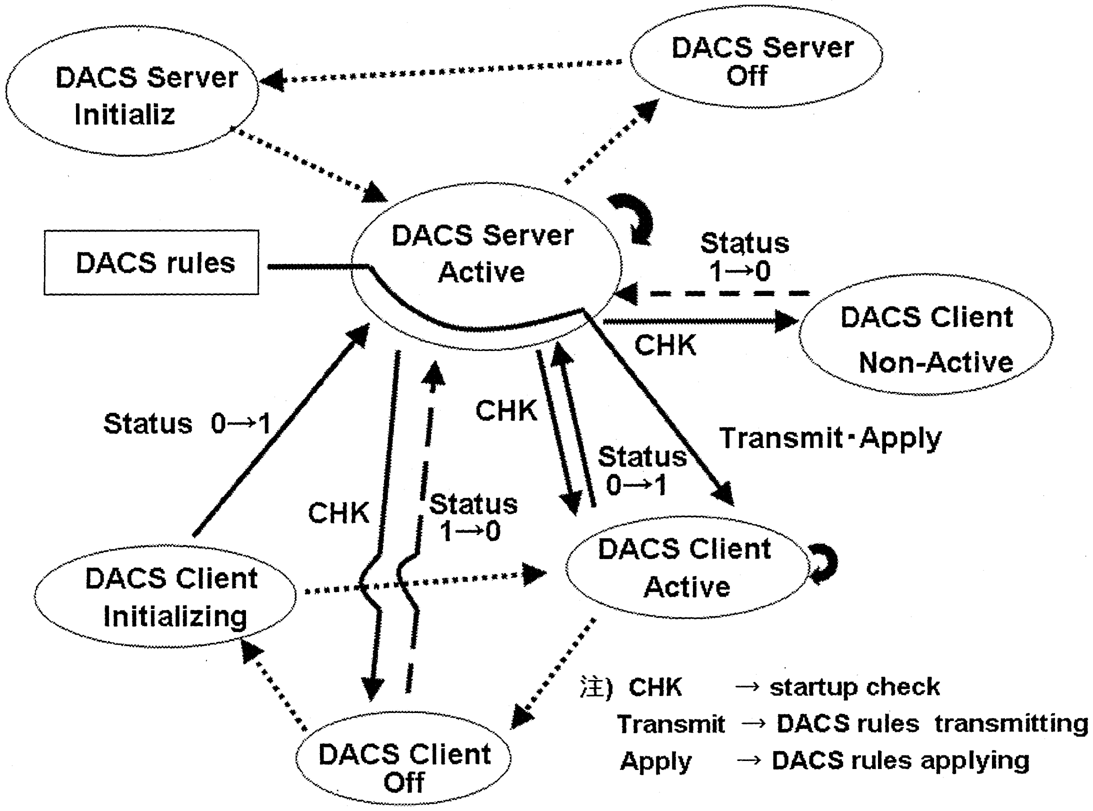


Figure 6. Status description of DACS Scheme

4.4 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.

4.4.1 Realization of Communication Control by a Client Unit

When a user logs in to a client, the IP address of the client is transmitted to DACS Server from DACS Client. Then, if DACS rules corresponding to IP address, is registered into the DACS Server side, it is transmitted to DACS Client. Then, communication control for every client can be realized by applying to 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.

4.4.2 Coexistence with Communication Control by a User Unit

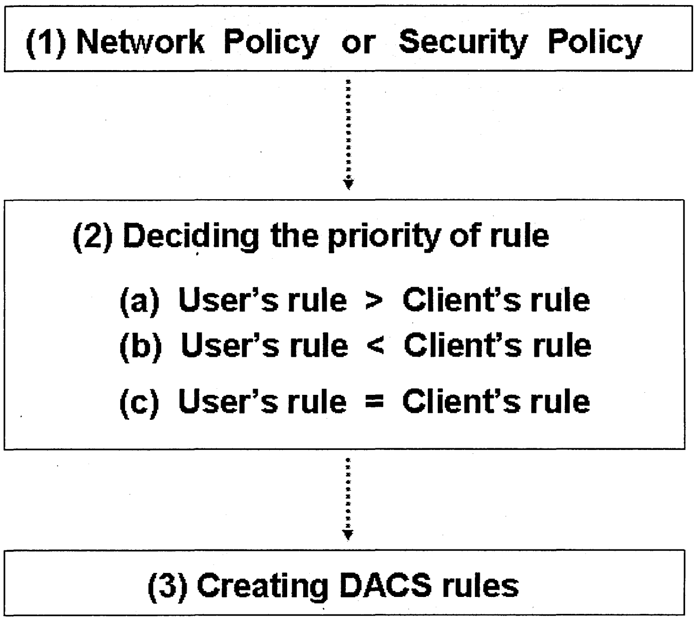

(1) Network Policy or Security Policy
(2) Deciding the priority of rule
(a) User's rule > Client's rule
(b) User's rule < Client's rule
(c) User's rule = Client's rule
(3) Creating DACS rules

Figure 7. Creating DACS rules in the DACS Server side

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 Figure7. 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 DACS rules are created (3). DACS rules are transmitted to DACS Client. In the DACS Client side, DACS rules are applied to DACS Control. The difference between the user's rule and the client's rule is not distinguished.

4.5 Functional Experiment and Experimental Results

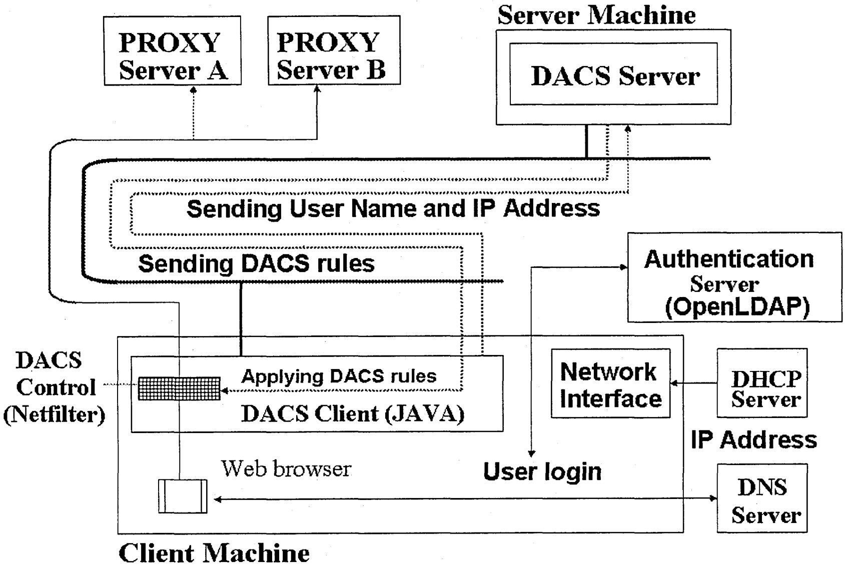
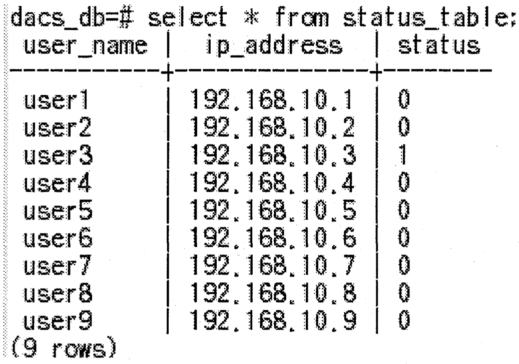


Figure 8. Prototype System

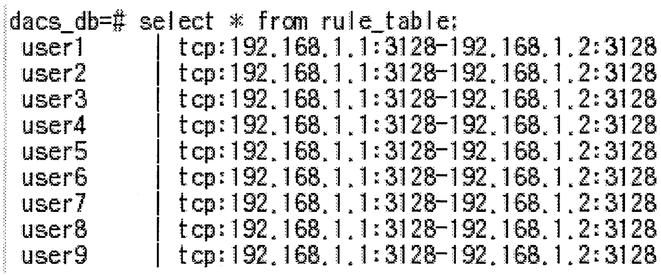
In order to prove the possibility of realization of the network services by DACS Scheme, the prototype was built. Then, the functional test was actually carried out under the operation. The prototype developed here, is shown in Figure8. Server Machine and Client Machine use FedoraCore3 as the OS.DACS Server and DACS Client is implemented by JAVA language. DACS Control uses the function of Netfilter, which is equipped in Unix or Linux. As the result of prototype construction, the function of changing a communicating PROXY server by a system administrator is realized as shown in Figure8. 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.



```
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
(9 rows)
```

Figure 9.　Window Results of the Content of Status Table

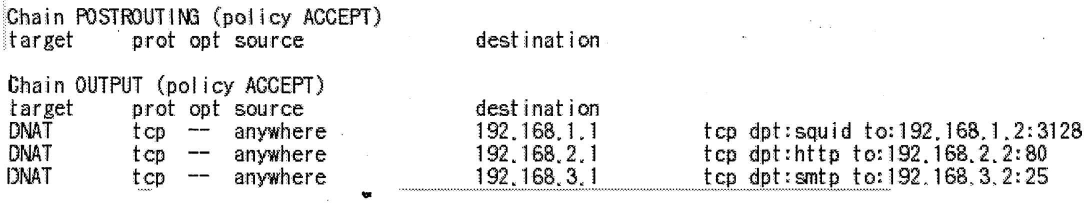
Here, the window results of the status table are shown in Figure9. In Phase1, the user name and the IP address of the login client are first transmitted from DACS Client. The IP address and the status flag are changed into the record of each user unit beforehand registered by the system administrator (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 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
```

Figure 10. Window Results of the Content of Rule Table

Next, the result of a rule table used by Phase1 and Phase2 of DACS Protocol is shown in Figure10.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.



```
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
```

Figure 11. Window Results after the Application of DACS rules to DACS Client

The result after the application of DACS rules from DACS Server to DACS Client (DACS Control) by Phase1 and Phase2 is shown in Figure11. In this prototype, the functionality of Netfilter is used for DACS Control, and the ip tables command is used for the application of DACS rules. The list of the rules is presented.

4.6 Evaluation of the Effectiveness

In this section, a discussion is performed from the viewpoint of a customer and a system administrator about the effectiveness by DACS Scheme.

4.6.1 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. To the user without almost knowledge, it is more effective.

4.6.2 Effectiveness from System Administrator's Viewpoint

(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.

(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.

4.6.3 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.

4.7 Conclusions

As a way for making the efficiency of an operation and management for network services better, DACS Scheme is proposed here. The characteristic of the operation and management by DACS Scheme is that the centralized management by the system administrator is possible after once the customer performs the initial setups. For the reason, it is not necessary to change the setups on client. Moreover, communication server is determined, and available services can be set for every user by performing the management of a user and DACS rules. DACS Protocol required to realize DACS Scheme was described, and the prototype was actually built. Then, experimental result was shown. The study was discussed from the viewpoint of the customer and the system administrator about the effectiveness of the operation and the management of the network services. For the customer, the load intensity of a management is reduced, such as changing the setups of the client, which shows as an advantage of the proposed DACS Scheme. On the other hand, since affinity with the existing system is high, for a system administrator, utility value is high 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.

5. Security Function of DACS Scheme

5.1 Introduction

In existing DACS Scheme, there are some security problems to be solved. It is assumed that DACS Client must be implemented on all clients. When the client which DACS Client is not installed in is connected to the network, each network server can be accessed from that client technically. Depending on network or security policy, access to each network server as shown in the above can be permitted or not permitted. For the purpose of corresponding to the non-permitted case, the function of preventing the communication from the client which DACS Client is not installed in is needed. Moreover, even if permitted, the communication needs to be encrypted when a user expects it. For example, in the service of handling information and contents for the specified user such as POP service, communication needs to be encrypted for the purpose of preventing information interception. However, when communication is encrypted, processing for encrypting and decrypting occurs in the server side. The function of encrypting only minimum communication is needed for reducing processing load in the server side where communications from a lot of users and clients concentrate.

Therefore, secure DACS Scheme is proposed and examined. Secure DACS Scheme has functions to prevent the communication from the client which DACS Client is not installed in and to prevent information interception. Then, the communication between the network server and the client which DACS Client is installed in is tunneled and encrypted. There are some methods of tunneling and encrypting under network layer (third layer) of OSI model [32] [33] [34], and some methods of tunneling and encrypting above transport layer (forth layer) [35] [36]. In the former method, because all communications to the network sever from the client are tunneled and encrypted, processing load in the server side is heavy. In the latter method, because the communication is tunneled and encrypted by a network service unit, processing load in the server side is light in comparison with the former method. By connecting the latter method with the DACS Scheme's function of communication control by a user unit, tunneling and encrypting the communication by a user unit is realized. By tunneling and encrypting the communication, the function of preventing the communication for one network service from the client which DACS Client is not installed in is realized. Moreover, when the communication from the client which DACS Client is not installed in is permitted, each user can select whether the communication is tunneled and encrypted or not. The function of preventing information interception is realized. In comparison with the method of only tunneling and encrypting the communication by a network service unit, it is realized to reduce the processing load in the server side. That function of tunneling and encrypting the communication is extended by using the port forwarding function of SSH [37], which is selected from methods of tunneling and encrypting.

In this section 5, the function for preventing the communication from the client which DACS Client is not installed in and preventing information interception is examined. The experimental results by prototype construction are shown to confirm the possibility of this function.

5.2 Examination of the Necessary Function

In existing DACS Scheme, it is assumed that DACS Client must be implemented on all clients. When the client which DACS Client is not installed in is connected to the network, each network server can be accessed from that client technically. Depending on network or security policy, access for each network server can be permitted or not permitted. For the purpose of corresponding to the non-permitted case, the function of preventing the communication from the client which DACS Client is not installed in is needed. Even if permitted, the communication needs to be encrypted when a user expects it. For example, in the service of handling information and contents for the specified user such as POP service, communication needs to be encrypted for the purpose of preventing information interception. When communication is tunneled and encrypted, processing for encrypting and decrypting occurs in the server side. The function of tunneling and encrypting only minimum communication is needed for reducing processing load in the server side where communications from a lot of users and clients concentrate.

From here, the adaptability for DACS Scheme is examined. At first, as the method for preventing the communication from the client which DACS Client is not installed in, access control on the network server side is examined. First, the method of using packet filtering mechanism is considered. By locating packet filtering mechanism on each network server, it is possible to perform access control based on IP address and TCP port. In existing DACS Scheme, communication control is performed by a user unit. To perform access control by a user unit on the network server, the mechanism, which makes it possible to identify which user is sending communication, is needed. That is, the packet filtering mechanism which corresponds to DACS Scheme is needed. The details of the method for corresponding to DACS Scheme are described in section 5.3. Because access control is performed according to the correspondence list of a client's IP address and a user name logging in that client, processing load comes to be very heavy. Then, the method of each network service's performing access control by a user unit is considered. Each network service is needed to correspond to DACS Scheme. Being same as packet filtering mechanism which corresponds to DACS Scheme, processing load is very heavy. Moreover, it is difficult to make all network service correspond to DACS Scheme. Access control on the network server side is not suitable to DACS Scheme.

Next, as another method to prevent the communication from the client which DACS Client is not installed in, the method of using the mechanism of single sign on operation such as Kerberos is considered. In this method, each network service must correspond to the mechanism of single sign on operation. However, because there is not always the guarantee, this method is not unsuitable to DACS Scheme.

Therefore, as the other method to prevent the communication from the client which DACS Client is not installed in, the method of tunneling and encrypting the communication between the network server and the client which DACS Client is installed in is considered. Essentially, only tunneling is needed to prevent such a communication. By adding the encrypting function, the information interception is prevented. To tunnel and encrypt the communication, there are some methods of tunneling and encrypting under the network layer (third layer) of OSI model by using PPTP and L2TP, IP sec etc. In addition, there are some other methods at the upper layer more than transport layer (forth layer) by using SSL and TLS, SSH etc. The protocol without the function of encrypting like L2TP needs to be incorporated with other encrypting function. In the case of tunneling and encrypting under third layer, all communications between a network server and a client are tunneled and encrypted. On the other hand, in the case of tunneling and encrypting above forth layer, the communication between a network server and a client are encrypted and tunneled by a network service unit. Since the processing to restore the tunneled and encrypted communication is needed in the network server, it is expected to tunnel and encrypt the minimum communication. In comparing the former method with the latter method, the latter method is advantageous to reduce the processing load in the server. However, it is insufficient only to tunnel and encrypt the communications between a network server and a client simply by a network service unit. In DACS Scheme, communication control is performed not only by a client unit but also by a user unit. Depending on the content of network or security policy, it may be needed for one specified users to use one network service with the communication tunneled and encrypted. Also, it may be needed for another specified users to use same network service with the communication not tunneled and unencrypted. This communication control is realized by connecting the function of communication control by a user unit in DACS Scheme and the function of tunneling and encrypting by a network service unit above the forth layer. In addition, because the unspecified number of network services moving on TCP/IP needs to be controlled, the communication will be tunneled and encrypted, not by the method that is effective for only specific network service, but by the method that is effective for the unspecified number of network services. In the method of using SSL and TLS, the communication for the unspecified number of network services is not always tunneled and encrypted. In the method of using the port forwarding function of SSH, it is possible to tunnel and encrypt the communication for the unspecified number of network services. To perform communication control with these requirements satisfied, the function of DACS Scheme is extended as shown in next section.

5.3 Explanation of Extended Function for Solving Security Problems

In this section, the functional extension of 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 client 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 DACS Scheme, is failed. The transparent use of a client means that a client can be used continuously without changing setups when configuration change of the network system is done. The function which doesn't fail the transparent use of a client is needed. The mechanism of that function is shown in Figure12.

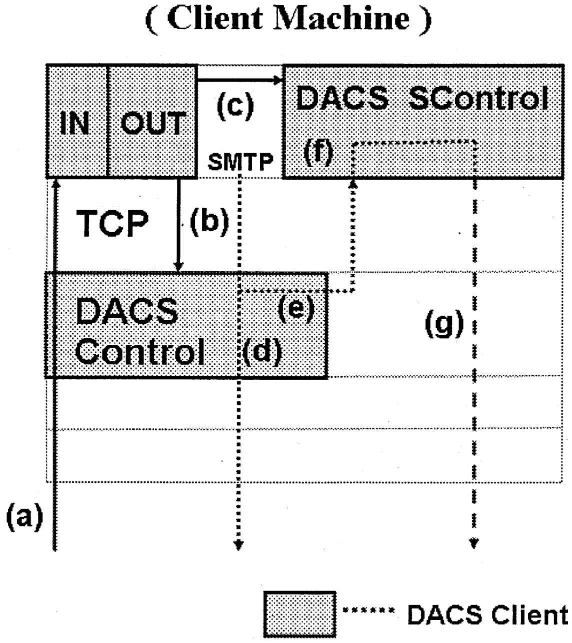


Figure 12. Extend Security Function

The changed point on network server side is shown as follows in comparison with existing DACS Scheme. SSH Server is located and activated, and communication except SSH is blocked. In Figure12, DACS rules are sent from DACS Server to DACS Client (a). By DACS Client which accepts DACS rules, DACS rules are applied to DACS Control in DACS Client (b). The movement to here is same as existing DACS Scheme. After functional extension, as shown in (c) of Figure12, DACS rules are applied to DACS SControl. Communication control is performed in DACS SControl with the function of SSH. By adding the extended function, selecting the tunneled and encrypted or not tunneled and encrypted communication is done for each network service. When communication is not tunneled and encrypted, communication control is performed by DACS Control as shown in (d) of Figure12. When communication is tunneled and encrypted, destination of the communication is changed by DACS Control to local host as shown in (e) of Figure12. After that, by DACS STCL, the communicating server is changed to the network server and tunneled and encrypted communication is sent as shown in (g) of Figure12, which are realized by the function of port forwarding of SSH. In DACS rules applied to DACS Control, local host is indicated as the destination of communication. In DACS rules applied to DACS SControl, the network server is indicated as the destination of communication. As the functional extension explained in the above, the function of tunneling and encrypting communication is realized in the state of being suitable for DACS Scheme, that is, with the transparent use of a client. Then, by changing the content of DACS rules applied to DACS Control and DACS SControl, it is realized to distinguish the control in the case of tunneling and encrypting or not tunneling and encrypting by a user unit. By tunneling and encrypting the communication for one network service from all users, and blocking the untunneled and decrypted communication for that network service, the function of preventing the communication for one network service from the client which DACS Client is not installed in is realized. Moreover, even if the communication to the network server from the client which DACS Client is not installed in is permitted, each user can select whether the communication is tunneled and encrypted or not. The function of preventing information interception is realized.

5.4 Functional Experiment and Experimental Results

To confirm the possibility of the function of tunneling and encrypting the communication for one network service by a user unit, and the function of preventing the communication from the client which DACS Client is not installed in, the functional experiments by prototype construction were done as shown in Figure13. As a new component of this system, DACS SControl, which diverts the function of SSH, is located in the DACS Client. Other components of this system except DACS SControl are same as existing DACS Scheme. The details of system configuration are described as following from (1) to (3). (In this prototype system, a server machine and a client machine are connected to the local area network, which is separated from the outside network. As the result, it is confirmed that the communication for the server machine is sent from the user who is sitting in front of the client machine.)

(1) Server Machine
CPU:Celeron M Processor340(1.5GHz)
OS:FedoraCore3
Language:JAVA(DACS Server)
Database:PostgresSQL
(2)Client Machine
CPU:Celeron M Processor340(1.5GHz)
OS:FedoraCore3
Language:JAVA(DACS Client except DACS Control and DACS

SControl)
others:Netfilter (DACS Control)
OpenSSH-3.9p1-7 (DACS SControl)

(3)Others
Authentication Server:OpenLDAP-2.1.22-8(FedoraCore1)
DHCP Server:Microsoft DHCS Server(WindowsNT4.0)
DNS Server:bind-9.2.2.P3-9(FedoraCore1)
PROXY Server:squid-2.5.STABLE3-3.fc1(RedHatLinux9)

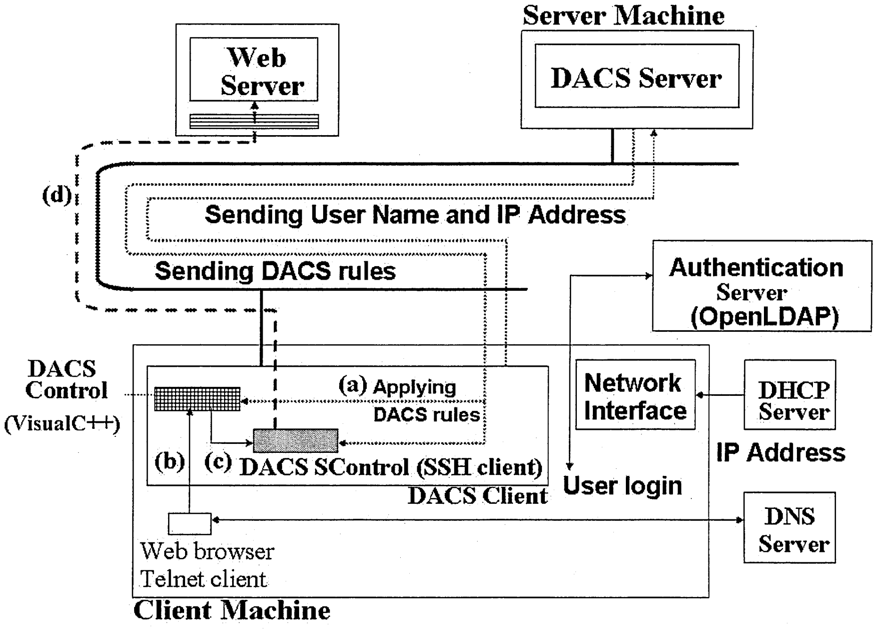
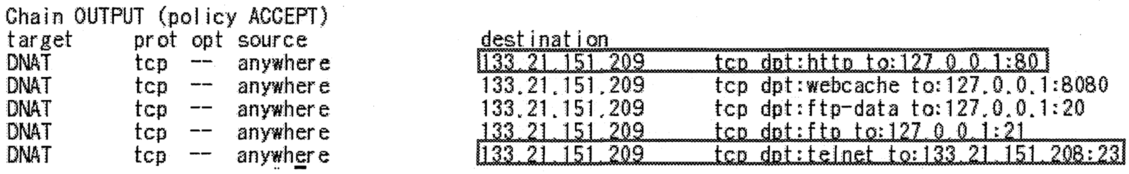


Figure 13. Prototype System

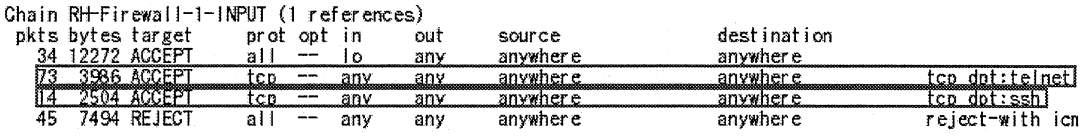
From here, experimental results by prototype construction are shown. First, it is explained about the case to access Web Server with the communication tunneled and encrypted and to access Telnet Server with the communication not tunneled and encrypted. As shown in (a) of Figure13, the client which DACS Client is installed in was initialized after one user's logging in a client. DACS rules were sent from DACS Server to DACS Client, and applied to DACS Control and DACS SControl. In the communication from Web Browser, destination changed by Destination NAT based on DACS rules was 80 port of localhost (127.0.0.1) as shown in the upper bold frame of Figure14.



```
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  anywhere             133.21.151.209      tcp dpt:http to:127.0.0.1:80
DNAT       tcp  --  anywhere             133.21.151.209      tcp dpt:webcache to:127.0.0.1:8080
DNAT       tcp  --  anywhere             133.21.151.209      tcp dpt:ftp-data to:127.0.0.1:20
DNAT       tcp  --  anywhere             133.21.151.209      tcp dpt:ftp to:127.0.0.1:21
DNAT       tcp  --  anywhere             133.21.151.209      tcp dpt:telnet to:133.21.151.208:23
```

Fugure 14. Window Results of DACS Rules

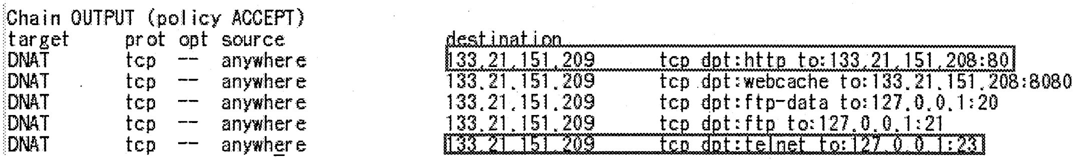
Then, destination changed by OpenSSH based on DACS rules applied to DACS SControl was the IP address (133.21.151.208) of the server machine. When the user accesses to Telnet Server, as shown in the bottom bold frame of Figure14, the IP address of server machine and 23 port was destination changed by Destination NAT based on DACS rules applied to DACS Control. When access from Web Browser to Web Server was performed, as the result of communication control by DACS Control, destination was changed to localhost (port:80) and communication was performed from (b) to (c) in Figure13. By using the function of port forwarding of OpenSSH as DACS SControl, destination of communication was changed to Web Server, and communication was tunneled and encrypted as shown in (d) of Figure13. As the result of reply from Web Server to Web Browser, Web page was displayed on Web Browser. Because communication except SSH (port:22) and Telnet (port:23) was blocked on the Web Server side, communication by SSH was confirmed by communication record through personal firewall on Web Server. Then, after logging in Telnet Server from Telnet client, the user easily operated a command. Because this communication was the basic function on existing DACS Scheme, which changed the destination server for same host name, the explanation about system movement is omitted. As shown in the bottom bold frame of Figure15, communication quantity by SSH was increased from 0 byte to 2504 byte. Then, as shown in the upper bold frame of Figure15, because communication quantity by Telnet was increased from 0 byte to 3986 byte, it was confirmed that the communication by Telnet had been performed. Moreover, when same user logs in same client and performs access from Web Browser to Web Server in the state of stopping DACS Client (including DACS Control and DACS SControl), reply from Web Server was not performed and Web page was not displayed on Web Browser. It was confirmed clearly that access to Web Server was not realized in the state of not tunneling and encrypting by SSH. That is, it was confirmed clearly that the function of preventing the communication from the client which DACS Client is not installed in and the function of preventing information interception were realized.



```
Chain RH-Firewall-1-INPUT (1 references)
 pkts bytes target     prot opt in     out     source               destination
   34 12272 ACCEPT     all  --  lo     any     anywhere             anywhere
   73  3986 ACCEPT     tcp  --  any    any     anywhere             anywhere            tcp dpt:telnet
   14  2504 ACCEPT     tcp  --  any    any     anywhere             anywhere            tcp dpt:ssh
   45  7494 REJECT     all  --  any    any     anywhere             anywhere            reject-with icm
```

Figure 15. Window Results of the Communication Quantity by SSH(1)

Next, in the same procedure, it was confirmed that access to Web Server with the communication not tunneled and encrypted and access to Telnet Server with the communication tunneled and encrypted were performed.

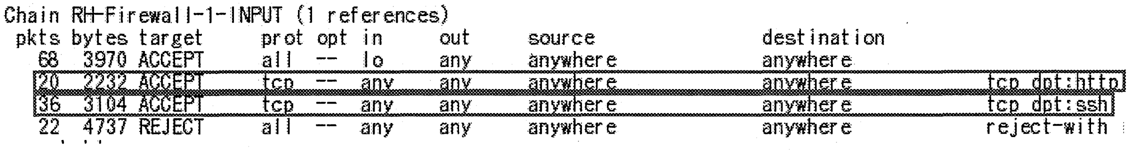


```
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  anywhere             133.21.151.209      tcp dpt:http to:133.21.151.208:80
DNAT       tcp  --  anywhere             133.21.151.209      tcp dpt:webcache to:133.21.151.208:8080
DNAT       tcp  --  anywhere             133.21.151.209      tcp dpt:ftp-data to:127.0.0.1:20
DNAT       tcp  --  anywhere             133.21.151.209      tcp dpt:ftp to:127.0.0.1:21
DNAT       tcp  --  anywhere             133.21.151.209      tcp dpt:telnet to:127.0.0.1:23
```

Figure 16. Window Results of DACS rules applied to DACS Client

In Figure16, the result of applying DACS rules to DACS CTL is shown. As shown in the upper bold frame, because the communication was not tunneled and encrypted in the case of accessing to Web Server, destination after changing was the IP address of the server machine and 80 port. Moreover, as shown in the bottom bold frame, because the communication was tunneled and encrypted in the case of accessing to Telnet Server, destination after changing was localhost.

In Figure17, communication quantity by SSH was increased from 0 byte to 3104 byte. Communication quantity by HTTP was increased from 0 byte to 2232 byte. As the results of these experiments, the possibility of the extended function was confirmed.



```
Chain RH-Firewall-1-INPUT (1 references)
 pkts bytes target     prot opt in     out     source               destination
   68  3970 ACCEPT     all  --  lo     any     anywhere             anywhere
   20  2232 ACCEPT     tcp  --  any    any     anywhere             anywhere            tcp dpt:http
   36  3104 ACCEPT     tcp  --  any    any     anywhere             anywhere            tcp dpt:ssh
   22  4737 REJECT     all  --  any    any     anywhere             anywhere            reject-with
```

Figure17 Window Results of the Communication Quantity by SSH(2)

5.5 Conclusions

As a method of network management, DACS Scheme had been proposed. However, DACS Scheme had some security problems to be solved. In existing DACS Scheme, it was assumed that DACS Client must have been implemented on all clients. When the client which DACS Client is not installed in was connected to the network, each network server could have been accessed from that client technically. Then, depending on network or security policy, access for each network server as shown in the above may be permitted or not permitted. For the purpose of corresponding to the non-permitted case, the function of preventing the communication from the client which DACS Client is not installed in was needed. Moreover, even if permitted, the communication needed to be encrypted to prevent information interception when a user expects it. To prevent the communication from the client which DACS Client is not installed in, and to prevent information interception, new function was needed to be implemented in existing DACS Scheme. To realize that function, the method of access control by use of packet filtering mechanism located on the network servers, was considered. Then, the method of access control by making each network service correspond to DACS Scheme, was considered. In addition, the method of access control by introducing single sign on operation was considered. However, it was unsuitable to DACS Scheme. Therefore, to prevent the communication from the client which DACS Client is not installed in and to prevent information interception, the method of access control by tunneling and encrypting the communication between a network server and a client which DACS Client is installed in was proposed and examined. By implementing the extensional function in existing DACS Scheme, secure DACS Scheme was realized.

6. Evaluation of the Processing Workload

6.1 Introduction

In computer networks where the usage policies are well defined, the network management is relatively easy. This is the case of enterprise computer networks, where security policies and access control lists are well defined. On the other hand, in campus-like computer networks, the management is quite complicated, because the computer management section manages only a small portion of the wide needs of the campus network. For example, in a laboratory, network servers are usually managed by users and not by the central networking office. Moreover, management of client machines is complicated or, at least, it is a time consuming operation whenever an update of network settings takes place. For example, when the SMTP server and the POP server are relocated to new sites or server machines, an update of user machine settings is necessary. Most of computer network users in a campus are student and, since students do not check frequently the e-mail, a usual operation is to make them aware of the settings update. This administrative operation is executed by means of web pages and/or bullettin boards. For the system administration, individual technical support is a stiff part of the network management. In this work, we discuss two models of network management: 1) INfrastructure-based Management model (INM), where the control of the network is performed by means of functionalities deployed along the path from clients to servers and 2) Client Management model (CM), where the management is performed by means of special services located into the client machines. In our previous studies, we proposed an implementation of the CM model in the form of a framework we called DACS Scheme. Essentially, the main features of DACS are the following.

- The user can use the client machine continuously, without changing its default settings.
- By means of a communication control of the client machine of the user, a whole local area network can be managed.

In this way, network system updatings is confined to the system administrator, only. When DACS scheme is used in real networks, the processing load of communication control can be heavy with respect to standard mechanisms of other schemes1. The representative schemes of communication control systems of CM type are SSL-VPN, which controls the communication from outside of the LAN, and Opengate, which controls the access from the LAN towards foreign networks. In these systems, communication control of the user client machine is partially implemented. Furthermore, communication control over the whole network is not implemented. Here, we are concerned with comparing the two models from the point of view of the processing workload. The experimental results collected in our testbed confirm the fact that DACS is an advantageous CM model with respect to INM solutions.

This section is organized as follows. First, we briefly describe the main characteristics of the DACS scheme. Then, we propose two simple network models of INM-like and CM-like solutions. DACS is assumed to be a CM model, while standard TCP port and IP address filtering are considered as INM mechanisms. On the basis of these two models, we explain our analysis and our preliminary results. Conclusions of the work and further investigations are presented.

6.2 Comparison of CM and INM models

The main problem of the CM model of network management, and in particular of DACS, is that the processing load could become as high as to jeopardize the system performance. In fact, the rules of communication control must be extracted from a set of global rules and for every user who logs in his/her machine. Existing solutions are SSL-VPN and Opengate. However, in these solutions communication control of the user machine is partially performed. Moreover, the control of the communications of the whole network is not possible except in the DACS framework. For this reason, it could be unfair to compare DACS performance with respect to other solutions. Therefore, we recast our performance analysis as a comparison of the processing workload of the system in scenarios where DACS is used and where DACS is not deployed. As said above, the second case is the INM model.

6.2.1 Two models for communication control

The INM model is shown in Figure. 18. Servers group and clients group are in separate networks, interconnected through the Communication Control Service (CCS), which is part of the network infrastructure. In this model, the communication of user clients is controlled by the CCS. Usually, there is a Control Information Management Server (CIMS), where the management of information and access control rules are stored in the so called Control Information (CI) database. From the point of view of the processing workload, the bottleneck is the CCS, which increases with the number of clients/users. This is not an unrealistic assumption, because, generally, the communication rate among clients and servers is high.

The alternate model is the CM model, such as DACS. This model is shown in Figure. 19. The CCS and the CI are now distributed within the client machines. After a user logging into a particular client machine, the CI set for that user and that client is extracted from the CIM. The extracted CI is applied to the CCS located onto the client machine, and the control of the communication is performed by the CCS. Compared to the INM model, the CM model differs because a small amount of the CI is distributed into the client machines. In both models, the CI is centrally managed by the CIMS. We see that this little share of information among client machines helps reducing the total workload sustained by the CCS.

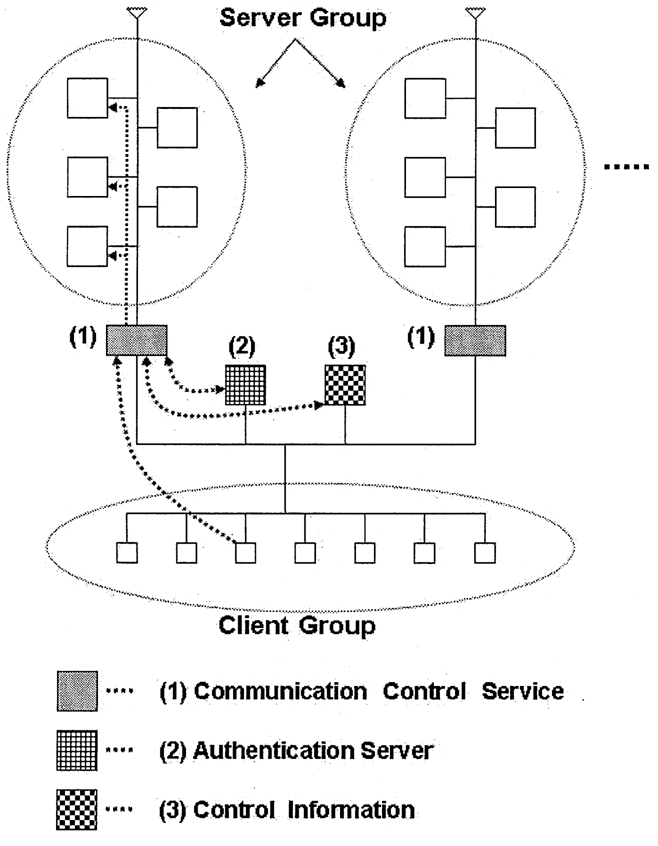

Server Group
(1)
(2)
(3)
(1)
.....
Client Group
▒ .... (1) Communication Control Service
▦ .... (2) Authentication Server
▩ .... (3) Control Information

Figure. 18 Infrastructure Management type model

6.2.2 Analysis of INM and CM Models

In this section, processing workload with respect to the communication control model is analyzed. When the communication between the client software and the network service in these two models takes place, the processing wokload can be divided as follows.

1. Processing by the network service of the requests from client machines.
2. Processing by the client machine of communication controls.
3. Other processing on the client machines.

The processing in 1 and 3 are the same for both models. Therefore, we should only compare the processing in 2 in the INM and the CM model, respectively.

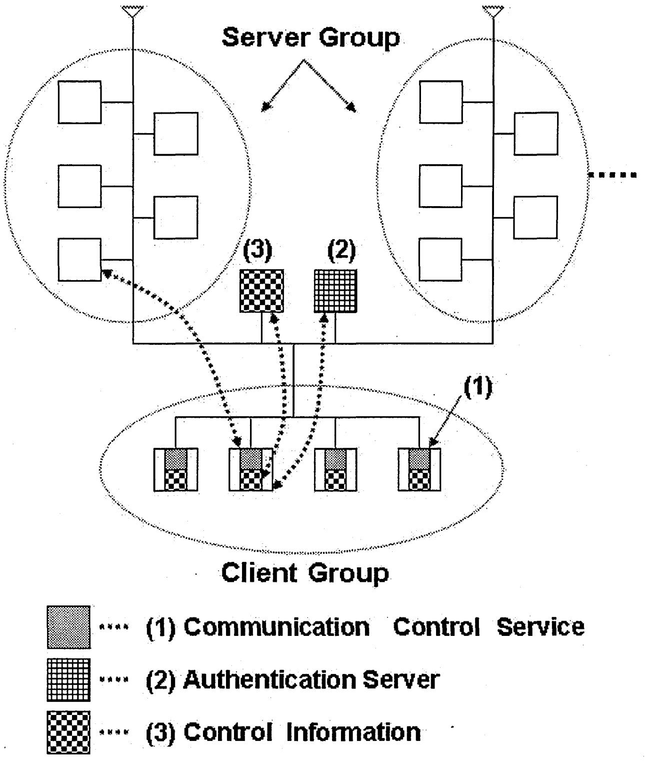

Server Group
(3)
(2)
(1)
.....
Client Group
▨ .... (1) Communication Control Service
▦ .... (2) Authentication Server
▩ .... (3) Control Information

Figure.19 Client Management type model

For instance, the processing workload of the communication control at 1) the CCS and at 2) the client machine. For the analysis, the INM and the CM models are draw as shown in Fig. 20 and Fig. 21, respectively. In both figures, network configuration is the same, except the place of the CCS. Moreover, each network service is referred to as NS1;NS2; : : : ;NSN, where N is the total number of network services. Similarly, CL1;CL2; : : : ;CLM represent the clients, where M is the total number of clients. The processing workloads due to communication between the network services and the clients are represented by p1; : : : ; pN. Other processing workload are kept unchanged, e.g. those of the clients and those of the network services. Then, processing performance of each server where each network service is located on, is the same, and processing performance of each client is also the same. Hereinafter, we assume that the processing capabilities are the same for every client. Thus, the analysis will focus on a generic client, only.

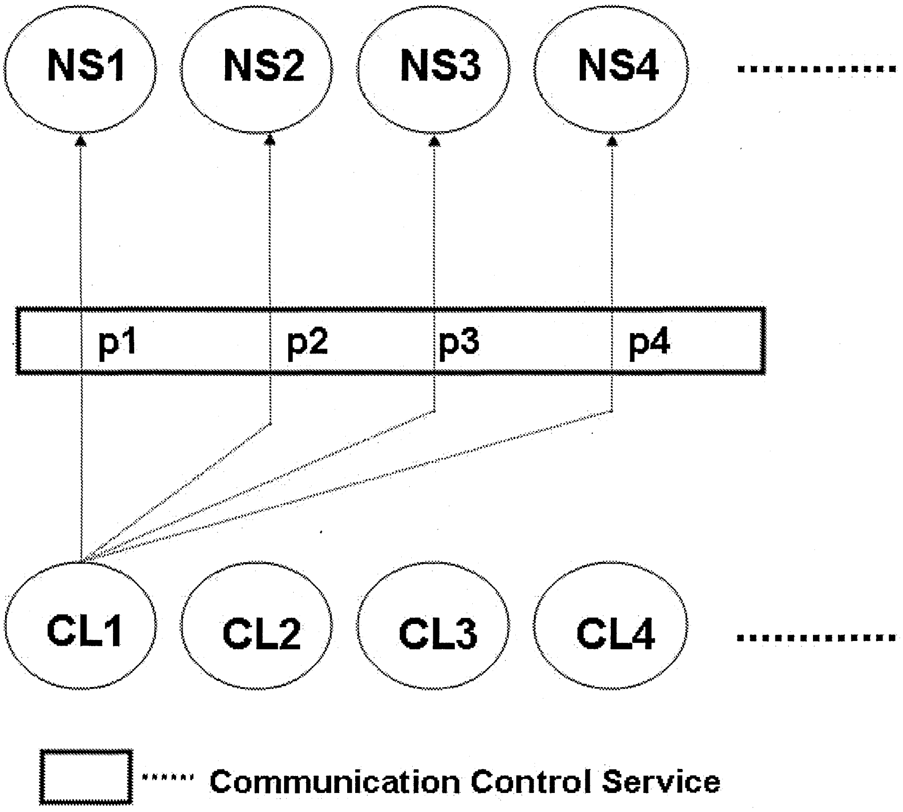


Figure. 20 Processing load in Infrastructure-based Management model

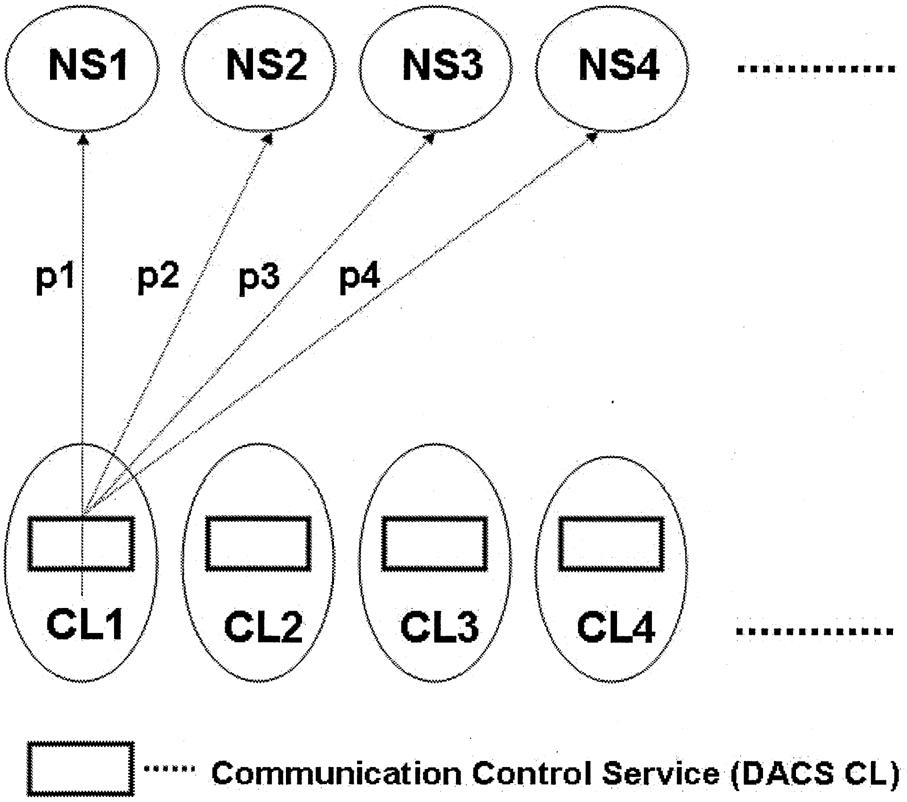


Figure.21 Processing load in the Client Management model

Under these assumptions, it is straightforward to show that the processing load of the INM model is:

$$W_{\mathrm{INM}} = M \sum_{k=1}^{N} p_k \qquad (1)$$

where WINM is the workload.
For the CM model, the processing load occurring in the CCS is now:

$$W_{\mathrm{CM}} = \sum_{k=1}^{N} p_k \,. \qquad (2)$$

The equation in 2 means that the workload is independent of the number of client machines, which is in accord with the CM model. It is clear that the workloads are upper bounded by physical constraints of the hardware of client and server machines. We refer to these upper bounds as UINM and UCM, respectively. Usually, since server machines are more powerful than client machines, UINM = kUCM; k > 1. Then, the processing rates can be defined as:

$$P_{\mathrm{INM}} = \frac{W_{\mathrm{INM}}}{100U_{\mathrm{INM}}}\% = \frac{MW_{\mathrm{CM}}}{100kU_{\mathrm{CM}}}, \quad \text{INM model,} \quad (3)$$

$$P_{\mathrm{CM}} = \frac{W_{\mathrm{CM}}}{100U_{\mathrm{CM}}}\%, \quad \text{CM model.}$$

Equation in 1 is a linear function of the number of clients. That is, given N, i.e. the number of network services requested by clients, WINM increases with M. This is shown also by the line (A) in Figure. 22. Obviously, the processing rate of the CM model is independent of M, as shown also in the line (B) of Figure. 22.

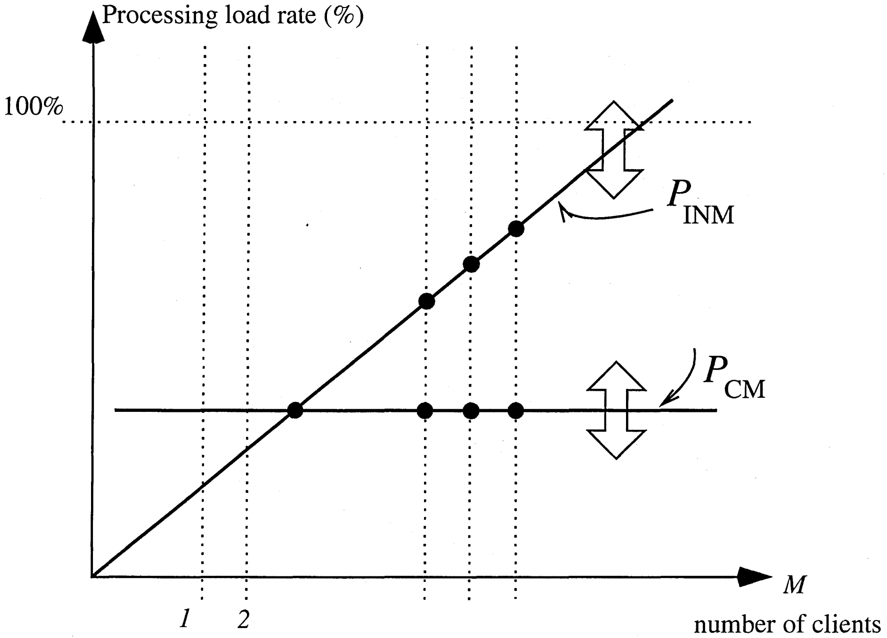


Figure. 22 Comparison of processing load

As final test, we also analyzed the impact of processing load due to the DACS software. In fact, actually we have

$$W_{\mathrm{CM}} = \sum_{k=1}^{N} p_k + \gamma \cdot$$

where γ is due to the processing workload of point 3. That is,

the client machine must sustain the additional workload of the DACS software. It is clear that if the client machine is used without DACS, the line (B) does not move and we conclude that CM model is always better than INM model. However, ° could be as high as to shift up the line (B). In our experiments, carried out on a campus LAN, we verified that always PINM ¸ PCM, for some M ¸ MC, where MC is the crosspoint (C) in Figure. 22. From these preliminary experiments, we are confident that DACS can assure a lower processing workload with respect to other INM-like solutions.

6.3 Conclusion

In this paper, we illustrated a new proposal for network management, where the control is distributed within the client machine pool. So far, the study of DACS framework was mainly about its functionalities, and the evaluation of applying DACS to real networks was not investigated. A legitimate doubt against CM solutions like DACS was that when they are deployed the processing workload could augment. In that direction, we presented a simple comparison of two types of communication control that we called INM and CM model, respectively. For instance, DACS framework fall into the CM models. Instead of compare other solutions with DACS, which could be unfair because of the way they are conceived, we compared the two models, i.e. a network with and without DACS scheme. The analytical evaluations of the processing workload are supported by real experiment in our computer network, and they confirm the fact that the increase of the processing workload is marginal. In particular, it is independent of the number of client machines managed. Future investigations concern the implementation of a more complete system and its evaluation in more real use cases. The optimization of DACS's variables, such as the value of the timers used by the server for checking procedure, is another important aspect to be investigated, because the response time of applications running on top of DACS depends on the delay the DACS server spends in distributing DACS rules to DACS client. We will investigate this analysis for further studies.

7. Realization of New User Support

7.1 Introduction

As a problem of user support, it is pointed out as follows. When some different network services such as SMTP service and POP3 service on the same server machine are divided into different server machines, that is, when system configuration of a network system is changed, a user has to change host name on a client application by oneself. As another problem of user support, it is pointed out that much time and effort are spent to cope with annoying communication such as virus infection under the management by DHCP [38]. The word of "annoying communication" means the communication which adversely affects processing performance and communication speed of other clients. There is not any clear evidence which client uses which IP address. In the conventional network scheme, it is difficult to solve these problems well without complicated works by the person. Because it is often necessary to support each user respectively, it takes trouble very much for the system administrator. To solve these problems, new form of user support is proposed and examined. That user support can be realized on the network introducing DACS (Destination Addressing Control System) Scheme. DACS Scheme is a network operation and management scheme for managing a whole network system by communication control of a client. An example of new from of user support is described as follows. First, the way of coping with annoying communication is considered. In conventional method, the user or client to send the annoying communication is specified by a person, and it is carried out to cope with that user or client. However, in the method by DACS Scheme, annoying communication of the client is stopped and the warning message is displayed on the screen of the client. The user who watches the warning message does an inquiry to the computer management section. Because the system administrator does not need to identify that client physically, network management is largely simplified.

To explain the new form of user support, problems of existing user support are described in section 7.2. The new form of user support which is realized by DACS Scheme is explained in section 7.3. In section 7.4, experimental results are shown to confirm the possibility of that new form of user support.

7.2 Problem of Existing User Support

In this section, problems for supporting each user are mainly described by showing examples for user support.

7.2.1 Support at Changing Setups of Client

Support at the time of changing setups of a client is described. When some different network services such as a SMTP and POP3 service on the same server machine are expected be divided into separate server machines, a user has to change setups of a client. When the same host name is being set on the client as the SMTP server name and POP3 server name, the host name of either must be changed. In this case, a notice of changing setups of the client is sent by E-mail, a homepage and a document announcement from a system administrator. The user who accepted the notice usually changes setups of the client by oneself. If changing setups can not be done, the user inquires to the network management section, and the system administrator replies those inquires through telephone. If the user can not change still, the system administrator goes to the place which the client exists and changes setups of the client.

If the system administrator can change the communication server for same host name under the central control freely and easily, the user does not need to change setups of the client.

7.2.2 Coping with Annoying Communication

It is pointed that, much time and effort are spent to specify which client or user is transmitting annoying communication, when DHCP service is used. As an example of annoying communication, the communication which is sent from the client infected by virus is considered. In this case, the source IP address of annoying communication is specified first. Next, the client having that IP address is found out as the virus infection client by a user or system administrator, and identified which user used that client. The main point of this process is shown as following. If an IP address is dynamically managed using DHCP service, the IP address of the client may be changed according to the lease period of an IP address and the use situation of the client (the period to next use). Therefore, the IP address of the client is not necessarily grasped. As the result, after the source IP address of annoying communication is specified by the network management section, the client having that IP address must be specified among many clients by the user or system administrator. If this process for specifying the virus infection client is simplified, the burden for the user and system administrator is reduced.

As another example, the communication problem using UDP (User Datagram Protocol) such as streaming of the moving picture and the sound which may generate the congestion of the network [39] is described. The congestion of the network becomes the cause of holding down the communication using TCP (Transmission Control Protocol). To cope with this problem, it is necessary to specify which user is using the client at that time. About this point, it can not be specified easily in the scheme of the conventional network. There is no guarantee that the user can certainly be specified. If the user can be specified just after capturing the annoying communication, it is easy to cope with it. Further, if it is possible for the system administrator to block the communication by intensive management of the client, annoying communication is able to be blocked temporarily without specifying the place where the client is physically. To cope with these problems described in the above, the new form of user support by DACS Scheme is examined.

7.3 New Form of User Support

In this section, the process (Stage1) for introducing DACS Scheme and new form of user support (Stage2) after introducing DACS Scheme are described.

7.3.1 Process of Introducing DACS Scheme (Stage1)

As an example of introducing DACS Scheme in the university network, the process of introducing DACS Scheme into the laboratory is described as shown in Figure23. At first, the policy for using a laboratory network is determined by discussion of a network management section and a laboratory (1). At this point in time, permission or disapproval for the use of each network service, and communication server for each network service, that is, the contents of DACS rules, are decided. In the side of the Network management section, DACS rules are registered into DACS Server according to the policy for using a laboratory network (2). In the side of the laboratory, a setup of a client (3) and a setup of DACS Client (4) are performed. After these setups are completed, the operating in DACS Scheme becomes possible. When a client is newly introduced in the operating state, only setups of a client (3) and DACS Client (4) are required in the side of the laboratory. When DACS Scheme is not introduced, the policy for using a laboratory network must be originally decided in the laboratory side. However, it is difficult in the laboratory where the network can not be managed by a technical factor. In introducing DACS Scheme, because the policy for using a laboratory network is reviewed under the cooperation with a network management section, there is a merit for a laboratory. In addition, because the network management along the policy can be realized, there is also a merit for the system administrator.

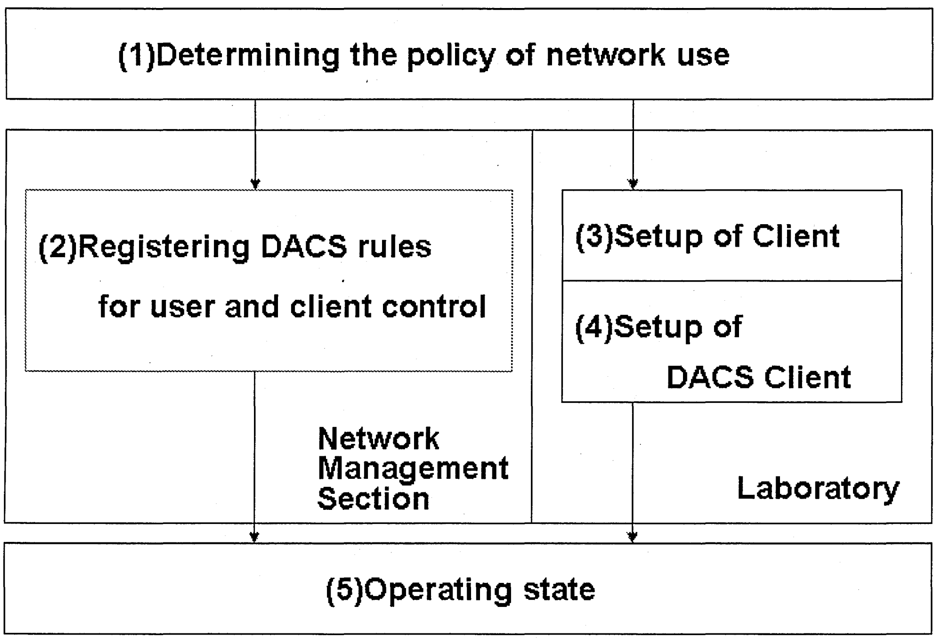

(1)Determining the policy of network use
(2)Registering DACS rules for user and client control
(3)Setup of Client
(4)Setup of DACS Client
Network Management Section
Laboratory
(5)Operating state

Figure 23. Stage1

7.3.2 Process of New User Support (Stage 2)

(1) Support at Changing Setups of Client with DACS Scheme

When network configuration is changed, user support by DACS Scheme is compared with user support by Non-DACS Scheme, and an advantage of user support by DACS Scheme is described. User support processes after changing the network configuration are described in Figure24. When DACS Scheme is not introduced, notification for changing setups is sent to a user in a laboratory (2) after changing the network configuration (1). It is sent by E-mail and a homepage or a document. The user who accepts that notification changes setups of a client (3). If there is no problem in changing setups of the client, it is enabled to start the operating (4). When it is not possible to change setups by some causes, the user inquires to the network management section (5). In the network section, investigation by hearing comprehension for the user or investigation in the field is done (6). If a cause is specified, the coping way are considered, and carried out (7). It is a burden for a system administrator to support each user for every inquiry. When DACS Scheme is introduced, a system administrator has only to change DACS rules (8) at the time of changing the network configuration. After changing DACS rules, communication control corresponding to new network configuration is started at a point in time when the user logs in to a client again (4). Because the system administrator with understanding the policy for using a laboratory network sets DACS rules, a trouble by a cause except an artificial factor such as missing setups of DACS rules does not occur. This process of user support is largely simplified in comparison with the process of user support by Non-DACS Scheme.

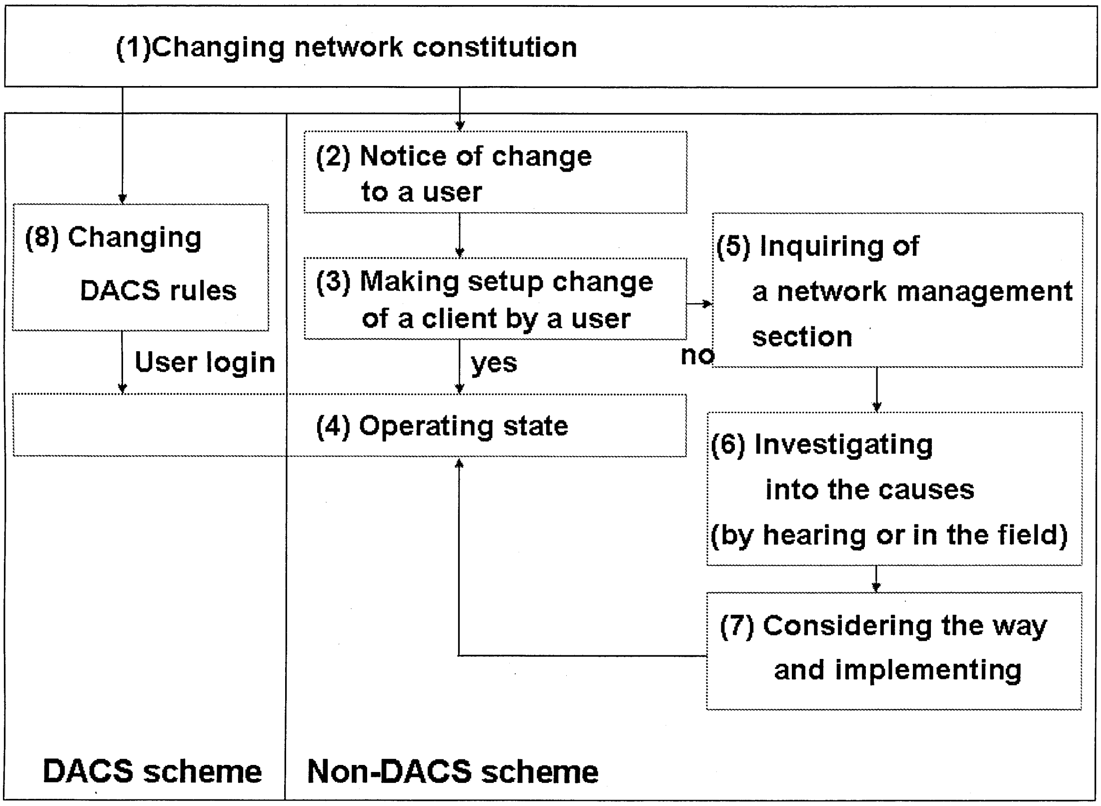
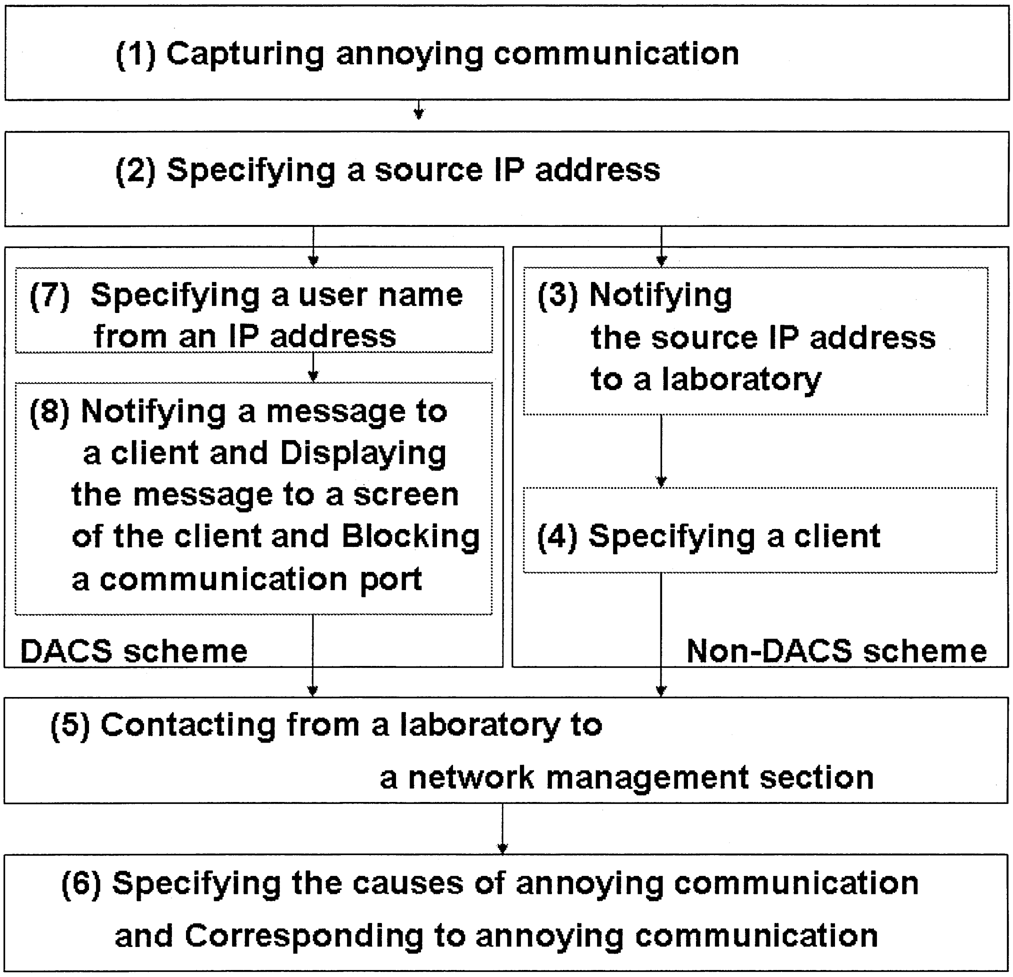

(1)Changing network constitution
(2) Notice of change to a user
(8) Changing DACS rules
(3) Making setup change of a client by a user
(5) Inquiring of a network management section
User login
yes
no
(4) Operating state
(6) Investigating into the causes (by hearing or in the field)
(7) Considering the way and implementing
DACS scheme
Non-DACS scheme

Figure 24. Process introducing DACS Scheme

(2) Coping with Annoying Communication by DACS Scheme

To cope with the communication from a virus infection client and the communication with annoyance to other user such as streaming of moving and sound, a system administrator needs to specify which user or client is transmitting the communication to. For example, when there is a direct cause in the client itself such as virus infection, the client must be specified. A user must be specified, when there is a direct cause in user oneself. When the IP address is managed dynamically by DHCP service, much time and effort is spent to specify the client or user. The coping process for annoying communication is described as shown in Figure25 and explained with an example of the user support for a laboratory. A characteristic of this mechanism is the next two processing on Web Server.

(a) User authentication is performed by user information.
(b) Information related to user is searched and extracted from data which is accumulated beforehand.



(1) Capturing annoying communication
(2) Specifying a source IP address
(7) Specifying a user name from an IP address
(8) Notifying a message to a client and Displaying the message to a screen of the client and Blocking a communication port
DACS scheme
(3) Notifying the source IP address to a laboratory
(4) Specifying a client
Non-DACS scheme
(5) Contacting from a laboratory to a network management section
(6) Specifying the causes of annoying communication and Corresponding to annoying communication

Figure 25. Change of User Support

Processing of (a) is performed after processing of (5) in Figure28. This processing is necessary to perform processing of (b) and becomes essential so that Web Service premises anonymous user. Web page as Personal Portal is generated by the program such as CGI on the Web Server. Because the program is introduced by system administrator and can't usually be changed by a user, the Personal Portal can't always be easy to use for each user or customize for personal use. In this paper, to overcome this problem, two kinds of functions of Web Service based on DACS Scheme, which make each user creates Personal Portal freely and easily, were developed. By using these functions, when each different user inputs same URL on Web Browser, the different information for each user is searched and extracted from database or document medium, and displayed on Web Browser. However, in these functions, it is possible only to send and accept information by a user unit. Because it is necessary to send and accept information by a group unit and by all users unit, these functions are insufficient. In addition, these two kinds of functions are independent with each other. So, to use in actual network, these two kinds of functions need to be integrated as one service, and integrated interface needs to be brought to each user. Therefore, after extending these two kinds of functions of Web Service to send and accept information not only by a user unit, but also by a group unit and by all users unit, DACS Web Service, is proposed, which is realized as the result of having integrated these extended two kinds of functions of Web Service.

At first, annoying communication for other users is captured by communication detection through the mechanism such as F/W or IDS (1). Next, a source IP address of the annoying communication is acquired (2). To here, it is the same thing when DACS Scheme is introduced or not introduced. When DACS Scheme is not introduced, the process of user support is described in the following. Under using DHCP Service, if a whole network is divided into multiple subnetworks, and each subnetwork is assigned to each laboratory, a system administrator can manage scope of the IP address used in a laboratory. If not so, the system administrator can not manage it. In the case of the former, the IP address is notified to the laboratory (3), and the client transmitting the communication is specified (4). In the laboratory, because it is impossble to manage which client uses which IP address, the client is specified after investigating the network setups information of each client. It takes trouble very much. In the case of the latter, it is difficult to specify the client. This is because the system administrator can not know the laboratory using the IP address. Even if the system administrator can know it, because it is needed to investigate the network setups information of each client, it takes trouble very much. After the client is specified, the user of the laboratory contacts a network management section (5). In the situation that a laboratory cooperates with a network management section, the cause specification of annoying communication and coping with it are done (6). On the other hand, when DACS Scheme is introduced, source IP address of the annoying communication needs to be acquired (2) to specify the client first. When a user needs to be specified, a user name is specified from the IP address (7). When a user has a direct cause such as streaming of the moving picture and the sound, the message to notify abnormality is transmitted to the IP address of the client which a user logs in. If a client has a direct cause such as infection by virus, the message to notify abnormality is transmitted to the IP address of the client. The message is displayed in the screen of the client. At the same time, the used port by annoying communication is blocked (8). The user sees the message of the screen, and contacts the network management section (5). In the situation that a laboratory cooperates with a network management section, specification of annoying communication and coping with it are done (6). It is shown that DACS Scheme is effective at the following two points. The first point is that the client which transmits annoying communication is specified simply. The client which has a problem is specified by seeing the message of a screen at a glance. The second point is shown as follows. Because the influence to others is prevented by blocking a communication port of the client, time margin for the cause specification of annoying communication and the coping with it is generated effectively. When the urgent degree such as virus infection is high, DACS Scheme is particularly effective.

7.4 Functional Experiment and Experimental Result

To realize new form of user support as shown in the previous section, the functions from (a) to (c) as follows are needed.

(a)The function of changing destination for one host name by a system administrator

(b)The function of blocking the communication form the client by a system administrator.

(c)The function of displaying the message sent from a system administrator on the screen of a client.

To simplify the support at the time of changing setups of a client, the function of (a) is needed. Then, to cope with annoying communication simply, the functions of (b) and (c) are needed. Because the functions of (a) and (b) are basic functions of existing DACS Scheme, the possibility of these functions has been already confirmed. Therefore, only the possibility of the function of (c) needs to be confirmed. To confirm the possibility of the function of (c), prototype system was built as shown in Figure26. The configuration of this prototype system is described as follows from (1) to (3).

(1)Server Machine

CPU:Celeron M Processor340(1.5GHz)
OS:FedoraCore3
Language:JAVA(DACS Server)
Database:PostgresSQL

(2)Client Machine

CPU:Celeron M Processor340(1.5GHz)
OS:FedoraCore3
Language:JAVA(DACS Client except DACS Control)
others:Netfilter (DACS Control)

(3)Others

Authentication Server:OpenLDAP-2.1.22-8(FedoraCore1)
DHCP Server:Microsoft DHCS Server(WindowsNT4.0)

DNS Server:bind-9.2.2.P3-9(FedoraCore1)

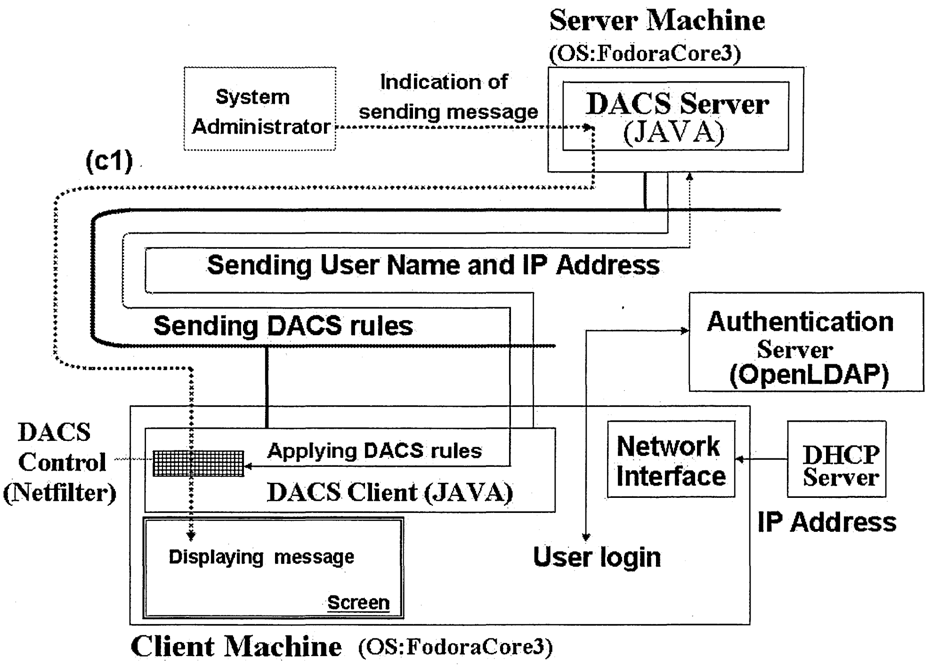
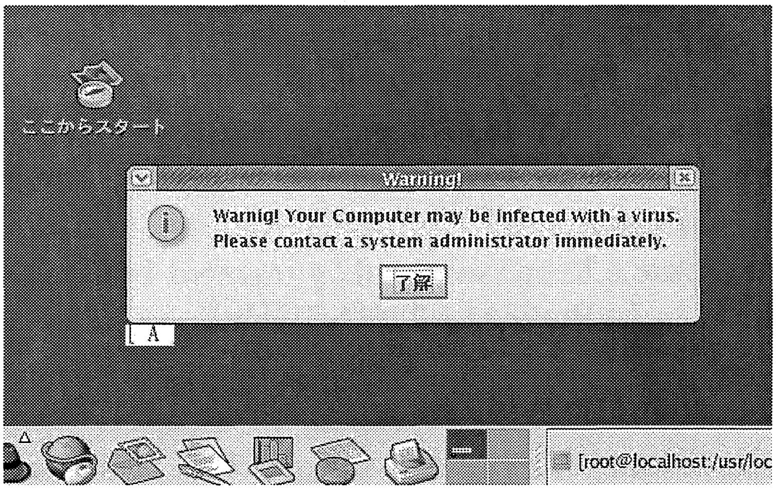


Figure 26. Prototype System

Because DACS Server knew the IP address of a client and user name logging in that client, a system administrator could send messages to the target user and client as shown in (c1) of Figure26.



Warnig! Your Computer may be infected with a virus.
Please contact a system administrator immediately.

Figure 27. Window Results of the Message from System Administrator

In Figure27, the experimental result is shown. The message of "Warning! Your computer may be infected with a virus. Please contact a system administrator immediately." was displayed on the screen of a client. Because the possibility of the function of (c) was confirmed, the possibility of new form of user support was confirmed.

7.5 Conclusions

In this section, new form of user support in university network was examined. As an example, a support for the laboratory was described. To be concreted, the support in the case of changing setups of the client and coping with annoying communication were described. In those case, it took trouble very much for a network management section, because much time and effort were spent. Therefore, the new form of user support by DACS Scheme was proposed and examined. In comparing the user support by DACS Scheme with the user support by Non-DACS Scheme, it was shown that the process of user support by DACS Scheme was simple and effective.

8. Realization of New Network Service

8.1 Introduction

Web pages are often used as communication means other than E-mails and telephones. As a communication mean, static Web pages are used. Static Web pages are often used as a communication mean for the unspecified number of users, and are unsuitable to communicate among respective individual users for respective purposes or interests. As another communication mean, Personal Portal realized by Web Service which can change the contents of Web page by a user unit dynamically, is used. The word of "Web Service" used in this paper, is different from "Web

Services" which is defined in W3C [40], and means the network service which is provided to users through Web Server. Moreover, though the word of "Portal" often indicates Web page for information searching [41] [42] such as Google and Yahoo, the word of "Personal Portal" used in this section is different from "Portal". "Personal" Portal indicates the entrance where each user can acquire his/her interested information on the network, and can display the different information for respective individual users on Web Browser dynamically by using the program such as CGI [43]. Therefore, Personal Portal is suitable to communicate among respective individual users for respective purposes or interests. To display the necessary information for individual user on Web Browser, that information is searched and extracted from databases on the network, and notified to each user by the program such as CGI. When each database is distributed on the network, the program to pick up the information from each database, will be large-scaled and complicated. Because the program is introduced by a system administrator and can't be changed by a user freely, Web page as Personal Portal is not always useful for each user. To solve this problem, new form of Personal Portal, which each user can create and customize freely and easily, is needed. To realize Personal Portal such as this, DACS Web Service is proposed and examined. DACS Web Service is realized by extending two kinds of functions of Web Service, which is realized on the network introducing DACS Scheme. Two kinds of functions of Web Service are described as follows. The first function of Web Service is that, data which is stored in database dispersed on the network, can be used efficiently. The second function of Web Service is that, data which is stored in document medium as PDF file and simple text file, can be used efficiently. By using both functions, when each different user inputs same URL on Web Browser, the different information for each user is searched and extracted from database or document medium, and is displayed on Web Browser. By implementing various kinds of URL into a static HTML file, each user can create and customize Personal Portal freely and easily. That is, by letting these two kinds of functions of Web Service coexist, the service which a user can use information on the network regardless of information storage form is realized. However, in actual network, function of sending and accepting information not only to a specific user but also to grouped users and all users, is also necessary. By extending two kinds of functions of Web Service respectively, DACS Web Service with those functions is realized. DACS Web Service has the characteristic of using data stored in database or document medium with integrated interface for a user, and of sending and accepting information by a user unit, by a group unit and by all users unit. By using this DACS Web Service, each user can create and customize Personal Portal for oneself freely and easily regardless of information storage form such as database and document medium.

In this paper, the problem of existing Personal Portal is described. To explain DACS Web Service, from section 8.3 to 8.5, two kinds of functions based on that DACS Scheme, system configuration by these functions to realize the customized Personal Portal, are shown. In section 8.6, DACS Web Service is proposed. In section 8.7, experimental results to confirm the possibility are explained.

8.2 The Issue on Mechanism of Existing Personal Portal

So far, various researches have been performed on Personal Portal [44] [45]. In addition, it is possible to realize Personal Portal by a commercial product. In both cases, basic mechanism, which is processed in the sequence from (1) to (9), is shown in Figure28. An arrow of a dotted line in Figure28, the movement which user performs for Web Browser is shown. Also, an arrow of a solid line shows processing movement.

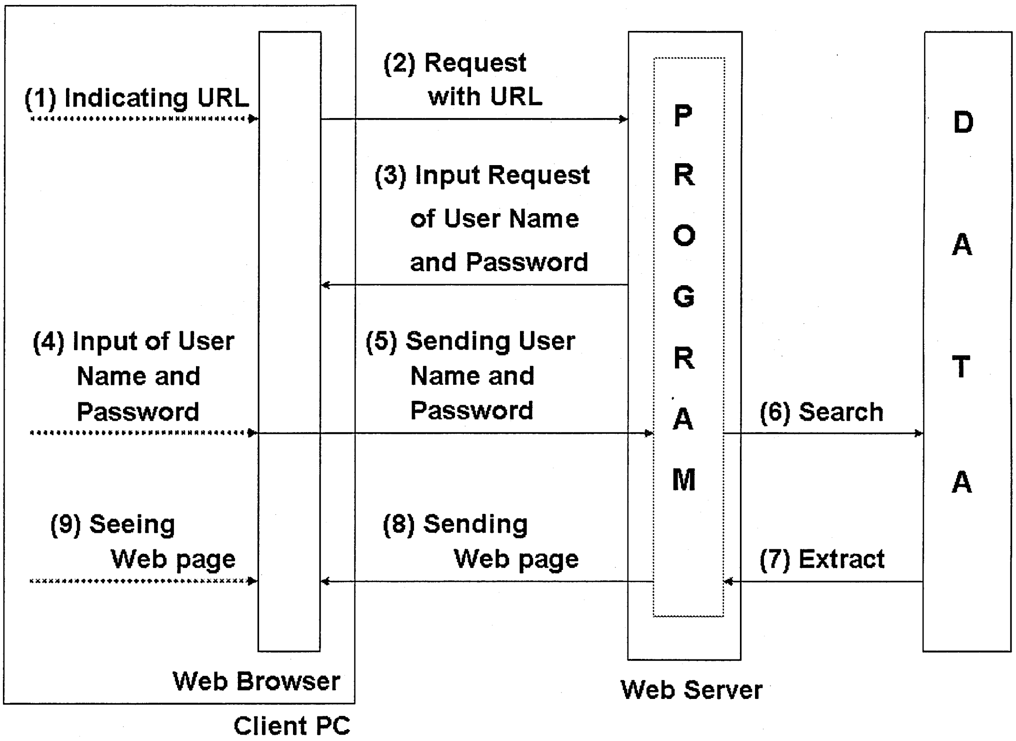


Figure 28. Basic Mechanism of Existing Personal Portal

From here, this mechanism is explained along the movement. User inputs URL into a Web Browser (1). Then, Web Server corresponding to URL is accessed (2) and the program corresponding to URL is executed. At that time, since the program in Web Server side does not grasp user information (a user name and a password), the input demand of user information is performed on Web Browser side (3). Then, user inputs user information (4) and it is sent to the program on Web Server (5). In existing mechanism, user authentication is performed at this point. As the result, if an access is permitted, the information related to user is searched from the data which is accumulated beforehand (6). To accumulate the data, there is a method with relational database or a method with text file for example. It may not be accumulated on one server. It can be accumulated on the plural servers on the network. After the search, data related to each user is extracted (7). The Web Server side program such as CGI which received the data, generates Web page dynamically from the data, and Web page is sent to Web Browser side (8). It is possible for each user to see the information related to oneself, that was displayed in the form of Web page (9).

8.3 Function to Use Data from Database

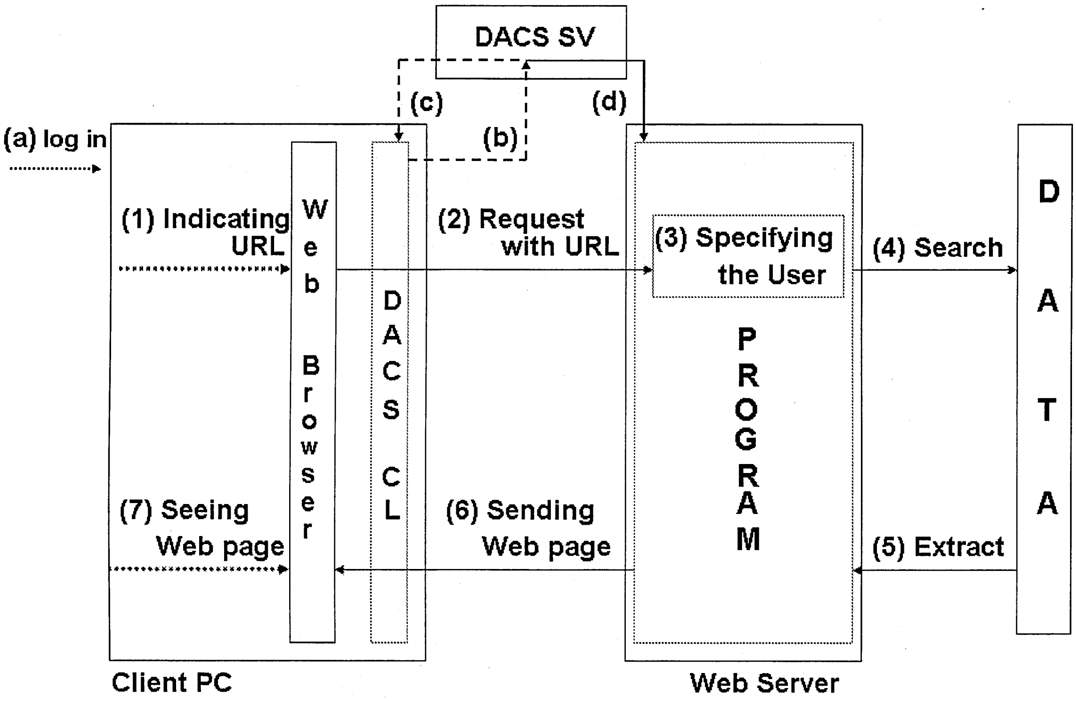


Figure 29. Function to Use Data from Database

At First, the function to use data from database [46] is developed. To realize this function, DACS Scheme needs to be extended, and the program on Web Server needs to be implemented in correspondence to the extended DACS Scheme as shown in Figure29. In existing DACS Scheme, after a user's logging in a client (a), user name and IP address are sent to DACS SV (b). Then, DACS rules are sent back to DACS CL (c). In the extend DACS Scheme, moreover, user name and IP address are sent to the program on Web Server. A characteristic of extended DACS Scheme is that, the server side program on Web Server identifies the user by checking the login information and the source IP address from the client, and the processing of the program is different for each user. When each different user accesses the program with same URL, different information for each user can be searched and extracted from database, and be displayed on Web Browser. On extend DACS Scheme such as this, the processing from (1) to (7) is performed.

8.4 Function to Use Data from Document Medium

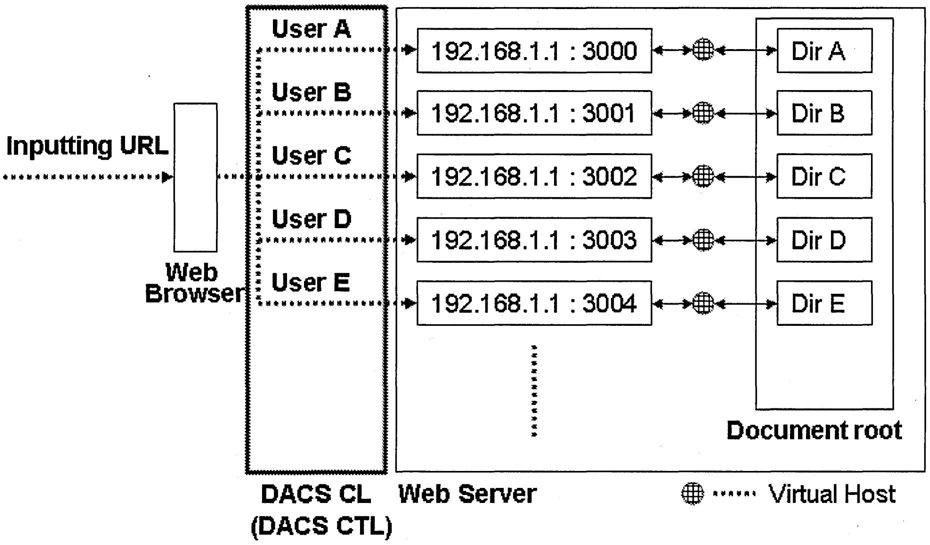


Figure 30. Function to Use Data from Document Medium

Next, function to use data from document medium [47] is developed for the respective user. In the network with DACS scheme, different IP address and TCP port can be assigned for one host name by a user unit. Therefore, different document medium with same file name on different Web Server can be referred for each user by inputting same URL to Web Browser. If this principle is combined with the function of virtual host which is equipped as Web Server, it is possible to use Web Server as shown in Figure30.

8.5 System Configuration of New Portal System

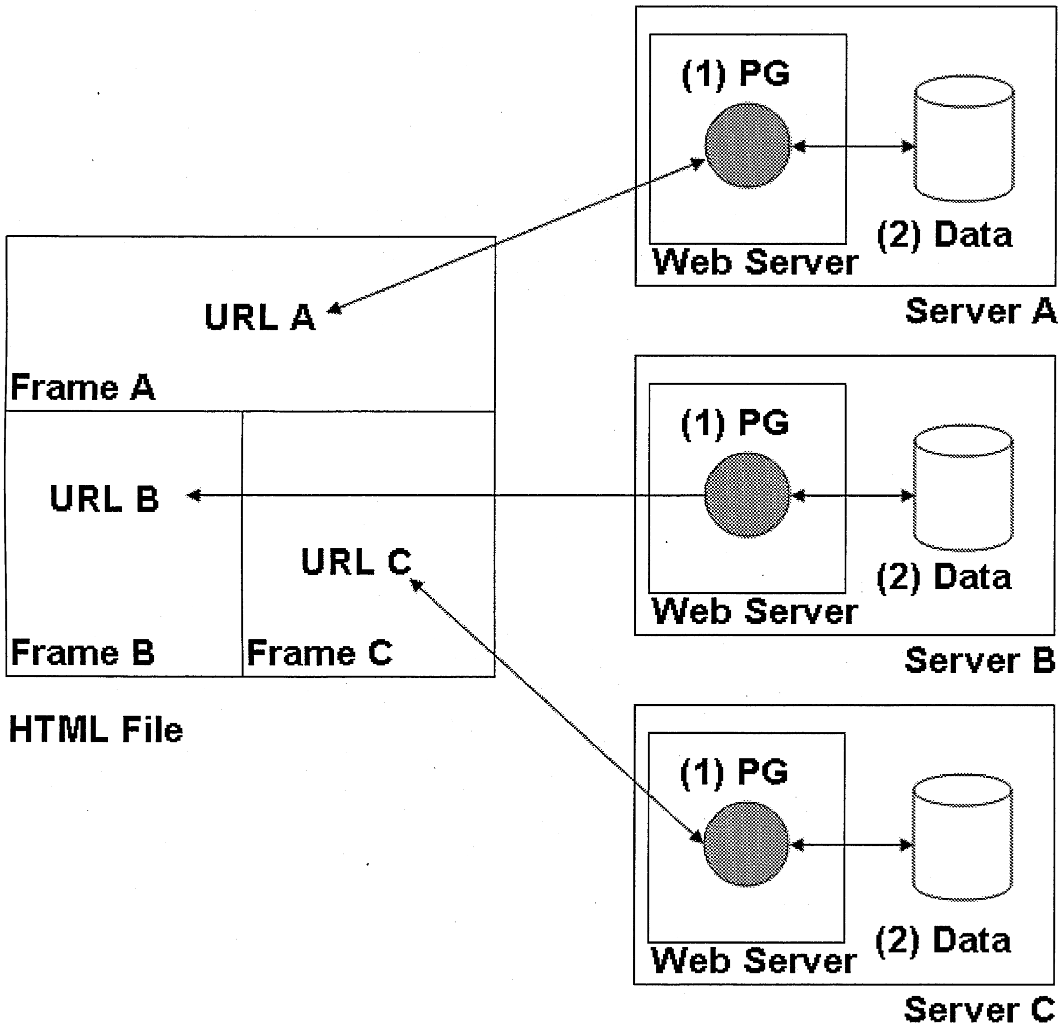


Figure 31. System Configuration of Type1

By using the function to use data from database, the system configuration of Type 1 is enabled as shown in Figure31. First, in Figure31, Server A-C which has programs based on extended

DACS Scheme (1) and data (2), respectively, are distributed on the network. In extended DACS Scheme, information related to user is displayed on Web Browser by only inputting the URL. The following mechanism is built based on this principle. One window of Web Browser is divided into some frames. For example, it is divided into three frames (Frame A-C). The static HTML file with each URL (URLA-C) in each frame is created for displaying Web page as Personal Portal. The static HTML File is put on Web Server or on the client. When the static HTML file is opened through Web Browser, information extracted from each server is distributed on Web Browser. In extended DACS Scheme, URL corresponding to each server is only incorporated in the static HTML file. Thus, if the static Web page is created, user can create the customized Web page as Personal Portal easily.

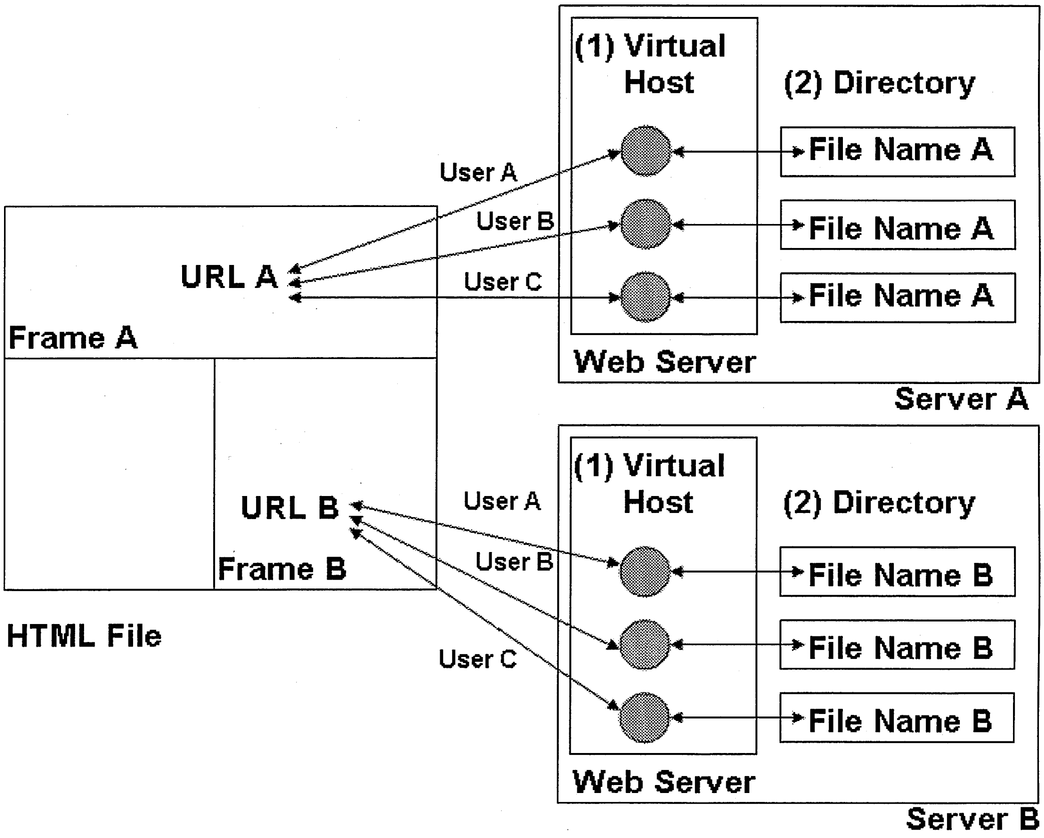


Figure 32. System Configuration of Type 2

The system configuration of Type 2 as shown in Figure32 can be realized by using the function to use data from document medium. Each URL (URL A,B) is prepared. URL and the kind of information which can be seen after inputting the URL to Web Browser are notified to users. For example, URL for acquiring an issue in one classroom and URL for communicating from office to each individual user is enumerated as a kind of URL. By inputting URL to Web Browser, the file with same name (File Name A or B) is referred. The file is stored in each directory for each user. Each user can see the file which is stored in the directory for oneself. In other words, each user can see the information to oneself. Therefore, the customized Personal Portal with static HTML File same as Type 1 can be created.

8.6 DACS Web Service

In section 4, synopsis of DACS Scheme was explained. In addition, two kinds of functions of Web Service which could be realized in DACS Scheme or extended DACS Scheme, and system configuration by these two kinds of functions to realize the customized Personal Portal, was explained. Because these functions of Web Service are used to send and accept information by a user unit, it is not enough to create the customized Personal Portal for using in actual network. Three functions which are shown in the following, are needed.

(1) Function to send and accept information by a user unit
(2) Function to send and accept information by a group unit
(3) Function to send and accept information by all users unit

Among these three functions, the function to send and accept information by a group unit and by all users unit doesn't exist. Therefore, in this section, those two kinds of functions of Web Service are integrated after extending the function to cover this insufficient point. DACS Web Service, which is realized by the integrative function, is proposed to realize Personal Portal for using in actual network.

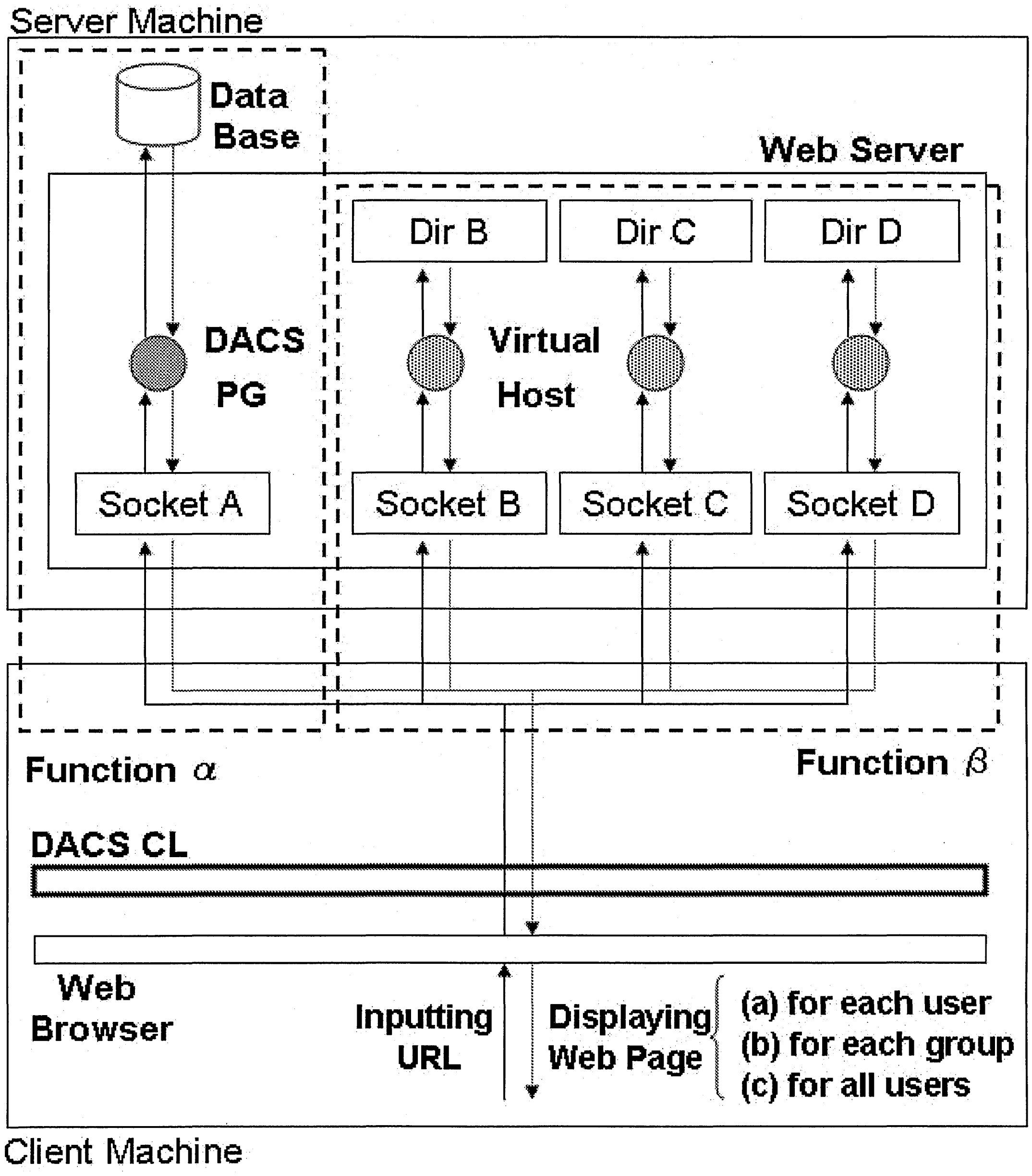


Figure 33. DACS Web Service

8.6.1 Perspective of the DACS Web Service

In Figure33, synopsis of DACS Web Service is shown. The function to use data from database of information system such as a system managing results for a student, is shown as Function α. The function to use data from document medium such as a simple text file and PDF file, is shown as Function β. After a user's inputting URL into Web Browser, communication control by DACS CL (DACS CTL) is performed. As the result, function α or Function β is used. Because the function of either is automatically selected every each URL according to DACS rules, a user can use data from information system or document medium dispersing on the network without being conscious of which function is used. In other words, a user can use information regardless of storage form and storage place of data freely and easily, if a user knows URL and the kind of information acquired by that URL. Even if whichever of Function α or Function β is used, data is displayed on Web Browser after inputting URL. Three kinds of data, which are sent by a user unit (a) and by a group unit (b) and by all users unit, are displayed.

8.6.2 Practical Function to Use Data from Database (Function α)

In Figure34, the content of Function α is shown. Function α extends the function of using data form database by a user unit (Function α1 in Figure34. After extension, data can be used by a group unit(Function α2 in Figure34, and by all users unit (Function α3 in Figure34. There are differences among Function α1, Function α2 and Function α3 in the program extracting data of database for a request from Web Browser. In the program of Function α1, data is extracted by a user unit as shown by (1). In the program of Function α2, data is extracted by a group unit as shown by (2). In the program of Function α3, data is extracted by all users unit as shown by (3).

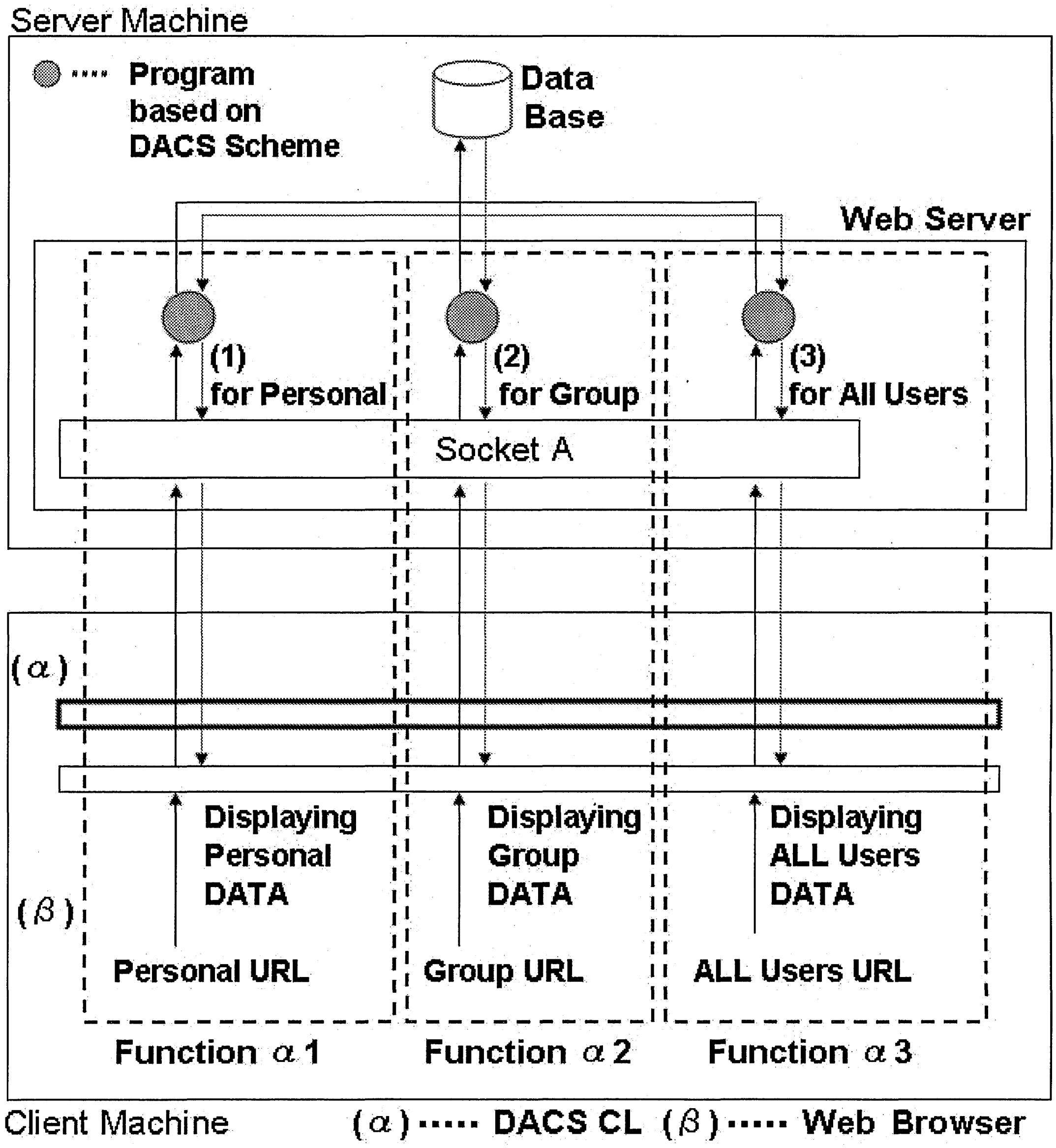


Figure 34. Content of Function α

In the existing function to use data from database as shown by (1), it is possible to specify which user sends communication through Web Browser. Therefore, the function is extended to set a correspondence list of user name and group name in DACS SV and send that correspondence list from DACS SV to the program of Function α2. As the result, because the program of Function α2 can know the group which a user belongs to , it is possible to extract information by a group unit. Even if a user belongs to multiple groups, it is possible to extract data of all groups. In addition, it is possible to extract data of a specific group by sending its group name as a parameter of URL. In the program of Function α3, data is extracted by all users unit. Because it is the function as normal Web Service not introducing DACS Scheme, it is realized without a technical problem normally.

8.6.3 Practical Function to Use Data from Document Medium (Function β)

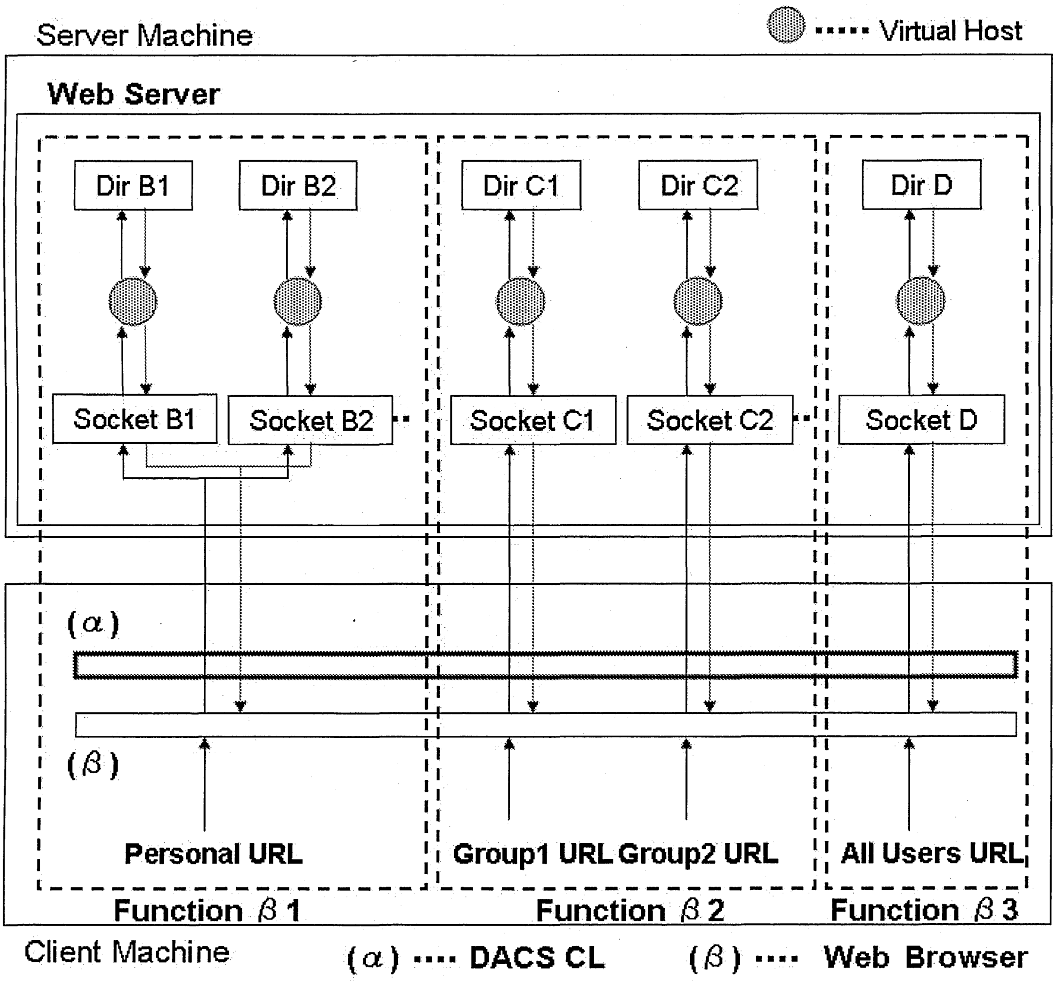


Figure 35. Content of Function β

In Figure35, the content of Function β is shown. In the Function β1, data of document medium is displayed dynamically by a user unit. The function by a group unit and the function by all users unit are realized by the same mechanism of Function β1. URL for each group (Group URL1,Group URL2....) and URL for all users (All Users URL) correspond with each document medium, which is stored in each directory (Socket C1,Socket C2,Socket D), via each Virtual Host. To send information, only uploading a file as document medium into the predetermined directory (directory for each user, directory for each group, directory for all users) is needed. Information for each group can be accepted by use of URL for each Group. In addition, if a user's access is not permitted by DACS rules, it is not possible for the user not belonging to that group to access information by use of that URL. Information for all users can be accepted by use of URL for all users. By using DACS Web Service, not only information for each user but also information for each group and for all users, can be used from document medium.

8.7 Functional Experiment and Experimental Results

To confirm the possibility, the functional experiments by prototype construction were done as shown in Figure36. The details of system configuration are described as following from (1) to (4).

(1)Server Machine
CPU:Celeron M Processor340(1.5GHz)
OS:FedoraCore3
Language:JAVA(DACS Server)
Database:PostgresSQL

(2)Server Machine2

CPU:Celeron M Processor340(1.5GHz)

OS:FedoraCore3

Tomcat:tomcat-4.1.27-14

Apache:httpd-2.0.49-4

Database:postgresql-7.4.2-1

(3)Client Machine

CPU:Celeron M Processor340(1.5GHz)

OS:FedoraCore3

Language:JAVA(DACS Client except DACS Control)

others:Netfilter (DACS Control)

(4)Others

Authentication Server:OpenLDAP-2.1.22-8(FedoraCore1)

DHCP Server:Microsoft DHCS Server(WindowsNT4.0)

DNS Server:bind-9.2.2.P3-9(FedoraCore1)

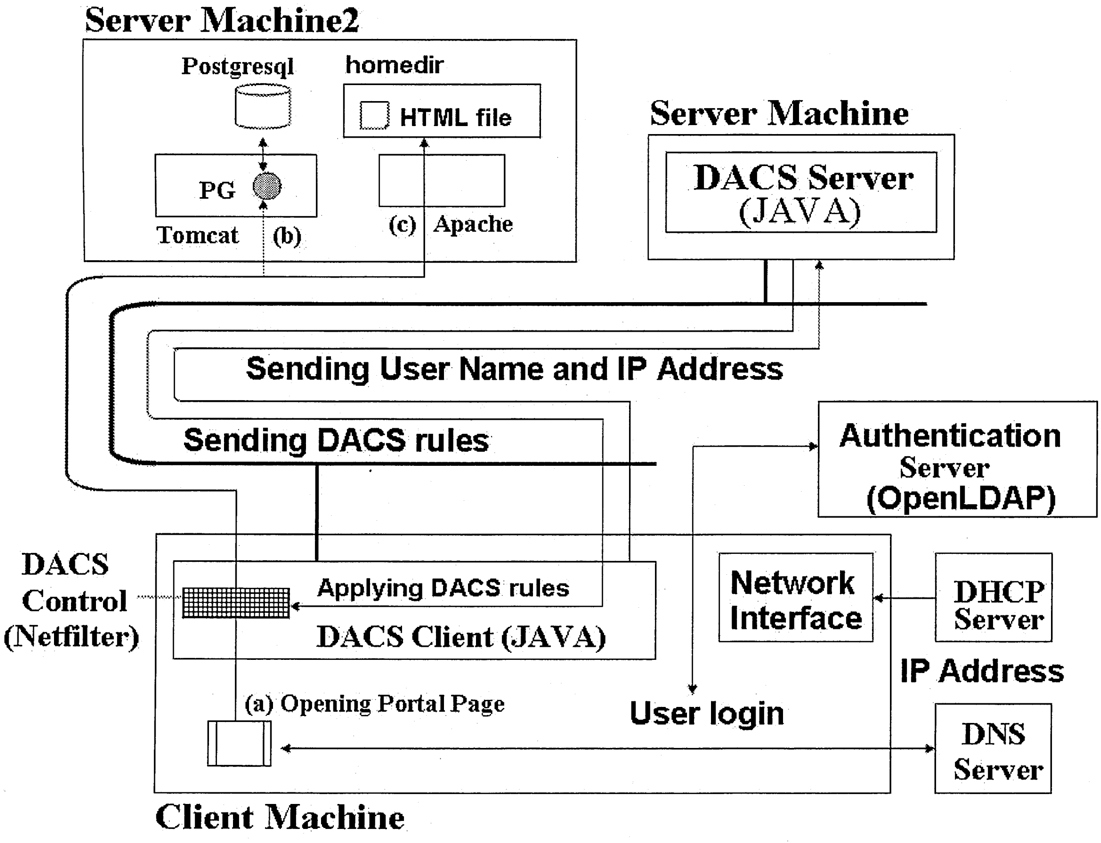
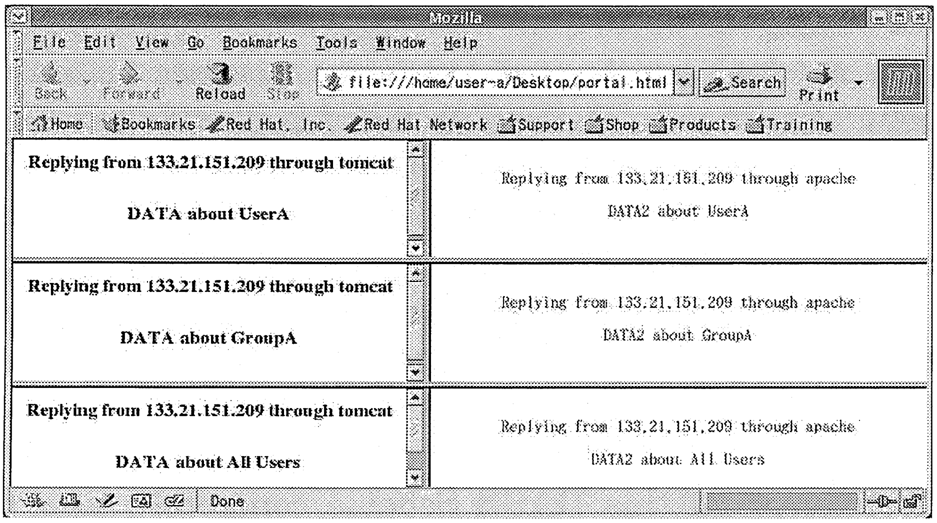


Figure 36. Prototype System

The movement of this system is explained. First, three URLs for accessing the function to use data from database by a user unit, by a group unit, by all users unit and three URLs for accessing the function to use data from document medium by a user unit, by a group unit, by all users unit, are implemented into the static HTML file located on a client machine. When that static HTML file as Personal Portal is opened as shown in (a) of Figure36, the data which is extracted from database, is displayed on Web Browser through the program on Tomcat as shown in (b) of Figure36. The content of static HTML file which is stored into home directory, is displayed on Web Browser through Apache as shown in (b) of Figure36. By using this system, the following experiments were done. First, when the static HTML file as Personal Portal was opened after UserA's logging in a client, the page as shown in Figure37 was displayed on Web Browser. The left side three frames of that page are explained. Date stored in database for UserA, that is, character string of "DATA about UserA" was displayed in the top frame. Date stored in database for GroupA where UserA belongs to, that is, character string of "DATA about GroupA" was displayed in the middle frame. Date stored in database for All users, that is, character string of "DATA about All Users" was displayed in the bottom frame. Moreover, the right side three frames of that page are explained. The content of static HTML file stored in home directory for UserA, that is, character string of "DATA2 about UserA" was displayed in the top frame. The content of static HTML file stored in home directory for GroupA where user A belongs to, that is, character string of "DATA2 about GroupA" was displayed in the middle frame. The content of static HTML file stored in home directory for all users, that is, character string of "DATA2 about All Users" was displayed in the bottom frame. Next, when the HTML file as Personal Portal was opened after UserB's logging in a client, in the same way as the case that UserA logged in to, the data related to UserB was displayed on each frame of Web Browser. In this experiment, the function to use data from database by a user unit, by a group unit, by all users unit and the function to use data from document medium by a user unit, by a group unit, by all users unit, are located on the same server machine. However, even if each function is located on different server machines, it is a same thing. As the result, it was confirmed that, in the form of implementing URLs into a static HTML file, a user could create a web page as Personal Portal for using in actual network easily and freely.


Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
file:///home/user~a/Desktop/portal.html
Search
Print
Home Bookmarks Red Hat, Inc. Red Hat Network Support Shop Products Training
Done

Replying from 133.21.151.209 through tomcat

DATA about UserA

Replying from 133.21.151.209 through apache

DATA2 about UserA

Replying from 133.21.151.209 through tomcat

DATA about GroupA

Replying from 133.21.151.209 through apache

DATA2 about GroupA

Replying from 133.21.151.209 through tomcat

DATA about All Users

Replying from 133.21.151.209 through apache

DATA2 about All Users

Figure 37. Window Result of Portal Page

8.8 Conclusions

In this section, DACS Web Service was proposed to realize the customized Personal Portal for using in the group actually. DACS Web Service is realized by integrating two kinds of functions of Web Service after extending these functions respectively. It has the characteristic of using various kinds of data by a user unit, by a group unit, by all user unit, without distinguishing data stored in database from in document medium. By using DACS Web Service, data dispersing on the network in database or in document medium such as PDF file or text file, can be used as Personal Portal efficiently. From the view point of sending information in the group, it is possible to send information efficiently via DACS Web Service. The reason is why information sending can be realized through document medium. Conversely, from the view point of accepting and using information, data related to each user and to the group to, to all users, are acquired and used freely and easily.

9. General Conclusions

In this paper, first, the content of DACS Scheme which was a new network management scheme was shown. By this DACS Scheme, the whole network is managed through communication control of the client computer by a user unit and a client user unit. The scheme by the idea to control the whole network by a user unit finely was not found except this DACS Scheme. In the DACS Scheme, there was a problem that a network service could be used from the client which didn't have communication control mechanism. Therefore, Secure DACS Scheme which prevented that problem by the functional extension by use of the port forwarding function of SSH was shown. In addition, to exemplify the effectiveness of this DACS Scheme concretely, new form of user support and new portal system which was realized on the network introducing DACS Scheme, were shown. In this new form of user support, the effect to promote efficiency of user support was provided. For example, the correspondence to the annoying communication which was problems in conventional user support was largely simplified. Then, in the new portal system, because each user can create the portal page as user interface to meet one's idea freely and easily, the information was used effectively. Moreover, because not only the data stored in database but also the data stored in the document medium such as Excel file and PDF file was used, it became possible to use the wide range data. As future works, the system development to operate in the real network and the evaluation by that operation will be done.

Acknowledgments

I would like to thank my adviser, Professor Naohiro Ishii for guiding me during my graduate study in Graduate Course of Business Administration and Computer Science, Aichi Institute of Technology. Especially, I was influenced by his attitude toward researches, and his advice encouraged me to research. This thesis owes its shape and content to him.

I also wish to express my deep gratitude to Professor Masaharu Tadauchi in Toyota technological Institute and Associate Professor Rihito Yaegashi in Shibaura Institute of Technology for constructing my framework described in thesis.

List of Publications

(A1) Papers in Journals

[1] Kazuya Odagiri, Nao Tanoue, Rihito Yaegashi, Masaharu Tadauchi, and NaohiroIshii, "User Free Portal System with Practical Web Service in DACS Scheme," IEICE Transactions. (submitted)

[2] Kazuya Odagiri, Nao Tanoue, Rihito Yaegashi, Masaharu Tadauchi, and Naohiro Ishii, "New-Type Access Control Method on the Network Introducting DACS Scheme," IPSJ Journal. (submitted)

[3] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, "Basic Portal System with the Function of Communication Control Every User, " Journal of Convergence Information Technology. (submitted)

[4] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, "New User Support in the University Network with DACS Scheme," International Journal of Interactive Technology and Smart Education. (in printing), 2007.

[5] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, "Secure DACS Scheme," Journal of Network and Computer Applications, Elsevier. (in printing), 2007.

[6] Kazuya Odagiri, Naohiro Ishii, "The Simplification of the User Support Process by DACS Scheme, " Transaction of the Japan Society for Production Management, Vol.4, No.1, pp.157-162, October, 2007.

[7] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, "New Function for Displaying Static Document Dynamically with DACS Scheme, " Int. Journal of Computer Science and Network Security, Vol.6, No.5, pp.81-87, May, 2006.

[8] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, "New Web Service Based on Extended DACS Scheme," Int. Journal of Computer Science and Network Security, Vol.6, No.3, pp.8-13, March, 2006.

[9] Kazuya Odagiri, "New Network Management with DACS Scheme: Study of New User Support Form," Business Administration and Computer Science, The Society of Business Administration and

Computer Science in Aichi Institute of Technology, Vol. 1 ,No. 1 , pp. 1-15, May, 2006.

[10] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, "Efficient Network Management System with DACS Scheme : Management with communication control, " Int. Journal of Computer Science and Network Security, Vol.6, No.1, pp.30-36, January, 2006.

(A2) Papers in Proceedings of International Conference

[1] Kazuya Odagiri, Giuseppe De Marco, Nao Tanoue, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, "Evaluation of the Processing Workload for two Models of Communication Control in IP Networks," The IEEE 22nd Int. Conf. on Advanced Information Networking and Applications (AINA2008), GinoWan, Okinawa, Japan, IEEE Computer Society, March, 2008.(in printing)

[2] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, "Evaluation of Processing Load in the Network with DACS Scheme" , The 10th Asia-Pacific Network Operations and Management Symposium (APNOMS2007), Sapporo, Japan, Lecture Notes in Computer Science, Springer, Vol.4773, pp.555-558, October, 2007. (short paper)

[3] Kazuya Odagiri, Nao Tanoue, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, " New Access Control on DACS Scheme" , Asia-Pacific Network Operations and Management Symposium (APNOMS2007), Sapporo, Japan, Lecture Notes in Computer Science, Springer, Vol.4773, pp.134-143, October, 2007.

[4] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, "DACS Web Service" Int. Conf. on Knowledge-Based and Intelligent Information & Engineering Systems (KES2007), Vietri sul Mare, Italy, Lecture Notes in Computer Science, Springer, Vol.4693, part, pp.995-1004, September, 2007.

[5] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro

Ishii, “Functional Extension for solving the loophole problem of DACS Scheme,” Proc. of Int. Conf. on Software Engineering Research, Management and Applications (SERA2007), pp.315-322, Busan, Korea, IEEE Computer Society, August, 2007.

[6] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, “Efficient User Support with DACS Scheme,” Proc. of Int. Conf. on Software Engineering Research, Management and Applications (SERA2007), pp.323-330, Busan, Korea, IEEE Computer Society, August, 2007.

[7] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, “Information Usage System by Static Portal Page” , Proc of Int. Conf. on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD2007), Vol.1, pp.805-811, Qingdao, China, IEEE Computer Society, July, 2007.

[8] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, “Examination of Processing Load in Applying DACS Scheme to Practical Network” , Proc of Int. Conf. on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD2007), Vol.2, pp.102-107 ,Qingdao, China, IEEE Computer Society, July, 2007.

[9] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, “Practical DACS Web Service for User's Free Portal Page Creation” , Proc, of Int. Conf. on Web Services (ICWS), pp.952-959, July, 2007, Salt Lake City, Utah, USA, IEEE Computer Society, July, 2007.

[10] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, “Extended DACS Scheme implementing Security Function”, Proc. of Int. Conf. on Networking and Services (ICNS’ 07), Athens, Greece, IEEE Computer Society, June, 2007.

[11] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii,“Simplified Network Management with DACS Scheme”, Proc. of Int. Conf. on Networking and Services (ICNS ‘07), Athens, Greece, IEEE Computer Society, June, 2007.

[12] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, “Free Information Usage System on the Network introducing

DACS Scheme" , Proc of Int. Conf. on Internet and Web Applications and Services (ICIW ' 07), Mauritius, IEEE Computer Society, May, 2007.

[13] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, " New Network Management Scheme with Client's Communication Control " , Int. Conf. on Knowledge-Based Intelligent Information and Engineering Systems (KES2006), Lecture Notes in Computer Science, Springer, Vol.4252, pp.379-386, 2006.

[14] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, " Efficient Network Management System with DACS Scheme" , Proc. of Int. Conf. on Networking and Services (ICNS' 06), Silicon Valley, USA, IEEE Computer Society, July, 2006.

[15]Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, "New Network Management System with Communication Control of the Client" , Proc. of Int. Conf. on Computer and Information Science (ICIS2006), Honolulu, Hawaii, USA, IEEE Computer Society, pp.292-298, July, 2006.

(A3) Other Papers

[1] Kazuya Odgairi, Naohio Ishii, "The Simplification of the User Support Process by DACS Scheme," The Japan Society for Production Management,26th Papers for the 26th Conference of the Japan Society for Production Management, pp.89-94.

[2] Kazuya Odagiri, Naihiro Ishii, Rihito Yaegashi, Masaharu Tadauchi,"DACS(Destination Addressing Control System) Scheme for Realizing New Network Service" , Technical Report of IEICE, IN2005-129, pp.1-6, January, 2006.

[3] Kazuya Odagiri, Naihiro Ishii, Rihito Yaegashi, Masaharu Tadauchi, "Suggestion of a client transmission of a address control method to raise the availability of a network service" , Paper at Tokai-Section Joint Conference of Electrical and Related

Engineering, Q-232, 2005.

References

[1] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, " Efficient Network Management System with DACS Scheme : Management with communication control," Int. Journal of Computer Science and Network Security, Vol.6, No.1, pp.30-36, January, 2006.

[2] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, " New Network Management Scheme with Client's Communication Control " , Int. Conf. on Knowledge-Based Intelligent Information and Engineering Systems (KES2006), Lecture Notes in Computer Science, Springer, Vol.4252, pp.379-386, 2006.

[3] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, "Efficient Network Management System with DACS Scheme" , Proc. of Int. Conf. on Networking and Services (ICNS' 06), Silicon Valley, USA, IEEE Computer Society, July, 2006.

[4] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, "New Network Management System with Communication Control of the Client" , Proc. of Int. Conf. on Computer and Information Science (ICIS2006), Honolulu, Hawaii, USA, IEEE Computer Society, pp.292-298, July, 2006.

[5] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, "Secure DACS Scheme," Journal of Network and Computer Applications, Elsevier. (in printing), 2007.

[6] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, "Functional Extension for solving the loophole problem of DACS Scheme," Proc. of Int. Conf. on Software Engineering Research, Management and Applications (SERA2007), pp.315-322 ,Busan, Korea, IEEE Computer Society, August, 2007.

[7] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, "Extended DACS Scheme implementing Security Function", Proc. of Int. Conf. on Networking and Services (ICNS' 07), Athens, Greece, IEEE Computer Society, June, 2007.

[8] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro

Ishii, “New User Support in the University Network with DACS Scheme,” International Journal of Interactive Technology and Smart Education. (in printing), 2007.

[9] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, “Simplified Network Management with DACS Scheme” , Proc. of Int. Conf. on Networking and Services (ICNS’ 07), Athens, Greece, IEEE Computer Society, June, 2007.

[10] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, “DACS Web Service” Int. Conf. on Knowledge-Based and Intelligent Information & Engineering Systems (KES2007), Vietri sul Mare, Italy, Lecture Notes in Computer Science, Springer, Vol.4693, part, pp.995-1004, September, 2007.

[11] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, “Practical DACS Web Service for User's Free Portal Page Creation” , Proc, of Int. Conf. on Web Services (ICWS), pp.952-959, July, 2007, Salt Lake City, Utah, USA, IEEE Computer Society, July, 2007.

[12] Y.Shiraishi,Y.Fukuta,M.Morii,Port randomized VPN by mobile codes, CCNC, pp.671-673,2004.

[13] S.Tadaki, E.Hirofumi,K. Watanabe, Y.Watanabe, Implementation and Operation of Large Scale Network for User’ Mobile Computer by Opengate ,IPSJ Journal ,Vol.46, No.4 pp.922-929,2005.

[14] Y.Watanabe, K.Watanabe, E.Hirofumi, S.Tadaki, A User Authentication Gate-way System with Simple User Interface, Low Administration Cost and Wide Ap-plicability, IPSJ Journal, Vol.42, No.12, pp.2802-2809 ,2001.

[15] http://noside.intellilink.co.jp/product/product_se.asp#Inv

[16] http://www.nec.co.jp/univerge/solution/pack/quarantine/

[17] 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.

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

[19] 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.

[20]http://www.ntt-east.co.jp/business/solution/security/quarantine/index.html

[21] http://www.macnica.net/symantec_sygate/ssep.html

[22] 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.

[23] E.Lupu, D.Marriotto, M.Sloman, and N.Yialelis, " A Policy Based Role Framework for Access Control, " First ACM/NIST Workshop on Role Based Access Control, Maryland USA, ACM,1995.

[24] E.Lupu and M. Sloman, " Conflicts in Policy-based Distributed Systems, " IEEE Transactions on Software Engineering, ,Vol.25 (Special Issue on Inconsistency Management), pp.852-869.1999.

[25] J. Moffett and M.Sloman, " Policy Hierarchies for Distributed Systems Management ," IEEE Journal on Selected Areas in Communcations, Vol.11,pp.1404-1414,1993.

[26]K.Yoshihara, M.Isomura, and H.Horiuchi, " Distributed Policy-based Management Enabling Policy Adaptation on Monitoring using Acitive Network Technology," 12th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management, Nancy France, 2001.

[27] D.Chess, C.Palmer, and S.White, " Security on autonomic computing environment, " IBM SYSTEM JOURNALS, Vol.42, 2003.

[28] N.Badr, A.Taleb-Bendiab and D.Reilly, " Policy-Based Autonomic Control Service ," IEEE 5th International Workshop on Policies for Distributed Systems and Network, New York, June, 2004.

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

[30] J.Chauki,M.M.Shahsavari,"Component-based distributed network management," Proc.of Southeastcon 2000, pp.460-466, IEEE Pub., 2000.

[31] L.Raman,"OSI systems and network management,"IEEE Commun. Mag., vol.36, No.3, pp46-53, Mar, 1998.

[32] C. Metz, :"The latest in virtual private networks: part I," IEEE

Internet Computing,Vol.7, No.1, pp.87–91 ,2003.

[33] C. Metz, :"The latest in VPNs: part II," IEEE Internet Computing, Vol.8,No.3, pp.60–65, 2004.

[34] P. Knight, C. Lewis, :"Layer 2 and 3 virtual private networks: taxonomy, technology, and standardization efforts, " IEEE Communications Magazine,Vol.42, No.6, pp.124–131, 2004.

[35] D.V. Bhatt, S. Schulze, G.P. Hancke, :"Secure Internet access to gateway using secure socket layer," IEEE Tran. on Instrumentation and Measurement, Vol.55, No.3, pp.793–800, 2006.

[36] FirePass Remote Access Controller: http://www.f5networks.co.jp/product/firepass/index.html

[37] SSH : The Secure Shell Connection Protocol, RFC 4254, 2006.

[38] R.Dromos, "Automated configuration of TCP/IP With DHCP, "Internet Computing, IEEE, Vol.3, no.4, pp.45-53, 1999.

[39] H.Hu, J.Kashio, Y.Honda, H.Suzuki, "Rate Control Method for Real Time Protocol (RTP) Enabling the Coexistence with TCP," IEICE Tran. on Communications, Vol.J84-B, No.11, pp.1994-2004, 2001.

[40] http://www.w3.org/2002/ws/

[41] J.Hartmann,Y.Sure,"An infrastructure for scalable, reliable semantic portals," IEEE Intelligent Systems, Vol.19, No.3, pp58-65, 2004.

[42] N.Lowe,A.Datta,"A New Technique for Rendering Complex Portals," IEEE Tran. on Visualization and Computer Graphics, Vol.11, No.1, 2005.

[43] D.Robinson,"The WWW Common Gateway Interface Version 1.1,Internet Draft,"1995.

[44] C.Bouras,V.Kapoulas,I.Misedakis,"Web Page Fragmentation for Personalized Portal Construction," Proc. of the International Conference on Information Technology: Coding and Computing (ITCC'04), Las Vegas, Nevada, USA, IEEE Computer Society, 2004.

[45] N.Hanakawa,Y.Akazawa,A.Mori,T.Maeda,S.Inoue,S.Tsutsui, "A Web-Based Integrated Education System for a Seamless Environment among Teachers, Students, and Administrators,"

Trans. of IEICE,Vol.J88-D-I, No.2, pp.498-507, 2005.

[46] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, " New Web Service Based on Extended DACS Scheme," Int. Journal of Computer Science and Network Security, Vol.6, No.3, pp8-13, March, 2006.

[47] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, " New Function for Displaying Static Document Dynamically with DACS Scheme, " Int. Journal of Computer Science and Network Security, Vol.6, No.5, pp81-87, May, 2006.