Implementation of User Authentication Processes for the Cloud Type Virtual Policy Based Network Management Scheme for the Specific Domain

Kazuya Odagiri[†] **Shogo Shimizu**[††], **Naohiro Ishii**[†††]
kodagiri@sugiyama-u.ac.jp
[†]Sugiyama Jogakuen University, 464-8662, 17-3Hosigaokamotomachi Chiksa-ku,Nagoya, Aichi, Japan
[††]Gakushuin Women's College, Tokyo, Japan
[†††]Advanced Institute of Industrial Technology, Tokyo, Japan

Summary
In the current Internet system, there are many problems using anonymity of the network communication such as personal information leaks and crimes using the Internet system. This is why TCP/IP protocol used in Internet system does not have the user identification information on the communication data, and it is difficult to supervise the user performing the above acts immediately. As a study for solving the above problem, there is the study of Policy Based Network Management (PBNM). This is the scheme for managing a whole Local Area Network (LAN) through communication control for every user. In this PBNM, two types of schemes exist. As one scheme, we have studied theoretically about the Destination Addressing Control System (DACS) Scheme with affinity with existing internet. By applying this DACS Scheme to Internet system management, we will realize the policy-based Internet system management. In this paper, to realize management of the specific domain with some network groups with plural organizations as middle stage, implementation for user authentication processes is performed.

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

1. Introduction

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

In the existing PBNM, there are two types of schemes. The first is the scheme of managing the whole LAN by locating the communication control mechanisms on the path between network servers and clients. The second is the scheme of managing the whole LAN by locating the communication control mechanisms on clients.As the second scheme, we have studied theoretically about the Destination Addressing Control System (DACS) Scheme. As the works on the DACS Scheme, we showed the basic principle of the DACS Scheme, and security function [14]. After that, we implemented a DACS System to realize a concept of the DACS Scheme. By applying this DACS Scheme to Internet system, we will realize the policy-based Internet system management. Then, the Wide Area DACS system (wDACS system) [15] to use it in one organization was showed as the second phase for the last goal. As the first step of the second phase, we showed the concept of the cloud type virtual PBNM, which could be used by plural organizations [16]. In this paper, as the progression phase for the last goal, we implement user authentication processes of the cloud type virtual PBNM for the use in plural organizations. In Section II, motivation and related research for this study are described. In Section III, the existing DACS Scheme and wDACS Scheme is described. In section IV, the results are of implementation is described.

Manuscript received May 5, 2020
Manuscript revised May 20, 2020

2. Motivation and Related Researches

In the current Internet system, problems using anonymity of the network communication such as personal information leak and crimes using the Internet system occur. Because TCP/IP [1] protocol used in Internet system does not have the user identification information on the communication data, it is difficult to supervise the user performing the above acts immediately. However, it becomes possible to use PBNM, which has two types of schemes. The first scheme is the scheme described in Figure 1. The standardization of this scheme is performed in various organizations. In IETF, a framework of PBNM [2] was established. Standards about each element constituting this framework are as follows. As a model of control information stored in the server called Policy Repository, Policy Core Information model (PCIM) [3] was established. After it, PCMIe [4] was established by extending the PCIM. To describe them in the form of Lightweight Directory Access Protocol (LDAP), Policy Core LDAP Schema (PCLS) [5] was established. As a protocol to distribute the control information stored in Policy Repository or decision result from the PDP to the PEP, Common Open Policy Service (COPS) [6] was established. Based on the difference in distribution method, COPS usage for RSVP (COPS-RSVP) [7] and COPS usage for Provisioning (COPS-PR) [8] were established. RSVP is an abbreviation for Resource Reservation Protocol. The COPS-RSVP is the method as follows. After the PEP having detected the communication from a user or a client application, the PDP makes a judgmental decision for it. The decision is sent and applied to the PEP, and the PEP adds the control to it. The COPS-PR is the method of distributing the control information or decision result to the PEP before accepting the communication.

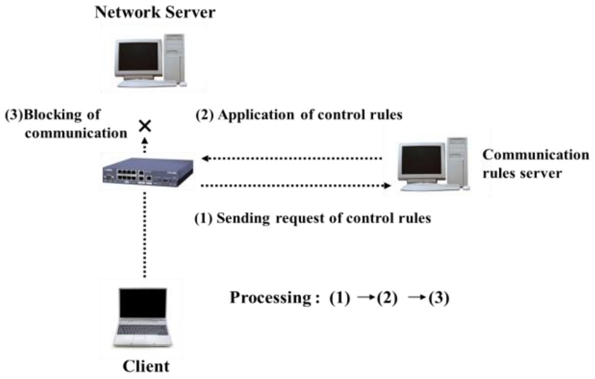

Network Server
(3)Blocking of communication
(2) Application of control rules
Communication rules server
(1) Sending request of control rules
Processing : (1) →(2) →(3)
Client

Fig. 1 Principle in First Scheme

Next, in DMTF, a framework of PBNM called Directory-enabled Network (DEN) was established. Like the IETF framework, control information is stored in the server storing control information called Policy Server, which is built by using the directory service such as LDAP [9], and is distributed to network servers and networking equipment such as switch and router. As the result, the whole LAN is managed. The model of control information used in DEN is called Common Information Model (CIM), the schema of the CIM (CIM Schema Version 2.30.0) [11] was opened. The CIM was extended to support the DEN [10], and was incorporated in the framework of DEN.

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

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

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

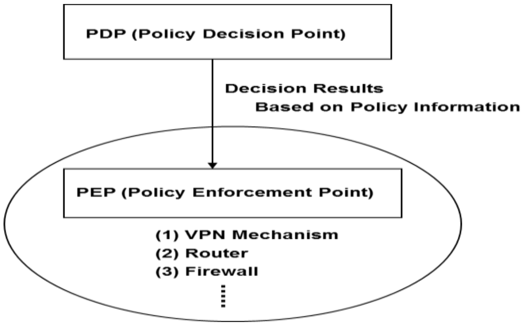

PDP (Policy Decision Point)
Decision Results
Based on Policy Information
PEP (Policy Enforcement Point)
(1) VPN Mechanism
(2) Router
(3) Firewall
⋮

Fig. 2 Essential Principle

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

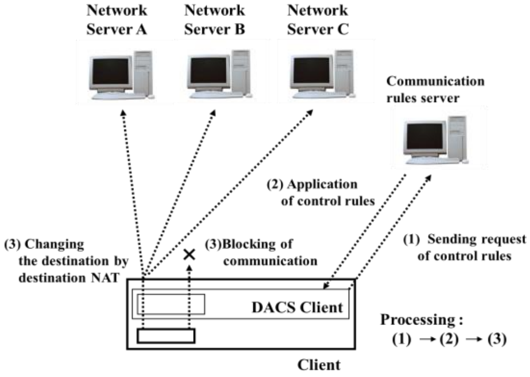

Network Server A
Network Server B
Network Server C
Communication rules server
(2) Application of control rules
(3) Changing the destination by destination NAT
(3)Blocking of communication
(1) Sending request of control rules
DACS Client
Processing :
(1) → (2) → (3)
Client

Fig. 3 Principle in Second Scheme

3. Existing DACS SCHEME and wDACS System

3.1 Basic Principle of the DACS Scheme

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

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

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

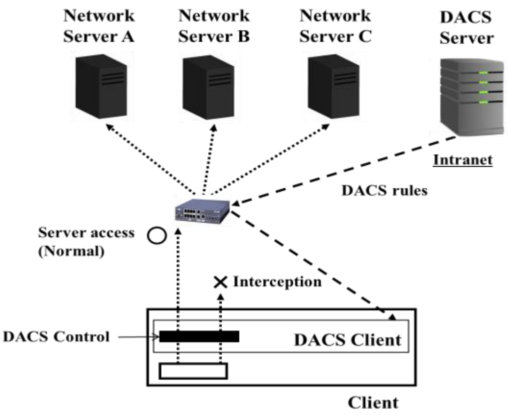


Fig. 4 Basic Principle of the DACS Scheme

According to the distributed DACS rules, the DACS Client performs (1) or (2) operation as shown in the following. Then, communication control of the client is performed for every login user.

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

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

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

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

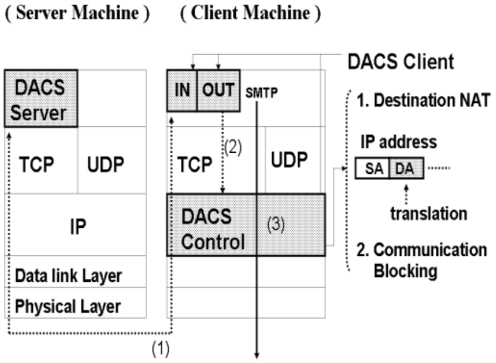


Fig. 5 Layer Setting of the DACS Scheme

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

3.2 Application to cloud environment

In this section, the contents of wDACS system are explained in Figure 6.
First, as preconditions, because private IP addresses are assigned to all servers and clients existing in from LAN1 to LAN n, mechanisms of NAT/NAPT are necessary for the communication from each LAN to the outside. In this case, NAT/NAPT is located on the entrance of the LAN such as (1), and the private IP address is converted to the global IP address towards the direction of the arrow. Next, because the private IP addresses are set on the servers and clients in the LAN, other communications except those converted by Destination NAT cannot enter into the LAN. But, responses for the communications sent form the inside of the LAN can enter into the inside of the LAN because of the reverse conversion process by the NAT/NAPT. In addition, communications from the outside of the LAN1 to the inside are performed through the conversion of the destination IP address by Destination NAT. To be concrete, the global IP address at the same of the outside interface of the router is changed to the private IP address of each server. From here, system configuration of each LAN is described. First, the DACS Server and the authentication server are located on the DMZ on the LAN1 such as (4). On the entrance of the LAN1, NAT/NAPT and destination NAT exists such as (1) and (2). Because only the DACS Server and network servers are set as the target destination, the authentication server cannot be accessed from the outside of the LAN1. In the LANs form LAN 2 to LAN n, clients managed by the wDACS system exist, and NAT/NAPT is located on the entrance of each LAN such as (1). Then, F/W such as (3) or (5) exists behind or with NAT/NAPT in all LANs.

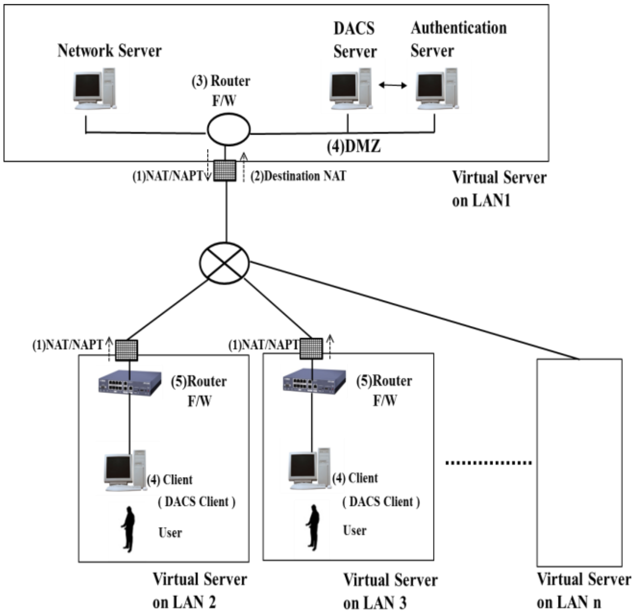


Fig. 6 Basic System Configuration of wDACS system

3.3 The Cloud Type Virtual PBNM for the Common Use Between Plural Organizations

In this section, after the concept and implementation of the proposed scheme were described, functional evaluation results are described.

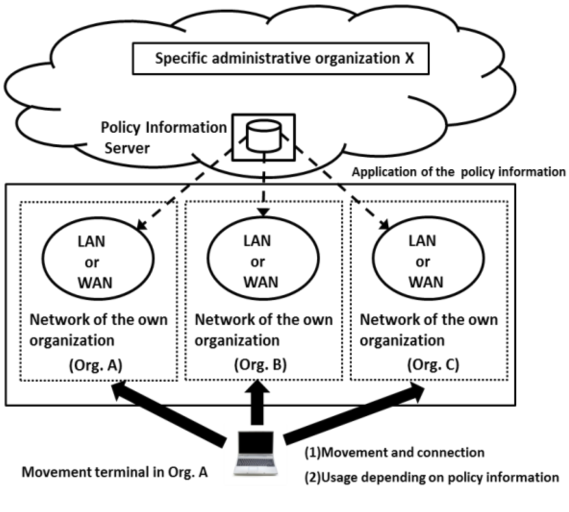

Specific administrative organization X
Policy Information Server
Application of the policy information
LAN or WAN
Network of the own organization
(Org. A)
LAN or WAN
Network of the own organization
(Org. B)
LAN or WAN
Network of the own organization
(Org. C)
Movement terminal in Org. A
(1)Movement and connection
(2)Usage depending on policy information

Fig. 7 Cloud Type Virtual PBNM for the Common Use between Plural Organizations

In Figure 7 which is described in [16], the proposed concept is shown. Because the existing wDACS Scheme realized the PBNM control with the software called the DACS Server and the DACS client, other mechanism was not needed. By this point, application to the cloud environment was easy. The proposed scheme in this paper realizes the common usage by plural organizations by adding the following elements to realize the common usage by plural organizations: user identification of the plural organizations, management of the policy information of the plural organizations, application of the PKI for code communication in the Internet, Redundant configuration of the DACS Server (policy information server), load balancing configuration of the DACS Server, installation function of DACS Client by way of the Internet. In the past study [14], the DACS Client was operated on the windows operation system (Windows OS). It was because there were many cases that the Windows OS was used for as the OS of the client. However, the Linux operating system (Linux OS) had enough functions to be used as the client recently, too. Therefore, to prove the possibility of the DACS Scheme on the Linux OS, the basic function of the DACS Client was implemented in this study. The basic functions of the DACS Server and DACS Client were implemented by JAVA language.

4. Consideration of Implementation Method for the scheme to manage the specific domain

4.1 Concept of this scheme

Here, the concept of the proposed is shown in Figure 8.This scheme is to manage the plural networks group. In Figure 8, the concept is explained. Specifically, as a logical range to manage organization A and organization B, network group 1 exists. Similarly, as a logical range to manage organization C and organization D, network group 2 exists. These individual network groups are existing methods listed in Figure 7. When plural network groups managed by this existing scheme exist, those plural network groups are targeted for management by this proposed method.

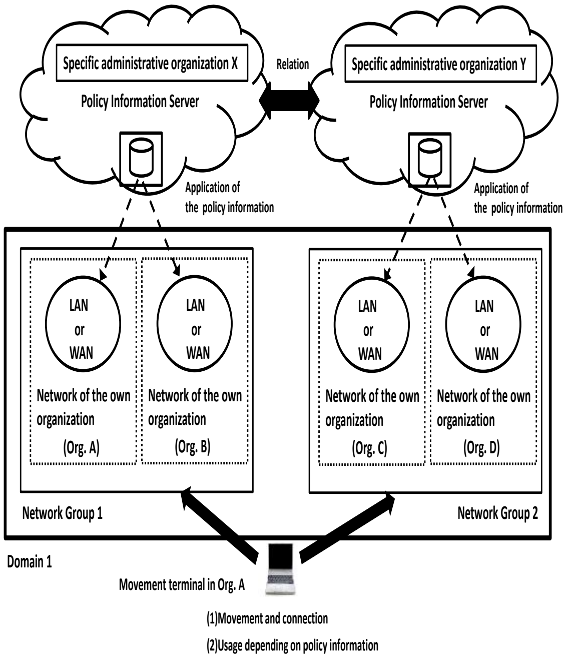

Specific administrative organization X
Relation
Specific administrative organization Y
Policy Information Server
Policy Information Server
Application of the policy information
Application of the policy information
LAN or WAN
LAN or WAN
LAN or WAN
LAN or WAN
Network of the own organization (Org. A)
Network of the own organization (Org. B)
Network of the own organization (Org. C)
Network of the own organization (Org. D)
Network Group 1
Network Group 2
Domain 1
Movement terminal in Org. A
(1)Movement and connection
(2)Usage depending on policy information

Fig. 8 Concept of the proposed scheme

For example, when user A belonging to org. A in network group1 uses the network which org. C belonging to network group2 which is a different network group holds, administrative organization Y for network group2 refers for policy information of user A for administrative organization X of network group1 and acquires it. After it, in the form that policy information registered with Network Group2 beforehand is collated with the policy information, the final policy information is decided. As a result, the policy information is applied to the client that user A uses in network group2, and the communication control on the client is performed. When a user moves plural network groups as well as the specific network group, it is thought that the PBNM scheme to keep a certain constant management state is realized. To realize this scheme, it is necessary to consider the following three factors.

(Factor1) Method of user authentication

(Factor2) Determination method of the policy information

(Factor3) Distribution method of the policy information

Here, the proposed method of user authentication which is suitable of this method is described in Figure.9. Because the proposed PBNM method is for the method to manage the whole Internet system, the proposed user authentication system also has a distributed system form. For example, when user A belonging to org. A in network group1 accesses the network of the network group1, the user authentication process is generated for the user authentication server for the network group1. On the other hand, when user A belonging to org. A in network group1 accesses the network of the network group 2, the user authentication process is generated for the user authentication server for the network group1. The server name with domain name are required as the information which are necessary for this user authentication. Based on the server name with domain name which is incorporated in the DACS CL in advance, the first access for the user authentication server is performed. After that, input of user name and password is requested. When these pieces of information are sent over the network, they need to be encrypted and sent by SSL (TLS). That is, the user authentication is handled by the organization to which the user belongs. The point to be noted here is the meaning of user authentication. Maybe, in some way, the user authentication server which is possessed by the network group that the user accesses may need to be used. However, that is only a complementary measure. The user authentication referred to here is the one before distribution of DACS rules as policy information. It is explicitly necessary to distinguish it from user authentication for permitting network connection as a separate one. Depending on the implementation, it may be descriptively possible to integrate these two user authentications as one process, but this is a matter to be considered at the implementation stage.

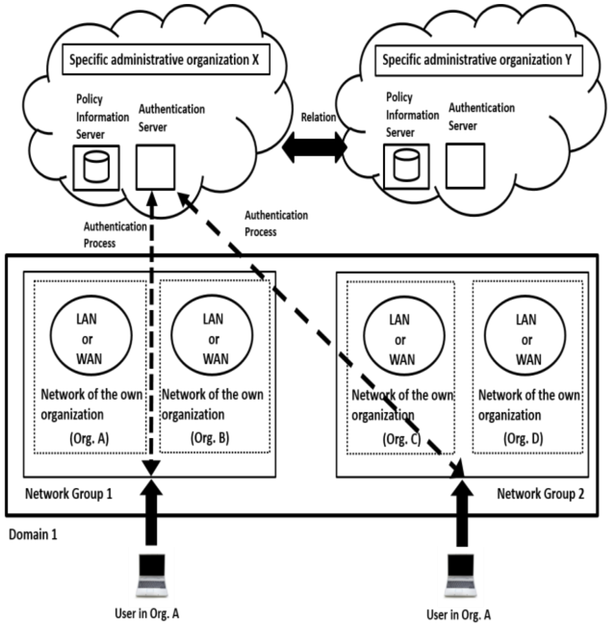

Specific administrative organization X
Policy Information Server
Authentication Server
Relation
Specific administrative organization Y
Policy Information Server
Authentication Server
Authentication Process
Authentication Process
LAN or WAN
Network of the own organization
(Org. A)
LAN or WAN
Network of the own organization
(Org. B)
LAN or WAN
Network of the own organization
(Org. C)
LAN or WAN
Network of the own organization
(Org. D)
Network Group 1
Network Group 2
Domain 1
User in Org. A
User in Org. A

Fig. 9 Concept of the proposed user authentication method

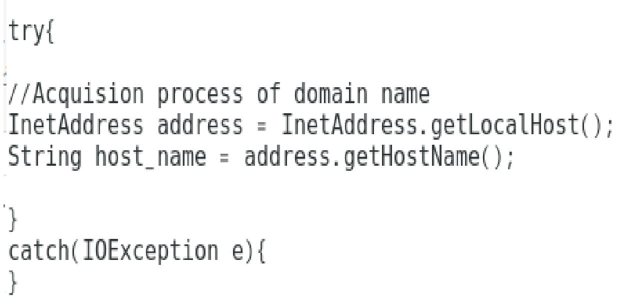
4.2 Results of inplementation

In this section, content of implementation and results of functional evaluation are described.

Implementation

The DACS server and on the cloud and DACS Client on each client were implemented by JAVA language. This is the same as the previous system.

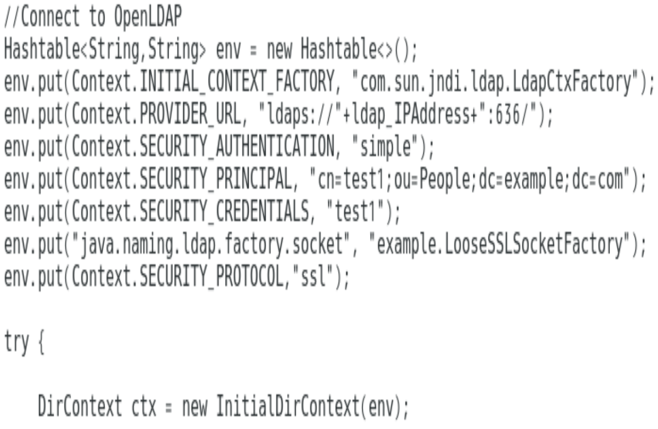
First, programming codes of acquisition process of domain name is described in Figure.10. In line 1, the client's IP address and domain name are obtained in variable “address”. In line 2, from it, domain name is obtained. After it, based on it, IP address of the OpenLDAP Server is obtained by making a query to DNS Server.



```
try{

//Acquision process of domain name
InetAddress address = InetAddress.getLocalHost();
String host_name = address.getHostName();

}
catch(IOException e){
}
```

Fig. 10 Domain name acquisition process

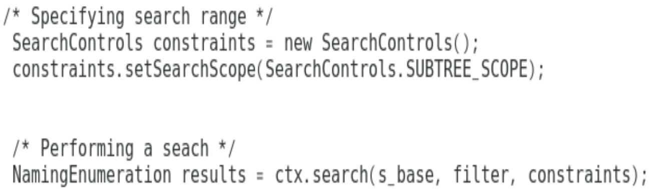
Next, as connection process for OpenLDAP of own organization, programming codes were written as Figure. 11.



```
//Connect to OpenLDAP
Hashtable<String,String> env = new Hashtable<>();
env.put(Context.INITIAL_CONTEXT_FACTORY, "com.sun.jndi.ldap.LdapCtxFactory");
env.put(Context.PROVIDER_URL, "ldaps://"+ldap_IPAddress+":636/");
env.put(Context.SECURITY_AUTHENTICATION, "simple");
env.put(Context.SECURITY_PRINCIPAL, "cn=test1;ou=People;dc=example;dc=com");
env.put(Context.SECURITY_CREDENTIALS, "test1");
env.put("java.naming.ldap.factory.socket", "example.LooseSSLSocketFactory");
env.put(Context.SECURITY_PROTOCOL,"ssl");

try {

    DirContext ctx = new InitialDirContext(env);
```

Fig. 11 Programming Code for OpenLDAP Access

The initial setting for OpenLDAP access is shown in the part from line 2 to line 8. Then, in the last row, connection processes to OpenLDAP are established by SSL communication.



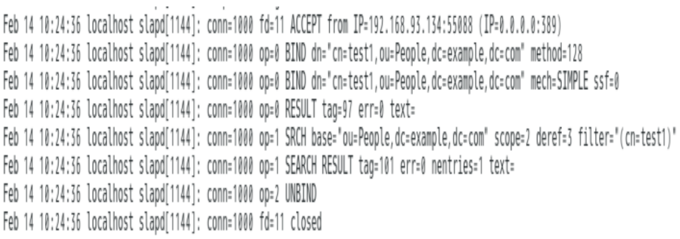
```
/* Specifying search range */
 SearchControls constraints = new SearchControls();
 constraints.setSearchScope(SearchControls.SUBTREE_SCOPE);


 /* Performing a seach */
 NamingEnumeration results = ctx.search(s_base, filter, constraints);
```

Fig. 12 Programming Code for OpenLDAP's Search

In Figure. 12, two processes of specifying search range and performing a search of user existence in OpenLdap's database are described. Because the search result is stored in the variable “rusults”, login user, when the value in it matches the login user name, it is permissible as a result of user authentication. It then leads to the process of retrieving and retrieving DACS rules.

(1) Functional evaluation

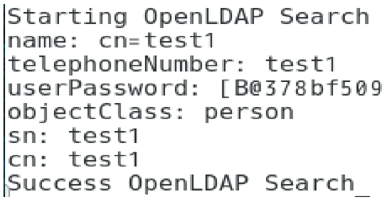
Here, the result of access from the client of other network group is described. In Figure. 13, access log from other network group's client are described.



```
Feb 14 10:24:36 localhost slapd[1144]: conn=1000 fd=11 ACCEPT from IP=192.168.93.134:55088 (IP=0.0.0.0:389)
Feb 14 10:24:36 localhost slapd[1144]: conn=1000 op=0 BIND dn="cn=test1,ou=People,dc=example,dc=com" method=128
Feb 14 10:24:36 localhost slapd[1144]: conn=1000 op=0 BIND dn="cn=test1,ou=People,dc=example,dc=com" mech=SIMPLE ssf=0
Feb 14 10:24:36 localhost slapd[1144]: conn=1000 op=0 RESULT tag=97 err=0 text=
Feb 14 10:24:36 localhost slapd[1144]: conn=1000 op=1 SRCH base="ou=People,dc=example,dc=com" scope=2 deref=3 filter="(cn=test1)"
Feb 14 10:24:36 localhost slapd[1144]: conn=1000 op=1 SEARCH RESULT tag=101 err=0 nentries=1 text=
Feb 14 10:24:36 localhost slapd[1144]: conn=1000 op=2 UNBIND
Feb 14 10:24:36 localhost slapd[1144]: conn=1000 fd=11 closed
```

Fig. 13 Access Log on OpenLDAP

Connection process from the client having IP address of “192.168.63.134” is written in Line 1. On the following lines, records in which the verification with the user name transmitted from the client has been made is described.



```
Starting OpenLDAP Search
name: cn=test1
telephoneNumber: test1
userPassword: [B@378bf509
objectClass: person
sn: test1
cn: test1
Success OpenLDAP Search_
```

Fig. 14 Display result of LDAP entry

In Figure.14, display result of LDAP entry which was sent from OpenLDAP Server is listed. In order to confirm the operation, it was made to display it dare. As the result, it was confirmed that the information of “test1” which was the login user to the client was successfully returned from OpenLDAP of other network group. It has been demonstrated that the proposed user authentication could be realized functionally.

5. Conclusion

In this paper, results of the authentication processes in the proposed scheme is described. Considering affinity with the Internet system, the distributed authentication method was proposed. The authentication server of the network group to which the organization to which the user belongs is used as the authentication server. In the future, distribution processes of DACS rules will be implemented.

Acknowledgments

This work was supported by the research grant of JSPS KAKENHI Grant Number 17K00113, and the research grant by Support Center for Advanced Telecommunications Technology Research, Foundation (SCAT). We express our gratitude.

This work was supported by KDDI Foundation. We express our gratitude

References

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

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

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

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

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

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

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

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

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

[10] M. Wahl, T. Howes, S.Kille, “Lightweight Directory Access Protocol (v3),” IETF RFC 2251, 1997.

[11] CIM Schema: Version 2.30.0, 2011.

[12] ETSI ES 282 003: Telecoms and Internet converged Services and protocols for Advanced Network (TISPAN); Resource and Admission Control Subsystem (RACS); Functional Architecture, June 2006.

[13] ETSI ETSI ES 283 026: Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control;

Protocol for QoS reservation information exchange between the Service Policy Decision Function (SPDF) and the Access-Resource and Admission Control Function (A-RACF) in the Resource and Protocol specification, April 2006.

[14] K. Odagiri, R. Yaegashi,M. Tadauchi, and N. Ishii, "Secure DACS Scheme, "Journal of Network and Computer Applications," Elsevier, Vol.31, Issue 4, 2008, pp.851-861, November.

[15] K. Odagiri, S. Shimizu,M. Takizawa and N. Ishii, "Theoretical Suggestion of Policy-Based Wide Area Network Management System (wDACS system part-I)," International Journal of Networked and Distributed Computing (IJNDC), Vol.1, No.4, November 2013, pp.260-269.

[16] K. Odagiri,S. Shimizu, N. Ishii, M. Takizawa, "Suggestion of the Cloud Type Virtual Policy Based Network Management Scheme for the Common Use between Plural Organizations," Proc of Int. Conf. on International Conference on Network-Based Information Systems (NBiS-2015),pp.180-186,Septmber, 2015

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

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

Naohiro Ishii received the B.E., M.E. and Dr. of Engineering degree from Tohoku University, Japan in 1963, 1965 and 1968, respectively. He was a professor in Department of Intelligence and Computer Science at Nagoya Institute of Technology. From 2003, he was a professor in Department of Information Science at Aichi Institute of Technology until 2019. He belongs to Advanced Institute of Industrial Technology now. His research interest includes computer engineering, artificial intelligence, and human interface.