Virtual Use Method of CGI by DACS Web Service Based on the Next Generation PBNM Scheme Called DACS Scheme

Kazuya Odagiri
Advanced Institute of Industrial Technology
Tokyo, Japan
odagiri@aiit.ac.jp, kazuodagiri@yahoo.co.jp

Syogo Shimizu
Advanced Institute of Industrial Technology
Tokyo, Japan
shimizu-syogo@aiit.ac.jp

Naohiro Ishii
Aichi Institute of Technology
Aichi, Japan
ishii@aitech.ac.jp

***Abstract*—as a work for managing a whole network effectively without a limited purpose, there is the work of a PBNM (Policy-based network management). The PBNM has two structural problems such as communication concentration from many clients to a communication control mechanism called PEP (Policy Enhancement Point) and the necessity of the network system updating at the time of introducing the PBNM into LAN. Moreover, user support problems in campus-like computer networks such as troublesome user support in updating a client's setups and coping with annoying communication cannot be improved by the PBNM. To improve these problems, we have been studied a next generation PBNM, which overcomes theses problems and has the function that does not exist in the existing PBNM, and called it a DACS (Destination Addressing Control System) Scheme. By the DACS Scheme, communication concentration from many clients to the PEP is solved, and system updating becomes unnecessary. Moreover, user support at updating the client's setups and coping with annoying communication by the DACS Scheme becomes very effective. In this study, to raise the effectiveness of this scheme, we show a virtual use method of CGI (Common Gateway Interface) by using the DACS Web Service, which is the Web Service realized by the DACS Scheme that we have been proposed before.**

Keywords- CGI; DACS Scheme; PBNM; destination NAT; packet filtering

I. 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, there are some user support problems as follows. For example, when the mail boxes on one server are relocated to different server machines, an update of user machine's setups is necessary. Most of computer network users in a campus are students. 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 posters. For the system administration, individual technical support is a stiff part of the network management.

As the work of network management, there are various kind of works such as the server load distribution technology [1][2][3], VPN (Virtual Private Network) [4][5]. However, these works are performed forward the specified different goal, and don't have the purpose of effective whole network management. As the work for managing a whole network, there is the work of Opengate [6][7], which controls Web accesses from LAN (Local Area Network) to internet. This work has the limited purpose of controlling Web access to internet. As the work for managing a whole network effectively without the limited purpose, there is the work of a PBNM (Policy-based network management) [8][9][10][11] in IETF (Internet Engineering Task Force). However, the PBNM has two structural problems such as communication concentration from many clients to a communication control mechanism called Policy Enforcement Point (PEP) and the necessity of the network updating at the time of introducing the PBNM into LAN. Moreover, it is often difficult for the PBNM to improve the user support problems in campus-like computer networks explained above.

To improve these problems of the PBNM, we show a next generation PBNM, which overcomes theses problems and has the function, which does not exist in the existing PBNM, and called it DACS (Destination Addressing Control System) Scheme. As the works of DACS Scheme, we showed the basic principle of the DACS Scheme [12], and security function [13]. In addition, we showed new user support realized by use of the DACS Scheme [14]. The past work of the DACS Scheme's mechanism was executed as a network management scheme for campus-like computer networks. In this paper, to raise the effectiveness of this scheme, we show the virtual use method of CGI (Common Gateway Interface) by using the DACS Web Service. The DACS Web Service is the Web Service realized by the DACS Scheme that we have been proposed before. The rest of paper is organized as follows. Section II shows motivation of this research. In Section III, we describe the content of the DACS scheme. Then, in Section IV, the content of DACS Web Service is explained. In Section V, virtual use of the CGI program is shown.

ISBN: 978-1-61208-133-5

II. MOTIVATION

In the world of Internet, programs as the CGI [15] are often disclosed so that many users can use them without any charge. Because they are developed at an individual level, it is often impossible to use them in a company and university practically. However, when they are developed by a skilled developer, it is possible to use them practically. For example, in the software such as a bulletin board and groupware, they are not always referred only form same group members in each user's group. In many cases, when they are used in multiple groups, they are placed by being multi-copied. Because they are accessed from users in other group, there is the possibility of data leak. To be concrete, when they don't have an authentication mechanism, it becomes possible for users in other group to access the program. When they can acquire the URL for the program, the data of them is referred through the program by using the URL.

Therefore, in this study, the virtual usage method of the CGI program is shown. To be concrete, by using the DACS Web Service that the authors have been studied, it is realized. The DACS Web Service is the service that is realized on the network introducing the DACS Scheme, which is a scheme of Policy Based Network Management (PBNM). Because it is a service limited to Local Area Network (LAN) at this time, the method is also limited to the usage on the LAN.

III. THE DACS SCHEME

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

A. *Existing PBNM*

As the works on existing network management, there are various works such as authentication [16][17], the server load distribution technology [1][2][3], VPN [4][5] and quarantine network [18][19]. However, these works are performed forward the specified different goal. Realization of effective management for a whole network is not a purpose. These works are performed for the specific purpose, and don’t have the purpose of managing a whole network. As the work for managing a whole network, there is the work of Opengate [6][7], which controls Web accesses from LAN to internet. However, this work has the limited purpose of controlling Web access to internet. As the work for managing a whole network effectively without the limited purpose, there is the work of the PBNM [8][9][10][11] in IETF. The content of the PBNM is described in Figure 1.

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 firewall 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.

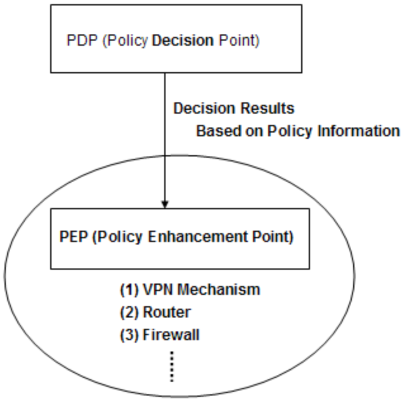
PDP (Policy Decision Point)
Decision Results
Based on Policy Information
PEP (Policy Enhancement Point)
(1) VPN Mechanism
(2) Router
(3) Firewall

Figure 1. PBNM in IETF

B. *Basic Principle of the DACS Scheme*

Figure 2 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.

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

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

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

An example of the case (1) is shown in Figure 2. In Figure 2, 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.

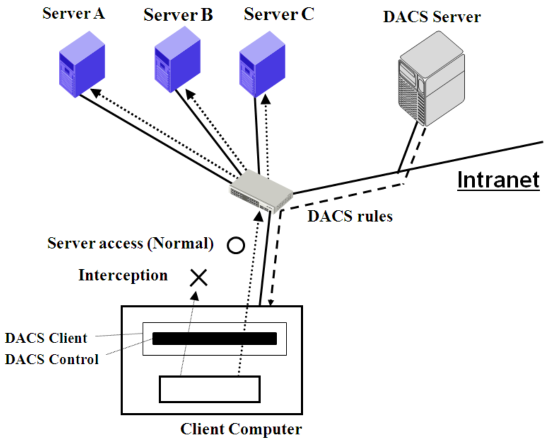

Figure 2. Basic Principle of the DACS Scheme

In order to realize the DACS Scheme, the operation is done by a DACS Protocol as shown in Figure 3. As shown by (1) in Figure 3, the distribution of the DACS rules is performed on communication between the DACS Server and the DACS Client, which is arranged at the application layer. The application of the DACS rules to the DACS Control is shown by (2) in Figure 3. 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 3.

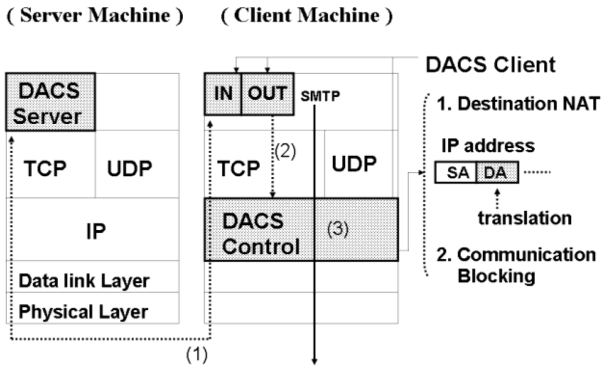

Figure3. Layer Setting of the DACS Scheme

C. Communication Control on Client

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

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

When using communication control on every user and every client, communication control may conflict. In that case, a priority needs to be given. The judgment is performed in the DACS Server side as shown in Figure 4. Although not necessarily stipulated, the network policy or security policy exists in the organization such as a university (1). The priority is decided according to the policy (2). In (a), priority is given for the user's rule to control communication by the user unit. In (b), priority is given for the client's rule to control communication by the client unit. In (c), the user's rule is the same as the client's rule. As the result of comparing the conflict rules, one rule is determined respectively. Those rules and other rules not overlapping are gathered, and the DACS rules are created (3). The DACS rules are transmitted to the DACS Client. In the DACS Client side, the DACS rules are applied to the DACS Control. The difference between the user's rule and the client's rule is not distinguished.

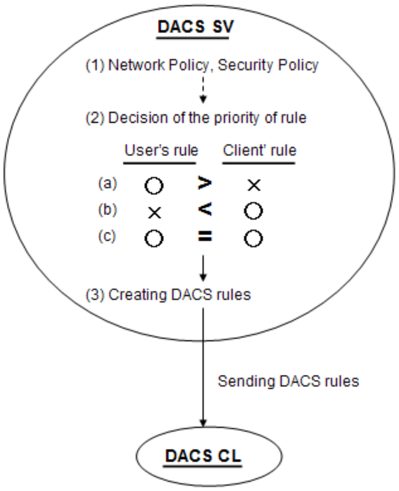

Figure 4. Creating the DACS rules in the DACS Server side

D. Security Mechanism of the DACS Scheme

In this section, the security function of the DACS Scheme is described. The communication is tunneled and encrypted by use of SSH. By using the function of port forwarding of SSH, it is realized to tunnel and encrypt the communication between the network server and the, which DACS Client is installed in. Normally, to communicate from a client application to a network server by using the function of port forwarding of SSH, local host (127.0.0.1) needs to be indicated on that client application as a communicating server. The transparent use of a client, which is a characteristic of the DACS Scheme, is failed. The transparent use of a client means that a client can be used continuously without changing setups when the network system is updated. The function that doesn't fail the transparent use of a client is needed. The mechanism of that function is shown in Figure 5. The changed point on network server side is shown as follows in comparison with the existing DACS Scheme. SSH Server is located and activated, and communication except SSH is blocked. In Figure 5, the DACS rules are sent from the DACS Server to the DACS Client (a). By the DACS Client that accepts the DACS rules, the DACS rules are applied to the DACS Control in the DACS Client (b). The movement to here is same as the existing DACS Scheme. After functional extension, as shown in (c) of Figure 5, the DACS rules are applied to the DACS SControl. Communication control is performed in the 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 the DACS Control as shown in (d) of Figure 5. When communication is tunneled and encrypted, destination of the communication is changed by the DACS Control to localhost as shown in (e) of Figure 5. After that, by the DACS STCL, the communicating server is changed to the network server and tunneled and encrypted communication is sent as shown in (g) of Figure 5, which are realized by the function of port forwarding of SSH. In the DACS rules applied to the DACS Control, localhost is indicated as the destination of communication. In the DACS rules applied to the 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 the DACS Scheme, that is, with the transparent use of a client. Then, by changing the content of the DACS rules applied to the DACS Control and the 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.

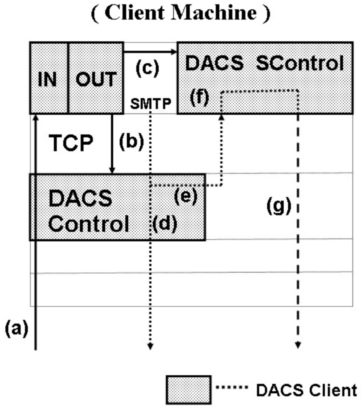

Figure 5. Extend Security Function

E. *Effectiveness of the DACS Scheme*

(a) Effective User Support at Changing Setups of Client with the DACS Scheme

When network system is updated, user support by the DACS Scheme is compared with user support by the Non-DACS Scheme, and an advantage of user support by the DACS Scheme is described. User support processes after updating the network system are described in Figure 6.

When the DACS Scheme is not introduced, notification for changing setups is sent to a user in a laboratory (2) after updating the network system (1). It is sent by E-mail and a homepage or a document. The user who accepts that notification updates a client' s setups (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 update 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 the DACS Scheme is introduced, a system administrator has only to change the DACS rules (8) at the time of updating the network system. After changing the DACS rules, communication control corresponding to new network system 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 the DACS rules, a trouble by a cause except an artificial factor such as missing setups of the DACS rules does not occur. This process of user support is largely simplified in comparison with the process of user support by the Non-DACS Scheme.

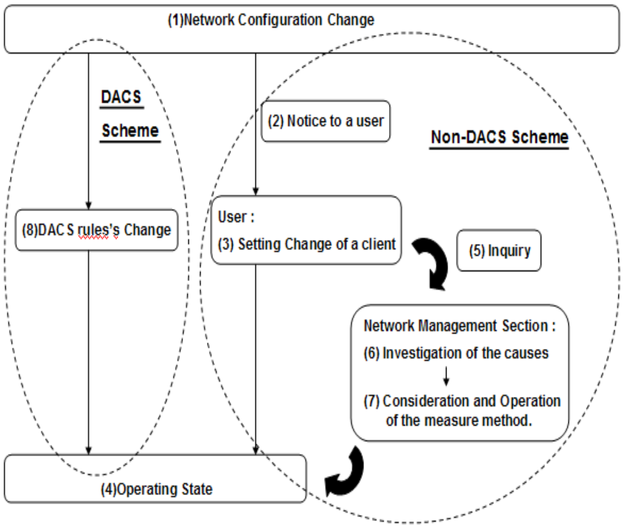
(1)Network Configuration Change
DACS
Scheme
(2) Notice to a user
Non-DACS Scheme
(8)DACS rules's Change
User :
(3) Setting Change of a client
(5) Inquiry
Network Management Section :
(6) Investigation of the causes
(7) Consideration and Operation of the measure method.
(4)Operating State

Figure 6. Process introducing the DACS Scheme

(b) Effective Coping with Annoying Communication by the 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 [20], 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 Figure 7 and explained with an example of the user support for a laboratory.

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 the DACS Scheme is introduced or not introduced. When the DACS Scheme is not introduced, the process of user support is described in

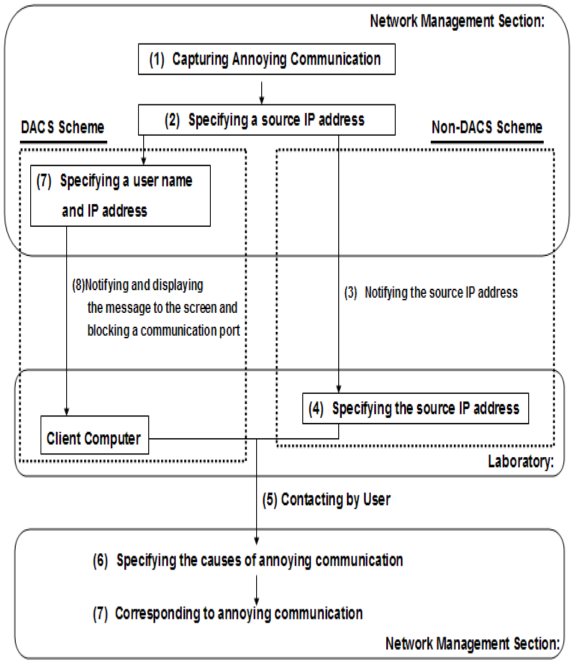
Network Management Section:
(1) Capturing Annoying Communication
(2) Specifying a source IP address
DACS Scheme
Non-DACS Scheme
(7) Specifying a user name and IP address
(8)Notifying and displaying the message to the screen and blocking a communication port
(3) Notifying the source IP address
(4) Specifying the source IP address
Client Computer
Laboratory:
(5) Contacting by User
(6) Specifying the causes of annoying communication
(7) Corresponding to annoying communication
Network Management Section:

Figure 7. Change of User Support

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 cannot 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 impossible to manage t the IP address that the client uses, 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 cannot 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 the 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 the DACS Scheme is effective at the following two points. The first point is that the client that transmits annoying communication is specified simply. The client that 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, the DACS Scheme is particularly effective.

IV. SYNOPSIS OF THE DACS WEB SERVICE

In this section, the synopsis of the DACS Web Service is described.

A. *Two Kinds of Functions of Web Service Based on DACS Scheme*

Two kinds of functions of Web Services based on DACS Scheme are described, here.

At first, the function to use data from database 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 Figure 8.

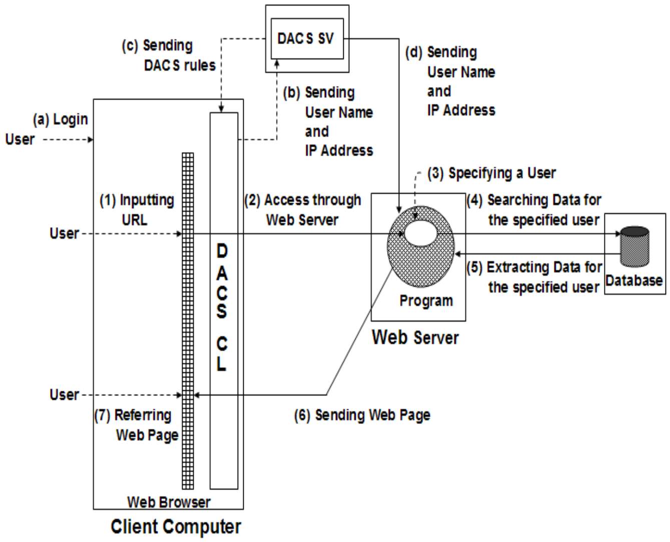

Figure 8. Function Using Data from Database

In the network with 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). Moreover, user name and IP address are sent to the program on Web Server. Then, the server side program on Web Server can identify the user by checking the login information and the source IP address from the client, and can change the processing of the program every 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. Through the processing from (1) to (7), this new function is performed.

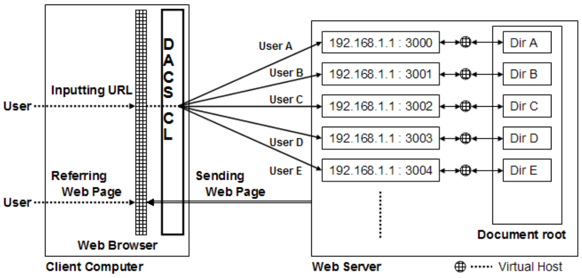

Figure 9. Function Using Data from Document Medium

Next, the function to use data from document medium 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. When this principle is combined with the function of virtual host that is equipped as Web Server, it is possible to use Web Server as shown in Figure 9.

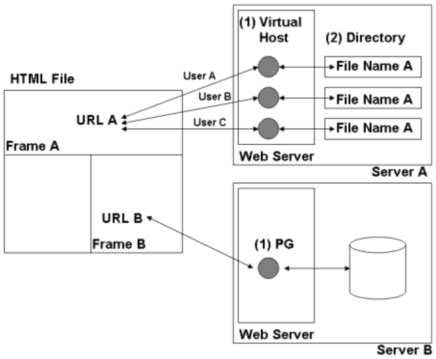

Figure 10. Web Service by two functions

By the function of virtual host, multiple groups of socket (IP address and TCP port) can be assigned for one Web Server. The referred document can be changed every socket. First, in Document root of Web Server in Figure 9, directories (Dir A,B,C,D….) are prepared for each user. By the function of virtual host, each directory is connected to each socket as one pare. By changing TCP port number (3000,3001,3002….) for one IP address (192.168.1.1), sockets corresponding to each directory are prepared. Next, movement on this mechanism is described. One user inputs one URL to Web Browser. When the URL is inputted by User A, the file in Dir A that is connected to the socket (192.168.1.1:3000) is referred. Equally, when by User B, the file in Dir B that is connected to the socket (192.168.1.1:3001) is referred. When by User C, the file in Dir C that is connected to the socket (192.168.1.1:3002) is referred. When the document medium with same name exists in each directory (Dir A,B,C….), each user can see different contents by inputting same URL to Web Browser. For information sender, because it is possible to notify information to the specific user by uploading document medium to the predetermined directory, information usage becomes largely wide. Because information sender can describe the content of document medium easily and freely, it is possible to communicate the information with much expressive power and impact.

As the result, by letting both functions coexist as shown in Figure 10, the Web Service that a user can use information on the network regardless of information storage form is realized.

B. *Contents of the DACS Web Service*

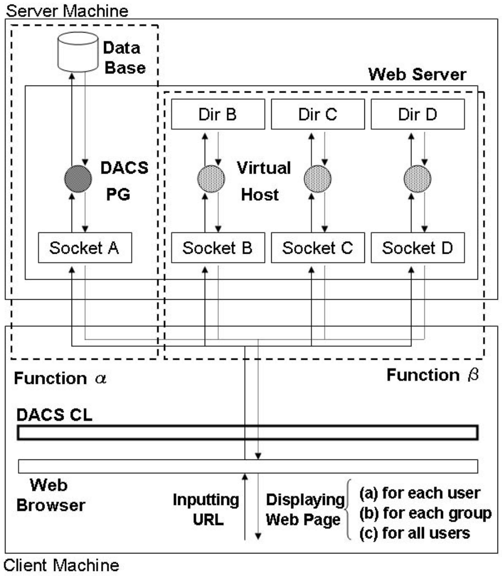

Figure 11. DACS Web Service

In Figure 11, 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 a 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 that 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.

Here, details of Function α are shown. After extension, the functions of retrieving data for each group (Function α2) or for all users (Function α3) can be used. There are differences among Function α1, Function α2, and Function α3 in the program extracting data from a database for a request from a Web browser.

In the program of Function α1, data is extracted for each user, as shown by (1). In the program of Function α2, data is extracted for each group, as shown by (2). In the program of Function α3, data is extracted for all users, as shown by (3). In the existing function to retrieve data from a database, as shown by (1), it is possible to specify which user is sending communication through the Web browser. Therefore, the function is extended to set a correspondence list of the user and group name in the DACS Server and send that correspondence list from the DACS Server to the program of Function α2. As a result, because the program of Function α2 can recognize the group to which a user belongs, it is possible to extract information for each group. Even if a user belongs to multiple groups, it is possible to extract the data of all groups. In addition, it is possible to extract the data of a specific group by sending its group name as a parameter of the URL. In the program of Function α3, data is extracted for all of these users. Because it is the function of a normal Web Service that does not introduce DACS Scheme, it is generally realized without a technical problem.

Next, details of Function β are shown. Function β1 displays data of the document medium dynamically for each user. By use of this function, the function for each group (Function β2) and the function for all users (Function β3) are realized. Function β2 relates the URL for each group (Group URL1, Group URL2….) to each document, which is stored in each directory for each group. Function β3 relates the URL for all users (All Users URL) to the document, which is stored in the directory for all users. To send information, only uploading a file as a document medium into the predetermined directory (directory for each user, directory for each group, and directory for all users) is necessary. Information for each group can be recieved by the specific URL for each group. In addition, the users not belonging to each group can not access it by using the URL. Information for all users can be recieved by use of the URL for all users. By using the DACS Web Service, not only information for each user but also information for each group and for all users, can be used from the document medium.

V. VIRTUAL USAGE METHOD OF THE CGI

In this paper, the method that is realized by the Function α1 is proposed. By using this function, programs of the CGI is accessed virtually through same URL from users in each group. To be concrete, this method is realized by the following procedure.

(Step1) First setting of the CGI programs

First, CGI is set by a normal procedure. For example, the program files as the CGI are placed on the Web Server, and initial setting is performed. For example, the setting of initial parameter of the CGI and permission of the program files. As the result, users can use the programs of the CGI by inputting one URL into a Web Browser.

(Setp2) Setting for virtual use of the CGI programs

After copying the directory that stores the programs, it is pasted as another directory with another name. By repeating a similar operation, multiple directories for each group are prepared. At the same time, the content of the DACS rules is changed. As the result, users that belong to same group become possible to access the programs of same directory by use of a URL. On the other hand, users that belong to other group become impossible to access the above programs by use of same URL.

By these procedures, in the form of using same URL, users in each group can access the programs of the directory in each group, and can not access the programs of other group. Virtual use of the CGI programs is realized without a special mechanism.

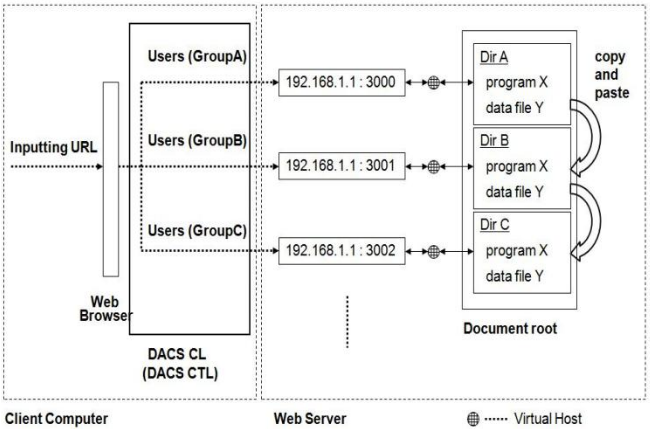

Figure 12. Virtual Usage of the CGI program

A concrete example of it is shown in Figure 12. As first step, the program X as the CGI program and other files such as data file are placed in directory A (Dir A in Figure 12), and initial setting of it is performed. As the result, users can access and use it. Next, second step is as follows. At first, Dir A is copied and pasted with another name. In Figure 12, Dir B and Dir C are the pasted directories. Each directory is named with the regularity. Though each socket is connected to each directory through the virtual host by the system setting, each name is allocated to be easy to automate the setting. At the same time, by changing the DACS rules, the host name in URL and the communication port is converted to each socket every group. In Figure 12, when users in Group A inputs one URL into a Web Browser, they access the program X in Dir A through by way of 192.168.1.1:3000. In the case of users in Group B, they access the program X in Dir B through by way of 192.168.1.1:3001. In the case of users in Group C, they access the program X in Dir C by way of 192.168.1.1:3002. Then, users in Group A con not access the program in Dir B and Dir C. Users in Group B con not access the program in Dir A and Dir C. Users in Group C con not access the program in Dir A and Dir B. In this way, virtual use of the CGI program is realized simply.

REFERENCES

[1] 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.

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

[3] 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.

[4] C. Metz,“The latest in virtual private networks: part I,” IEEE Internet Computing, Vol. 7, No. 1, pp. 87-91, 2003.

[5] C. Metz,“The latest in VPNs: part II,” IEEE Internet Computing, Vol. 8, No. 3, pp. 60-65, 2004.

[6] Y. Watanabe, K. Watanabe, E. Hirofumi, and S. Tadaki, “A User Authentication Gateway System with Simple User Interface, Low Administration Cost and Wide Applicability,” IPSJ Journal, Vol. 42, No. 12, pp. 2802-2809, 2001.

[7] S. Tadaki, E. Hirofumi, K. Watanabe, and 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.

[8] S. Jha and M. Hassan,“Java implementation of policy-based bandwidth management,” Int. J. Network management, John Wiley&Sons, Vol. 13, isuue. 4, pp. 249-258, July, 2003.

[9] G.M. Prerez, F.G. Skarmeta, S. Zeber, and T. Symchych,“Dynamic Policy-Based Network Management for a Secure Coalition Environment,” IEEE Communications Magazine, Vol. 44, issue. 11, pp. 58-64, November, 2006.

[10] D.C. Verma,“Simplifying Network Administration Using Policy-Based Management,” IEEE Network, Vol. 16, issue. 2, pp. 20-26, March-April, 2002.

[11] M. Sugano, S. Tanaka, Y. Sakata, K. Oguma, and N. Shiratori,“Application and Implementation of Policy Control Method ”PolicyComputing” in Computer Networks,” IPSJ Journal, Vol. 42, No. 2, 2001.

[12] K. Odagiri , R. Yaegashi , M. Tadauchi, and N. Ishii, “ Efficient Network Management System with DACS Scheme : Management with communication control,” Int. J. of Computer Science and Network Security, Vol. 6, No. 1, pp. 30-36, January, 2006.

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

[14] K. Odagiri, R. Yaegashi, M. Tadauchi, and N. Ishii, “New User Support in the University Network with DACS Scheme,” Int. J. of Interactive Technology and Smart Education.

[15] D. Robinson,“The WWW Common Gateway Interface Version 1.1,Internet Draft,” 1995

[16] K. Wakayama, Y. Decchi, J. Leng, and A. Iwata,“A Remote User Authentication Method Using Fingerprint Matching,” IPSJ Journal, Vol. 44, No. 2, pp. 401-404, 2003.

[17] S. Seno, Y. Koui, T. Sadakane, N. Nakayama, Y. Baba, and T. Shikama,“A Network Authentication System by Multiple Biometrics,” IPSJ Journal, Vol. 44, No. 4, pp. 1111-1120, 2000.

[18] http://www.nec.co.jp/qxseries/solution/04.html 10.3.2011

[19] http://www.ntt.co.jp/journal/0512/files/jn200512049.pdf 10.3.2011

[20] H. Hu, J. Kashio, Y. Honda, and 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.