Secure Enterprise Network Access Control System—Overview

Takeshi Kaji[†]*, Takao Yamashita, Shinya Matsumoto, Masayuki Kobayashi, and Masayuki Nakajima*

Abstract

We have developed a secure enterprise network access control system (SENACSY) to make an enterprise network secure and to free users from the effort of configuring their personal computers (PCs). Users can connect their PCs to the enterprise network without considering where they are. We give an overview of this system in this letter and describe the quarantine function in the April issue.

1. Role of an enterprise network in the business world

Information stored in an enterprise system is very useful and helps users make decisions and respond to customers' orders quickly. An enterprise system occupies an essential position in the business world and is connected to an enterprise network so that various kinds of information can be shared by many users. Users need to access the enterprise network to get various kinds of information from the enterprise system wherever they are. Therefore, many enterprises have provided various different access methods to their network. For example, many enterprises have introduced wireless access points and remote access servers into their network and users often access it with network devices such as wireless local area network (LAN) devices and cellular phones from inside or outside their office buildings.

Since proprietary and confidential information stored in an enterprise system affects the enterprise's competitive position and must be protected against disclosure, theft, and inadvertent loss, it is important to make an enterprise network secure. Therefore, new network equipment that supports high-security technologies has been introduced into the enterprise network. For example, many enterprise networks contain 802.1X-enabled switches [1] and IPsec security gateways [2].

2. Problems caused by highly secure enterprise network

When there are alternative network devices for accessing the enterprise network and strong security technologies are implemented in the enterprise network, new problems arise [3].

(1) More troublesome configuration burden on users and higher network management cost

Ordinary users, such as ones belonging to the sales department, are not experts in network protocols, but they are required to learn to configure various network devices and protocols that enable high security. However, it is difficult for ordinary users to develop such skills in a short time. Hence, the configuration burden imposed on ordinary users interferes with their main role. In addition, the number of inquiries to the network administrator increases when ordinary users cannot configure their personal computers (PCs).

(2) Difficulty of enforcing a network management policy to be followed by users and preventing unauthorized access to the enterprise network

To secure an enterprise network, it is insufficient to simply introduce network equipment that supports high-security technologies. When users configure

† NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan
E-mail: kaji.takeshi@lab.ntt.co.jp

their PCs by themselves, they may connect them to the Internet without using antivirus software and firewall settings. Unexpected configurations could allow in viruses, worms, and so on or allow unauthorized access to the enterprise network, leading to leaks of proprietary and confidential information stored in an enterprise system.

(3) Complicated user operations to access the enterprise network

To effectively connect their PCs to the enterprise network, the user must choose the most suitable network device and protocols and perform suitable actions to access it. This is complicated for ordinary users. Whenever the users move from one location to another where the network environment is different, they must perform complicated operations again.

3. System development purpose

NTT Information Sharing Platform Laboratories has developed a secure enterprise network access control system (SENACSY). This system reduces the management cost of the enterprise network, achieves high security, and improves the user's operations at the same time. Some examples of using this system are shown in **Fig. 1**. When a user moves to various places inside or outside his office buildings, he can connect his PC to the enterprise network safely by a simple operation. The quarantine network shown in Fig. 1 is based on the quarantine function in the SENACSY, which will be described in the April issue.

4. System overview and operation flow

An overview of the system is shown in **Fig. 2**. This system consists of two components: a profile generating system that issues profiles, including authentication information needed to access the enterprise network, and a SENACSY tool that is used by users to access the enterprise network. The network administrator issues a profile and an authentication token supporting PKCS#11 [4] using the profile generating system. The features of this system and the operation flow are described below.

(1) Issuing of profiles

The network administrator issues a profile using the profile generating system and distributes it to the user. This profile includes network settings and authentication information needed to access the enterprise network. The user can connect his PC to the enterprise network just by importing the given profile into his SENACSY tool. In other words, the user can access the enterprise network without any knowledge of networks or security. Furthermore, the network administrator distributes the profile to the users after verifying that it can establish a connection to the enterprise network. Therefore, the users expe-

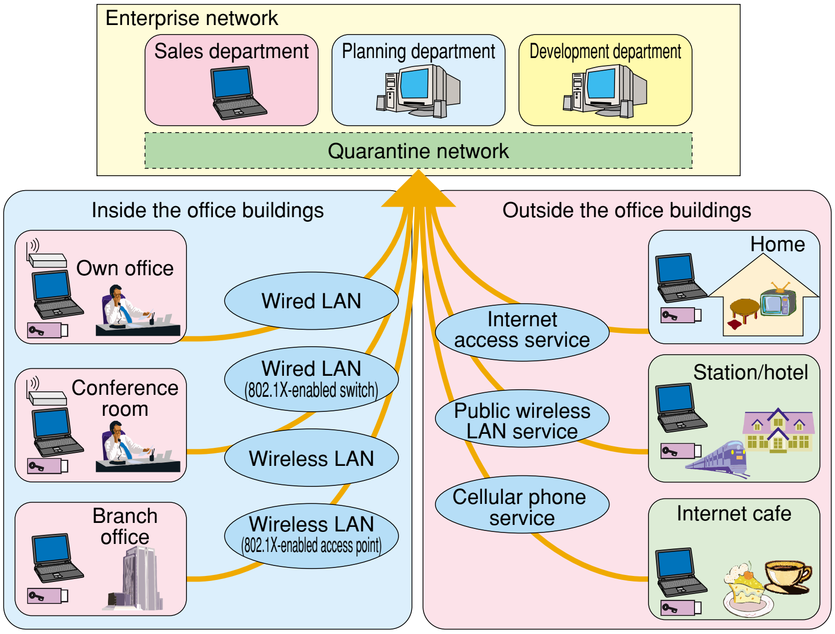


Fig. 1. Examples of system usage.

rience less trouble. This system frees users from the troublesome configuration burden and reduces the network management cost.

(2) Issuing of authentication tokens

The network administrator issues an authentication token and distributes it to the user along with the profile. The profile is encrypted to prevent its contents from being exposed to anyone. Encryption also prevents users from modifying the contents. However, if the key that is used to decrypt the profile is inadequately managed, it is impossible to protect their contents against the threats mentioned above. We chose to store the key within an authentication token and make it impossible to extract the key from it. This scheme can prevent even a legal user from knowing the authentication information needed to access the enterprise network. Therefore, this system can solve the problem of forcing users to follow the network management policy.

After installing the SENACSY tool onto his PC and importing the profile into the SENACSY tool, the user can connect his PC to the enterprise network. The installation and importing operations are ordinary procedures, so we omit their descriptions here.

(3) User authentication

The user authentication screen of the SENACSY tool is shown in **Fig. 3**. The user inserts the authentication token into his PC and inputs his user ID and personal identification number (PIN). This two-factor authentication and the use of encryption for the profile solve the problem of unauthorized access to the enterprise network.

(4) Connection to the enterprise network

The main screen of the SENACSY tool is shown in **Fig. 4**. There are two drop-down lists in the main screen. The upper one lists target networks. The user chooses the network he wants to connect to, such as his enterprise network or the Internet. The lower one

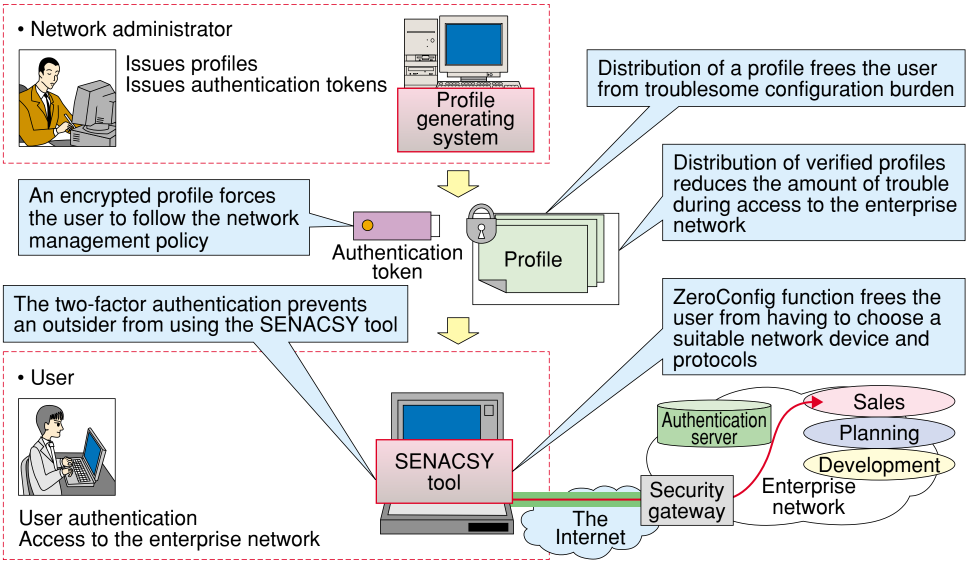
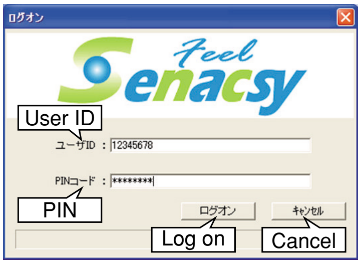

• Network administrator
Issues profiles
Issues authentication tokens
Profile generating system
Distribution of a profile frees the user from troublesome configuration burden
An encrypted profile forces the user to follow the network management policy
Authentication token
Profile
Distribution of verified profiles reduces the amount of trouble during access to the enterprise network
The two-factor authentication prevents an outsider from using the SENACSY tool
ZeroConfig function frees the user from having to choose a suitable network device and protocols
• User
User authentication
Access to the enterprise network
SENACSY tool
Authentication server
Sales
Planning
Development
Enterprise network
Security gateway
The Internet

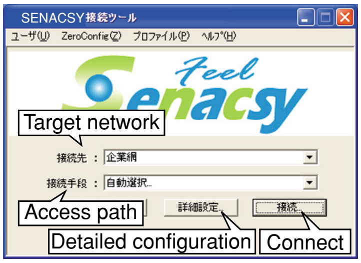
Fig. 2. System overview.



ユーザID : 12345678

PINコード : *********

Fig. 3. User authentication screen.



接続先 : 企業網

接続手段 : 自動選択...

Fig. 4. Main screen.

lists access paths. An access path consists of a series of procedures that describes the configuration of network devices and protocols. If there are multiple access paths to reach the target network and the user does not know which is appropriate, he can choose “auto selection”. In this case, the SENACSY tool chooses the most suitable access path and connects his PC to the target network automatically. The user does not have to perform any troublesome settings, because the profile contains all the information needed to access the target network. Thus, this system solves the problem of complicated user operations to access the target network. We call this function for automatically accessing the enterprise network a “ZeroConfig function”. It is achieved by the profile structure. The following section explains the profile structure and the ZeroConfig function.

5. Profile structure and ZeroConfig function

5.1 Profile structure and profile issuing function

An example of a profile structure is shown in **Fig. 5**. The profile is organized hierarchically. It has four levels called profile list, profile group, access profile, and profile component. The profile group corresponds to the target network in Fig. 4. The access profile corresponds to the access path in Fig. 4. Each profile component has network or authentication protocol parameters. The network interfaces and protocols supported by the SENACSY tool are shown in **Table 1**. Almost all the protocols used in enterprise networks are supported.

An access profile and a profile group consist of one or more profile components and access profiles, respectively. Access profiles in a profile group have

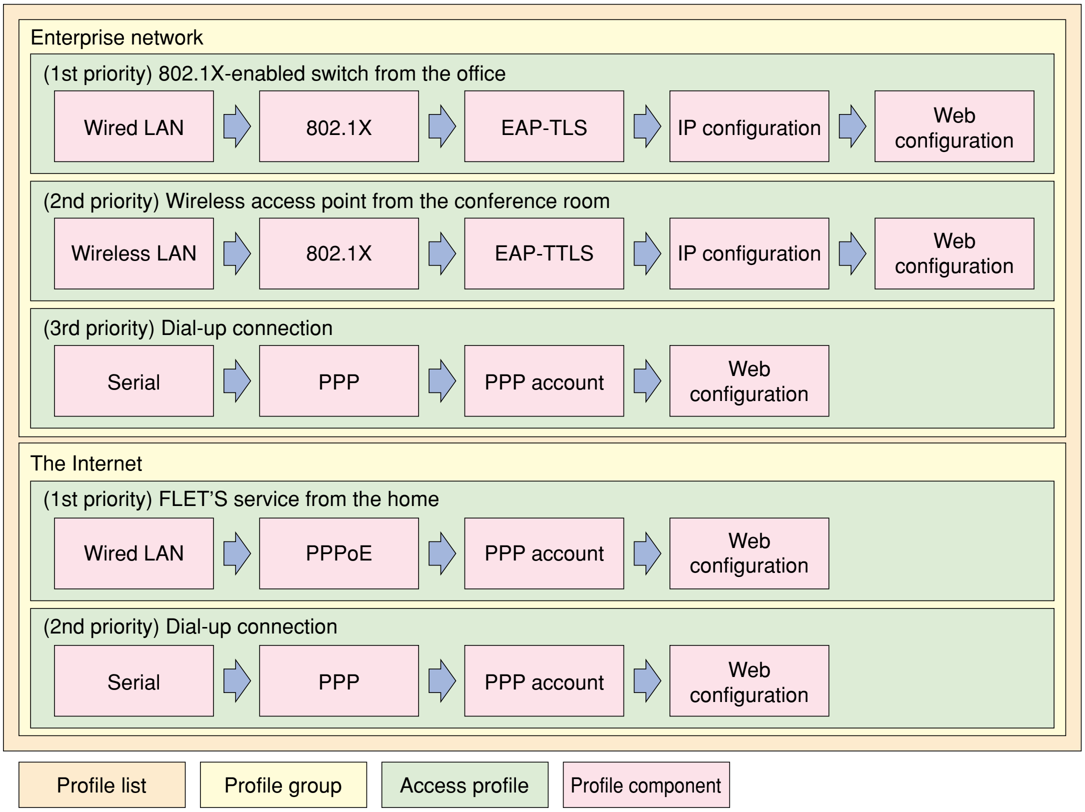


Fig. 5. Example of a profile structure.

Table 1. Supported network interfaces and protocols.

Network interface	Wired LAN (IEEE802.3), wireless LAN (IEEE802.11), serial
Protocol	IP(v4), PPP, PPPoE, IPsec (manual-key, preshared-key, PKI), IEEE802.1X (EAP-TLS/ EAP-TTLS)
Others	Web configuration, routing configuration, quarantine configuration (with personal firewall)

IP: Internet protocol, PPP: point-to-point protocol, PPPoE: PPP over Ethernet, PKI: public key infrastructure, EAP: PPP extensible authentication protocol, TLS: transport layer security, TTLS: tunneled TLS the same target network. When a profile group includes multiple access profiles, each access profile is given a priority. If the profile group is for the enterprise network in Fig. 5, then “802.1X-enabled switch from the office” has the highest priority, “wireless access point from the conference room” has second priority, and “dial-up connection” has third priority. A user can change the priorities in a profile via the SENACSY tool. A profile list includes one or more profile groups as shown in Fig. 5.

It is very important that profiles are issued effectively because the profile generating system issues all the profiles for all users. The fields of a profile can be classified into two types: individual and common information fields. The network administrator generates a profile through two steps. First, he generates a template that includes the common information for all users. Then, he generates a profile by adding individual user information. By decreasing the number of fields required to generate the complete profile, the system enables the network administrator to issue profiles effectively.

The network administrator must consider the relationship between profile components because an access profile is a series of profile components. For example, he must select one out of “serial”, “wired LAN”, and “wireless LAN” for the first profile component in an access profile. In addition, he must select a “PPP” profile component after the “serial” profile component. However, the system constrains the network administrator so that mistakes cannot be made.

5.2 ZeroConfig function

Here, we explain the operation of the ZeroConfig function using the example in Fig. 5. In this example, we assume that the user accesses his enterprise network from outside his office buildings.

First, the SENACSY tool tries the first access profile: “802.1X-enabled switch from the office”. However, this fails because the user is outside his office buildings and there is no wired LAN cable connected to his PC. Second, the SENACSY tool searches for the wireless access point specified in the profile component of “wireless LAN” to access the enterprise network. However, this also fails because the user is outside his office buildings and the SENACSY tool cannot find the wireless access point in the conference room. Finally, the SENACSY tool tries “dial-up connection”. If his PC is equipped with a wireless dial-up device such as a cellular phone and it is in a communication area, the user can connect his PC to the enterprise network.

The SENACSY tool tries to access the target network in the order of priority associated with the access profile. However, the user can choose a specific access profile in the main screen when he wants to specify the access profile to use. In this case, the SENACSY tool tries to access the target network directly by that method.

6. Comparison with other products and introduction example

6.1 Comparison with other products

There are some products that help users to connect their PCs to their target network. For example, “IBM Access Connections” [5] is a connectivity-assistant program for ThinkPad*. Users of the “IBM Access Connections” are able to create and modify network configurations for their PCs. Therefore, it is difficult to force the users to follow the network management policy and to prevent the configuration information from being exposed to anyone.

As another example, Kyocera Communication System Co, Ltd provides an integrated authentication service called “NET BUREAU” [6], which enables a network administrator to force the users to follow the network management policy. However, it does not support as many protocol combinations as SENACSY does, so it is difficult to introduce “NET BUREAU” into existing enterprise networks without any change.

SENACSY supports many protocols, as shown in Table 1, and can combine protocols if the combination conforms to protocol standards, so SENACSY can be easily introduced into existing enterprise networks without any change or much additional cost. This is an important feature because most enterprises already have networks.

6.2 Introduction example

The operating systems (OSs) required by this system are shown in **Table 2**. The SENACSY tool is installed on the user’s PC. The profile generating system consists of a server and clients so that this system can be operated by multiple network administrators simultaneously.

We introduced this system into the Otemachi communications building of the NTT holding company in March 2005 and 60 users are currently utilizing it. This system is part of the “storage centric security system” announced in a news release in April 2005 [7].

* IBM personal computer division was acquired by Lenovo group in 2005.

Table 2. Required OSs.

Component	OS
SENACSY tool	Windows XP Professional & Home Edition, Windows 2000 Professional
Profile generating system (server)	RedHat Enterprise Linux ES3.0, RedHat Linux9
Profile generating system (client)	Windows XP Professional (Internet Explorer 6.0)

7. Future work

This system automates the procedure for establishing a network connection. In the future, we will examine various functions such as one that enables the enterprise system to be available after a user logs in to the OS. We are also planning to support other authentication tokens being developing in the NTT group besides the currently supported iKey1000 [8] produced by SafeNet Inc.

References

[1] LAN/MAN Standards Committee in IEEE Computer Society, "Port-Based Network Access Control," IEEE Std 802.1X, 2004.

[2] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC2401, 1998.

[3] Y. Kagei, K. Nakagawa, T. Tachi, M. Takeda, and T. Nakagawa, "Cyber Security Project for Safe and Secure Network Services," NTT Technical Review, Vol. 3, No. 5, pp. 17-24, 2005.

[4] http://www.rsasecurity.com/rsalabs/node.asp?id=2133

[5] http://www.pc.ibm.com/us/think/thinkvantagetech/accessconnections.html

[6] http://www.kccs.co.jp/products/netbureau/ (in Japanese).

[7] http://www.ntt.co.jp/news/news05/0504/050426.html (in Japanese).

[8] http://www.safenet-inc.com/products/tokens/ikey1000.asp

Takeshi Kaji

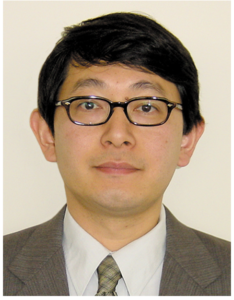
Research Engineer, Communication Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.S. degree in computer science from Osaka University, Osaka in 1996 and the M.S. degree in computer science from Nara Institute of Science and Technology, Nara in 1998. In 1998, he joined NTT Multimedia Network Laboratories in Tokyo. He is a member of the Information Processing Society of Japan (IPSJ).

Takao Yamashita

Research Engineer, Communication Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.S. and M.S. degrees in electronics engineering from Kyoto University, Kyoto in 1990 and 1992, respectively. In 1992, he joined NTT Software Laboratories in Tokyo. He is a member of IEEE, the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan, and IPSJ.



Shinya Matsumoto

Research Engineer, Communication Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.E. degree in electronics and the M.E. degree in electrical engineering from Doshisha University, Kyoto in 1987 and 1989, respectively. In 1989, he joined NTT Communication Switching Laboratories in Tokyo. He is a member of IEICE.

Masayuki Kobayashi

Senior Research Engineer, Communication Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.S. degree in electrical engineering from Shinshu University, Nagano in 1981. In 1981, he joined the Electrical Communication Laboratories, Nippon Telegraph and Telephone Public Corporation (now NTT). He is currently engaged in R&D of secure network access systems. He is a member of IEICE.

Masayuki Nakajima

Senior Research Engineer, Communication Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.S. and M.S. degrees in physics from the University of Tokyo, Tokyo in 1983 and 1985, respectively. In 1985, he joined NTT Atsugi Electrical Communication Laboratories. He studied LSI fabrication equipment for twelve years. After a temporary transfer to Plala Networks Inc. as a director, he moved to his present position and is developing ubiquitous network software that includes communication, authentication, and cipher functions. He is a member of the Physical Society of Japan.