UDC 621.395.74:681.32.004.4

Total Security Solution System: @SECUREVISION – Essential Security for Net Businesses –

●Takashi Ohgo

(Manuscript received September 24, 2000)

The numerous cases of cracking into government agency Web pages since the end of January 2000 have brought the necessity for Web site security very close to home. Success in Internet business requires an effective means for preventing unauthorized or illegal accesses. Besides making its access authorization system even stronger, Fujitsu has introduced "@SECUREVISION," a total security solution for supporting corporate security that can be flexibly tailored to specific customer needs.

1. Necessity for a secure environment

Because of Internet technology (e.g., IP protocol), corporate networks are expected to experience a big expansion in the 21st century, regardless of a company's industry or its type of business. Examples include extranet conversion of corporate information systems, direct transactions with individual consumers utilizing browsers, and SFA implementation for building marketing systems fully supplied with information. Security is a vital issue that must be addressed in this age of global IP networks. However, because the term "security" is so broad and the introduction of security systems does not directly contribute to convenience or effectiveness, not to mention business profits, it is often apt to be neglected. Even though many companies recognize the need for security, many do nothing about it because the effects of the investment are invisible.

Information systems are constantly being threatened by attacks in such forms as cracking into Web pages via networks, SPAM mail,[note 1)] and programs known as viruses. Internet security to combat such threats must utilize solutions that feature a good balance between the technical and operational aspects.

The recent illegal accesses to Japanese government agency Web pages, denial of service (DoS) attacks on search sites, computer viruses such as "LOVELETTER," and ISO standardization of security measures have caused a significant change in the security environment, as evidenced by the action now being taken by many organizations. Now that the threat of the Y2K problem is behind us and signs of economic recovery are appearing, particularly in the IT area, the year 2000 marks the beginning of full-scale efforts at network security.

Although Fujitsu has been offering security solutions to its customers primarily through our Secure Systems Promotion Section, beginning in February 2000, we aim to further reinforce our organizational structure, particularly to ensure system security that meets the requirements of an Internet connection environment.

---

note 1) SPAM mail:
Electronic mail sent to a recipient regardless of whether the recipient requested it and whose purpose is commercial and/or to annoy.

2. Features of @SECUREVISION

Fujitsu unveiled @SECUREVISION in May 1998 as an integrated security solution system to support network computing security. Since then, we have been significantly upgrading the product and its services by adding such features as "PC Security Solution," which uses a smart card[note 2] and other personal authentication technology (explained in detail later). In September 2000, we unveiled an enhanced version of the system by adding to and enhancing the services, for example, by acquiring the authentications of ISO/BS and observing and auditing network security. The features of @SECUREVISION are explained below.

1) Complete provisions for planning, configuring, and operating a system based on a specific security policy

With the requirements of the IP age becoming increasingly complex, it is now very important to select and operate products that use security technologies based on a good security policy. @SECUREVISION offers a total solution to security, spanning all aspects from the formulation of a company-wide security policy to the building and operation of a secure system.

2) Integrated security management functions

The products and services incorporated in @SECUREVISION conform to international standards and are integrated to have excellent interconnectivity with other companies, even companies in other countries. Furthermore, they also have interoperability features such as total management of security servers and unified authentication.

3) Services and supports with specialized organizations and experts

Security services such as consulting, security server configuration, and 24-hour/365-day monitoring are provided to customers by security experts in specialized organizations within the Fujitsu Group. They support not only planning, configuration, and system operation, but also help customers acquire the ISO15408 and ISO17799 (BS7799) security authentications.

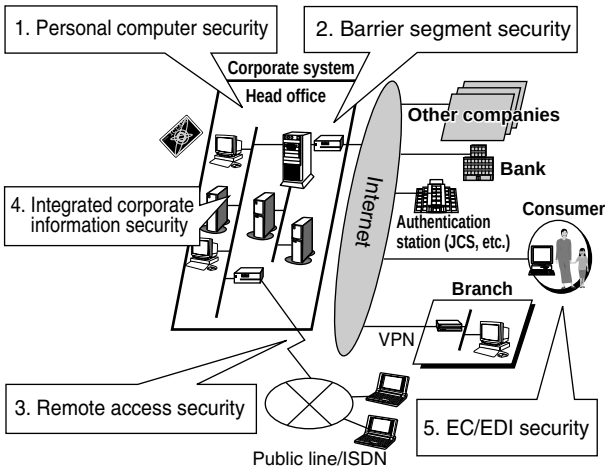

Figure 1
Examples of security solutions.

3. Overview of @SECUREVISION

As already described, the term "security" has an extremely broad meaning. @SECUREVISION is therefore divided into five parts to enable Fujitsu to meet the precise needs of each user (**Figure 1**). The main parts and services of @SECUREVISION are described below.

There are two important facets of the enhanced version, which was unveiled in August 1999. The first facet concerns personal identity authentication, which is a very important security measure that verifies the identity of the user. Providing a high degree of security with conventional systems using only personal IDs and passwords has proved difficult at best. In response, we offer the PC security solution shown in **Figure 2**. This solution combines our recently developed Smart Card Authentication software for high-reliability, high-expandability personal authentication with a fingerprint recognition device. The use of smart cards eliminates the trouble of having to memorize multiple passwords. It also

note 2) Smart card:
An IC card having an embedded IC chip in which data can be stored as well as functions for authentication based on the user's personal identification number (PIN) and calculation function.

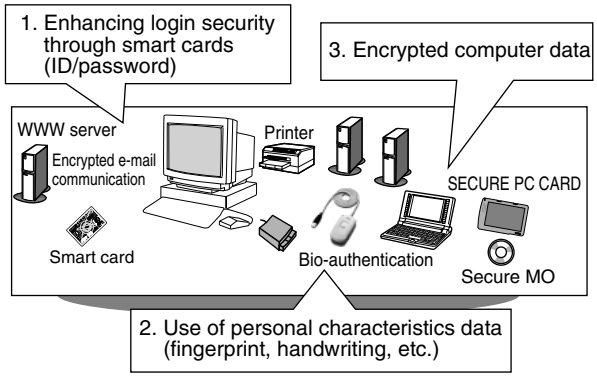

Figure 2
PC security – enhanced PC security and protection of resources.

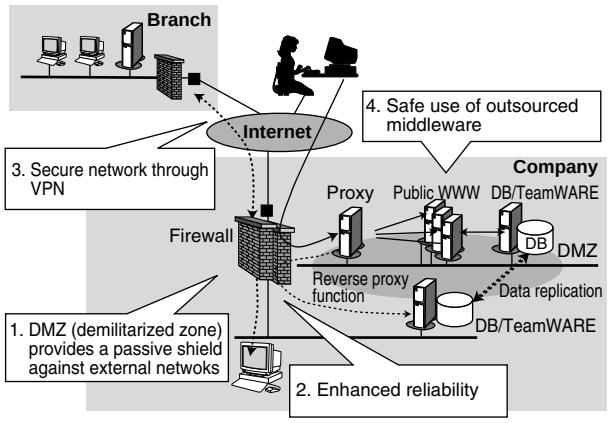

Figure 3
Barrier segment security – prevention of unauthorized access from outside the system.

prevents impersonation resulting from the theft of passwords and IDs as well as tapping into networks. The initial features of the sophisticated PKI environment unique to @SECUREVISION include the storing of digital certificates[note 3] in smart cards to facilitate access by the user, mail encryption, and single sign-on.[note 4] These features also facilitate expansion of the security measures.

The second facet is the addition of Netshelter, a hardware/software single-unit dedicated security device, to the Barrier Segment Security solution for preventing unauthorized access (**Figure 3**). When the Internet is used, VPN[note 5] and firewall functions can easily be installed.

4. Smart card authentication

Smart Card Authentication is a PC authentication package that uses smart cards (**Figure 4**). As well as providing a method for logging on to a Windows system, a single smart card also enables construction of high-level security systems as explained below.

1) Windows logon
Records the user ID and password on the smart card to enable user authentication.

2) WWW browser user authentication and encrypted communication
Uses the digital certificates in the smart card to facilitate client authentication (SSL v.3.0[note 6]) and encrypted communication via Internet Explorer and Netscape Communicator.

3) Electronic mail encryption and digital signatures
Uses digital certificates in the smart card for S/MIME mail encryption, user authentication, and the prevention of cracking with Outlook Express and Netscape Messenger.

4) Upgraded personal computer security
The smart cards have a function for locking

note 3) Digital certificate:
Part of the secret key or public key used for encryption in a public key encryption system by which the authentication station determines whether the public key of a communicating party is the registered public key of the party that the communicating party claims to be. Also called a "public key certificate."

note 4) Single sign-on:
A mechanism by which a user performs a single authentication procedure and is then given access to all systems for which the user has access authority.

note 5) VPN (Virtual Private Network):
A technology or network for the implementation of virtual dedicated line networks utilizing encryption, user authentication, etc., on a public network. Also called a "virtual restricted area network."

note 6) SSL (Secure Socket Layer):
A mechanism for maintaining data security when using a Web browser, etc. Proposed by Netscape Communications of the U.S.

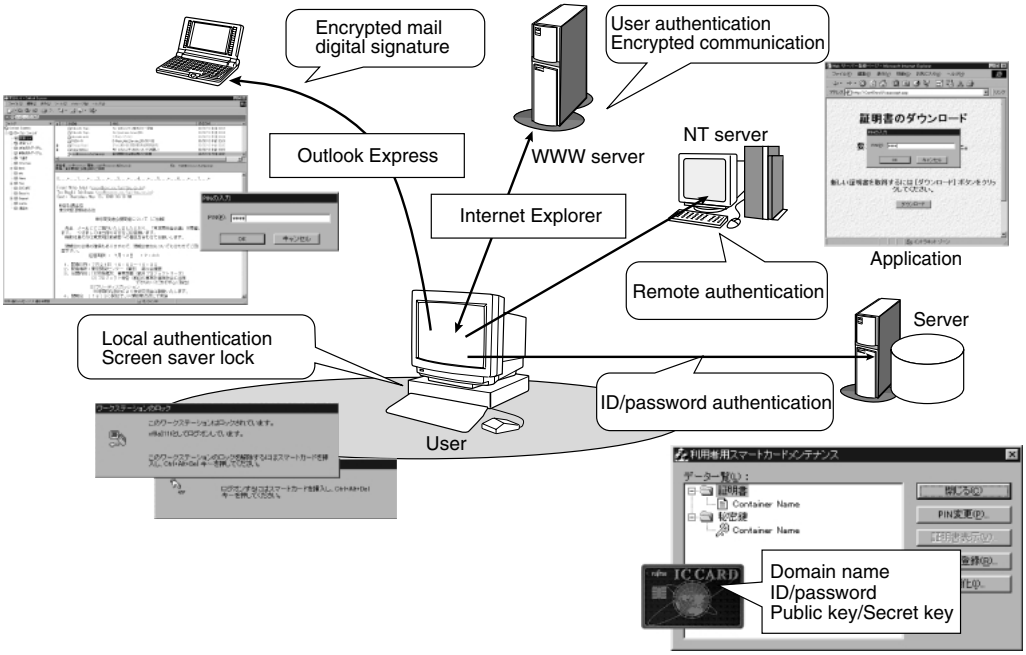

Figure 4
Smart card authentication.

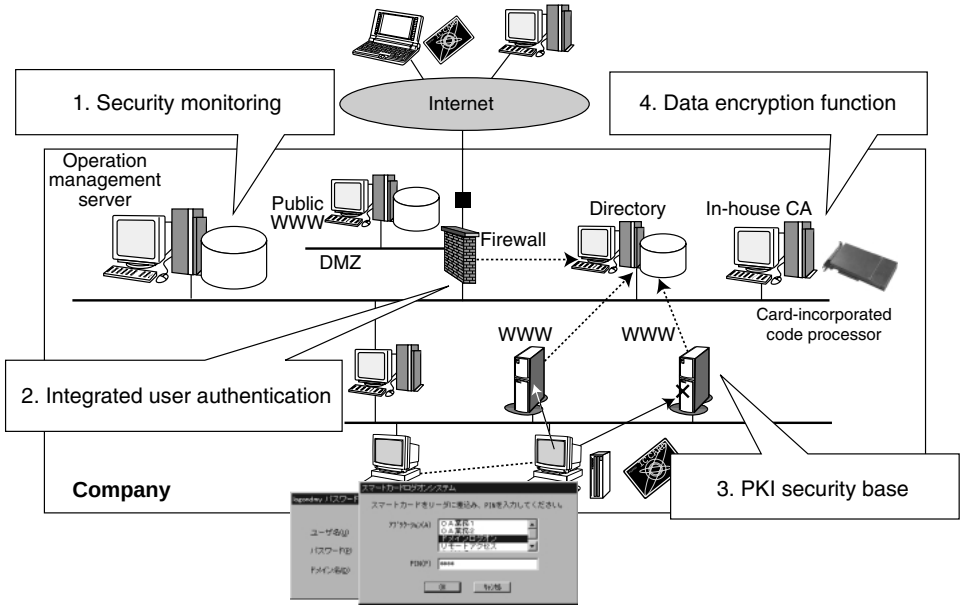

Figure 5
Integrated corporate information security.

and unlocking screen savers and a function that enables the specification of the operations that individual users are allowed to perform.

5. Sophisticated PKI environment

The PKI environment, shown together with the Integrated Corporate Information Security solution in **Figure 5**, is closely linked to smart cards and has been a special feature of @SECUREVISION since it was first released. The PKI environment consists of a CA server which issues public key identity certificates, InfoCA for Enterprise PKI Manager, InfoCA Key Protection

Option, a directory server that stores certificates and other user information, and InfoDirectory and Enterprise PKI Manager, which manage certificates. These elements not only provide for encrypted communication, identity authentication, and the prevention of cracking and impersonation, but they also provide centralized management of user information such as IDs, passwords, and certificates and single sign-on through SystemWalker/getAccess. Previous systems had problems with the management of the certificates and secret keys of users stored in the client's personal computer. With this system, each user carries his or her own smart card, making it possible for many people to use the same client PC. This has also enabled dependable, precise authentication for mobile computing.

Recently, many insurance and agent systems, manufacturing transaction terminals, and shared school terminals have been installed. Also, open networks are becoming increasingly utilized to make declarations and apply for licenses under such themes as "Electronic Government," which is a part of the Millennium Project.

6. Barrier segment products matched with application size

Our barrier segment products prevent unauthorized access at the front line. Of these products, the firewall plays the most important role. A wide range of firewalls can be selected depending on the size of the application, ranging from a hardware/software single unit type to personal computer server and UNIX server types (**Figure 6**). NetShelter, a single-unit dedicated security device provided with enhancements, is available in two types: NetShelter/VPN, which provides VPN functions; and NetShelter/FW, which has both VPN and firewall functions. Because NetShelter does not require an operating system installation and has simple parameter settings, it makes it easy to build a secure system.

Because Safegate, NetShelter/FW, and NetShelter/VPN all employ the Safegate architecture using the firewall management software, "Safegate Central Control," management can be conducted in the same way as for the personal computer server and UNIX server types of Safegate. Installing a Safegate client also enables VPN

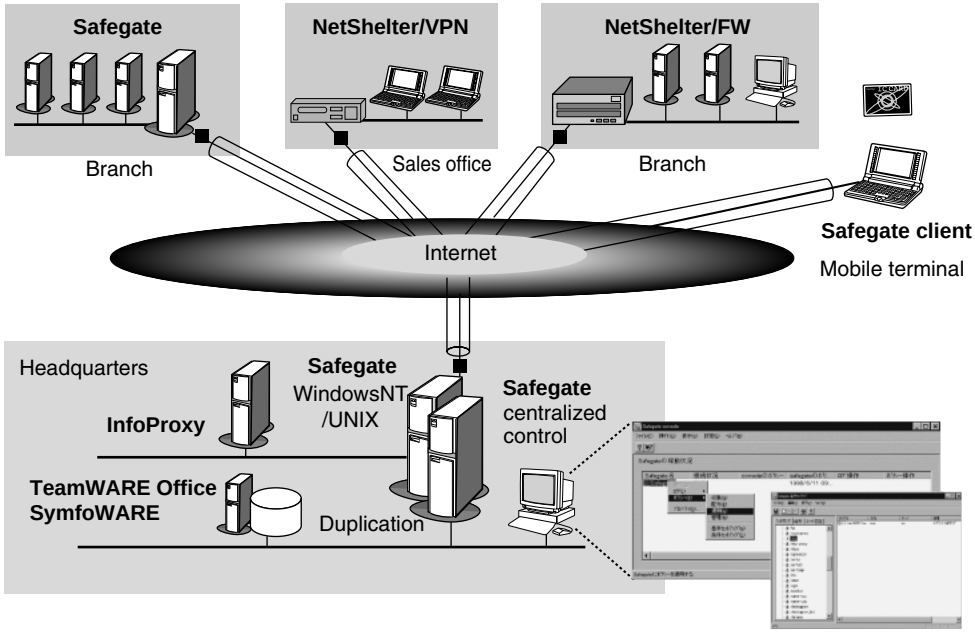

Figure 6
Barrier segment products for a wide range of applications.

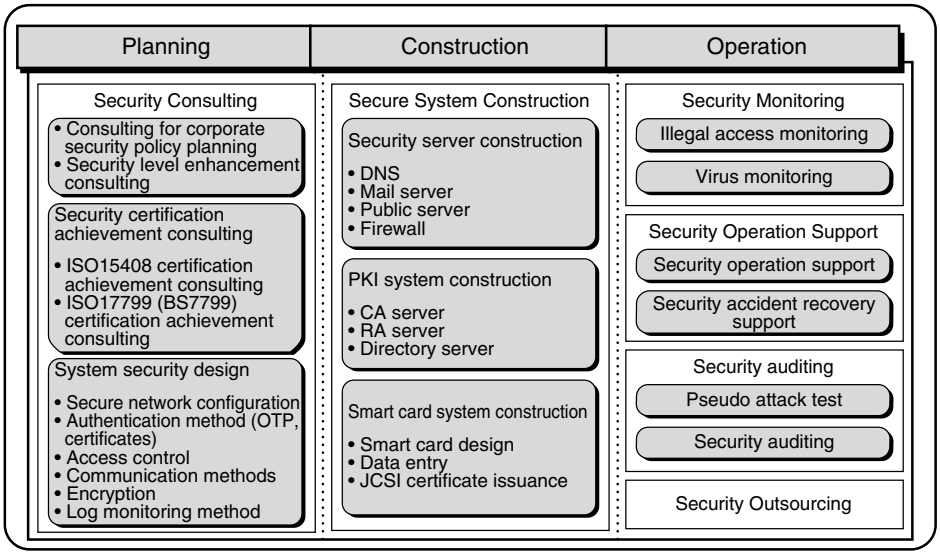

Figure 7
@SECUREVISION service system.

communication between mobile clients. Safegate is the first Fujitsu security product to obtain ISO15408 certification.

7. Information security service – InfoSecure

The @SECUREVISION service system is shown in **Figure 7**. For the "upstream processes" of system configuration, @SECUREVISION uses the InfoSecure service for formulating information security policy based on international standards (ISO/IEC 15408, Guidelines for the Management of IT Security, A Code of Practice for Information Security Management, etc.).

The achievement of adequate security requires a clarification of the company's security policy and also requires product selection, system construction, operation, and monitoring in accordance with this policy. Recently, Fujitsu surveyed 350 companies regarding their current information security provisions. The results were analyzed and classified into nine categories (organization, operation management, education, etc.). We found that none of the averages for the nine categories met international standards (**Figure 8**).

To implement InfoSecure, a security policy

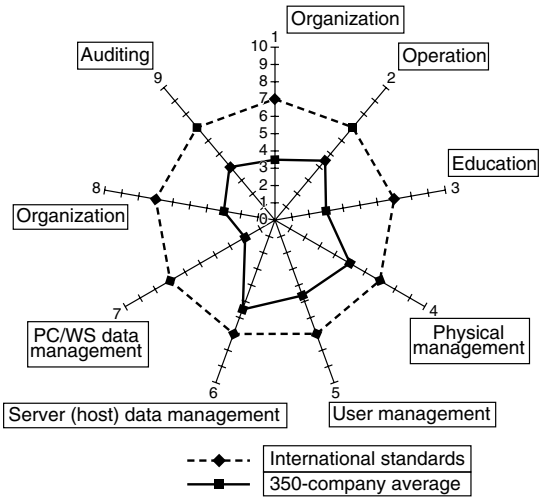

Figure 8
Analysis of current information security systems.

is drawn up and the client's current problems are analyzed through the following procedure:

- Simple evaluation of information security
- Consultation on formulation of information security policy
- Consultation on reinforcing information security support

Then, within a short space of time, we propose system improvements that will fulfill the minimum requirements for information security, which could even be regarded as part of a

company's responsibility to society. Fujitsu also actively supports the implementation of the most effective information security solutions for the least amount of investment.

Furthermore, we added new services in September 2000 called "ISO15408 certification achievement consulting" and "ISO17799 (BS7799) certification achievement consulting." These are based on the results of configuring and operating Internet banking systems, making Internet data centers conform to security standards, and experiences gained from the first overseas acquisition of authentication for the Safegate firewall.

In our ISO15408 certification achievement consulting service, we give consultations on making a system conform to ISO15408 and help customers obtain the authentication of the Communications-Electronics Security Group (CESG), which is an important British authentication organization. Customers can quickly obtain the authentication because the estimations are made in Japan. In the ISO17799 (BS7799) certification achievement consulting service, we provide consultations on the various phases of a system's lifecycle, for example, system organization, training, and operation, and consultations for acquiring CESG authentication.

These two services help customers obtain a certificate from a respected authentication organization and therefore can improve their corporate image and show to their own customers that their security can be trusted.

8. Brand new security service

The most conspicuous point of the enhancement of September 2000 is the addition of a brand new security service (**Figure 9**). In this service, using the Internet, security specialists monitor customers' systems round the clock from the Fujitsu Network Monitoring Center to ensure that the wisest security measures are being taken. If there is an emergency, the center immediately calls the customer and the security experts of Fujitsu Security Partners' Network take appropriate measures to cope with the situation. Fujitsu Security Partners' Network is a professional group that provides high-grade customized services. When the service was started in September, 44 companies of the Fujitsu group participated.

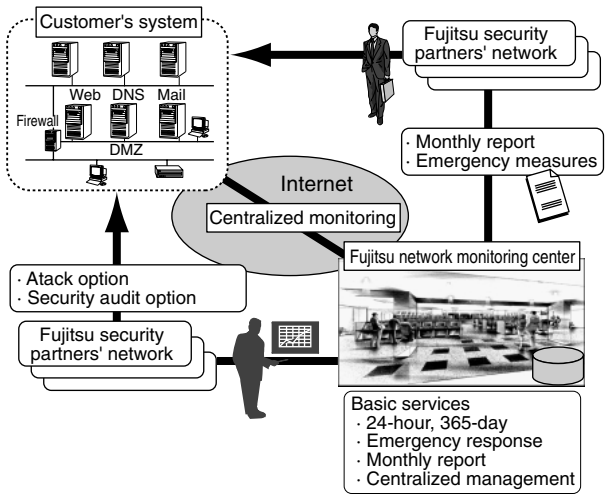

Figure 9
New security service.

In addition, this new service has many other advantages, for example, it can monitor not only the barrier segment but also an intranet, there are no initial costs for the standard service, the standard service includes an insurance policy for damage compensation, and audit/operation advice options are available.

As described at the beginning of this paper, security to protect against unauthorized and illegal accesses has become a big theme for company systems. However, developing countermeasures against the increasingly sophisticated tools being used for illegal access, searching for and monitoring security holes, and providing 24-hour monitoring has become a huge burden on the systems divisions of companies. Therefore, Fujitsu's new security service supports corporate security to provide total safety and reliance. The new service is partly based on the knowledge Fujitsu gained by analyzing the security aspects of 3000 company systems, 2000 configurations, and 24-hour monitoring for 200 systems.

Takashi Ohgo received the B.A. degree from the Department of English of Obirin University, Tokyo, Japan in 1987. He joined Fujitsu Keihin Systems Engineering Ltd., Yokohama, Japan in 1987, where he was engaged in development of UNIX packaging software, construction of large-scale business systems using UNIX servers, and Internet support business. He transferred to Fujitsu Ltd., Kawasaki, Japan in 1998, where he has been working on the support of security technologies.
He is a member of Firewall Defenders and the Japan Network Security Association.