Fujitsu Enterprise Security Architecture

● Tetsuo Shiozaki   ● Masayuki Okuhara   ● Nobuo Yoshikawa

Recently, there has been a growing need for enterprises to respond to compliance requirements and an open framework in order to better serve society. To address this need, information security plays a vital role. Moreover, establishing predetermined Enterprise Security Architecture (ESA) in corporate systems is also becoming increasingly important. This paper describes Fujitsu's approach toward the concept of ESA.

1. Introduction

In recent years, the ratio of information security investments to total corporate investments has been rising annually. These investments are indispensable for enterprises that intend to counter security risks. However, the effectiveness and efficiency of information security investments have yet to be discussed in great detail. It is thus necessary to maintain Enterprise Security Architecture (ESA) as a guideline to ensure the efficiency of information security investments.

This paper first describes the need for ESA, and then the characteristics required of that architecture. Finally, it introduces ESA originally developed by Fujitsu.

2. Need for ESA

ESA is a documented concept that systematizes the vision of security countermeasures to clarify a technical, basic policy of information security measures in an enterprise. When planning a system of information security measures and procuring the security equipment necessary, an enterprise should always check the adaptability to its own ESA. By making this check, the enterprise can avoid adopting a system and related equipment that do not comply with its ESA. In this way, the information security measures taken in the enterprise become adjustments that can be easily integrated, and thus ensure the effectiveness and efficiency of security investments.

The Need for ESA in enterprises

When computers were initially commercialized, people considered information security to be "a means of preventing illegal data access." In the mid-1980s the U.S. Department of Defense settled on "the Trusted Computer Security Criteria" as a security requirement standard for computer systems. As a result, many engineers began to consider the various functions of information security, such as records of certification and logs. Moreover, as the world of computers entered the era of open systems in the 1990s, the world of information security measures changed significantly. Computer makers originally embraced, designed, and incorporated the concept of information security during the age of the mainframe.

However, given the proliferation of open standards, systems composed of equipment

provided by multiple manufacturers became mainstream. In conjunction with this change, the information security function became subdivided into many functional components. This provided the user with many advantages, including enhanced cost reduction and a greater degree of freedom in selecting equipment. Conversely, it became the user's own responsibility to select each unit of component equipment. In fact, the user became responsible for all considerations regarding system operation, like the interconnectivity of equipment, compliance with data formats, and an applicable management method to ensure standardization. In particular, since safety could be adversely affected by combining different types of equipment and software in the field of information security, the user had to pay close attention to this matter. Consequently, many accidents and problems could occur due to improper combinations, and thus gave rise to the idea that, "information security is difficult and costs too much." ESA was developed to resolve this situation.

3. What is ESA?

In Japan at the beginning of 2000, security investments were considered necessary to control risks. This period was referred to as "the age of security risk measures." The investments made for security countermeasures were considered somewhat of a "sacred cow" and organizations were prohibited from reducing such investments. Moreover, security countermeasures were also considered a cost that did not generate profit. The targets of security countermeasures were to achieve confidentiality, integrity, and availability.

Today, however, security investments are believed to enhance the value of an enterprise. The current era is called "the age of information security governance." Thus, security investments are no longer considered a sacred cow but "part of normal company activities." Security countermeasures are not costs but "investments to ensure profit in the future." Therefore, it is necessary to add effectiveness and efficiency to the targets of security countermeasures.

In many enterprises, various types of security equipment and software were introduced to counter threats. However, many diverse issues were posed in enterprises where such security countermeasures were taken separately. For instance:

1) Two or more sets of software cannot coexist, thus causing problems .

2) Performance deteriorates as files are increasingly encrypted on telecommunication lines.

3) User information on individuals is separately managed by many systems.

4) Computer systems that handle important information rely on password authentication, even though the latest PCs are equipped with fingerprint recognition capability.

5) Authentication must be done four times before receiving service after PC startup.

Why do such problems occur? There are many answers to the question posed by what security countermeasures to take.[1)-5)] For instance, security standards such as ISO27000, security guidelines, and regulatory system offer some answers. However, there is no answer to the question of how to take security countermeasures. An enterprise should be responsible for designing its own security countermeasures. ESA is necessary for this design. ESA is a documented standard intended to protect property that answers such questions as, "How many measures are necessary, what technology is used, and what technologies are combined?"

ESA can also be described as "a second security policy." A typical security policy is a document that explains what should be done. On the other hand, ESA is a document that explains how things should be done. **Figure 1** shows position of ESA.

4. Measurement of the establishment level of ESA

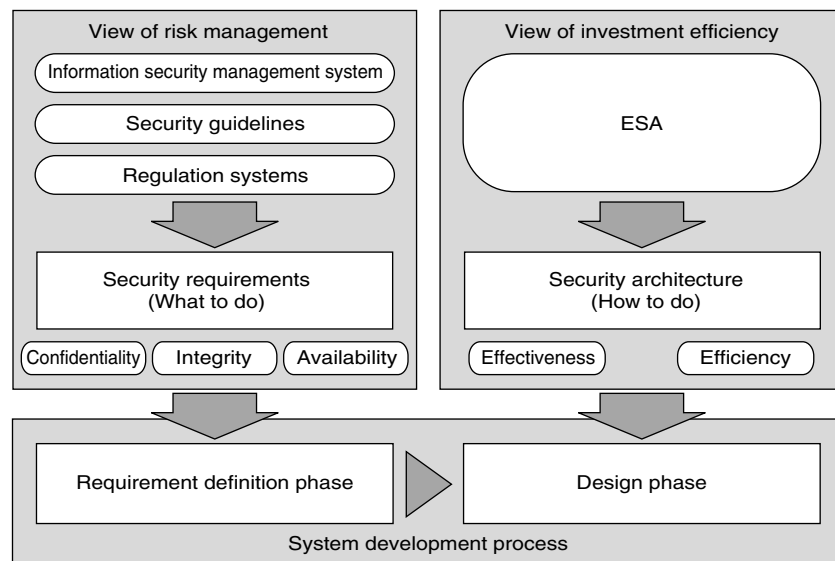In an enterprise, the degree to which ESA has been established can be measured by using

Figure 1
Position of ESA.

the checklist shown in the **Table 1**.

5. Fujitsu ESA[6]

ESA was originally a documented concept intended to be created at each organization. To support enterprises that intend to create ESA in the future, Fujitsu prepared a standard ESA document called the "Fujitsu ESA." This document describes the security architecture necessary for an average organization. For instance, the guidelines for monitoring security cover the following fields:

1) Identification and authentication
   • Type of authentication (what you know, what you have, and who you are)
   • Authentication mechanism and certification devices
   • Authentication model (local, network, or application)
   • Authentication components (LDAP, Active Directory, Proxy Web SSO, and Radius)
   • Next-generation authentication mechanism (SAML and XACML)
2) ID management
   • ID management model
   • ID management architecture
3) Access control
   • Discretionary access control (e.g., ACL, RBAC)
   • Mandatory access control
   • Usage control (UCON) model
   • Access control policy management
   • Technical reference model
4) Audit trail management
   • Audit log collection mechanism
   • Archive framework
   • Audit log analysis
5) Centralized management
   • Incident management
   • Change management
   • Asset management
   • Next-generation security management architecture
6) Cryptography
   • Encryption algorithm and framework
   • Key management
7) Physical security

Fujitsu's ESA can be downloaded from Fujitsu's official Web site. Only a Japanese version is now being offered.

FUJITSU Sci. Tech. J., **43**,2,(April 2007)

155

Table 1
ESA establishment check list.

Category	Check items
Identification and authentication	☐ Is the method of authentication selected according to the degree of importance given to system standardization? ☐ Is the operation load imposed on the user greater than necessity, such as using many passwords together? ☐ Can the user's account be maintained in the latest state at any time with moderate operating cost? ☐ Are duties separated and privileges minimized?
Audit trail management	☐ Does the organization stipulate what logs the equipment and system should record? ☐ Has a mechanism been considered to consolidate and preserve such logs for a long time? ☐ Are there classes of information that should be contained in the logs, as well as standardized forms and meanings in the entire organization? ☐ Are the names of equipment and users recorded in the logs standardized? ☐ Are there methods and tools provided for analyzing the logs?
Access control	☐ Is there a document in the organization that describes what access control to employ in necessary situations? ☐ Are the needs for rule-based access control and roll-based access control examined? ☐ Is the need for minimum privileges examined? ☐ Are not only the users but also identification and authorization of the equipment (such as PCs) examined?
Centralized management	☐ Are the objects (such as users, resources, and equipment) that should be managed clarified in the organization? ☐ Is there a basic policy on the data format of information to be managed (repository)? ☐ Is there a clear set of rules in the organization about the function requirements necessary for such centralized control as management interfaces? ☐ Are the assessment of vulnerabilities and a method of correction clearly defined?
Cryptography	☐ Is there a clear indicator of necessary situations in which to use cryptography? ☐ Is there a selection guideline for the extent and method of encryption? ☐ Is there a clear policy in the organization about the methods of managing and storing encryption keys?
Physical security	☐ Is there a standard provided that covers the facility management technology and building entry point protection that should be used? ☐ Is the correspondence between user information used at room entry and user information on the system examined? ☐ Are appropriate measures taken against earthquakes, fire, and flooding?

6. Structure of Fujitsu ESA

To construct a business system, two or more components that make up the system are extracted, the function requirements for the components are decided according to system requirements, and then the best solution and products to satisfy those specifications are combined. At this time, it is necessary to answer the following questions to ensure security:

1) Is a necessary component corresponding to the demand of the business system properly extracted?

2) Do the function requirements for each component follow security requirements for the organization?

3) Is there any discrepancy (excess or deficiency regarding functions and data) in the combination of components?

4) Do the selected solution and products satisfy the specifications of the component?

The purpose of ESA is to provide appropriate indicators and the best practices regarding security in response to the four questions above. **Figure 2** shows the structure of Fujitsu's ESA.
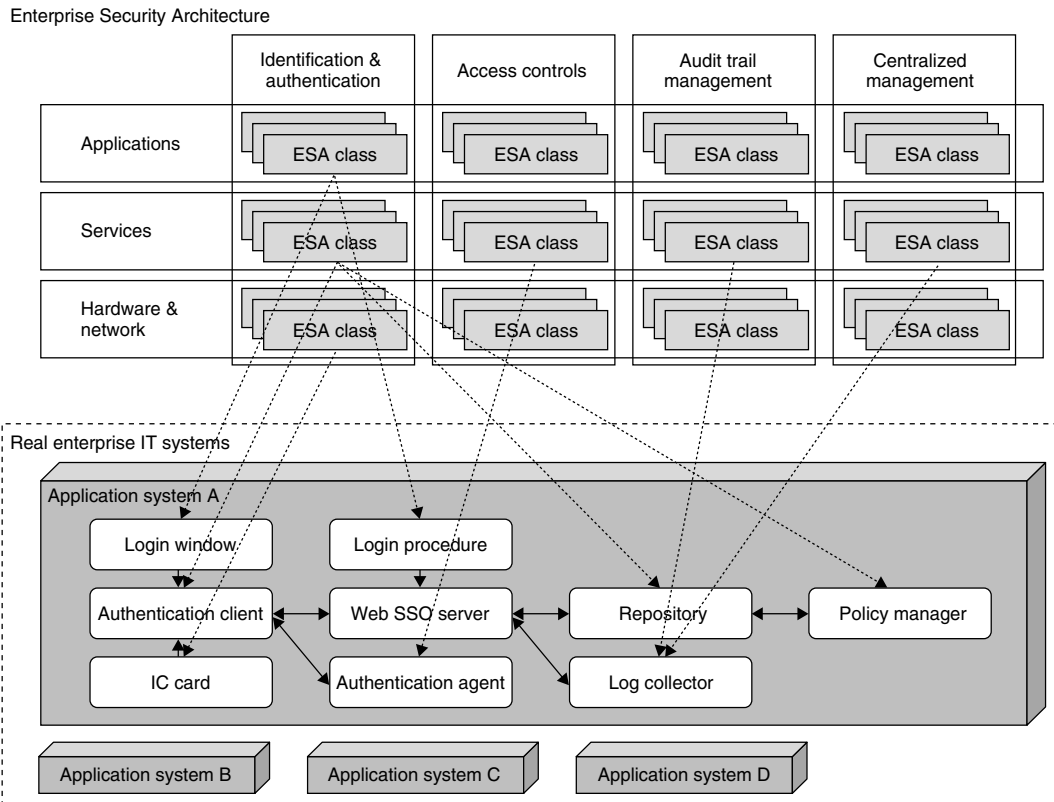
Enterprise Security Architecture

Figure 2
Structure of Fujitsu ESA.

1) ESA prepares the component group (ESA class) that can be selected according to the form of business system.
2) ESA specifies the relationship between the security requirements for the organization and those for the components, and criteria for the selection thereof.
3) ESA describes the combination of components (pattern) and the data exchanged between them.
4) ESA provides a solution and Fujitsu products that suit the components.

As mentioned above, Fujitsu's ESA is not a catalog according to the functions regarding a mere independent solution and related products. It materializes a proven security system in the form of Fujitsu products, a solution where the interrelationship and selection criterion are specified, and the know-how applied according to usage and the requirements.

7. Conclusion

This paper clarified the efficiency of information security investments demanded by enterprises today. To ensure the efficiency of information security investments, it was shown that ESA must be established. Finally, it introduced the content of Fujitsu's ESA.

References
1) ISO/IEC 27001: Information technology — Security techniques — Information security management systems — Requirements. 2005.
2) ISO/IEC 13335-1: Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management. 1995.

3) ISO/IEC 13335-3: Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT Security. 1998.
4) ISO/IEC 13335-4: Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards. 2000.

5 J. A. Zachman: A framework for information systems architecture. *IBM Systems Journal*, **26**, 3, p.276-292 (1987).
6) Fujitsu: Fujitsu Enterprise Security Architecture. (in Japanese). *http://segroup.fujitsu.com/secure/solution/esa/index.html*

Tetsuo Shiozaki, *Fujitsu Ltd.*
Mr. Shiozaki received the B.S. degree in Metal processing industry from the Kyushu Institute of Technology, Fukuoka, Japan in 1980. He has more than 25 years of experience in distributed information systems, security, and risk management. He developed an open vendor system for protection against unauthorized access introduced at the Computer Security Symposium at the Computer Security Symposium held in 1998, and established the SOC (Security Operation Center) in 2002. He has supported Japan G-PKI and provided information security consulting services, ISMS, and information security audits. He is a member of the Japan Information Security Audit and (ISC)2 Common Body Knowledge Forum.

Nobuo Yoshikawa, *Fujitsu Ltd.*
Mr. Yoshikawa received the M.E. degree in Oceanic Architecture and Engineering from Nihon University, Tokyo, Japan in 1992. He joined Fujitsu Ltd., Kawasaki, Japan in 1992, where he has been engaged in development of application systems.

Masayuki Okuhara, *Fujitsu Ltd.*
Mr. Okuhara received the M.E. degree in Mechanical Sciences and Engineering from Tokyo Institute of Technology, Tokyo, Japan in 1990. He joined Fujitsu Ltd., Kawasaki, Japan in 1990, where he has been engaged in the development of security systems. He is a member of the Information Processing Society of Japan (IPSJ).

158

FUJITSU Sci. Tech. J., **43**,2,(April 2007)