

# **Fujitsu Enterprise Security Architecture**



---

May 2007

FUJITSU LIMITED  
Information Security Center

- Microsoft and Windows are registered trademarks of the Microsoft Corporation.
- Sun is a registered trademark of Sun Microsystems Incorporation.
- ITIL (IT Infrastructure Library) is a registered trademark of the OGC (Office of Government Commerce) of the United Kingdom and respective nations of the European Union.
- All other company names, product names, and other similar names are the trademarks, registered trademarks, or product names of their respective companies or products. Note that the trademark symbol and registered trademark symbol are not included in this document.

---

## CONTENTS

1. Introduction .....	1
2. Terminology.....	2
Section 1 What is Enterprise Security Architecture? .....	5
3. Corporate IT Security and Information Security Governance.....	6
4. Enterprise Security Architecture (ESA) .....	7
4.1. The Need for Corporate Enterprise Security Architecture .....	7
4.2. ESA and Security Management Framework (SMF).....	7
4.3. Establishment of ESA .....	8
4.4. Relationship between Corporate ESA and This Document's ESA (Fujitsu's ESA) .....	9
4.5. Layout of this Document .....	10
Section 2 General Principles of Enterprise Security Architecture .....	12
5. Basic Model .....	13
5.1. Enterprise Security Architecture System .....	13
5.2. Access Control Basic Model.....	14
5.3. General Access Control Model.....	15
6. Authentication .....	17
6.1. Identification.....	17
6.2. Authentication and Authentication Elements .....	17
6.3. Two Element Authentication .....	19
6.4. Authentication Devices.....	20
6.5. Authentication Model.....	21
6.6. Other Security Requirements for Authentication .....	22
7. Identity Management .....	24
7.1. The Necessity of ID Management .....	24
7.2. ID Management Requirements .....	24
7.3. LDAP Directory .....	25
7.4. Identity Management.....	26
8. Access Control .....	29
8.1. Access Control Methods .....	29
8.2. Access Control Technologies .....	30
8.3. Bases of Access Control Implementation and Effective Operation.....	32
8.4. Access Control Implementation.....	32

---

8.5. Access Control Policy Consistency and Centralized Management .....	32
8.6. Access Control Mechanism Types .....	33
8.7. Damage Isolation due to Defense In Depth Model.....	33
9. Audit Trail Management .....	35
9.1. Types of Audit Trails .....	35
9.2. Audit Trail Collection and Recording Approach .....	36
9.3. Audit Log Technical Requirements .....	37
9.4. Audit Trail Management Model.....	42
10. Centralized Management.....	43
10.1. ITIL and Centralized Management Background Information .....	43
10.2. Centralization Overview .....	44
10.3. Incident & Problem Management.....	46
10.4. Change Management, Release Management.....	48
10.5. Centralized Management Architecture .....	51
10.6. Next Generation Operation Management Architecture.....	52
10.7. Asset Management .....	54
10.8. Integrated Security Management (Integration with Operation Management System).....	56
11. Encryption .....	58
11.1. Encryption Technology .....	58
11.2. Standardization.....	59
11.3. Shared Key Encryption.....	59
11.4. Public Key Encryption .....	60
11.5. Export Regulations .....	61
11.6. Approach to Encryption Length .....	61
11.7. Hash Functions .....	62
11.8. Response to Algorithm for Encryption in Danger of Losing Centrality of Privacy.....	63
11.9. Encryption Schema .....	63
12. Key Management.....	64
12.1. Fundamentals .....	64
12.2. Key Types and Related Information .....	65
12.3. Key Generation .....	65
12.4. Key Distribution .....	66
12.5. Secure Key Archival .....	67
12.6. Key Backup.....	67
12.7. Key Replacement and Disposal .....	68

---

---

12.8. Key Management Architecture .....	68
13. Physical Security.....	70
13.1. What is Physical Security? .....	70
13.2. Physical Security Demands .....	71
13.3. Access Control .....	71
13.4. Audit Trail Management .....	71
13.5. Centralized Management .....	71
13.6. Security Specification Demands Which Must Be Given Consideration .....	72
13.7. Physical Security Convenience .....	74
13.8. Points to Consider for Biometric Authentication Equipment .....	74
13.9. Use of Video.....	74
Section 3 ESA Based Systems.....	77
14. System Design.....	78
14.1. Security Function Implementation Model .....	78
14.2. Aggregation and Aggregation Deployment.....	80
14.3. ESA Based Model Implementation Example .....	81
15. System Operation .....	96
15.1. System Operation Overview .....	96
15.2. Objectives of This Chapter .....	97
15.3. Overview of System Operation Process.....	97
15.4. Overall Picture of System Operation Processes .....	100
15.5. Concrete Subprocess Examples .....	106
15.6. Relationship between IT Service and Other Processes .....	109
15.7. Summary.....	114
Section 4 Appendices.....	115
16. Representative Frameworks .....	116
16.1. ISO/IEC 27001, JIS Q 27001 .....	116
16.2. ISO/IEC 17799 (JIS Q 27002).....	116
16.3. Information Security Management Standard .....	117
16.4. JIS Q 15001 .....	117
16.5. ITIL (IT Infrastructure Library) .....	117
16.6. ISO/IEC20000:2005.....	117
16.7. COBIT (Control Objectives for Information and related Technology).....	118
16.8. System Management Standard and Supplement.....	118

---

---

17. Risk Analysis Methodology (Example) .....	119
17.1. Risk Control .....	119
17.2. Risk Management Overview .....	119
18. Risk Management Process .....	121
18.1. Plan Establishment .....	121
18.2. Asset Assessment .....	121
18.3. Risk Assessment .....	121
18.4. Threat Evaluation .....	122
18.5. Vulnerability Evaluation .....	122
18.6. Risk Evaluation .....	122
18.7. Remaining Risk .....	123
18.8. Action Plan .....	123
18.9. Risk Reduction Methods .....	123
18.10. Information Asset RTO (Recovery Time Objectives) .....	123
19. Fundamentals of Quantitative Risk Analysis .....	124
19.1. Expected Value .....	124
19.2. Quantitative Determination of Risk .....	124
19.3. Risk Indicator Determination .....	125
19.4. Courtney Method .....	128
19.5. Approach to Vulnerability and Countermeasures .....	128
19.6. Applications .....	129
19.7. Example of Mistakes .....	132
19.8. Limits of Expected Value Based Quantitative Risk Analysis .....	133

---

# 1. Introduction

---

In recent years, the focus on information security has moved from external threats, such as viruses or hacking, to internal threats, such as leakage of personal information.

The report produced by the Ministry of Economy, Trade and Industry's "Corporate Information Security Governance Research Committee" gave the following examples of changes in perspective regarding security countermeasures.

- "Technology" oriented → "Management" oriented
- "Prevention oriented" → "Understanding of inevitability of accidents "
- "Information system problem" → "Manager problem"
- "Don't stop system operation" → "Don't stop business operation"
- "Unprofitable field" → "Field which provides reliability"

There is also a growing demand for consideration of compliance with laws and regulations such as the Private Information Protection Law and the Financial Instruments and Exchange Law (J-SOX), as well as global open frameworks (ISO). In the future, there is also expected to be growing interest in security strategies development in harmony with corporate strategies, specific security activity objectives and monitoring structures, and "information security governance", including security investment evaluation.

We at Fujitsu believe that information security architecture and management framework establishment are important for the establishment of information security governance.

Architecture can be defined as the ordering (unity) of system specifications, much as a building's architectural style is consistent through the entire building. Corporations have a variety of business systems, but by organizing necessary security function elements and providing unified order independent of system conditions and business systems, not only can confidentiality, integrity, and availability be provided, but also information security management which takes into account efficiency and effectiveness.

This document uses our experience in the establishment of (ISC)2 CISSP CBK, and our knowledge of international standards, guidelines, and enterprise architectures (EA), to present and describe security functions and the approach to their design and operation.

The items presented herein apply to the basic requirements for products and services used in our own security solution(SafetyRing), but the principles also apply to general business systems. We hope that this document can be of assistance in establishing your own information security strategies and implementations.

Information Security Center  
General Manager Tetsuo Shiozaki

## 2. Terminology

Below are the main terms used in this document, and their definitions? References for terms, when they exist, are included in brackets at the end of the definition.

I	IT governance	Leadership and organization design and processes for guaranteeing that company IT contributes to organization strategy and organization objective maintenance and expansion.
	IT system	General term for IT infrastructure composed of data, programs, and hardware sources used in business processes. (Chapter 14)
	Identity	Concept of packaging of information regarding a subject.
	Access control	Prevention or limitation of access to an IT system. It includes prevention or limitation of access to data as well as programs.
E	Enterprise Security Architecture	Structured information regarding security for corporate business systems.
A	Availability	Prevention of unauthorized access to information or materials [ITSEC]. The characteristic of an authorized entity being able to access or utilize something when requested [JIS Q 13335-1:2006].
	Audit trail	General term for information needed for auditing.
	Audit log	Formatted information generated automatically by IT systems as a form of audit trail information.
	Integrity	Prevention of unauthorized modification of information [ITSEC]. The characteristic of protection of accuracy and completeness of an asset [JIS Q 13335-1:2006].
C	Confidentiality	Prevention of unauthorized publication of information [ITSEC]. The characteristic of information being unusable or closed to unauthorized individuals, entities, and processes [JIS Q 13335-1:2006].
	Mandatory Access Control	A data access control method using security demands (labels) contained in objects (data) to control security permissions for subjects (users / programs).
C	Corporate Governance	Structure for external monitoring of whether business management is being performed in the interests of shareholders.
	Compliance	Conformance with and observation of rules, laws, regulations, and social norms in corporate management and corporate activities.
L	Least privilege	For both system users and processes, the policy of limiting access to the least number of resources necessary to carry out a particular function.
	Subject	General term in access control for people, programs, etc. which perform access.



I	Identification	Clear categorization and recognition of a subject.
	Asset	Anything which has value for an organization [JIS Q 13335-1:2006].
	Information security	Maintenance of information confidentiality, integrity, and availability. It may also include maintenance of characteristics such as authenticity, accountability, nonrepudiation, or reliability [JIS Q 13335- 1:2006].
	Information security governance	Approach to strategic investment in which effectiveness and efficiency of information security investment is justifiable to stakeholders.
	Information Security Control	Collection of items which must be performed to achieve information security objectives. Also referred to as security control or security management measures.
	ITSEC	Security evaluation standard established in 1990 by the United Kingdom, Germany, France, and the Netherlands.
	Information security policy	Overall organizational security approaches and commands [GMITS].
	Information security management	Organization activities for implementing information security control.
	ISMS	Information security establishment, implementation, operation, monitoring, review, maintenance, and improvements based on approach to corporate risk within management systems [JIS Q 27001].
S	Separation of duties	One of the requirements for control activities. Logical separation of duties for personnel and business processes.
	Security function	Functions for providing security. In this document, "security functions" refer to "authentication", "identity management", "access control", "audit trail management", "centralized monitoring", "encryption", and the like.
	Security functional requirement	Requirements for implementing security functions.
D	Social engineering	Unauthorized access by people to people.
	Defense in depth	Approach to security using multiple security measures in order to improve security and increase amount of time necessary for breaking through security defenses.
T	TCSEC	Security evaluation standard established by the United States Department of Defense Computer Security Center in 1985 (DoD 5200.28 - STD). Known as "Orange Book".
D	Discretionally access control	Access control method in which access to an object is decided based on information for the group to which a subject (user / program) belongs.
	Authorization	Evaluation of whether access is allowed to certain data, as well as the processing which follows this evaluation.

---

	Authentication	Evaluation of whether access is allowed to a system, as well as the processing which follows this evaluation.
R	Resource	Unit for hardware resources containing programs or assets containing programs and data. Ex.) Web servers, DB servers, etc. (Chapter 14)

---

## Section 1 What is Enterprise Security Architecture?

### 3. Corporate IT Security and Information Security Governance

---

IT systems are essential parts of modern corporate infrastructures. Security measures are critical for protecting these IT systems from risks. Generally, 3 - 5% of overall IT investment is for security purposes. Japanese security investment ratios generally exceed that, at a reported average of slightly over 5%.<sup>1</sup>

However, there is an endless stream of incidents involving companies leaking personal information, system failures, and other serious security incidents. This shows that even now, company security measures are often implemented on a case-by-case basis, resulting in security measure effectiveness which is not commensurate with the amount of money invested.

This has resulted in a shift in perception of information security measures, from a backward-looking approach to forward-looking investment approach by companies as a whole, with the goal of increasing corporate worth. This is "information security governance".

One goal of information security governance is the ability to explain the effectiveness of implemented information security measures objectively to third parties. That is, it is necessary to be able to explain to stakeholders such as shareholders the effectiveness (whether the measure is successful) and efficiency (are the results of the measure commensurate with the investment involved) of information security measures. The Corporate Information Security Governance Research Committee Findings Report published by Information Security Policy Office, IT Security Policy Bureau of the Ministry of Economy, Trade and Industry in March 2005 provides the following three types of tools to support information security governance advancement.

- Information security measure benchmarks
- Information security reporting models
- Business contingency plan establishment guidelines

These tools can be used by corporations to clearly communicate the effectiveness and efficiency of their information security measures. They also make it possible to explain the necessity and validity of information security measures, making organizational information security measure implementation easier.

---

<sup>1</sup> Japan Network Security Association "Survey of IT Security Measure Implementation, Operation Status, and Satisfaction", 2004.

---

## 4. Enterprise Security Architecture (ESA)

---

### 4.1. The Need for Corporate Enterprise Security Architecture

When mainframes were first developed, information security consisted of little more than "preventing people from handling other peoples' data". The creation of the United States' Department of Defense "Trusted Computer System Evaluation Criteria" (known as "the Orange Book") in the mid 1980s spread the concepts of information security measures such as authentication and logging. In the 1990's, the "open period", the world of information security changed drastically.

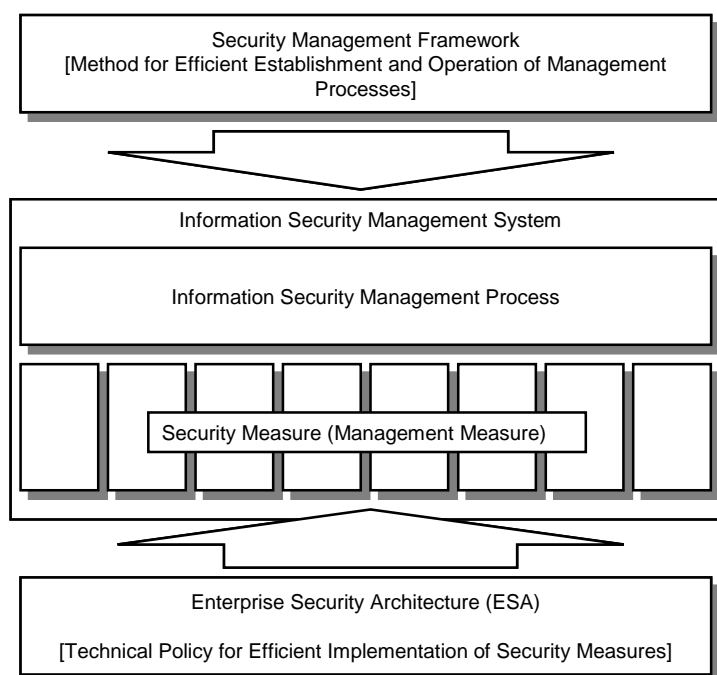
During the mainframe era, manufacturers developed, designed, implemented, and shipped their own information security concepts and approaches. However, with the rise of open standards, it became the norm to have systems composed of equipment from multiple manufacturers and vendors, and with this came the division of information functions into a range of specific functional units. This provided cost reductions as well as increased selection. However, with this came a need for users to select these components themselves. Determining the compatibility of devices, data formats, management method consistency, and other considerations necessary for unified system operation all became the responsibility of the user. Especially in the information security field, the specific combinations of devices and software may have far reaching changes in security levels, requiring special attention from users. As a result, improper combinations of equipment and software resulted in a large number of security incidents and problems, resulting in the common view of information security as difficult and expensive.

Enterprise Security Architecture (ESA) solves these problems. Enterprise security architecture is documentation of a systematized view of a corporation's security approach, clearly delineating the basic technical approach to information security. When a company designs an information security system, or procures equipment, it always confirms compatibility with the company's enterprise security architecture. Equipment which is incompatible with the enterprise security architecture cannot be used. This results in unified corporate information security, and guarantees the effectiveness and efficiency of security investment.

### 4.2. ESA and Security Management Framework (SMF)

General information security management systems, such as ISMS, require the development of management processes for managing the effectiveness of a variety of security measures (management measures). Management processes implement PDCA (Plan-Do-Act-Check), maintaining and improving security management levels through continuous improvement and

proposal activities. Management measures are selected based on organizational risks, and management processes are also responsible for measuring their effectiveness. The Security Management Framework (SMF) consists of the establishment of these management processes, and a systematization of the methodology and know-how involved in operating them efficiently. ESA provides a unified technical approach to these management measures, providing for the efficiency of security investment and effectiveness of security measures. So SMF and ESA are both systematizations which support information security management systems, one from the standpoint of management, and one from the standpoint of technology.



**Figure 4-1 Relationship between ESA and SMF**

#### 4.3. Establishment of ESA

The process for establishing a security architecture in an organization is roughly as follows.

(1) General Security Requirement Survey

First, general security requirements are investigated, focusing on international standards and individual guidelines.

(2) Analysis of Organization's Security Requirements

In addition to determining general security requirements, the specific security requirements of one's own organization are analyzed and organized. For example, this includes restrictions due to security functions in the existing information system, or requirements

imposed by one's own security policy.

(3) Creation of Model Offering Security Functions

In order to evaluate how security functions should be implemented system-wide, a security implementation model is defined. Section 2 of this document contains examples of this type of model.

(4) Clear Statement of Architecture

The implementation model is used to determine a security architecture which suits the particular requirements and conditions of the organization, and this architecture is clearly codified. Individual cases may vary, but this clear security architecture may be reflected in the documentation below.

Organizational security standard documentation

Information system procurement requirement documentation

Protection profile (PP)

(5) System Implementation

System implementation is performed in accordance with the defined security architecture.

The degree to which system requirements should be limited by architecture varies, but generally the stricter the architecture's imposed limitations are, the more unified the architecture becomes, but the less freedom there is in system design.

Established security architecture may fall behind the times as security technology progresses. When this happens, the security architecture needs to be reevaluated. However, this should not take place too frequently. It should always be kept in mind that changing the security architecture goes against one of the primary goals of the architecture, which is the unification of system functions.

#### 4.4. Relationship between Corporate ESA and This Document's ESA (Fujitsu's ESA)

A company's enterprise security architecture is guided by that company's information investment strategy, and a different and unique architecture will exist for each company. However, there are currently a wide range of procurable security technologies, and selecting an architecture with compatible technologies is not a simple matter, and requires a large investment in time and money.

Fujitsu has analyzed the common shared security requirement needs of companies, and developed a widely applicable standard enterprise security architecture. This is the "Fujitsu Enterprise Security Architecture" (this document).

This architecture presents and describes the common information security knowledge platform

needed for architecture consideration, the structure of corporate information security operation, and the information system security function requirements for implementing information security.

#### 4.5. Layout of this Document

This document is composed of three sections and appendices.

"Section 1" explains the background and position of enterprise security architecture.

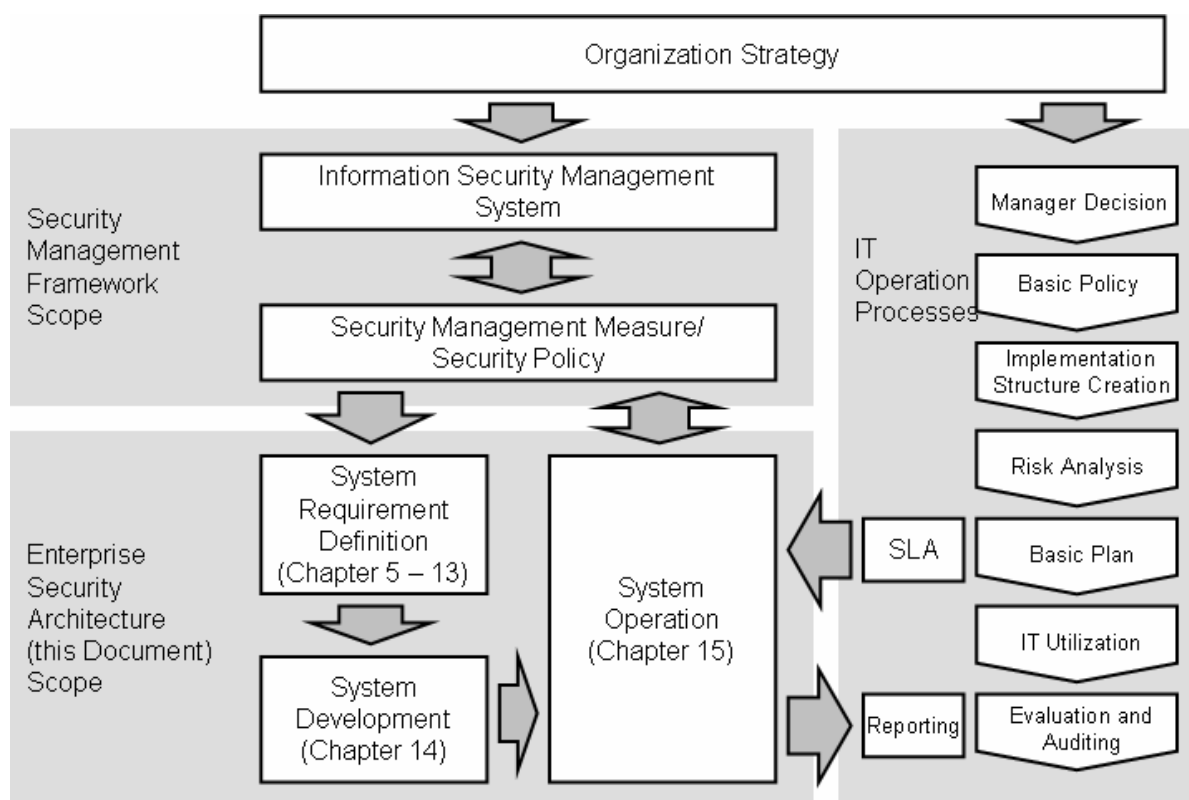
"Section 2" covers the basic concepts needed when establishing enterprise security architecture. For example, it provides overviews, terminology explanations, current trends, representative technologies, and representative models involved in representative security functions such as "authentication", "identity management", and "access control", making up the core section of this document.

"Section 3" uses the approach to architecture provided in section 2 to provide basic approaches to actual system design and operation, as well as descriptions of representative models.

The "Appendices", though falling out of the normal scope of enterprise security architecture, provide risk analysis materials and security policy samples for use as examples for the management framework creation which accompanies enterprise security architecture design. They also contain additional materials which may be valuable when establishing enterprise security architectures.

The relationships between the contents of each chapter and the information security governance activities needed for organization management are shown below. Organization strategy defines information security management systems and their resulting security management measures and security policies. Determining how to systematize and operate them falls under the scope of enterprise security architecture. Service Level Agreements (SLA) when using information systems as services are another factor in security management.





**Figure 4-2 Relationship Between Scope of This Document and Related Scopes**

## Section 2 General Principles of Enterprise Security Architecture

## 5. Basic Model

### 5.1. Enterprise Security Architecture System

The security needs of modern information systems are extremely varied. In order to define an efficient architecture, first security requirements must be efficiently categorized and schematized. Many attempts to schematize security needs have been made in the past. For example, ISO/IEC15408<sup>2</sup> provides a highly complete schema covering functional requirements and security requirements for information systems. However, understanding this schematization requires a background of specialist knowledge. Also, in discussing the high level, abstract subject of organizational systems, it is easy to become bogged down in the granular details of the standard, and lose sight of the big picture.

As such, we have taken here a different approach to organizing security needs. We have placed "authentication and identity management", "access control", "audit trail management", and "centralized management" as the primary foundations when discussing organizational security control, and used them to schematize their related technologies.

In Section 2, we will explain security requirements in accordance with the chart below.

**Table 5-1 Categorization Schema**

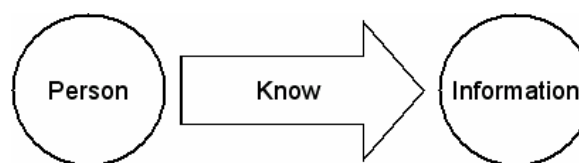
General Category	Functional Category	Chapter in Section 2
Authentication and Identity Management	Authentication	Chapter 6
	Identity Management	Chapter 7
Access Control	Access Control	Chapter 8
Audit Trail Management	Audit Trail Management	Chapter 9
Centralized Management	Centralized Management	Chapter 10
Individual Technologies	Encryption	Chapter 11
	Key Management	Chapter 12
	Physical Security	Chapter 13

<sup>2</sup> ISO/IEC 15408-1:2005 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model, etc.

## 5.2. Access Control Basic Model

The first requirement of information security is "providing information only to specific people, and preventing others from obtaining that information". For example, encryption is a technology designed to do just this. This type of security need is usually referred to in the information security world as "maintaining confidentiality". However, as the extent of information systems increases, and the volume of information expands, additional security needs besides maintaining confidentiality have become evident. One of these is the prevention of unauthorized modification of information in order to maintain reliability. This is generally referred to as "maintaining integrity". Also, in order to eliminate fear of intentional destruction of data or system going down, there is also a need to keep information, and the information systems which handle that information, available when necessary. This is referred to as "maintaining availability". These three elements, "confidentiality", "integrity", and "availability", are often called "the three elements of information security". This concept of the three principles of information security developed from the late 1980's to the early 1990's. For example, the European Information Technology Security Evaluation Criteria (ITSEC)<sup>3</sup> established in 1991 use these three elements of information security as the definition of information security itself.

It is useful to consider a general model when thinking about how to establish a system for satisfying these conditions. Let's consider an example of the most basic form of confidentiality. First, there is "information" to be protected. There is also a "person" who needs to know this information. Then there is the "act" of knowing this information. Confidentiality consists of separating the combination of the person allowed to know the information, and the information itself, from the combination of a person who is not allowed to know the information, and the information itself, together with the ability to enforce this separation.



**Figure 5-1 Confidentiality Model**

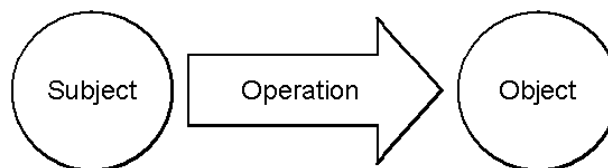
If we change the "act" in question from "knowing" to "changing", we arrive at integrity. Let us, then, change the content of the "act" to the general term "operation". We can express confidentiality, then, using the phrase "operation in the form of reading", and integrity to "operation in the form of writing". By rephrasing things in such a way, one can say that the basic elements of information security consist of allowing or prohibiting "people" from performing "operations" on "information".

<sup>3</sup> IT Information Technology Security Evaluation Criteria, 1990

When the object is information, the possible actions can be narrowed down to "reading" and "writing". However, UNIX and other contemporary operating systems took the approach of treating access control for programs in the same way as for data files, and as such additional concepts come into play. First, "programs" have been added to "information" as objects for "operation". As a result, "execution" must be added to the list of possible "actions". Doing so provided the benefit of being able to describe a range of security providing access controls with a single format.

As a result, the number of possible objects governed by access controls has continued to grow. In addition to information and programs, directories, IO ports, and other objects have become the object of access controls. With this, there came a need for a term to refer to these objects of access control, and we now refer to the items which are the subject to operation as "objects"<sup>4</sup>, and "resources". We will refer to them herein as "objects".

In addition, "operations" can be performed by more than just "people". For example, they can be performed by programs started by people, by processes, by remote hosts, etc. As such, the parties which can perform operations are referred to as "subjects"<sup>5</sup> or "principals". We will refer to them herein as "subjects".



**Figure 5-2 General Access Model**

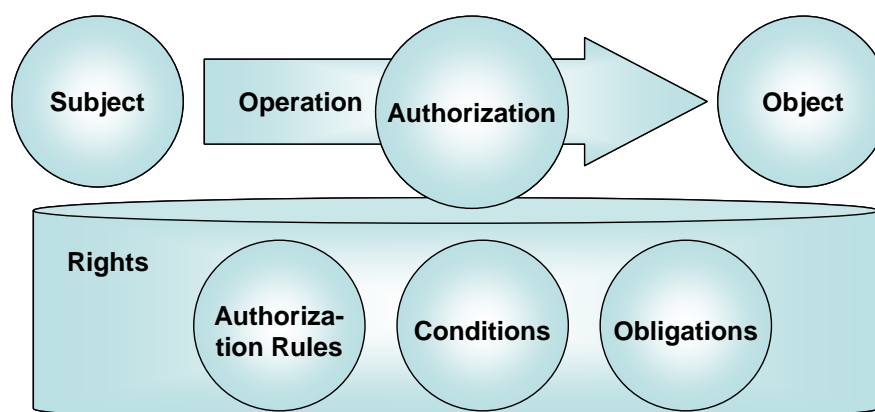
By using these concepts, we can say that systems can be built wherein access controls necessary for information security can clearly separate permitted operations and prohibited operations, and enforce those distinctions. In the next chapter, we will discuss a more general model.

### 5.3. General Access Control Model

The functional model of access controls for information systems is composed of "objects" which are operated on, "subjects" which perform the operations, "permissions" for deciding whether subjects can perform operations on objects, and "rights" used in evaluating permission processing. These "rights" are composed of "authorization rules" describing combinations of subjects and objects, "conditions" describing the environment in which the subjects and objects exist, and "obligations" for the subject during or after operations.

<sup>4</sup> Ex. ISO/IEC 15408

<sup>5</sup> Ex. ISO/IEC 15408



**Figure 5-3 Access Control Function Model**

Following are examples of each element.

- Subject: User, processes serving as user agents (representatives)
- Object: Data, processes, I/O, network, and other calculation resources
- Operations: RWX (Reading, Writing, Execution), rights operations, copying, printing, editing, etc.
- Authorization Rules: Label security, RBAC, access control lists
- Conditions: Time periods, terminals (hard disk ID & TCG chips), and other environmental variables
- Obligations: Access logs, watermarked printing (visible, transparent), etc.

---

## 6. Authentication

---

### 6.1. Identification

For information systems, the basis of all security is in determining whether the subject is indeed who it claims to be. As such, all information systems require "identification" and "authentication" functions.

Identification consists of accurately categorizing and identifying the subject. In order to identify a subject in an information system, a unique name must be assigned to the subject. The name assigned to a subject for the purposes of identification is referred to as an identifier, or ID.

An identifier which is only used for one subject, with no duplicates, is called "unique", so information system identification functions use "unique identifiers". People are usually identified by their names. However, since some people share the same first and last names, names are not usually unique, and if identification is required, addresses and other additional information are added to create a unique identifier.

In information systems, identifiers usually consist of strings of numbers and letters. Because identifiers are used in a wide range of applications, fixed length identifiers are often used for processing efficiency, but with the continued advance of information system processing capabilities, the number of systems using variable length identifiers is growing.

When assigning an identifier, it is important to consider how the uniqueness of the assigned identifier can be guaranteed. Below are some examples of possible approaches.

- Numbering in order to provide uniqueness within the system. For example, sequential numbers are used for identifiers, and when a new identifier is assigned, the next number after the last assigned identifier is used.
- Using preexisting unique information. For example, using employee numbers or email addresses as identifiers.
- Using freely selectable identifiers, but checking candidates before assigning them to check for duplication.

For systems in which the identifier must be remembered by users, it is important to make sure that those identifiers are easily memorable.

### 6.2. Authentication and Authentication Elements

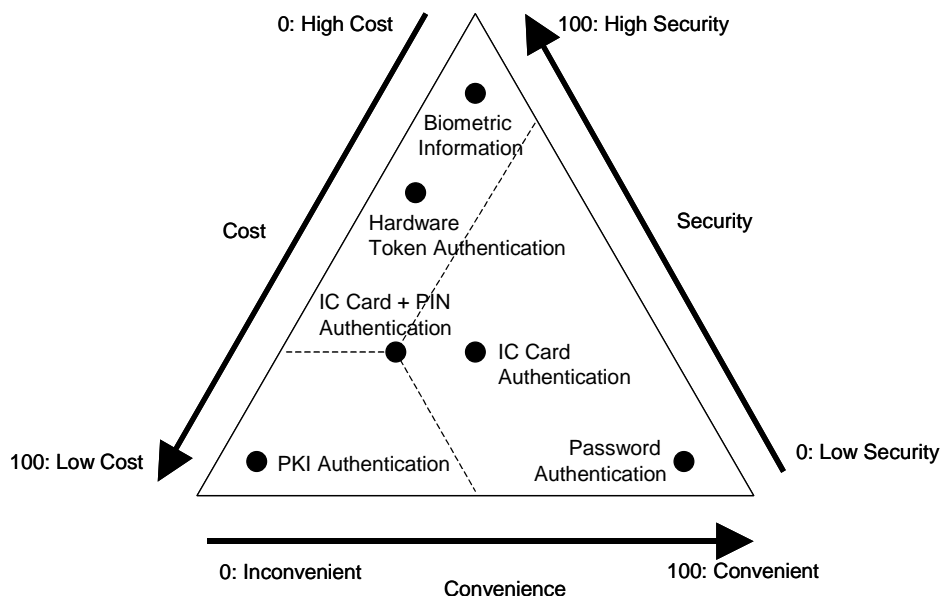
Authentication refers to the function or process of evaluating whether a subject is the subject expected by the information service supplier. Generally, the system supplying the service will request information that only the correct subject can provide, and by providing that information, the subject is recognized as being who they say they are, and authenticated. The easiest

example is that of the password.

Passwords are based on the idea that they are information known only to the subject, and used to evaluate whether someone stating they are a given subject is actually said subject. As in the example of passwords, the information which serves as the foundation for authenticating a subject is called authentication information credential, credentials<sup>6</sup>, or secrets<sup>7</sup>.

If the authentication information credential is stored somewhere, the place it is stored is sometimes referred to as a token. For example, if the authentication information credential is stored in a USB drive, that USB drive is sometimes called a token.

Authentication information credentials, tokens, and other items used in authentication are referred to as authentication elements. There are many types of authentication elements. Different types of elements provide different levels of security, have different costs, and provide different benefits. As such, it is important to remember that authentication elements with the highest level of security are not always best. There is a saying in the security world: "Cheap, Fast or Secure? Pick two." The fact that not all three desires can be satisfied can be seen by the positioning of the different authentication elements on the triangle figure below. The diagram shows representative authentication elements. For example, the pairing of an IC card and PIN authentication provide relatively high security and relatively low cost, but less convenience than IC card authentication alone.



**Figure 6-1 Authentication Element Positioning**

Authentication elements for authenticating users can be broken down into the following three

<sup>6</sup> Ex. "Report on Current Status of Personal Identification Technologies" Information Processing Development Corporation, 2003

<sup>7</sup> Ex. ISO/IEC 15408-1



categories.

#### **Authentication based on known information (Something you know)**

This is authentication based on something the user remembers. It is information known only by the user, and unknowable by any third parties, and, as such, by knowing this information, the user proves their identity and is authenticated. This type of authentication information includes passwords, passphrases, and PINs (Personal Identification Numbers). Authentication using passwords requires no additional modification of terminals, and is widely used. However, from a security standpoint, this method relies quite heavily on the user's memory, and cannot be relied on for strong security. For situations requiring high levels of security, two element authorization, using authentication items or biometric authentication, is necessary.

#### **Authentication based on physical items (Something you have)**

Authentication based on physical items includes smart cards and other portable devices. The device contains the information necessary for authentication (passwords, private keys/certificates, etc.), and is used when performing authentication.

Using physical items for authentication runs the risk of use by third parties due to loss of the authentication item, and as such are used with PINs (Personal Identification Numbers) to ensure that the user of the item is the owner of the item. By using this approach, the security level is improved over knowledge based authentication through the required possession of the authentication item. The authentication item can also store multiple information, relieving the user from having to remember different information for different terminals or services, and preventing a decrease in the level of security due to operating problems.

#### **Authentication based on biometric information (Something you are)**

Examples of biometric information based authentication methods include fingerprint authentication and palm vein authentication. This biometric information differs from person to person, and yet changes little with time, and these characteristics allow the use of biometric information in authenticating users. Biometric authentication requires neither "knowing" nor "carrying" of any information, resulting in far more convenience for the user.

### **6.3. Two Element Authentication**

Different authentication methods have different advantages and disadvantages, but by using multiple methods of authentication which complement each other and make up for each others' disadvantages, authentication strength can be improved. Using two types of authentication elements in order to provide authentication is called "two element authentication".

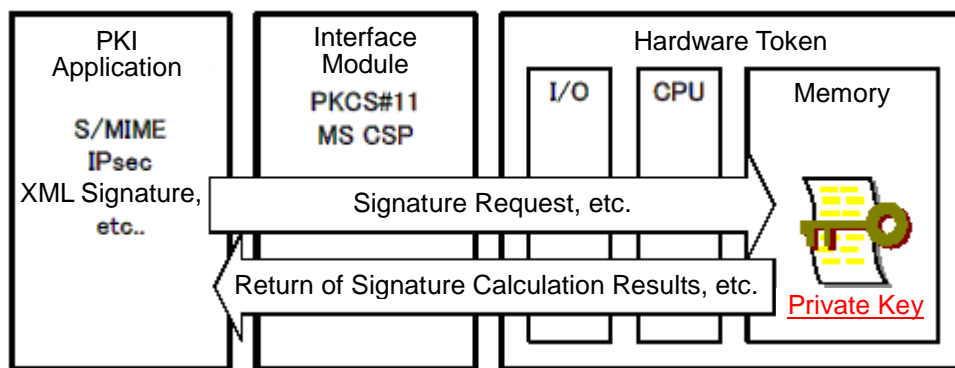
For example, passwords alone are prone to guessing and theft, resulting in possible impersonation, but by using a smart card containing a PKI key and certificate, and requiring a

password (PIN) to activate that key, impersonation will be impossible even if the card is lost without knowing the password, and will also be impossible if the password is discovered without possessing the card.

#### 6.4. Authentication Devices

An authentication device is one that stores confidential information such as passwords and PKI private keys securely. A representative example of an authentication device is the smart card, but there are a variety of other authentication devices. Contact smart cards have traditionally been used the most, but recently contactless smart cards have seen increasing use.

Authentication devices use different physical interfaces depending on the type of device. As such, the environments that authentication devices can be used in vary according to they type of authentication device. There are a number of incompatible standards for contactless smart cards as well.



**Figure 6-2 Authentication Device**

**Table 6-1 Authentication Device Types and Characteristics**

Type	Characteristics
Contact Smart Card	Contact smart cards have been in use for a long time, and are seen as standard authentication devices even in e-government. The smart card format is also standardized, and can be easily used as an ID card with a photograph printed on the front. On the other hand, due to the long history of the contact smart card, there are a number of specification branches, and problems with incompatibility. A card reader is required to use a smart card with a PC or the like.
Contactless Smart Card	A contactless smart card is used for the Basic Resident Register card, containing a certificate for public personal authentication.
USB Token	The physical format of a USB token is different than that of a smart card, but the basic design is the similar to that of a contact smart card. The physical interface is USB, allowing the USB token to be used on computers with USB interfaces without the need for a card reader.
Security Chip (TCG/TPM)	A security chip is an IC which is connected to a PC and which performs encryption, decryption, and signature validation. It is properly called a TPM (Trusted Platform Module), and its specifications were developed by TCG <sup>8</sup> . Because it is mounted on the PC's motherboard, it is not, technically, an authentication device, but PP <sup>9</sup> has been developed, EAL <sup>10</sup> 3+ authentication products have been released, and products providing security features using security chips as confidential information storage mediums have been produced.
Fingerprint Match on Card	This refers to smart cards with fingerprint identification devices built in.

## 6.5. Authentication Model

When considering the authentication model, it is first necessary to review the scope of authentication. Generally, the effective range of authentication will fit in one of the following three categories.

### 6.5.1. Local Environment Authentication

Local environment PC logon authentication, such as when logging on to client terminals, is only valid for the device itself. For local environment authentication situations, the security manager will use OS user management features to perform ID management. If there are

<sup>8</sup> Trusted Computing Group: The TCG is an open standards organization which provides support for industries in order to protect valuable data in a wide range of parts and platforms. It is a non-profit organization, developing, establishing, and promoting standardization of specifications for high security, high reliability hardware and software, from multiple platforms to peripherals and devices.

<sup>9</sup> Protection Profile: A document containing the terminology and basic security requirements defined in ISO/IEC 15408/JIS X 5070

<sup>10</sup> Evaluation Assurance Level: A grade reflecting the degree to which a particular system or product satisfies the functional requirements of the ISO/IEC 15408/JIS X 5070 Common Criteria. It is used as an evaluation of security strength. There are 7 levels, with larger numbers representing greater security.

materials which need to be protected within the local environment (for example, word processing documents or other materials created and managed on the client end), local authentication is the only authentication based protection point. In situations where network MAC addresses or other information unique to physical equipment is used for security purposes, the strength of local authentication becomes the foundation for security reliability. In situations such as this where there are advanced security level needs, two element authentication is used. In some cases, the security level can be further raised by using biometric information as one of the elements in the two element authentication.

#### 6.5.2. Network Environment Authentication

For corporate (inB) systems, when subjects (users or user equipment) are authenticated when connecting to the corporate network, they are able to enter the corporate network. For business-to-consumer (B2C) systems, subject authorization is performed by the service provider, and authentication of the subject allows them to connect.

#### 6.5.3. Business and Service Environment Authentication

Authentication for corporate business systems and customer oriented services consists of further authentication of subjects who have been authenticated in local environment and network environment authentication, permitting the use of corporate business systems and customer oriented services. It also includes direct authentication from dedicated terminals, such as in authentication systems provided by mainframes.

### 6.6. Other Security Requirements for Authentication

When using critical business systems, even if authentication has already been performed, additional thought should be given to repeating authentication. This is necessary when the authentication which has already been performed is not sufficiently strong, or when enough time has passed that it cannot be relied on that the current operator is the same as the one who performed the initial authentication. For example, when performing operations which are directly security related, such as changing passwords, it can be effective from a security standpoint to perform authentication again immediately before performing the requested operation, even if the subject has already been authenticated.

When using passwords for authentication, there is a need for the system to directly control the strength of the password (also referred to as the "quality of the password"). For example, simple passwords such as "1111" or "ABC" can be easily guessed by third parties, and as such do not adequately serve their roles as passwords. These passwords are called weak, or low quality. Many weak passwords can be recognized as such automatically by programs, and when an insufficiently strong password is chosen as a new password when changing passwords,

the system can reject the weak password. The following are examples of conditions for determining that passwords are weak.

- The password length is short
- There is a preference for certain characters in the password (letters, numbers, symbols)
- The password is the same as the ID
- The password can easily be determined based on the user (the user's birthday, telephone number, etc.)
- There are repeated characters in the password (1111, AAA, etc.)
- The password contains a simple sequence (1234, ABC, etc.)
- The password contains words from a frequently used word list (a password dictionary)

Passwords can also become weak due to the way they are handled by users. The following are examples of conditions used by systems for determining that passwords have become weak.

- The same password is used for a long period of time
- For systems requiring periodic password changes, the password is changed, but then changed back to the original password.
- 2 or 3 passwords are used in rotation.

It is best to use a system which automatically detects when passwords become weak like this, and which prohibit this type of user password usage. However, the actual degree of password strength required (for example, the minimum number of characters in the password) depends on the policies of the organization and system, so it is best to configure the system to allow password management based on security policies. Password policies will be discussed in more depth in the operation section.

---

## 7. Identity Management

---

### 7.1. The Necessity of ID Management

Open, large scale distributed corporate computing environments may contain a number of platforms, such as UNIX based operating systems (Solaris, HP/UX, AIX, etc.), Windows operating systems (Windows 2003), and Linux (Redhat). A large number of middleware, package software, and applications may also coexist, with their own authentication and authorization structures.

System architecture with fully integrated authentication and authorization for all operating systems, middleware, and applications, which provides services via a single login, is ideal, but it is difficult to completely redesign existing system architecture when adding systems to an existing environment. As such, it becomes unavoidable but necessary to expand while using multiple methods of user management, access control information management, and other ID management, and in most corporate systems with large scale computing environments, ID management is not integrated. This is especially true in open large scale distributed computing environments. This results in ID related access right management problems and inappropriate authentication ID management, and may result in security vulnerabilities. There have been cases where confidential information has been leaked due to these problems with ID management.

### 7.2. ID Management Requirements

The following security management improvements are requirements of internal IT control for Japanese SOX regulation compliance, scheduled to come into effect in 2008.

- Integrated management of platform privilege qualifications and administrator qualifications
- Complete separation between parties requesting IDs and access rights and the parties authorizing them
- Management of IDs for destroying all employee ID cards after retirement
- Control environments based on the least privilege principle

Corporate IT network security control is expected to come under even greater scrutiny in the future. ID management is an essential technological measure for improving this control.

It is extremely important to implement the security principle of separation of duties, between parties requesting rights modification, parties authorizing these modifications, and operation administrators. The least privilege principle, where people who access data and services are given the lowest level of privileges necessary to do so, is also essential. ID usage status

monitoring is required in order to revoke rights for users who have been granted access rights and have not used a service for a long period of time, in order to prevent the existence of those users' IDs from becoming a possible vulnerability. It is also important to establish an environment to manage life cycle control, including not only synchronization of ID information, but also ID information generation, attribute information modification, such as access right administration, and ID deletion.

### 7.3. LDAP Directory

One of the growing ID management technologies is the LDAP directory. The LDAP directory serves as a repository for user related information. The LDAP directory is often used for centralized management of basic information used for user authentication, providing centralized information management and control. The primary uses of LDAP directories are described below.

**Table 7-1 LDAP Directory Uses**

Item	Use	Search Object
Electronic Phone Book	Integrated with a search application for searching user data.	Name, departmental information, job title, email, telephone number, facsimile number, etc.
Integrated Address Book	Integrated with email clients and groupware email features for searching for email addresses.	Name, email address
User Authentication	Integrated with web servers and authentication systems in order to use user information for authentication, authorization, and access control.	User ID, password

The LDAP directory receives LDAP (Lightweight Directory Access Protocol)<sup>11</sup> requests. In order to deploy an LDAP directory, individual services must be configured to support LDAP when the system is designed.

LDAP directories have made sharing of user information across multiple computers and systems possible. However, it is difficult to use LDAP for sharing information regarding access controls for determining which users should have access to which data. In order to do this, information such as user job titles, roles, information access rules, and other information which LDAP directories have difficulty handling must be jointly managed.

One approach is adding a separate directory for managing the LDAP directory itself. This is referred to as a metadirectory. The metadirectory can be used to absorb differences between

<sup>11</sup> RFC2251-Lightweight Directory Access Protocol (v3)

LDAP directories, and to synchronize multiple LDAP directories. Another approach to integrated management of detailed user attributes is identity management.

## 7.4. Identity Management

Identity refers to the packaging of subject information. Identity is made up of elements such as identifiers assigned to subjects, subject credentials, and different attributes related to subjects. Attributes can be separated into two categories: static attributes, which are modified frequently, and dynamic attributes, which are modified infrequently. Static attributes include names, addresses, departments, and job titles. Dynamic attributes include users' current locations. The collection of all of these attributes are also called profiles.

Identity management is the integrated management of these identities. One form of identity management is the model supplied by OASIS<sup>12</sup>, which uses SOA architecture. This uses SAML<sup>13</sup>, XACML<sup>14</sup>, and other XML based protocols to share identity information.

### 7.4.1. SAML

SAML (Security Assertion Markup Language) is a standard specification defined by OASIS' Security Services Technical Committee. V1.0 became the OASIS standard in November, 2002, and V1.1 became the OASIS standard in September, 2003. V2.0 was established in 2005. There are several software package products using SAML2.0. SAML2.0 conformant products are expected to become the market standard.

SAML provides an XML base framework for sharing security information. This security information is expressed in the form of assertions regarding the subject.

Assertions using SOAP/XML carry information regarding authentication operations performed by the subject, attribute information for the subject, and authorization results regarding access rights to resources for the subject. Single assertions can contain statements regarding authentication, authorization, and attributes.

### 7.4.2. XACML

XACML is another access control policy standard specification like SAML defined by OASIS. XACML uses XML to describe policies such as authorization conditions for access control. It also defines protocols for condition confirmation requests and responses.

---

<sup>12</sup> Organization for the Advancement of Structured Information Standards

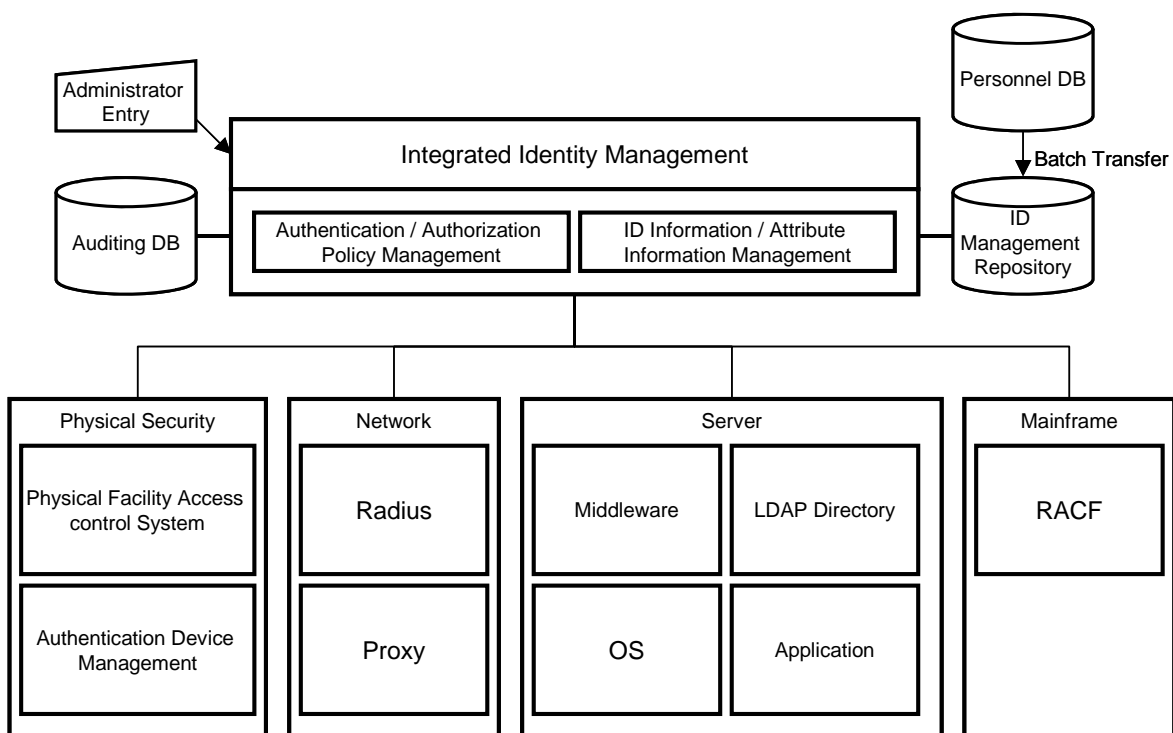
<sup>13</sup> Security Assertion Markup Language, OASIS

<sup>14</sup> eXtensible Access Control Markup Language, OASIS



## Identity Management Model

Synchronization of master ID management repositories and ID management ledgers for managed subjects/objects is called ID provisioning. ID provisioning provides integrated management of administrator and end user ID information and attribute information (access rights, administrator rights, etc.), and provides central creation, modification, and deletion functions. An integrated identity management structure must be deployed in order to carry out ID provisioning. Integrated identity management covers a wide range of systems, including physical security systems, networks, server operating systems, middleware, applications, and legacy systems with ID information management structures.



**Figure 7-1 Integrated Identity Management Model**

### 7.4.3. Identity Management Architecture

Identity management is composed of the elements shown below.

- ID Provisioning Server (Synchronization Function)
- ID Management Function
- Synchronization Adapter
- Local Agent
- Remote Agent
- Repository
- Work Flow
- Audit Trail and Audit Function

There are several methods for integrating the ID management adapter and the managed server (OS, middleware, application). Unique methods used in products utilize telnet and open SSH, or standard LDAP protocols for synchronization with the remote end. Individual ID management middleware often provides standard adaptors for the top selling ISV middleware, but individual development is necessary for applications.

---

## 8. Access Control

---

### 8.1. Access Control Methods

In the "Basic Model" chapter, we described access control as "clearly separating permitted operations and prohibited operations for combinations of subjects, objects, and access, and enforcing those distinctions". In this chapter, we will describe the actual technologies used in access control designs to realize this goal.

Access control methods for computing systems have a long history, and even now a large number of systems use the method wherein the owner of an object (file, etc.) specifies who has access to that object. For example, in Unix operating systems, subjects are separated into three categories: "myself", "other users in my group", and "other", as well as three categories of operations: "reading", "writing", and "executing", with permissions assigned for each. This type of access control is called DAC<sup>15</sup> (Discretionary Access Control).

Discretionary Access Control requires that a system maintain information concerning which users have the rights to perform which actions on an object. A table describing these rights is called an ACL (Access Control List). The ACL is the cornerstone of access control, and must be managed securely to avoid unauthorized access.

Discretionary Access Control leaves the setting of access rights entirely in the hands of the object owner. For this method of access control to function effectively, the owner of the object must always set the object's access rights correctly. If an object owner sets the object's access rights incorrectly, the Discretionary Access Control system will be unable to protect that object.

The larger an organization, the harder it is to ensure that object owners do, indeed, assign access rights to their objects correctly. For example, if a file creator accidentally, or maliciously, sets incorrect read permissions for a file, parties who normally would not have access rights to a file may be able to access that file. If, as in the case of a Trojan horse attack, a program with user rights is accessed without permission, it may be used to assign access rights that the user does not intend. In order to eliminate problems such as this, the fundamental principles of the Discretionary Access Control model, allowing object owners to freely assign object access permissions, must be changed.

One way of resolving this problem is to establish rules for the granting of access rights, and having all users follow those rules. With this method, access rights cannot be freely granted by the object owner. Instead, the system decides, based on the nature of the object, who has access rights to that object. This approach to access control is called MAC<sup>16</sup> (Mandatory

---

<sup>15</sup> Ex. Please refer to United States Department of Defense Trusted Computer System Evaluation Criteria, DoD 5800-28 STD

<sup>16</sup> Ex. Please refer to United States Department of Defense Trusted Computer System Evaluation Criteria, DoD 5800-28 STD

Access Control).

Mandatory Access Control requires constant awareness of object characteristics and subject conditions (which user with which rights is being used currently for access), and as such access control implementation is far more difficult than it is for Discretionary Access Control. In order to properly express the characteristics of objects, characteristic information must be assigned to each object, and the system must be capable of unifying and standardizing this information. The characteristic information assigned to objects in this case is called a "label", and the ability to operate in accordance with these labels is called "label security". As with ACL, labels must be managed securely by the system, and it must not be possible for users to delete or modify this information.

Mandatory Access Control and label security are provided by highly secure operating systems generally referred to as "trusted operating systems". For Mandatory Access Control, rules must be established in advance regarding the access rights for all objects. Implementing this in office automation systems which handle a wide variety of data results in extremely high operating costs. Mandatory Access Control provides strong access security functionality, but the operating costs, and the resulting reasonable scope of its implementation, must be considered. Generally, in organizations without strictly defined physical document management rules, Mandatory Access Control implementation is not effective.

The following sections will describe the technologies used for access control, as well as details regarding the demands placed on them.

## 8.2. Access Control Technologies

### 8.2.1. Role Based Access Control (RBAC) and Least Privilege

Role Based Access Control and the least privilege approach do not use the superuser accounts (such as UNIX system "root" accounts) with universal administrator rights, but instead define multiple roles, each with the least privileges necessary to carry out system administration work, and provide access control functions for each role. Each role is given the minimum role for the rights it is granted. This policy is called "Least Privilege". Least privilege functionality divides the maximum superuser rights into multiple roles (operation, auditing, etc.). This model is necessary for middle and large scale systems with multiple administrators, and implementation of this model can compartmentalize the damage due to internal malfeasance by users and administrators, and of external intrusion.

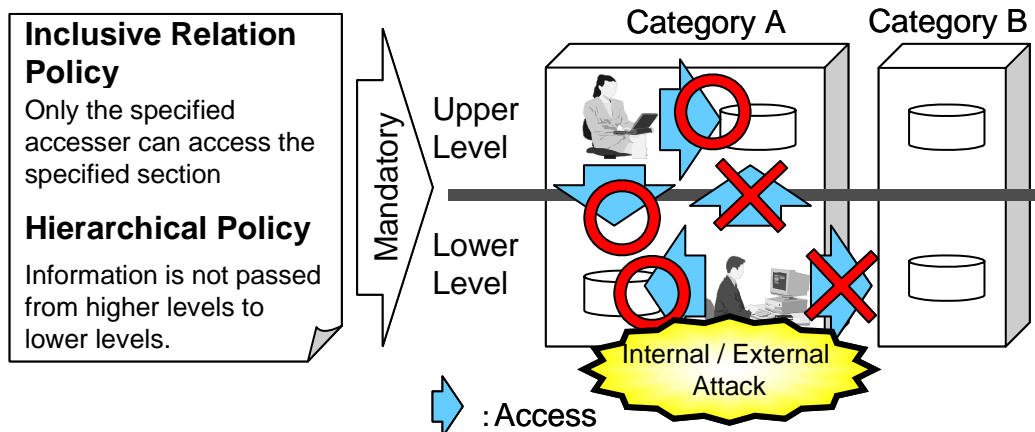
### 8.2.2. Label Security

As we described earlier, label security uses the Mandatory Access Control model. All subjects and objects are labeled with sections (domains / categories / levels), and authorization is handled in accordance with authorization rules for each section. Section

authorization rules are decided in the form of access control policies when the system is designed, and cannot be changed during operation by administrators. Authorization rules can be divided into the following two types.

- Inclusive Relation Policy: Only the specified subject can access the specified section.
- Hierarchical Policy: Information is not passed from higher levels to lower levels.

As with Discretionary Access Control, access between different sections is prohibited.



**Figure 8-1 Label Security**

#### 8.2.3. VM Based Compartmentalization

Protection of entire information systems through the use of virtual machines (VM), with their virtual walls free of vulnerabilities, regardless of their inclusive relation, are the equivalent of label security due to their compartmentalization and hierarchical policy. In the event of damage, the damage is limited to a single virtual machine.

#### 8.2.4. Usage Control (UCON)

The Usage Control model defines not only authorization rules, but usage conditions and responsibilities as right elements, enabling enforcement. Because it provides not only control of access to objects, but also detailed limitations after use (not just "execution"), it is called "Usage Control", and is expected to become the primary access control model.

The UCON model's authorization rules are composed of the three access control models above. The UCON model also offers Digital Rights Management (DRM) for managing usage conditions and duties as access rights, as well as privacy management.

### 8.3. Bases of Access Control Implementation and Effective Operation

Effective implementation of access control and its roles are predicated on the following design considerations and integration.

- Vulnerability Management: Vulnerability inspection and correction for all modules and module design used in access control mechanisms.
- Identification and Authentication: Proper logon status evaluation for users by access control structure and integrated user identification / authentication mechanisms.

Access control mechanisms are processing mechanisms which must be passed through whenever computation devices access resources, and also produce resource access logs of access evaluation results. Resource access logs serve as the most important auditing evidence in the form of audit trails.

### 8.4. Access Control Implementation

There are many things to consider when implementing vulnerability-free access control mechanisms, requiring extensive knowledge, experience, care, and testing. It is preferable to use existing secure OS, middleware, or other access control frameworks. Implementing new, proprietary access control mechanisms when developing applications may actually result in increased vulnerabilities, and is not recommended. Creating new, vulnerability-free access control mechanisms requires expensive design and development by high level security technicians, and is not normally feasible.

Label security is effective for improving system security, but when considering whether or not to deploy label security, one must take care not to underestimate the load and cost incurred in implementation and operation. Implementing and utilizing label security requires high levels of knowledge, experience, and skill regarding the relations between software modules including OS, middleware, as well as information security itself.

### 8.5. Access Control Policy Consistency and Centralized Management

Access control is configured and implemented at all layers, from VM and operating system to middleware and applications, so unless access control policies are consistent across the entire system, access control configurations may vary across different layers for the same resource. This lack of configuration uniformity may result in system vulnerabilities, so centralized management of access control policies is necessary for maintaining access control policy consistency and policy operation management TCO reduction. Please refer to "7 Identity Management" for details regarding management of user attribute necessary for access control policy.

## 8.6. Access Control Mechanism Types

The following types of access control mechanisms exist.

- Physical mechanisms (physical facility access control, tamperproof modules, electromagnetic shielding glass, etc.)
- Logical hardware mechanisms (circuitry-based control)
- Logical software mechanisms (programs using conditionals)
- Encryption

The type of access control mechanisms that can be used will vary based on the scope of protection offered by the access controls (physical area, internal network, computing systems, computing resources, or all). The scope of protection and applicable control mechanisms are shown below.

**Table 8-1 Access Control Mechanism Types**

Access Control Mechanism	Explanation
Network access control	Implemented as a network function. Firewalls, etc.
Remote access control	Control of network access from the outside to each server / client system. Web access control, NFS access control, etc.
Local access control	External and internal resource access control. OS and DB access controls.
Usage Control (UCON)	Operation control based only on subjects, objects, and operations, regardless of whether they're remote or local.

## 8.7. Damage Isolation due to Defense In Depth Model

There is a limit to the amount of damage prevention provided by information security measures such as access control, and it is important when designing a system for increased safety and reliability to pay serious attention to limiting the scope of damage in the event that it occurs. This approach is called "Defense in depth". Even authorized users, including the most trusted administrators, may accidentally or intentionally cause damage to a system, so it is important as part of access control to consider and implement at each layer the means to limit the scope of the damage.

**Table 8-2 Damage Isolation Scopes for Individual Access Control Methods**

Damage Isolation Scope (Unit)	Access Control Method
Internal network	Quarantined by filtering (firewall)
Computer system	Logon control (identification and authentication)
Virtual machine (VM)	Compartmentalization via VM
Scope of operation permitted by administrator	Least privilege specifying RBAC
Collected resources (type / category)	Label security
Resource (information, process, etc.)	ACL (Access Control List)



## 9. Audit Trail Management

### 9.1. Types of Audit Trails

Audit trails are necessary in a variety of modern corporate activities. The characteristics of these audit trails vary widely depending on their objectives. Some audit trails may require extensive record keeping, while others may require immediate notification of infrequent changes to administrators. Organizing and categorizing these audit trail characteristics is a fundamental aspect of effective audit trail management.

We will divide audit trails into the following four types, and consider each.

**Table 9-1 Audit Trail Types**

Category Symbol	Audit Trail Type Name	Definition
M Type	Management Status Assessment Type	Audit trails for confirming whether information security management systems and management processes are functioning correctly.
C Type	Control Status Assessment Type	Audit trails for confirming whether individual information security measures are functioning as intended.
D Type	Security Violation Detection Type	Audit trails for detecting information security measures violation attempts.
T Type	Security Tracking Type	Audit trails for post-fact confirmation of specific actions and scope of security violations.

#### 9.1.1. Management Status Assessment Type (M Type)

These are audit trails for confirming whether information security management systems and management processes are functioning correctly. These frequently use free formats such as documents and reports, and are not suited for automatic system processing. Using document management systems to handle them is effective, as there are usually a large number of version and authorization management requirements. The volume of audit trail data is low. There is also little need for centralized management.

#### 9.1.2. Control Status Assessment Type (C Type)

These are audit trails for confirming whether individual information security measures are functioning as intended. This includes patch application status, security software deployment status, and firewall operation status auditing. Daily security checklist entry items usually fall under this type.

Security measure failures must be detected quickly, so some degree of real-time reporting is

required of control status assessment audit trails. The volume of audit trail data is low. A centralized management infrastructure must be in place for accurate assessment.

#### 9.1.3. Security Violation Detection Type (D Type)

These are audit trails for detecting information security measures violation attempts. Security error logs and firewall access denial logs fall under this type. Some security violation detection audit trails require immediate handling, so there is usually a high degree of real-time reporting needed. The volume of audit trail data is relatively low. Due to the characteristics of this type of audit trail, it is often the object of security monitoring.

#### 9.1.4. Security Tracking Type (T Type)

These are audit trails for post-fact confirmation of specific actions and scope of security violations. In order to provide accurate and detailed information about what information was accessed, and what was done with it, these audit trails must also contain the results of normal business activities. As such, there is a tendency for these audit trails to have a high volume of data. There is a low need for real-time reporting, but in some cases, there may be time constrictions, like needing to be able to confirm the details of a security violation within 72 hours. Centralized management is preferable, but due to the volume of data, the cost of data collection can be high. Management of the data is usually performed using whatever method is best suited for archival of large amounts of data. When using audit trail data as evidence (that is, for forensic uses), there is also a need for data integrity measures, such as using storage media which cannot be overwritten, but because doing so would result in massive financial investment due to the volume of data, cost effectiveness considerations must be factored in.

When using audit trails for forensic purposes, concepts unique to forensics, such as the "chain of custody", which guarantees the reliability of all information handled by processes through which the audit trail passes, must be understood.

### 9.2. Audit Trail Collection and Recording Approach

In the previous section, audit trails were broken down into four types, but in reality these overlap in a more complex manner. For example, for a single piece of equipment, failure logs would be D type (security violation detection), while success logs would be T type (security tracking). There would be no particular problem in recording only one of the two log types, but if both are stored together, the requirements of both audit trail types must be met.

D type and T type audit trails can be continually taken when using resources on an IT system. We will refer to these D and T type audit trails taken when using resources as audit logs. Section 9.3 and later describe the general requirements of audit logs.

C type (control status assessment) and D type audit trails are usually monitored. Continuous PDCA security management and improvement are important. In order to do this, system operation must be monitored, and timely, accurate discovery of issues requiring appropriate countermeasures and review is required. For security management purposes, monitoring must be performed for the following.

- Confirmation of whether security functions (product configuration, etc.) are functioning as planned or not. When they have not, administrators must be notified.
- Notification and recording of events requiring countermeasures or review.

From the perspective of security problem effect assessment and business continuity, it is necessary to monitor whether the entire system is operating correctly. System monitoring and operation management, and security management monitoring, are inseparable. As such, there is a need for integrated management of security management and system operation, and management in accordance with specific roles (security administrators, operation administrators, business managers, etc.) The following issues are monitored.

- System errors (hardware, software)
- Capability information (CPU, memory, disk I/O, network traffic)
- Security management product alerts
- Log errors

Capability information monitoring can provide not only for system capacity planning, but also detection of network traffic increases due to DoS attacks, and as such also serves as an effective monitoring item for security purposes. Log errors refer to errors output to logs (such as IDS logs, etc.) directly providing error information, as well as log correlation monitoring providing alerts when certain patterns of log entries occur. Log correlation functions in monitoring are extremely effective for improving monitoring granularity, as they enable the addition of error detection patterns based on new know-how.

### 9.3. Audit Log Technical Requirements

#### 9.3.1. Items Which Should be Recorded

The following situations should be written to audit logs.

- Creation / modification / deletion of resources designated for protection
- Access right configurations / changes for resources designated for protection
- Access to resources designated for protection
- System design / configuration changes
- Operations necessary for logging on or privileges (rights acquisition)

Who, What, Where, When, and How information must be recorded for these events, with the following used as a base and additional information recorded in accordance with particular device features.

- Incident occurrence date and time
- User identifier (user ID, etc.)
- User location (requesting IP address, etc.)
- Incident type
- Affected resources
- Incident (request) success / failure

However, confidential or protected information (such as password or other authentication information) must not be output to the log, even if encrypted. It is unnecessary as audit information, and may result in increased security risks.

```
2006/06/30 01:30:10,user01,clientA,"Security: Information: 0001: Security policy
applied. (name:xxxx/value:yyyy)"
2006/06/30 01:40:25,user21,clientB,"Security: Warning: 0002: Security policy
modified (name:xxxx/value:zzzz)"
```

**Figure 9-1 Output Log Example**

When using multiple logs for auditing or analysis and cause determination, ideally, those logs should be normalized according to one rule. For example, for information which appears in multiple logs, such as incident date and time, user information, IP addresses, and the like, if the extended information in each log can be formatted in accordance with a shared schema, the logs will prove far more useful, and more valuable as information. This normalization is performed by shared platforms and conversion adapters for log output, possessing interfaces for attaching meanings to XML and other information.

### 9.3.2. Audit Log Output Platform

Once an audit log is generated, it must be completely protected from alteration or destruction. Currently, some individual applications which produce logs also provide protection. However, in order to protect logs at a system level, an audit log output platform providing shared log output features and alteration protection features is necessary. The following functions are necessary in an audit log output platform.

- Log Integrity: Guarantee that output log contents are not modified
- Log Content Normalization: Conversion of meanings, formats, units, and character codes based on a single common standard

In order to normalize and output a log, the format and schema of the output must be defined.

### 9.3.3. Time Synchronization

When a system is composed of multiple computers, if the times of each computer are not

synchronized, relating logs of processes which span multiple computers becomes difficult. In order to prevent this, times must be synchronized across the computers. It is also important for logs to reflect when, and to what degree, time synchronization corrections have happened.

#### 9.3.4. Audit Log Collection

People who have maliciously accessed a system will attempt to change or delete audit logs in order to cover their tracks. In order to prevent this, audit logs must be stored securely. Many logs are in the form of text files, which are added to when new events occur, and few are protected from modification or deletion. It is necessary to protect those logs.

- Logs on systems which have had problems have, themselves, problems with their reliability, so logs should be stored on separate systems
- Logs with different functions in a system must be managed centrally

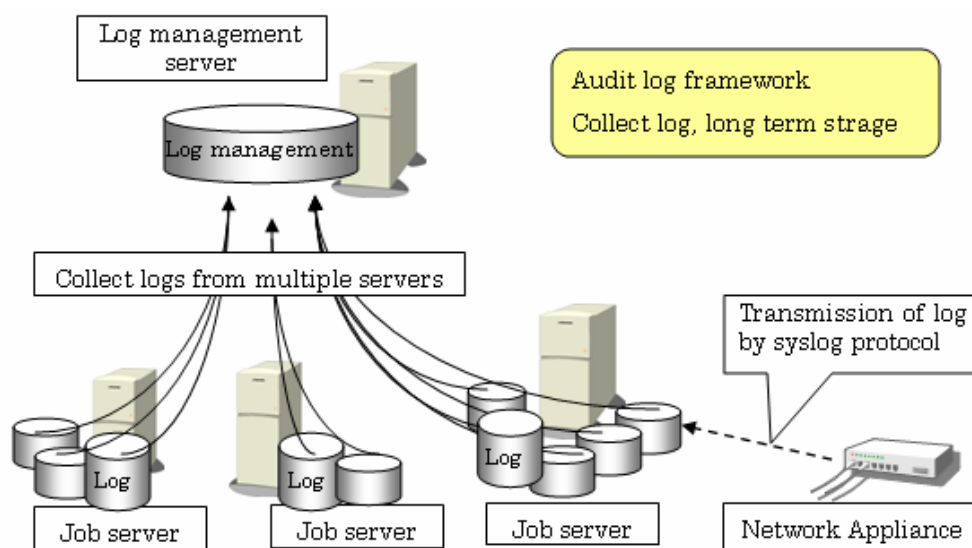
Below are some of the types of logs which should be collected.

- OS logs UNIX: syslog, lastlog, sulog, pact, etc. Windows: Event log
- Web server, application server logs
- Network device, security product logs (IDS, firewalls, etc.)
- Client activity logs
- Database audit logs
- System operation management logs

Logs can be collected by deploying collection agents on target servers, or by using agentless OS file transfer features (ftp, etc.) or syslog protocols to transfer the logs. Generally, using agents provides the benefits of enabling the use of freely configurable, secure, and reliable transfer functions.

#### 9.3.5. Audit Log Management Platform

It is very costly to collect and manage logs for each server and application across a group of servers. There are also problems with securely and reliably managing auditing information. Logs should, instead, be collected and managed centrally on an audit log management server. This can be done effectively by using an audit log management platform which supports multiple log formats and offers flexible log addition and modification features.



**Figure 9-2 Log Management Platform**

### 9.3.6. Audit Log Archival

Not all security incidents are immediately detected, and sometimes investigation of audit logs is necessary long after an incident has happened. In order to make this possible, a secure, long-term method of archiving audit logs must be decided on.

Log archives are stored for a bare minimum of one year, and usually for 3 to 7 years. Logs must be managed and archived for a period of time based on consideration of system, handled information, and security policy factors. Because log archival is long-term and involves large amounts of data, sufficient thought must go into selecting storage devices capable of handling the expected volume of data, as well as external storage media in the event that the archival data exceeds the capacity of the storage device.

In order to guarantee the integrity of the archived logs, using non-rewritable storage media can be effective. Storing log hash values separately from the logs themselves can be effective for guaranteeing archived log authenticity.

### 9.3.7. Log Auditing / Analysis

It is important to analyze logs not only when security incidents and outages occur, but also on a daily basis. Collecting information and assessing trends in processing contents for each day, day of the week, and time period can be effective in noticing the signs of irregularities. The status of the system can be monitored by performing this analysis regularly.

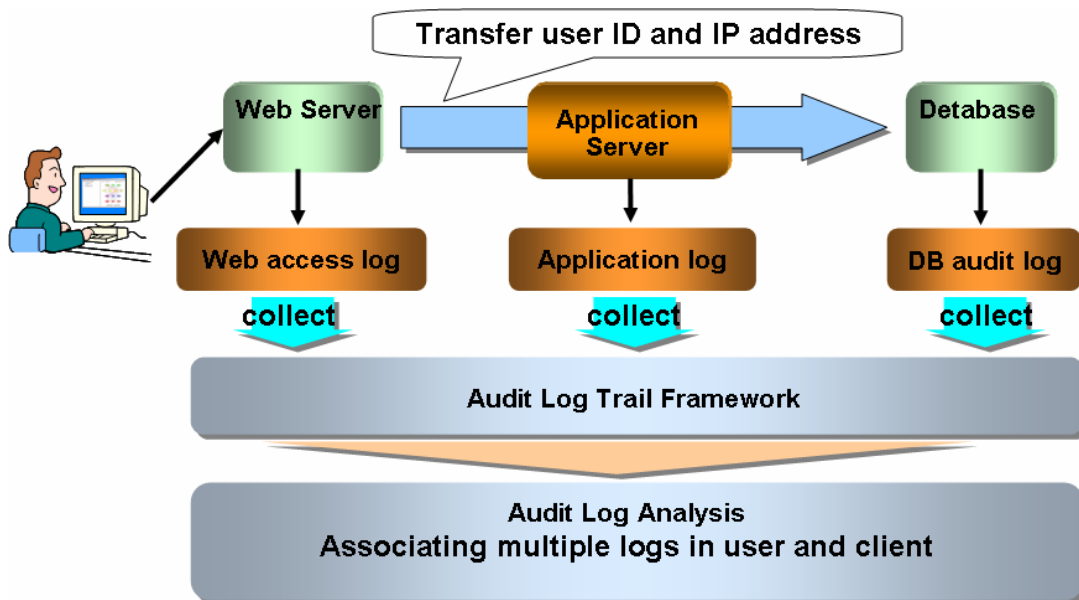
Log auditing and analysis should take the following points into account, and be integrated into the security management PDCA cycle.

- Regular auditing of logs in accordance with security policies, and alert notification for

detected irregularities

- Ability to perform analysis across multiple related logs in the event of an alert, and registration in an incident management system
- Ability to modify auditing rules as a result of log analysis results, rectification of previous problems by next audit, and verification of improvements

When relating and analyzing multiple logs containing a series of processes, the users' identifiers and requesting IP addresses will serve as the key. As such, relational information and client (terminal) information must be managed across multiple user management systems. This problem can be solved by integrating log analysis with integrated identity management and client management. The figure below shows a model of audit log collection and lateral analysis in a 3 layer web system.



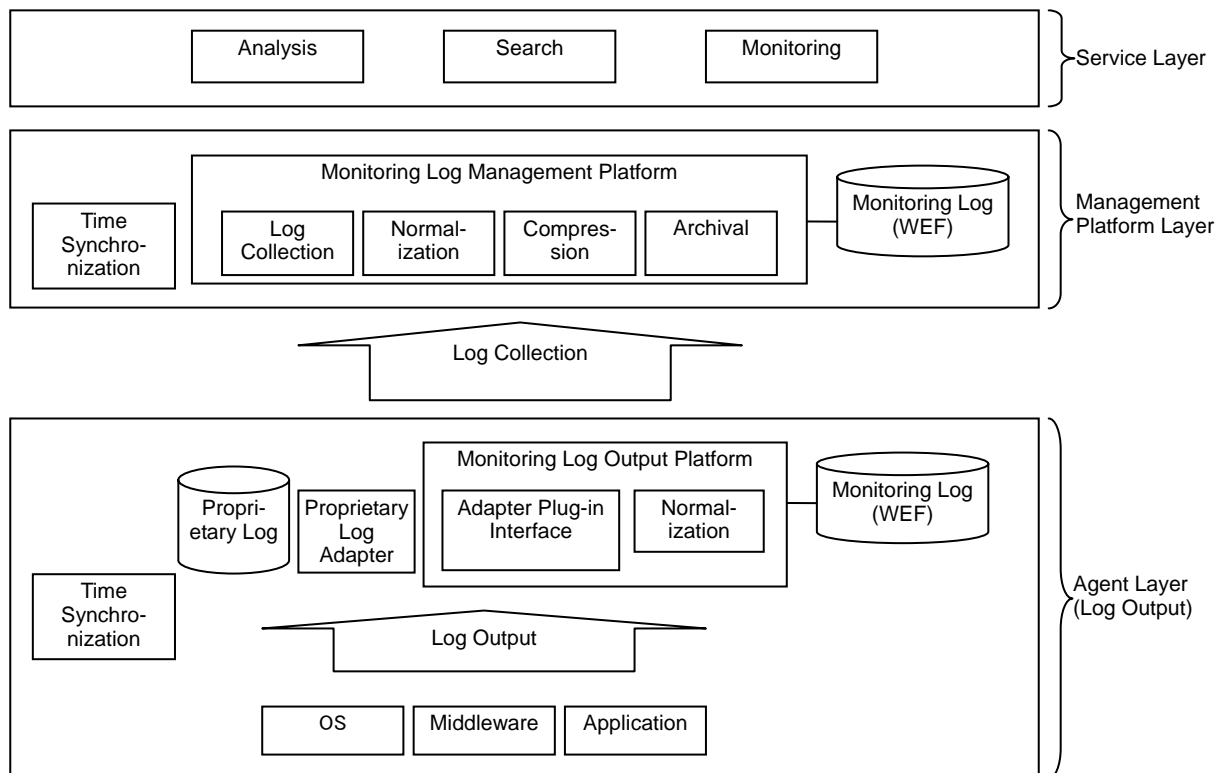
**Figure 9-3 Audit Trail Analysis Model**

The following features are also needed for log analysis.

- Filtering features, allowing the selection of log entries matching specified filter parameters
- Sorting features, allowing log entries to be sorted by specified fields
- Search features, allowing data to be searched by specified items (including regular expression matching)
- Clipping features, allowing the removal of log entries matching specified parameters
- Statistical features, such as determination of average values or quantity of data entries
- Correlation analysis features for analysis of relationships between log entries in multiple logs
- High level statistical analysis features, such as regression analysis and trend analysis

## 9.4. Audit Trail Management Model

The figure below shows a component model containing all the audit management features explained in this section.



**Figure 9-4 Audit Trail Management Model**



---

## 10. Centralized Management

---

### 10.1. ITIL and Centralized Management Background Information

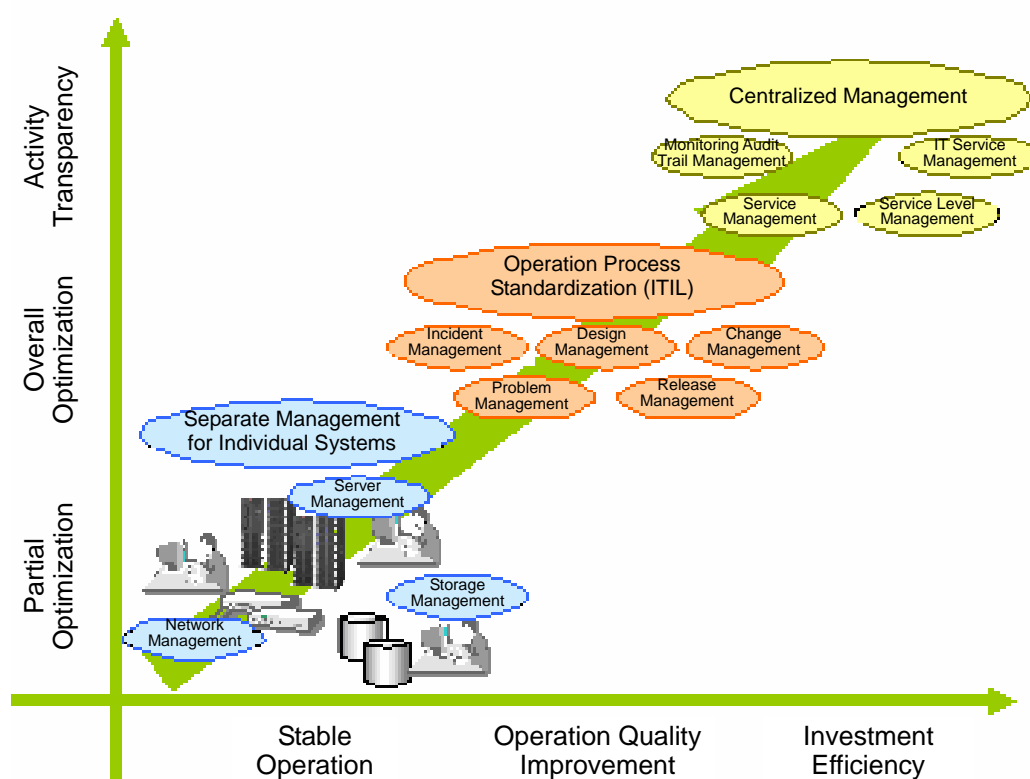
Operation management for information systems has been, traditionally, performed from the perspective of the managed system. That is, lifecycle management (design, implementation, configuration, operation, removal) was handled by server administrators for servers, by network administrators for networks, and by storage administrators for storage systems. There were different operation management products supplied by vendors for each of these managed objects.

However, because these elements interact extensively in information systems, separate management for individual system types makes stable operation of information systems difficult, and results in increased operating costs. There has also been increased demand for internal control and IT governance, and for optimization, not only of individual information systems, but overall corporate information systems. In order to satisfy these demands, standardization of operation processes based on unified corporate policies is essential for information system operation management. ITIL (IT Infrastructure Library)<sup>17</sup> is one of the more representative frameworks for unification and standardization of operation processes based on unified policies. ITIL defines standard processes such as incident management, problem management, change management, and release management, and performs operation management for the entire information system. This results in optimized operating costs and stable operation and operating quality improvements for information systems. In order to unify and standardize operation processes, the information handled by these processes must be centralized. This central management is performed using a CMDB (Configuration Management Database).

For information security and Japanese SOX compliance, corporate activity transparency, business effectiveness, and investment effectiveness evaluation are required. To make this possible, history management (such as information system operation logs, data access logs, system and application status changes, update logs, and the like) containing information regarding who performed what actions when, and how the system was affected as a result, and management of business system service level assurance status is necessary. ITIL handles information system operation management, service level management, and IT service management, but in addition, audit trail management is needed. It is important that these are centrally managed.

---

<sup>17</sup> For details regarding ITIL, please see the ItSMF site at <http://www.itsmf-japan.org/itil/index.htm>.



**Figure 10-1 Position Centralized Management**

## 10.2. Centralization Overview

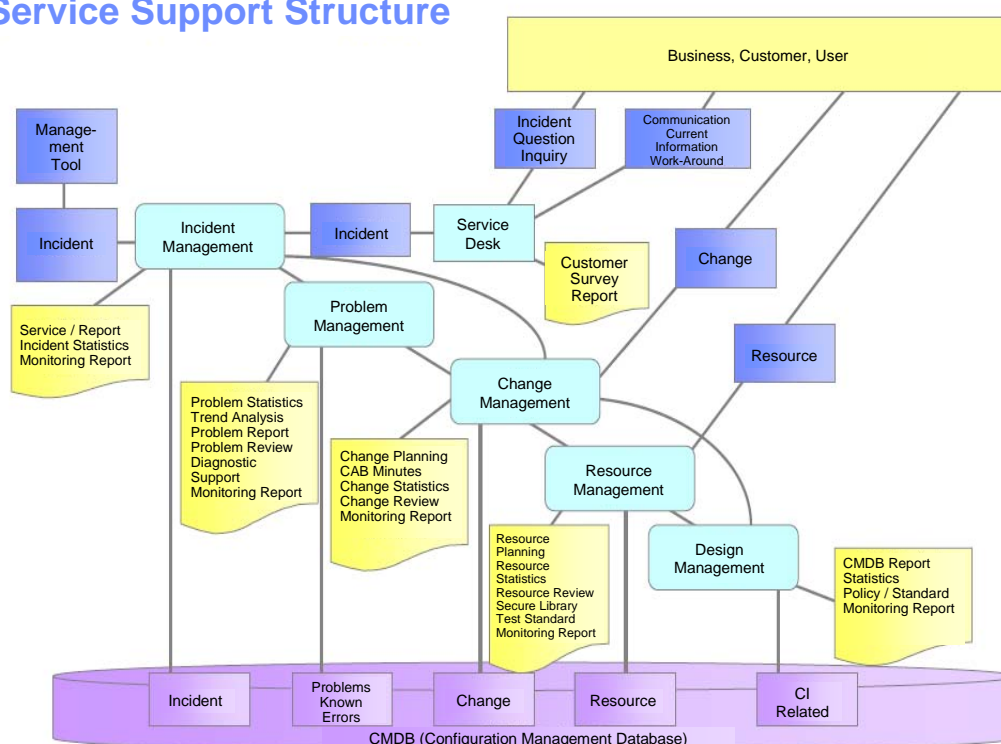
It is essential that design information, service information, and capability management be performed for the network, server, client, storage, application, and other design elements that make up an information system. First, management functions suited individually to the segments to be monitored, such as network management, system management, storage management, client management, and the like, are determined. Next, because these elements are not isolated, but interrelated elements which make up a system, the relationships between these management functions must also be managed. Centralized management consists not only of seamless integration of these management functions, but also standardization and unification of management of their interrelations (management information integration). Roles and processes involved in information system operation are unified and standardized from an information system operation perspective. The framework for managing unified, standardized operation process design, implementation, and evaluation is operation process management with workflow functionality. Information used in operation processes must be consistent and uniform between processes. Operation process management must be able to access centrally managed information when it needs to. Some operation processes require operations to be performed on information systems (system element changes and application status switching, etc.). By using operation processes governed by unified policies to use centrally managed

element information to control an information system, overall system operation can be performed optimally.

To rephrase this in ITIL terminology, service support categories such as incident management, problem management, change management, and release management place a focus on operation management, standardizing peoples' roles and operation processes.

These processes are interrelated. The Configuration Management Database (CMDB) is used to centrally manage the information passed between these processes.

## Service Support Structure



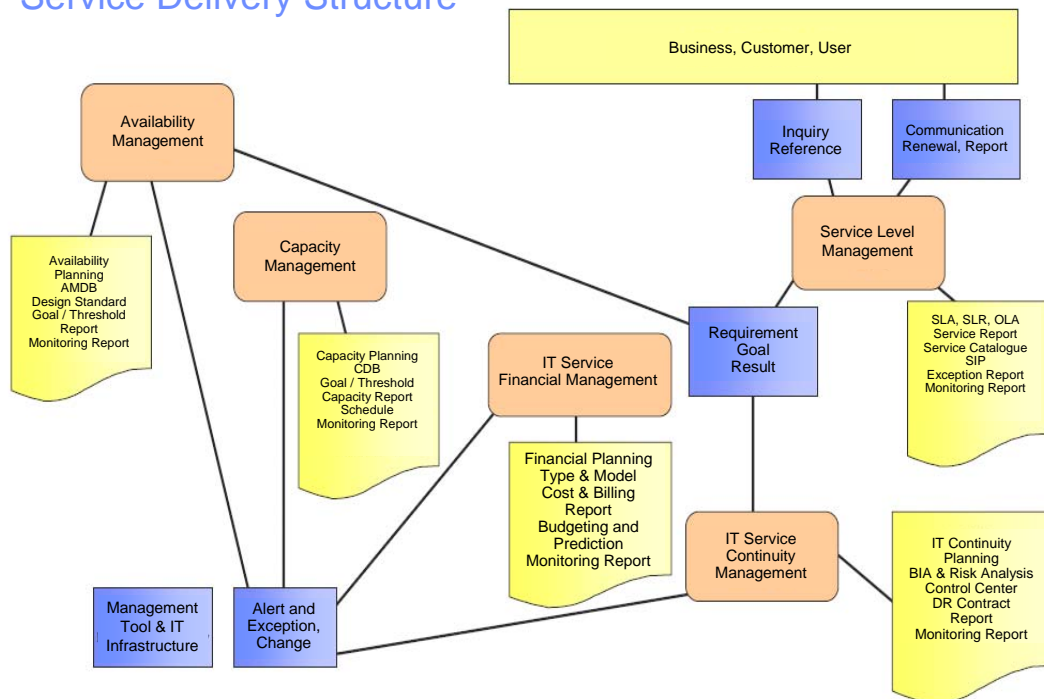
Source: "IT Service Management", published by itSMF Japan

**Figure 10-2 Service Support Structure**

Management of individual elements takes into account the impact on the information system as a whole, as well as investment efficiency, while providing a framework for providing stable operation and operation quality improvement of information systems.

The service delivery category regulates processes for assessing and analyzing business efficiency and investment effectiveness, as well as leading to improvements and reinvestment therein. It manages effective operation of elements composing business systems, as well as maintaining service levels, with a focus on overall information system business and investment effectiveness.

## Service Delivery Structure



Source: "IT Service Management", published by itSMF Japan

**Figure 10-3 Service Delivery Structure**

Reporting data which proves that prescribed roles and processes are being implemented as planned, and that planned service levels are being met, is necessary for information security governance. To do so, not only must products and tools be prepared, but a schema which delineates processes, information, and interfaces, must also be created.

Traditional network management, system management, storage management, and client management features are converted to SOA to allow use by operation processes, and integrated to allow use as functions of individual design elements managed by configuration management database (CMDB).

### 10.3. Incident & Problem Management

Incident management is a process for handling problems (incidents) affecting information systems, with the objective of stable operation of information systems and rapid resolution of problems. Incident management must make incident receipt times, recoveries, investigation, improvements, and other roles and operation processes clear, and provide centralized management of incident handling statuses and countermeasure result know-how. Below is an example of the process of typical incident management.

(1) Incident Receipt (Incident Creation)

Incidents may be received in the form of reports from information system users, or from notifications issued by information system operation management tools, but regardless of the source of the incident information, the incident is received in one location and centrally managed.

(2) Categorization / Investigation

The cause and recovery method for the incident are determined from the particulars of the incident.

(3) Resolution and Recovery

Past incidents and situations are analyzed, and problem resolution and information system recovery are performed.

(4) Incident Logging

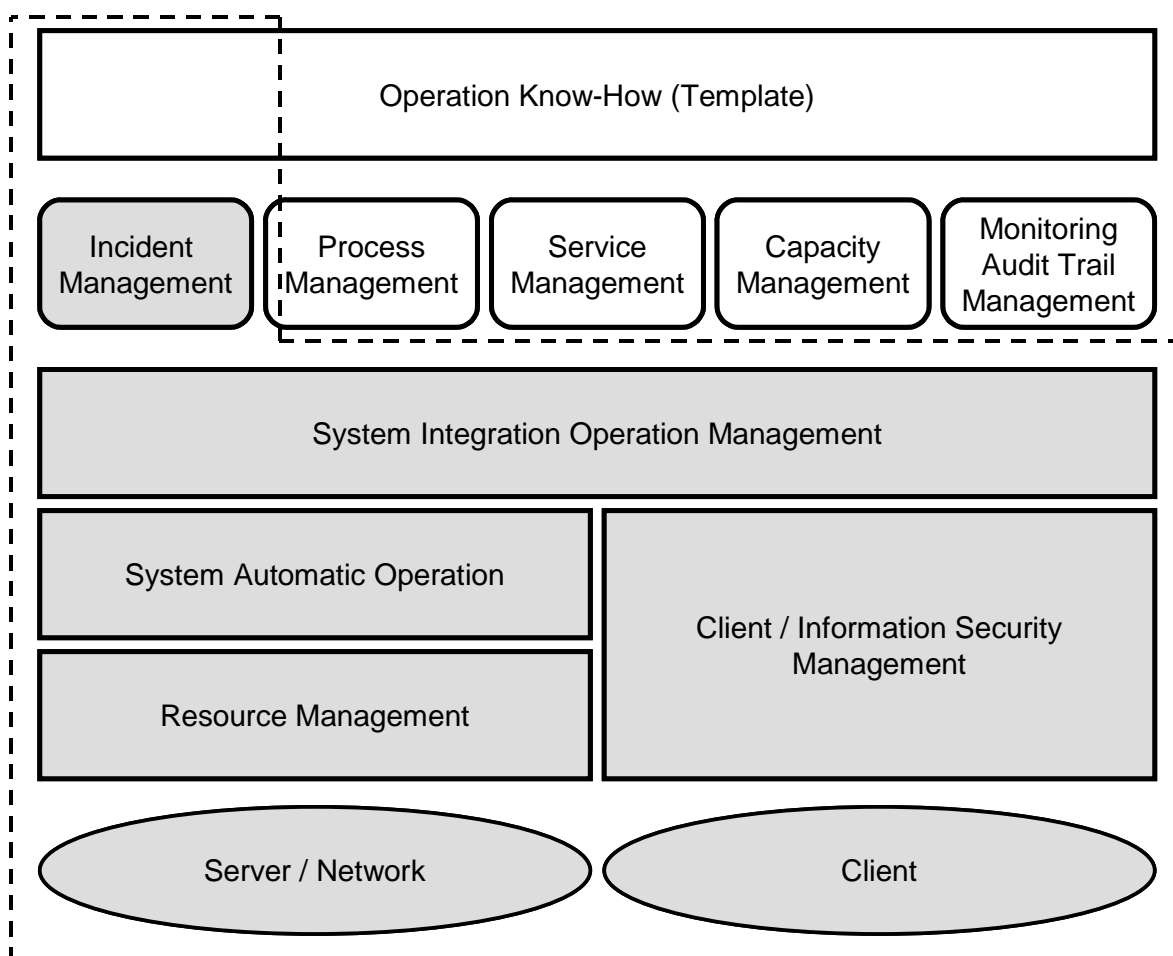
The recovery steps and recovery confirmation are logged and the incident is closed.

(5) Incident Analysis

Incidents are regularly analyzed and information system evaluation and problem point improvement are performed.

ITIL treats problem improvement based on incident analysis as problem management, separately from processes for long term improvements, but these are one line of operation processes.

There are many different categories of incidents, such as information system bugs and operator error, but from the vantage of information security governance, it is necessary to accurately monitor violations of corporate security policies (such as virus countermeasures, firewall entry detection, etc.), and to respond appropriately. In order to detect these incidents, a wide range of products and services are offered by multiple vendors, and these are combined together for incident detection. However, this makes unified security measure implementation difficult. Implementing a central integrated tool for managing security incidents is effective. Security incidents may include unauthorized access detection, virus detection, and confidential data leakage. Integrating the management tool and incident management makes unified, effective security incident detection possible. The following figure shows the position of operation management supporting incident management.



**Figure 10-4 Incident Management Positioning**

Integrated operation management uses individual monitoring features to collectively monitor errors (messages), service status, and capabilities for servers, networks, clients, and other components in information systems.

Integrated operation management uses predefined rules to provide notification to incident management tools.

Incident management provides support for processes such as recovery, investigation, and countermeasures for notified incidents, but, as necessary, can be integrated with integrated operation management, allowing reference to design and capability information, providing even faster countermeasure capabilities. Operations and processes performed during incident management work are stored as know-how, which can be used for analysis and improvements.

#### 10.4. Change Management, Release Management

Change management is the management of change schedules and results for information systems. For example, application changes must be performed with their effect on servers, storage, and operation in mind. When changes are performed, a Request For Change (RFC) is

created and the impact and effect of the change is analyzed before the change is performed. Below is shown a representative example of change management.

(1) Creation of Request For Change (RFC)

Change reason and contents are entered into management ledger.

(2) Impact Investigation (Impact Analysis)

The reasonableness and cost effectiveness of the planned change are analyzed.

(3) Creation of Change Plan

The impact investigation results, change schedule, and change procedure are created.

(4) Change Plan Authorization

The change plan is considered by all related departments, and determination is made whether or not to perform the change.

(5) Change Plan Pre-Testing

A rehearsal is performed using the change plan.

(6) Change Plan Performance

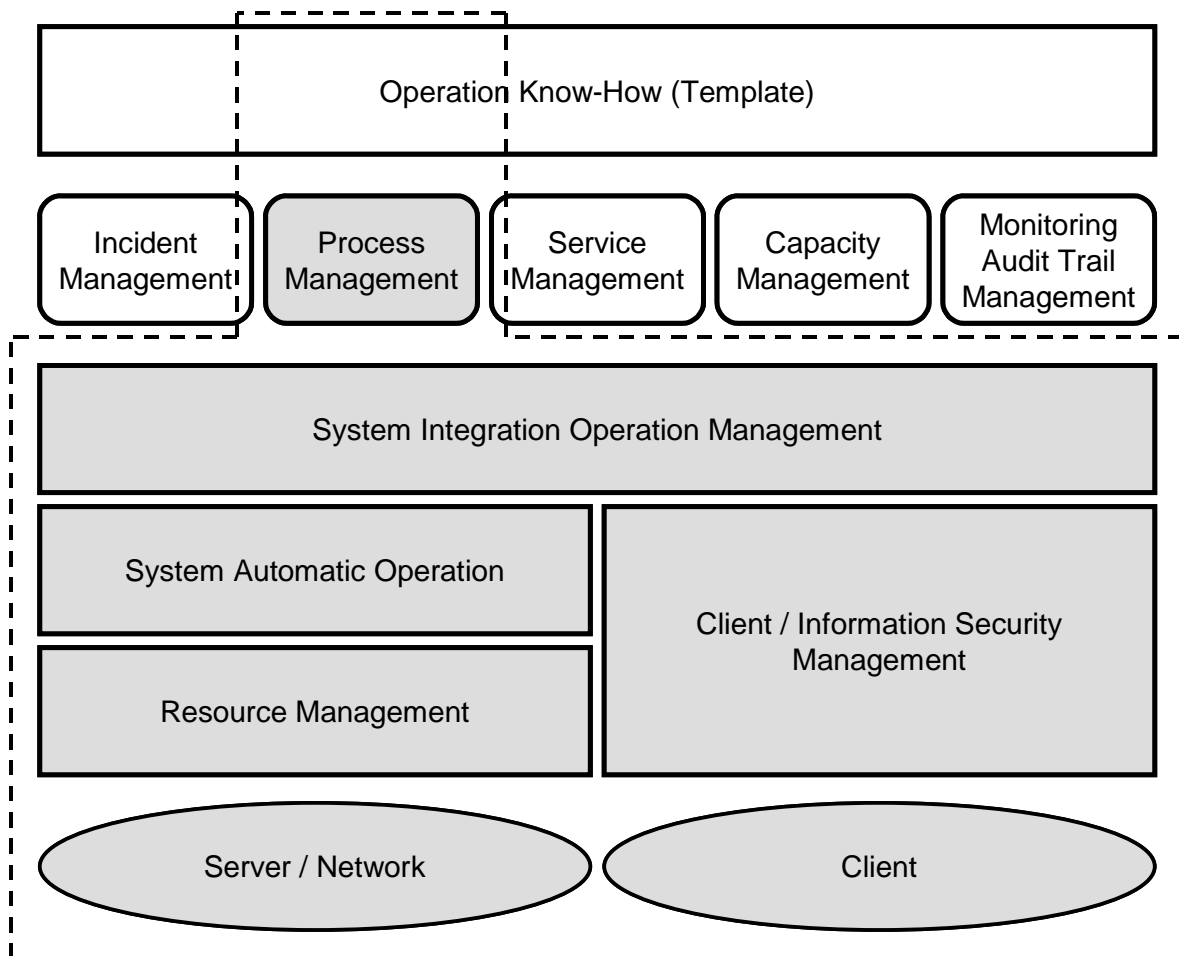
The change plan work is done in accordance with the change plan.

(7) Change Results Confirmation

The change plan and results are compared to audit whether the change was performed as planned.

ITIL treats steps 5 and on as "release management", separate from change management, but these are one line of operation processes.

For information security governance, process 3 (security level impact investigation), process 4 (decision based on investigation results), and process 7 (auditing of actual change plan performance results) are necessary to prevent change work from having negative effects on security levels. For internal control purposes, the performance of change work must be audited by collecting work logs. The following figure shows the position of operation management supporting change management.

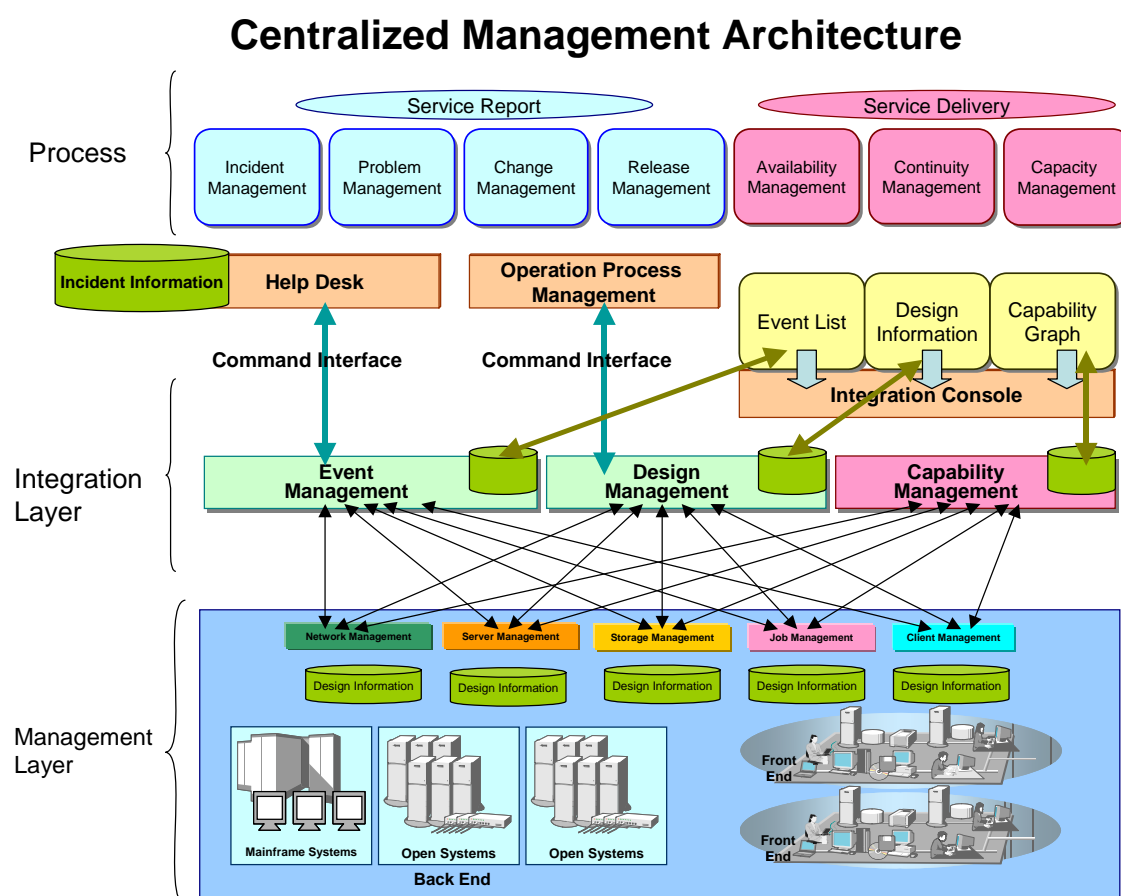


**Figure 10-5 Change Management Positioning**

Operation process management involves management of the processes involved in performing planned changes, performing the change as planned, and recording the work performed. Operations on the system and system changes occur in tandem with integrated operation management and automatic system operation. This prevents missed operation steps, confirmation, and operator error. It also provides management functionality for process progress status and implementation results history.



## 10.5. Centralized Management Architecture



**Figure 10-6 Centralized Management Architecture**

The management layer is composed of resource control functions for individual information systems. The back end of information systems is composed of networks, servers, and storage, and management features for each of these resources are required. Network management, server management, storage management, and the like fulfill this need. These provide management functions suited to the characteristics of the particular managed elements. The front end consists of information usable by client PCs and end users. Client management functions for lifecycle management are necessary for these.

Lifecycle management of the entire information system at the integration layer provides integrated management of varied management functions. "Event Management" integrates resources with the events output by the monitoring of those resources, allowing single-point assessment of them. It also provides automatic notification of incidents to the incident management tool.

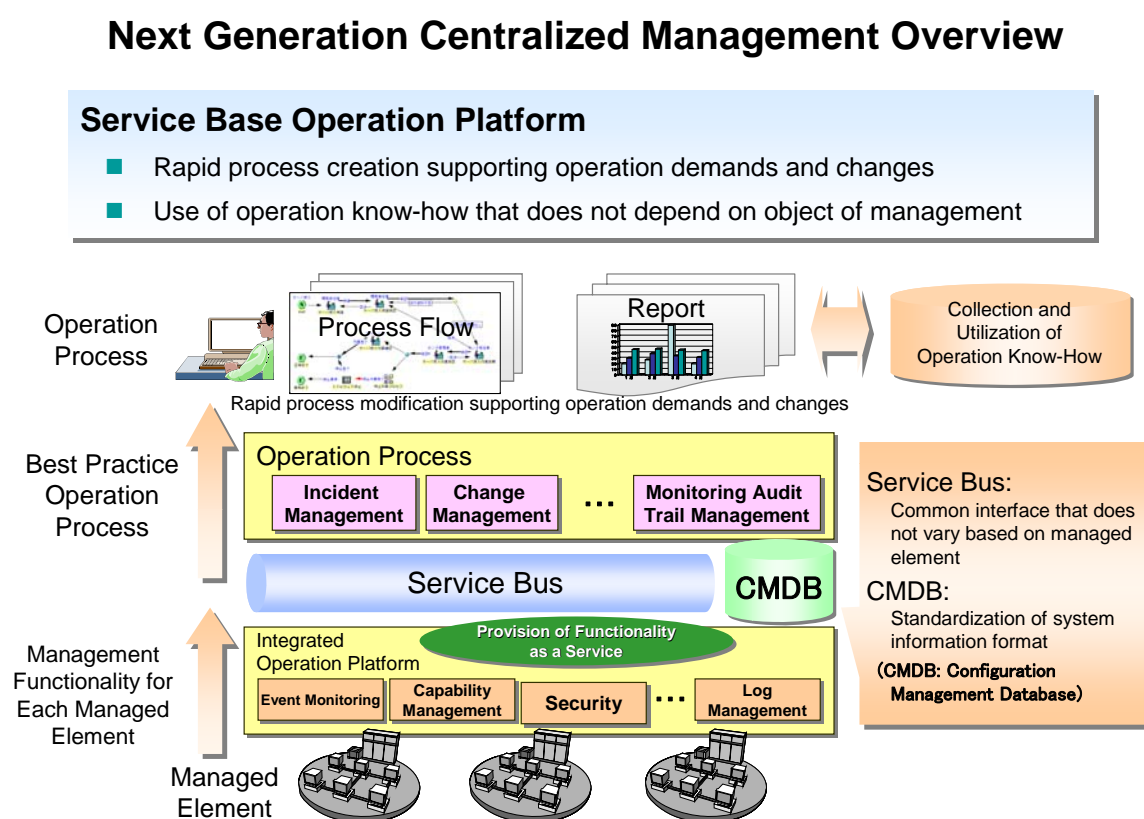
"Design Management" integrates a variety of information regarding resources which make up the information system, providing an overview of the entire information system. The details for

every single component resource in the information system cannot be displayed simultaneously, but design management uses a drill-down view approach, showing detailed management information for each management function as needed. During change management processes, it checks design and configuration information, as well as RFC information, before and after the change from the system itself, which is used to evaluate change performance and system quality.

"Capability Management" evaluates capability information for individual resources and for the information system as a whole, thus evaluating the service level of the entire system, and assisting in the detection of system bottlenecks.

## 10.6. Next Generation Operation Management Architecture

We will now introduce next-generation centralized management. The figure below provides an overview of next-generation centralized management.



**Figure 10-7 Next Generation Centralized Management Overview**

In order to provide efficient, real-time upper level operation processes and information integration, management functionality of individual management elements is converted into a service. Doing so makes it possible to access the appropriate functions and information when needed. These services are integrated by the service bus, and the information is managed in a shared

format (CMDB). This enables upper level operation processes to use the necessary functions and information in the appropriate format, smoothing integration with operation processes.

Next, we will discuss the next generation centralized management architecture. ITIL process architecture is divided into three layers.

① Management Layer (Element Manager)

Network management, server management, storage management, job management, and client management offering management functionality for individual elements. They provide functionality via web service interfaces for design information managed by the shared CMDB.

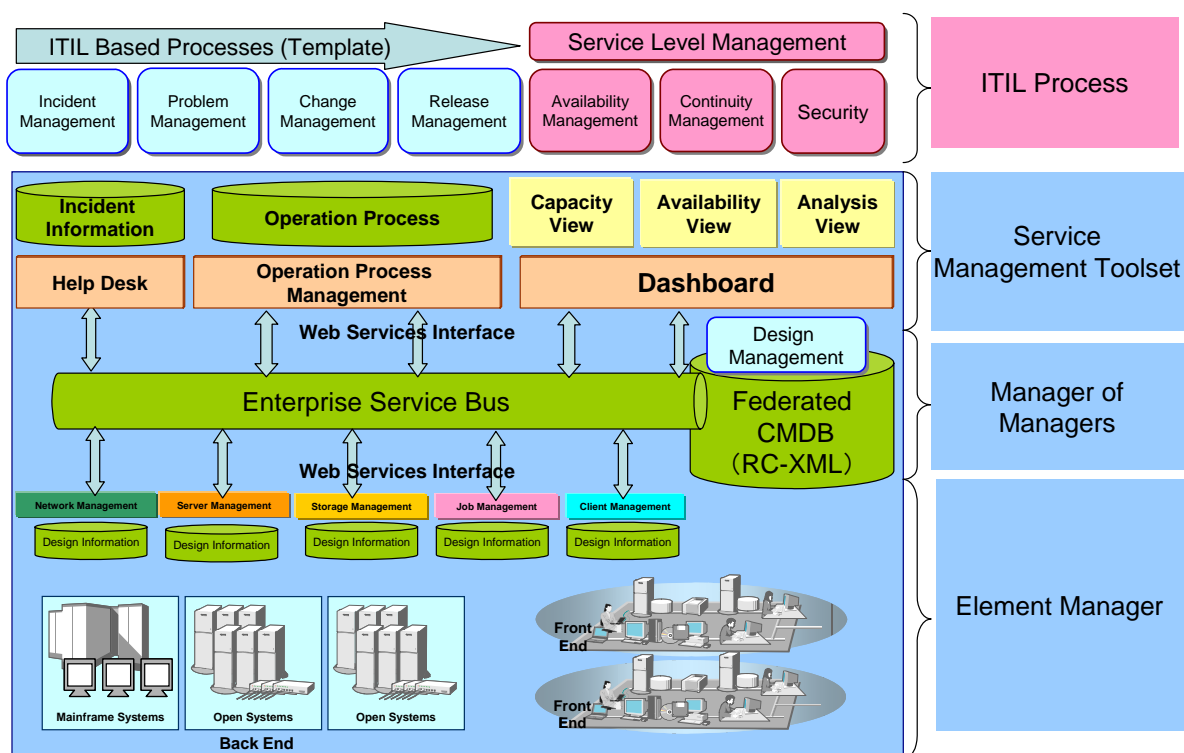
② Integration Layer (Manager of Managers)

The integration layer integrates the functions and information from the management layer, as well as their relationships via use of a shared schema. Federated CMDB belong to this layer. In order that web services interfaces (Enterprise Service Bus) can be used to connect management layer and ITIL layer functionality, the information managed by the management layer and ITIL layer, the functionality they offer, and their end points are managed. A common, consistent schema is used to manage all relationships, enabling centralized management, and access to necessary information and functions. Using a common schema makes integration of management tools provided by other vendors, and customer created proprietary management tools, possible as well. By expanding the schema, business management and business management information can also be integrated.

③ ITIL Layer (Service Management Toolset)

This layer consists of tools for managing operation processes. Help desk functionality for incident management, workflow functions for managing operation processes (operation process management), and information system status and other information viewing and analysis functions (dashboard) belong to this layer.

## Next Generation Centralized Management Architecture



**Figure 10-8 Next Generation Centralized Management Architecture**

### 10.7. Asset Management

Asset management, by providing centralized lifecycle management, from purchase to operating status and disposal corporate IT assets, both hardware, such as client PCs, servers, network devices, and storage devices, as well as the software that runs on them, serves as a process for assessing license usage and IT investment effectiveness. Below is a typical example of the asset management process.

(1) Establish an Asset Purchasing Plan

An asset purchasing plan is created in response to an objective.

(2) Receive Purchasing Plan Authorization

The purchasing plan is evaluated and authorized based on consideration of the purchasing objective and its cost effectiveness.

(3) Deployment / Configuration

The purchased asset is deployed and configured.

(4) Usage Status Assessment

Usage of the asset is monitored and relevant data gathered, for use in evaluation of the

utilization of the purchased asset.

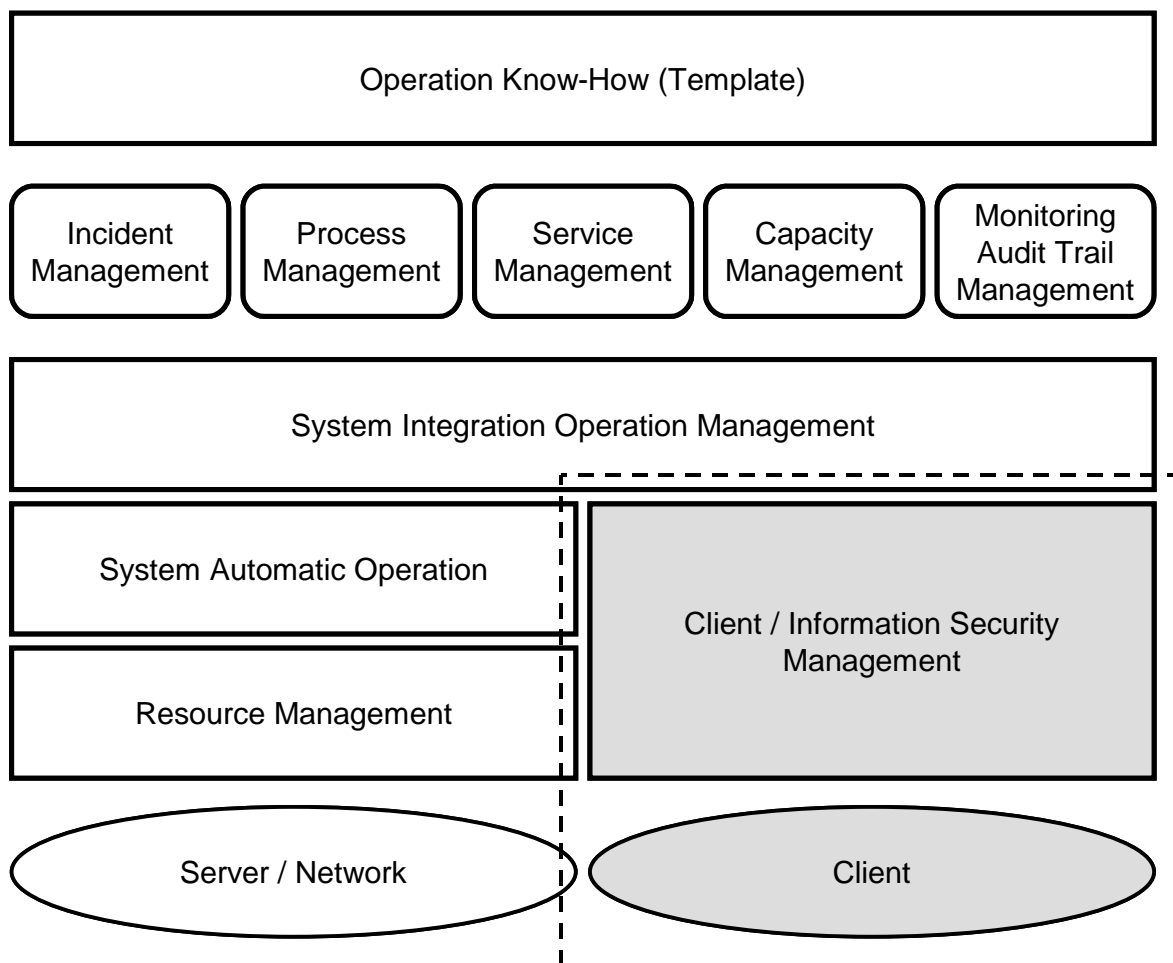
(5) Asset Disposal

The depreciated asset is disposed of.

Asset management information is used not only by system administrators, but by many other parties, such as financial managers and department information managers, for a variety of roles and purposes, and as such must be centrally managed.

From the standpoint of information security guidance, it is used for unauthorized copy prevention, virus protection purposes, and security measures. License management ensures, as an unauthorized copy protection measure, that the number of licenses in use fits the number of licenses that have been purchased. It is also used for managing license depreciation and disposal. In addition, it is also important, when disposing of a PC, to completely erase all data on its hard disk, and keep a record of said deletion.

Especially for software assets, virus protection and security measures are necessary, and, if left up to the end user, may not be thoroughly implemented, resulting in a plethora of problems. Virus patterns and security patch application must be centrally managed, their performance ensured, and evidence of this provided by management functions.



**Figure 10-9 Asset Management Positioning**

Client management provides management functions for lifecycles of PC clients, from planning to disposal, as well as software assets on the client PC. It also provides information security management functions for PC client information assets.

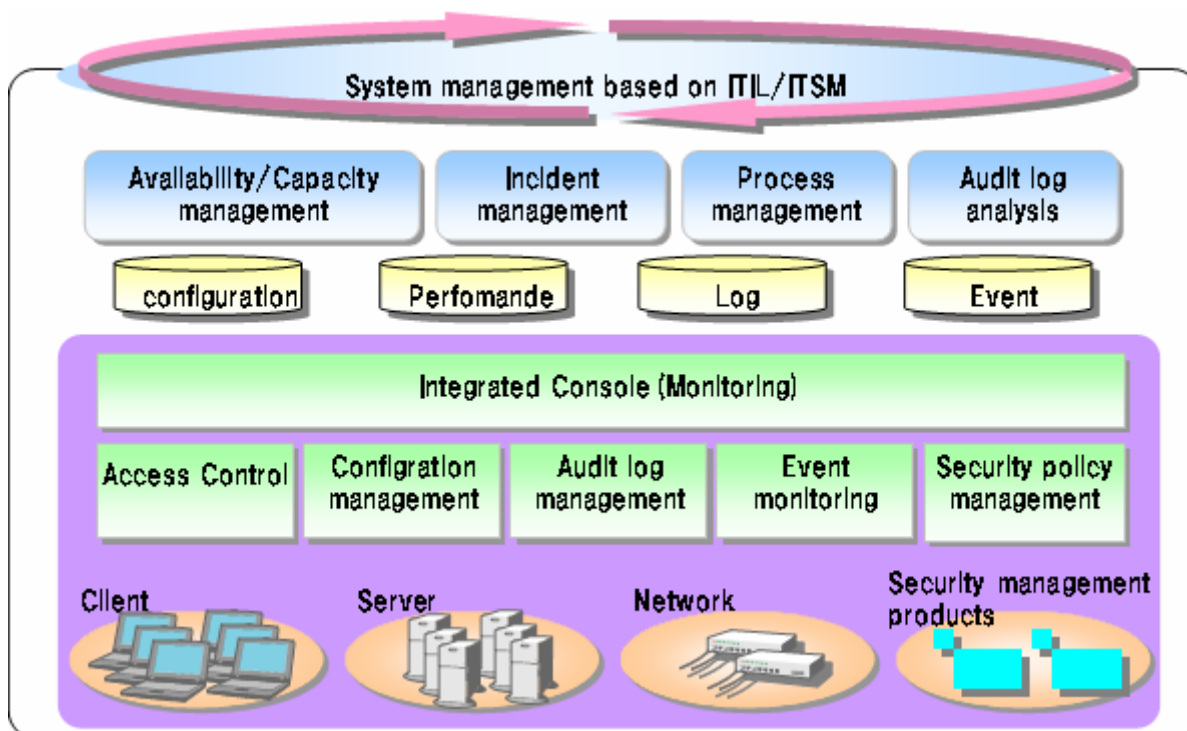
#### 10.8. Integrated Security Management (Integration with Operation Management System)

System operation management and security management are closely related, and monitoring for both should be integrated. Integrating operation and security management may provide the following benefits.

- Notification of alerts detected by security management products to operation management consoles, enabling central management of system-wide monitoring
- One of the following notification methods may be used.
- Notification via event notification commands / APIs on operating management system
  - SNMP trap based notification
  - Monitoring of messages output to event logs / syslog

- Monitoring of messages output to log files
- Remote command execution and automatic action settings for security management product alerts notified to operation management consoles
- Startup of security management product consoles from events displayed on operation management consoles and system components

The figure below shows the component model for integrated security management.



**Figure 10-10 Integrated Security Management Component Model**

## 11. Encryption

### 11.1. Encryption Technology

The goals of encryption technology can be divided into information scrambling (encryption) and authentication. Encryption for the purpose of obfuscation uses, as one technique, identical shared keys for encrypting and decrypting information, and, as another, public key encryption, which uses different keys for encryption and decryption. The former is appropriate for high speed processing, such as the encryption of large amounts of data, but key sharing is difficult. The latter is a slower technology, but since one of the keys can be publicly released, key sharing is unnecessary. Often, both types of encryption are used in a form of hybrid encryption. For authentication purposes, shared key MAC (Message Authentication Code) and public key digital signatures are used.

The figures below show an overview of both technologies.

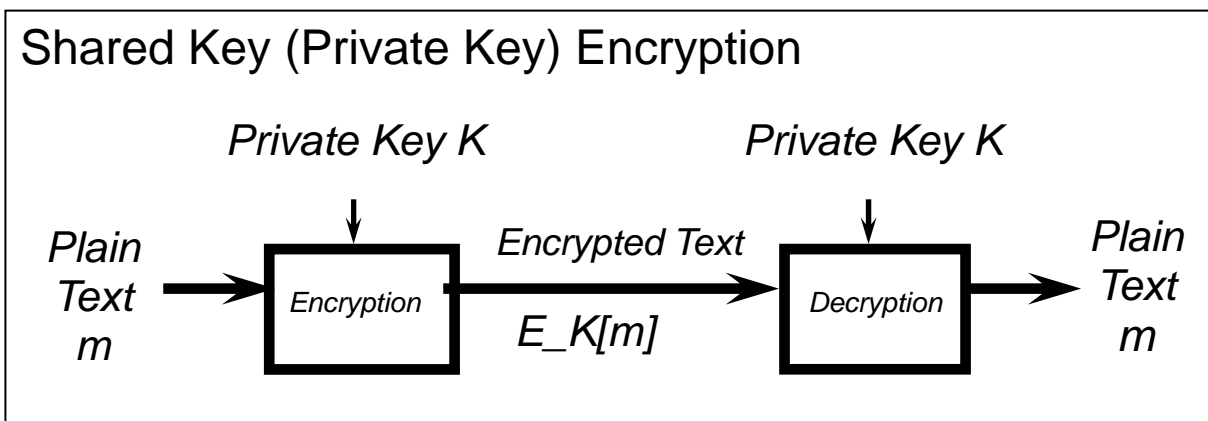


Figure 11-1 Shared Key Encryption

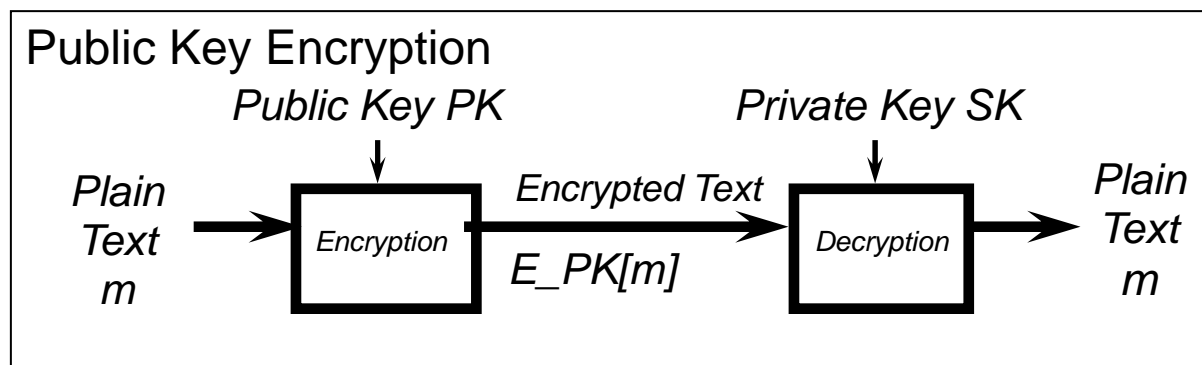


Figure 11-2 Public Key Encryption



The strength of an encryption algorithm increases with the length of the encryption key. However, the longer the key, the slower processing becomes. Applications must balance the strength of encryption and resulting processing speed, but there must be a minimum encryption strength standard. Depending on the encryption algorithm, encryption strength may vary even if the same key is used, so security bit length is used as a universal standard of encryption strength. To ensure future security, security bit length must be 80 bits or greater.

## 11.2. Standardization

In Japan, from 2000 to 2002, under the leadership of the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry, the recommended encryption algorithm for e-government was decided. As part of this project, leading encryption experts, both inside Japan and out, evaluated algorithms for public keys (security / signature / key sharing / authentication), shared keys, hash functions, and pseudorandom numbers. The results of this investigation have been released in the form of a report, available on the CRYPTREC site<sup>18</sup>.

In America, NIST ran a contest to determine the successor to the longstanding DES (Data Encryption Standard), establishing, in 2000, the shared key block encryption AES (Advanced Encryption Standard). In Europe, the joint corporate and academic NESSIE project established encryption algorithms in 2002.

On the international level, ISO / IEC 18033<sup>19</sup> standardized stream encryption, block encryption, public key encryption, and hash functions.

## 11.3. Shared Key Encryption

Shared key encryption uses the same key for encrypting and decrypting data, and is suited for high speed data encryption. Currently, the most popularly used shared key encryption algorithms are the American AES standard, and TDES (Triple DES).

AES is a cipher function which takes a 128-bit entry and outputs a 128-bit encrypted string. 128-bit (AES-128), 192-bit (AES-192), or 256-bit (AES-256) keys can be used. TDES is a cipher function which takes a 64-bit entry and outputs a 64-bit encrypted string. The key length can be either 112-bit 2TDES (2-key TDES), or 168-bit 3TDES (3-key TDES). AES is renowned for its security, and no attack methods for it have been found to be any more effective than brute force attacks ("security bit length" = "key bit length"), so unless there are any particular factors prohibiting its use, AES is recommended. The TDES encryption algorithm is one generation older, but is still practical for use if compatibility is an issue. However, attack vectors more effective than brute force attacks have been discovered for 2TDES, decreasing the encryption security to the equivalent of 57-bit security. As such, 2TDES should not be used except in

---

<sup>18</sup> <http://www.cryptrec.org/>

<sup>19</sup> ISO/IEC 18033-1:2005 Information technology -- Security techniques -- Encryption algorithms -- Part 1: General, etc.

cases where AES cannot be used because of compatibility needs. 3DES, for the same reason, drops in effectiveness to the level of 112-bit security, and should be avoided for the same reason. A wide range of other encryption algorithms have been produced and productized, but in general the use of encryption algorithms which have not been evaluated by third parties, and algorithms which have not been published, is not recommended. Also, modification of algorithms in order to improve processing speed or decrease their size may result in an unexpected decrease in encryption strength, and should not be performed. If algorithm modification is unavoidable, it should be done in consultation with an encryption specialist.

One of the lists of encryption methods which have undergone security evaluation in Japan is that in the e-government recommended encryptions selected by CRYPTREC. In Europe, the list of NESSIE Project selected encryption algorithms has also been released. Also in 2006, the ISO/IEC 18033 international encryption algorithm was established. No security problems have been discovered in these listed algorithms as of yet. When choosing an encryption algorithm, one of these should be selected. The AES algorithm is listed in all of these lists. AES and TDES encryption are license free. Note that some other publicly released secure algorithms, however, may require licensing.

#### 11.4. Public Key Encryption

Public key encryption is an encryption algorithm which uses different keys for encrypting and decrypting information, and is usually used to encrypt encryption keys and digital signatures. There are three basic types of public key encryption. IFC (Integer Factorization Cryptography), which uses the difficulty of prime number factorization as the basis for encryption security, such as RSA (Rivest-Shamir-Adleman) encryption, FFC (Finite Field Cryptography), which uses the difficulty of finite volume discrete logarithmic problems as the basis for encryption security, such as in DSA (Digital Signature Algorithm) and DH (Diffie-Hellman), and ECC (Elliptic Curve Cryptography), which uses the difficulty of elliptic curve discrete logarithmic problems as the basis for encryption security, such as in ECDSA (Elliptic Curve Digital Signature Algorithm).

Generally, the security of public key encryption increases as the length of the key increases, but increasing the key length also results in decreased processing speed. FFC and IFC offer roughly the same level of security for the same key length, but ECC can offer the same level of security with a shorter key. Specifically, encryption using a 1024-bit FFC key can be considered equally secure to a 160- to 223-bit ECC key.

The world record for RSA encryption deciphering is currently 663 bits, but 768-bit encryption is currently considered to be within feasible range. In order to provide sufficient security with RSA encryption, key lengths of 1024 bits or longer must be used. This is true for DSA and DH as well.

The world record for ECC encryption deciphering is currently 109 bits, but to provide sufficient

security with ECC in the future, keys of 160 bits or greater ("security bit length" is 80 bits) should be used. Please refer to "11.6 Approach to Encryption Length" for details regarding safe key lengths.

Generally, RSA is recommended. It can be used for both encryption and signing, and there is a large hardware and software library that supports it. The patent for RSA encryption has already expired, and DSA, while still covered by US patent, is license free. Some companies claim the rights to elliptical curve encryption, so it is necessary to confirm whether licenses will or will not be needed before use.

### 11.5. Export Regulations

Products containing encryption are subject to Japanese export regulations (note, however, that signatures are not covered by these regulations). Procedures vary depending on the country to which the product is being exported, the product itself, the length of the keys used, and the like. Relevant authorities and government offices must be consulted with before exporting products containing encryption.

### 11.6. Approach to Encryption Length

The table below shows the key lengths for equivalent security levels ("security bit length"). (NIST Special Publication 800-57 Table 2 on page 63). These are subject to change with computer technology and encryption theory advances. The table shows a comparison of key lengths for current technological and processing speed levels.

Security Bit Length	Shared Key Encryption	FFC (DSA, DH, etc.)	IFC (RSA, etc.)	ECC (ECDSA, etc.)
80	2TDES	L=1024 N=160	k=1024	f=160-223
112	3TDES	L=2048 N=224	k=2048	f=224-255
128	AES-128	L=3072 N=256	k=3072	f=256-383
192	AES-192	L=7680 N=384	k=7680	f=384-511
256	AES-256	L=15360 N=512	k=15360	f=512+

L: FFC public key length, N: FFC private key length, k: IFC key length, f: ECC key length

Generally, when using public key encryption to encrypt a shared key encryption key, the public key encryption key used must be stronger than the shared key being protected. As such, an AES-128 key must be encrypted an FFC3072 bit or greater key. With public key encryption, the

longer a key is, the more time and processing time it takes to generate it, so it is not currently included in the chart.

The table below<sup>20</sup> provides reference for US government recommended algorithms and minimum key lengths. For example, by looking at this chart, we can determine that to encrypt data in 2005, for use until 2015, TDES is not recommended. In this case, the public key encryption should not be 1024-bit RSA encryption, but 2048-bit RSA encryption.

Algorithm Security Lifetime	Shared Key Encryption (Encryption and MAC)	FFC (DSA, DH, etc.)	IFC (RSA, etc.)	ECC (ECDSA, etc.)
Until 2010 (strength is 80 bits or more)	2TDES 3TDES AES-128 AES-192 AES-256	L=1024 N=160 or greater	k=1024 or greater	f=160 or greater
Until 2030 (strength is 112 bits or more)	3TDES AES-128 AES-192 AES-256	L=2048 N=224 or greater	k=2048 or greater	f=224 or greater
2030 and after (strength is 128 bits or more)	AES-128 AES-192 AES-256	L=3072 N=256 or greater	K=3072 or greater	f=256 or greater

L: FFC public key length, N: FFC private key length, k: IFC key length, f: ECC key length

## 11.7. Hash Functions

A hash is a function which compresses from any length to a fixed length. Hashes are compressed values. There are currently 4 US standard (FIPS180-2) hashes used for security. These are SHA-1, SHA256, SHA-384, and SHA-512, and their hash values are 160 bits, 256 bits, 384 bits, and 512 bits respectively. SHA-1 is frequently used today. In addition to these standards, there are also European standards, such as RIPEMD-160 or Whirlpool.

Starting in August, 2004, there has been dramatic progress in the research of hash function security. Currently, SHA-1 collision tolerance security is considered to have fallen to the equivalent of a 61- to 62-bit security bit length (initially, it was the equivalent of 80 bits), and to ensure future security, hash values of 224 bits (112-bit security bit length) or greater should be used.

<sup>20</sup> Source: NIST Special Publication 800-57 66p. Table4

### 11.8. Response to Algorithm for Encryption in Danger of Losing Centrality of Privacy

During encryption algorithm research, sometimes new methods are found which enable deciphering of encryption more easily than was expected when the encryption method was developed. This is referred to as danger of losing centrality of privacy. An encryption algorithm comprising a major threat will not provide the security that is theoretically provided, so the algorithm should be changed to other algorithm as soon as possible. If, for some reason, an encryption algorithm or hash function is become almost danger, the security of keys under a certain length will diminish, and if it cannot be extended, a scheme should be developed in advance that allows encryption algorithm and key length changes.

### 11.9. Encryption Schema

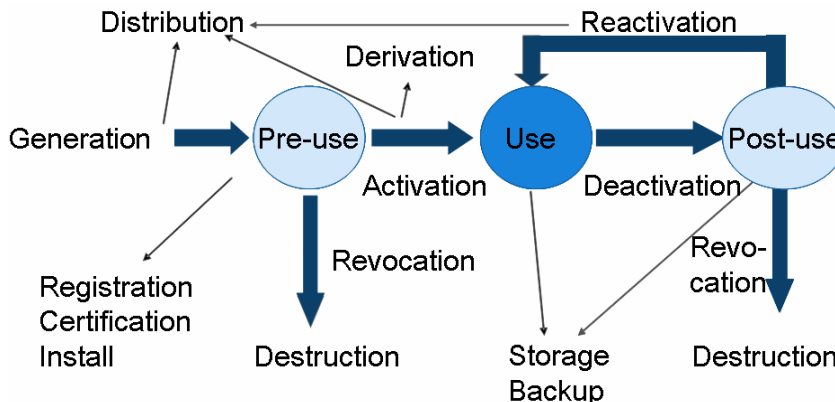
Modern encryption technology requires the prevention of any information (semantic security) for even the strongest type of attack, the adaptive chosen ciphertext attack. The most primitive encryption algorithms do not satisfy this demand, and as a result encryption primitive schematization has been developed in order to fortify these primitive encryption algorithms. An encryption schema is based on encryption primitives, using certain assumptions to guarantee security. That is, it is based on the difficulty of certain problems (such as prime factorization) to provide encryption security. If encryption can be broken, that indicates that these difficult problems can be solved. The schema asserts encryption security, and is referred to as provable security.

## 12. Key Management

### 12.1. Fundamentals

Encryption keys are used for encryption and digital signatures, and as such must be managed the most securely. The goal of key management is to control the use of keys necessary for performing encryption processing. It also provides confirmation of the security of the key lifecycle, from key generation to key destruction. An example of a more accurate definition would be FIPS140-2, which defines it as "the activities involving the handling of cryptographic keys and other related security parameters, including their generation, registration, verification, deregistration, distribution, installation, storage, archival, disposal, derivation, and destruction in accordance with security policies".

There are financial industry and smart card oriented international key management standards, as well as security demand standards for encryption modules providing encryption key protection and encryption processing, but generally the determination of whether a given key is sufficient is not always based on standards, but varies based on the security policies of the environment in which it is deployed, and the systems in which it is used.



**Figure 12-1 Key Lifecycle**

Below, as a concrete example of key management principles, is an example of the banking system specifications<sup>21</sup> for a retail store.

- 1) Individual access and confirmation of plain text private keys cannot be possible.
- 2) Systems must be able to provide protection for data, and prevent leakage of private keys which may be protected in the future.
- 3) Private keys which are generated must not be predictable.

<sup>21</sup> ISO 11568-1:2005 Banking -- Key management (retail) -- Part 1: Principles, etc.

- 4) The system must be capable of detecting private key compromising or attempts at unauthorized use.
- 5) The system must prevent and detect any attempts to change, use, replace, delete, or insert private keys, in whole and in part, for unauthorized purposes, accidentally, or when not permitted.
- 6) Keys must be changed to new keys before they expire.
- 7) Keys must be changed to new keys before the estimated amount of time determined to be necessary for a dictionary attack to succeed.
- 8) When a key is in danger of losing centrality of privacy, or believed to be compromised, the key can no longer be used.
- 9) If a key shared by a group is in danger of losing centrality of privacy, it cannot result in other group keys being compromised.
- 10) No information about replacement keys can be provided to a compromised key.
- 11) Keys can only be stored on devices if those devices have been confirmed to appropriately secure and be protected against modification or replacement.

## 12.2. Key Types and Related Information

Keys used in encryption systems are decided based on their type (encryption, signature, etc.) There is additional information related to keys, such as domain parameters for encryption algorithms and keys, and initial vectors. SP800-57, ISO/IEC11770, and the like contain specific information regarding key types and key related information. For example, data keys used for data encryption, and key encryption keys used for data key encryption, are two types of keys. Generally, any given key belongs to one type, that is, it should be used for only one purpose. Using one key for multiple purposes results in a decreased level of security. For example, when encrypting data, a key encryption key (a key used for encrypting data keys) should not be used. Key encryption keys must not be used to encrypt known plain text data.

## 12.3. Key Generation

Keys must be generated using secure random number generation functions. Random numbers must be unpredictable by third parties, and the results generated must not be usable in determining the values before or after the generated number.

Random numbers can be generated by using pseudorandom numbers as the seed data for generating a random number string, or via physical random numbers based on physical properties, such as thermal noise. In both cases, the numbers generated must be subject to randomization evaluation. When using pseudorandom numbers, the seed data must not be predictable by third parties. Attention must also be paid to establishing a health check system for evaluating whether random number generation functions are working properly.

Random number generation functions for encryption purposes, and their evaluation, are standardized in ISO/IEC18031 and ANSI X9.82. Pseudorandom number generation uses hash functions and public key encryption algorithms. There are also methods for using shared key encryption in pseudorandom number generation functions. ANSI X9.17 Annex C describes the generation of random numbers using a random seed and refreshed time stamp information in generating random numbers. X9.17 is written with 3DES as a base, but can also be used with AES and other block encryption. The random numbers generated can be used in key generation for shared key and public key encryption. The simple congruent random method and the linear feedback resistor method of generating random numbers are not secure, and must not be used for generating keys used in encryption or signatures.

#### 12.3.1. Shared Key Encryption Private Key Generation

Keys for shared key encryption are generated using the random number generation functions described above.

#### 12.3.2. Public Key Encryption Generation

For public key encryption, first a random number is generated, and then verification of whether its parameters satisfy various requirements is performed. Please refer to IEEE P1363 Annex A and FIPS186-3 Appendix 3 for details regarding public encryption key generation methods. For generation of necessary elements for RSA encryption, the Miller - Rabin test (see IEEE P1363A.15, ANSI X9.80) should be used, and for DSA and ECDSA, the method described in FIPS186 should be used. For RSA encryption key generation, strong random numbers, avoiding certain types of prime numbers, may be needed. In these cases, the Pocklington's theorem applies (see ANSI X9.80 5.2.4.1.2).

The elliptic curve parameters used in elliptic curve encryption should be secure if conformant with the standards contained in FIPS186-3 and ANSI X9.31, but when generating these parameters on ones own, the Scoof algorithm is preferable from a security standpoint to the CM algorithm.

Key generation must occur in a secure environment where key modification, replacement, and theft by third parties cannot occur. Specifically, it should occur in hardware tamper-proof modules referred to as encryptions modules. When generating a key with software, even if the key can be used from the software, the key should not be directly viewable from the software.

### 12.4. Key Distribution

There are two methods for securely moving encryption keys between systems: manual transfer using key loading devices, and automatic electronic transfer using distribution protocols. Key



distribution should normally be performed using automatic key distribution.

Automatic key distribution protocols for SSL/TLS and IPsec have been standardized. For IPsec, ISAKMP/Oakley should be used for automatic key distribution instead of manual key configuration. These use public key encryption and third party certificates to reliably transfer keys.

There are also methods for using shared key encryption with trusted third parties. Kerberos is the most well known example of this.

Design and use of new, proprietary automatic key distribution protocols should be avoided. This is because there are many demands on these protocols, such as resistance to spoofing and resend attacks, as well as methods for handling key invalidation. If, however, it is absolutely necessary to do so, the key distribution methods described in ISO/IEC11770 should be used as a base, and design should be performed in consultation with a security specialist.

### 12.5. Secure Key Archival

Secure key archival requires the ability to prevent everyone except from authorized key users from entering, operating, replacing, or deleting keys. Key archival space and archival methods must also be minimized.

Ideally, hardware should be used for secure key archival, but when using software, the key must not be viewable from the application, and APIs should be used to perform only the appropriate operations on the key. PKCS#11 is an example of API for doing this.

Hardware key archival must protect against both logical and physical attacks. FIPS140-2 and ISO/IEC 19790, based on it, describe the requirements for encryption modules. In order to protect certificate authority root keys, FIPS140-2 level 3 or greater security is needed.

In addition to these functional requirements, if there are any vulnerabilities, key extraction may be possible even though the key is believed to be archived securely. Security evaluation must be performed, from web application vulnerability based attacks to electromagnetic and fault attacks for IC cards.

### 12.6. Key Backup

When accessing an encryption module in order to backup or move a key, the principles of split knowledge and dual control must be applied. That is, processing should not be possible by a single person, but must require authentication by multiple parties. Likewise, when extracting a key from a non-secure environment, one person should not be able to access all (encrypted) key information, but this should be divided and managed by multiple personnel. Verifiable secret sharing is used to accomplish this. For example, a secret key may be divided into five pieces, and the original key reconstructible with three pieces of the key.

## 12.7. Key Replacement and Disposal

Key replacement refers to stopping the use of a certain key and using a different key instead as a means to improve encryption reliability and decrease the risk of leakage. Usage periods should be decided based on key types, such as data keys or key encryption keys, both for public and shared key encryption.

Generally, the more data encrypted by specific key obtained by a third party, the greater the likelihood of the encryption being cracked. The period for key renewal should, thus, be based on the frequency with which that key is used, the volume of encrypted, decrypted, or signed data, and the specific qualities of that data. Please refer to SP800-57 section 5.3.6 regarding the approach to key types and their key renewal periods.

In order to securely archive electronic documents in accordance with the recent electronic document law, a schema must be decided for key replacement, including signature keys and timestamp keys for long term archived documents. Likewise, a schema must be decided for secure key replacement in the event that a key, or part of a key, is leaked.

Keys must be completely deleted when disposed of. Specifically, if a key is owned by multiple parties, all encryption modules containing those keys must be completely reformatted or physically destroyed. Any backed up keys must be likewise destroyed. Destroying a key will make any data encrypted with that key inaccessible, and thus the method for handling this data must also be decided.

## 12.8. Key Management Architecture

Architecture for system-wide consistency in key management by individual applications is becoming necessary. In order to implement this, the structure of the system, the importance of the information it handles, and the lifecycles of keys used in the system must all be considered.

Key security improvement is based on first having a secure, dedicated hardware platform, consisting of highly tamper-proof encryption modules used in key management and operation, and a key management system based on the master key enclosed therein. In order to implement this, consideration from a variety of perspectives is essential.

### 12.8.1. Centralized Encryption Key Management of Multiple Encryption Modules

Currently, key management for applications requiring security is handled by storing keys on encryption modules for individual servers, and basing the system-wide key structure on that, using centralized management to perform system-wide key management. However, this requires a large amount of key management, and in the future an architecture which provides centralized key management with integrated server key management will be essential.

Integrating key management for individual applications makes appropriate integrated key management based on the importance of the data handled possible.

#### 12.8.2. Management of Multiple VMs on one Server with one Encryption Module

In the future, when integrating servers with virtual machines, an architecture will be necessary for integrated management of encryption modules for key management of multiple virtual machines on one physical server.

#### 12.8.3. Integration of Key Management for Multiple Applications on a Single Client PC

Online centralized management at a key management center of keys used by individual client PC applications enables the design of systems which can prevent corporate key leakage. Currently, PKI and Kerberos are used for authentication infrastructures, but in the future centralized management of master keys used in client PC file encryption, SSL, and IPsec will allow corporate systems to take a more secure approach.

#### 12.8.4. Approach to Secure Key Management for All User Equipment and Embedded Devices

Cellular phones and embedded devices used by users contain encryption modules to provide secure processing and transmission. These devices may contain private customer information and confidential corporate information, and may be integrated with corporate business systems. Because these devices may be lost or may break, information on them must be managed more securely. An architecture (for example, Trusted Platform Module [TPM], etc) providing key security to ensure confidentiality and authentication for these devices will become necessary.

## 13. Physical Security

### 13.1. What is Physical Security?

Physical security is not clearly defined by standards and codes. Instead, it is addressed in a number of standards from the viewpoint of protecting information assets. Broadly, it includes the physical, electrical, air-conditioning, and disaster facilities where information assets are stored.

Information security includes the separation of roles, with security measures implemented for each role. Physical security is a means of preventing unauthorized physical access, via keys, cards, biometric authentication, video, and the like. Physical security is defined herein as the implementation of overall corporate asset security based on a hierarchical model combining information security with security affecting personnel and information assets.

With the advance of technology, security measures may become almost danger, making it difficult to maintain initial security levels. For physical security as well, a PDCA cycle must be implemented, including authentication, access control, audit trail management, and centralized management, keeping abreast of changes in the security landscape.

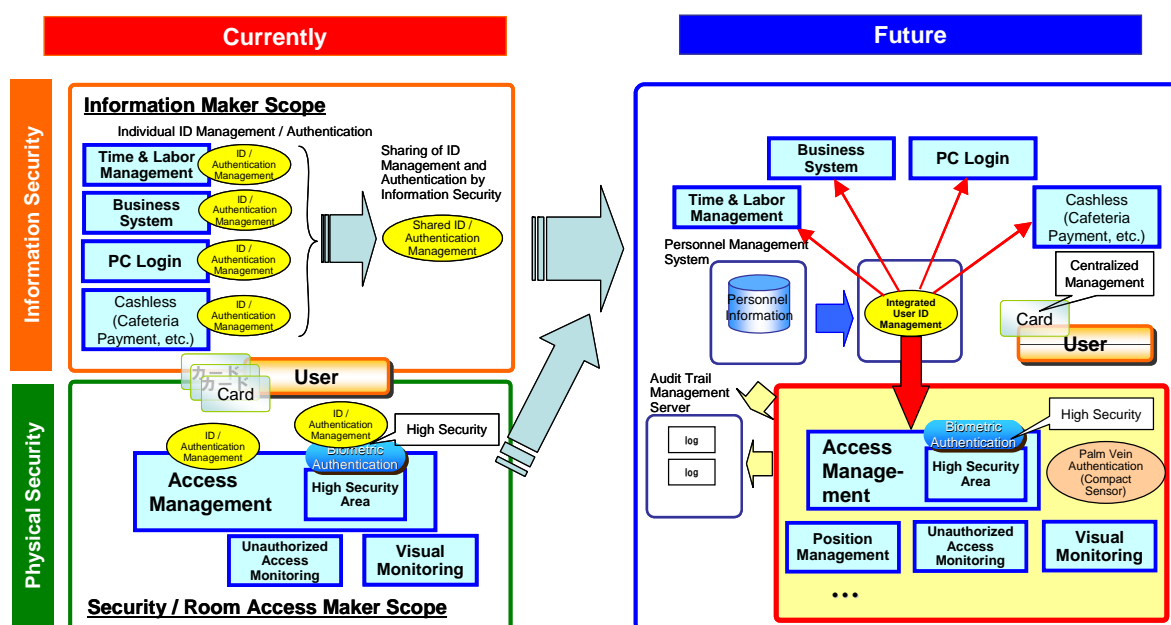


Figure 13-1 Physical Security

## 13.2. Physical Security Demands

### 13.2.1. Authentication / Identity Management

Identification in physical security, as with information security, utilizes IDs. Zones must be established where access is allowed based on IDs, and personnel and equipment must be identified in order to provide physical security management. Biometric authentication data is a form of ID data, and verification via IC cards or biometric authentication is required.

In order to perform physical security authentication, it is important to take ease of use and cost into account in design and operation. For ease of use, especially, physical access system and application integration, as well as identity management (integrated ID management) should be considered.

Basic physical security authentication is based on ID and password usage, but for stronger security, multiple element authentication, using highly unique biometric data, should be implemented. There are a number of methods of biometric authentication, but the high accuracy of palm vein authentication has resulted in an increase in its use.

## 13.3. Access Control

Access control in physical security uses personnel access identification and control based on zoning design, which determines whether a certain person can access a certain area. Another feature of access control is authentication which allows only the authorized person to enter a room (such as antipassback functionality), preventing unauthorized personnel from entering by following an authorized person. High level access control is necessary, especially for departments which handle customer information.

## 13.4. Audit Trail Management

For internal control and verification, it is important that logs for auditing are entered correctly. Physical security includes management of facility access (ingress and egress) for people and objects in the form of identification and authentication records. These logs must be collected, stored, and analyzed. Logs, and accompanying video, must be managed for personnel gaining access via impersonation, or for personnel who have gained access through improper means.

## 13.5. Centralized Management

Centralized management of physical security includes a wide variety of issues. The following are representative examples of management items for implementing security control.

- "Configuration Management", providing support for design changes, including configuration changes due to room additions, layout changes, and security level changes, and management of up-to-date configuration information.
- "Problem Management" and "Incident Management", providing contingency plans for

handling physical security issues and problems, and timely handling thereof.

Traditionally, authentication status, access status, and video data have been managed separately, but as audit trail data volumes grow larger and more complex, total management ability will become essential for reliable, efficient operation.

It is also recommended that integration with risk management systems (contingency plans) be implemented for video based intrusion monitoring, equipment monitoring, and the like, for important facilities.

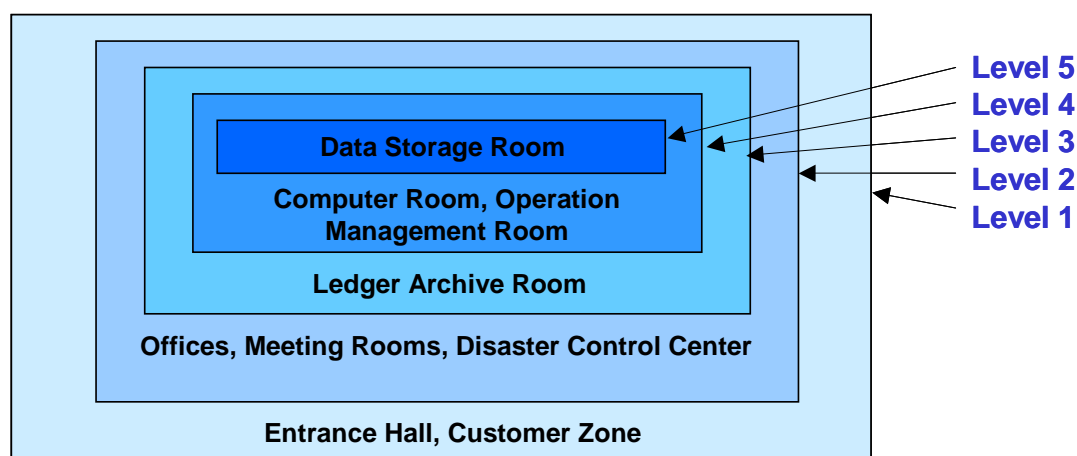
### 13.6. Security Specification Demands Which Must Be Given Consideration

Physical security design needs must be organized, not from the position of parties invisible to IT networks, but people in proximity to facilities and information assets which may be threatened. Below are some examples of points to be considered when implementing physical security.

#### 13.6.1. Physical Security Level Establishment

Security levels for individual zones must be established, taking into consideration corporate security policies as well as who does what within those facilities. Security measures must be established for individual levels, factoring in the work contents of employees and the importance of individual assets (layered security).

#### - Security Level Configuration Example -



**Figure 13-2 Security Level Configuration Example**

Security levels are higher the more the area they cover requires confidentiality. However, security levels must sometimes be released in order to allow evacuation in the event of a natural disaster, fire, or the like. When this occurs, IT security, such as shutting down of all network access, should be implemented while releasing physical security constraints.

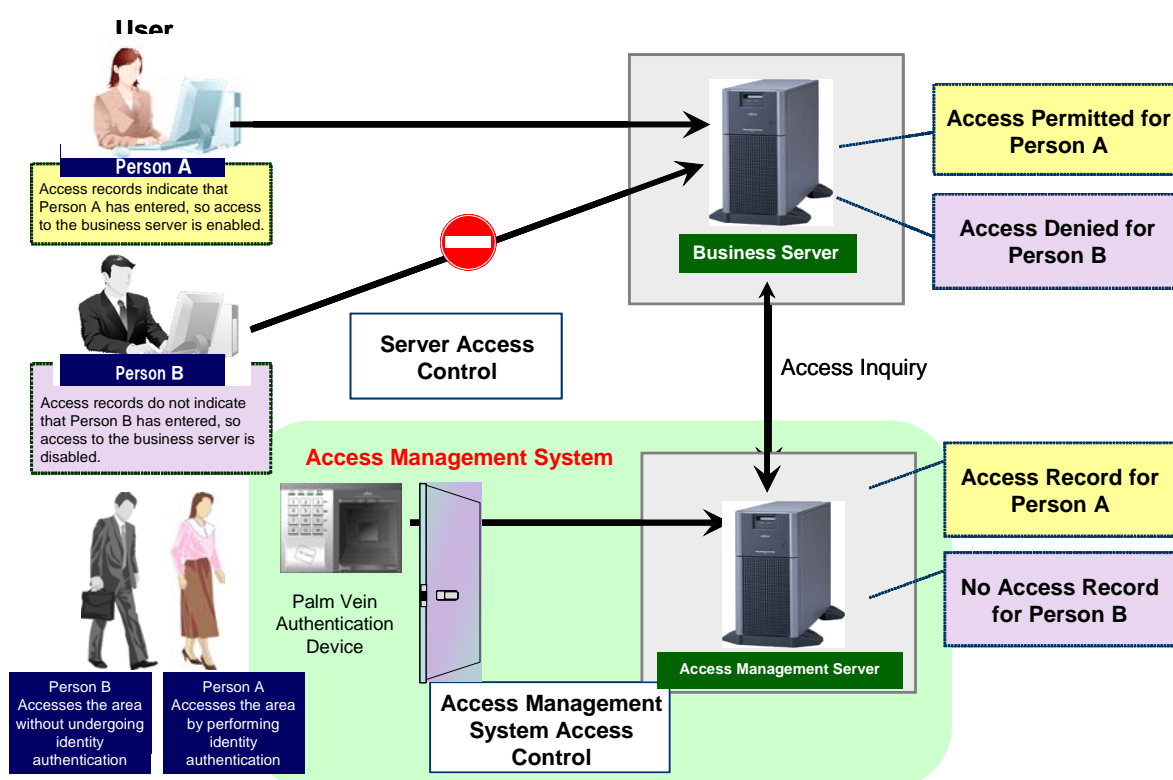
### 13.6.2. Flow Planning (Circulation Plan) and Zoning Planning

Flow planning is an essential facet of audit trail management. It requires planning of personnel movement for all possible personnel. Identification and authentication results log based activity history management are also essential for assessing unauthorized activities. Security level implementation for each zone, with graduated zone movement, enables the implementation of flow planning. Zones should be arranged such that adjacent zones are one step away from each other.

### 13.6.3. Integration with Information Systems

Integrating physical security systems and information systems results in increased security. However, in doing so, attention must be paid to data management methodology and synchronization methodology.

Integration of physical security identification, authentication, authorization, and ID management with information systems can be accomplished through the design of integrated identity management systems. The figure below illustrates this.



**Figure 13-3 Results of Identity Management Implementation**

As with information systems, audit trail collection and management are an important element of physical security. Below are some of the logs which must be collected as part of physical security.

- Zone entry and exit times
- IDs used to access zones
- Video data

The following differences with information systems log analysis must be observed with physical security.

- Zone access rights
- Zone access frequency/quantity
- Entry and exit status confirmation using video and number of entries and exits from zones

Necessary log management of zone entries and exits, entry and exit logs, personnel number reference, and video monitoring of log points can be performed by linking log information with video data in a database.

Security levels, monitoring methodology for providing audit trails, and recording methods must be taken into consideration for video security. Details concerning movement detection feature implementation, video recording quality levels, modification prevention, and archival periods for video monitoring of high security level areas must be decided in advance.

### 13.7. Physical Security Convenience

Thorough access management can be extremely restrictive, and negatively impact work effectiveness. As such, security levels and the ease of facility use must both be maintained, selecting appropriate materials based on zone security levels. For example, by using video, biometric data, and RFIDs, high levels of security can be maintained, enabling office terminal access and automatic security mode switchover when leaving ones desk.

Tag based flow management can be used to tie secure area access confirmation to video data, resulting in detailed auditing trails.

### 13.8. Points to Consider for Biometric Authentication Equipment

Due to the highly unique nature of biometric data, the implementation of biometric authentication devices can result in high security design. However, due to the fact that authentication happens on a one-by-one basis, care must be taken when determining where to install the authentication equipment such that it does not result in a backlog disrupting flow planning. Also, one must keep in mind that some people will be unable to use biometric authentication. Contingency plans must be considered for people who are unable to utilize biometric authentication which targets a specific part of the body.

### 13.9. Use of Video

Merely recording video is not in itself a security measure. It is important to consider how that video can be used as part of a security measure. The following two are examples of utilization



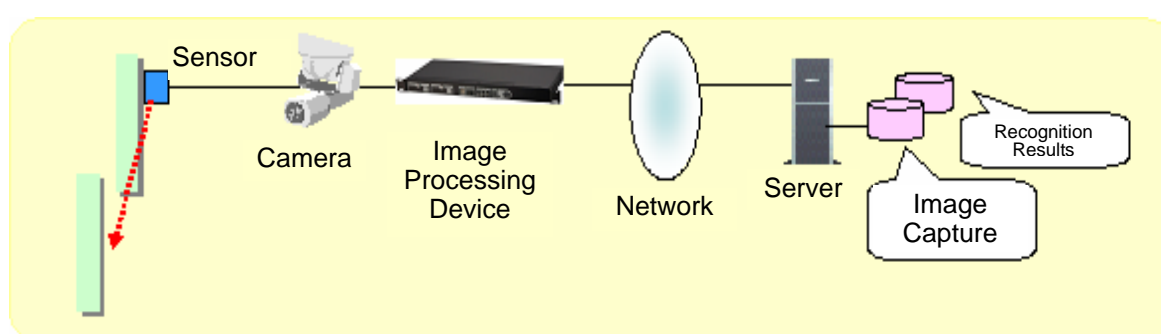
of video data in security measures.

- Identification and authentication accuracy improvement through integration of alert information and authentication information with video verification
- Identification, authentication, and warning information notification based on data changes in visual dynamic states

### 13.9.1. Access Control

Access control systems should be integrated, using ID cards and supplementary video data. Facility entry or exiting is detected, and video from immediately before and after the detected event is saved. This is effective for entry and exit verification.

Consideration should also be given to the recording of personnel entering or exiting areas with security levels which do not limit access. Cameras can be installed at gates, and image processing performed to identify and categorize personnel, with identification results and captured images stored. These can be used for statistical management of area usage, as well as security records.



**Figure 13-4 Image Processing**

### 13.9.2. Equipment Management

In addition to area management such as physical access prevention (locking) and access control system use, video and images can also be used for equipment management. Monitored equipment can be filmed with cameras, and equipment movement detected via image processing. It can also detect when unauthorized materials are brought into a work area, or when materials which have been brought in are left behind. For systems working 24 hours a day, 365 days a year, in addition to network monitoring, systematic direct visual inspection and video based remote monitoring are also possibilities.

Video data stored by the systems above must be managed appropriately, just as other management information is managed. When performing remote visual monitoring, video data must be encrypted or otherwise secured to prevent data leakage.

### 13.9.3. RFID Tag Security

There are two types of RFIDs: passive and active. Passive RFID is widely used in ID management and PKI. The uses of active RFID are currently limited, but there is growing anticipation regarding its future use for position detection. The advantages of active RFID; immediate detection and dozens of meters wide span, can be used in security measures.

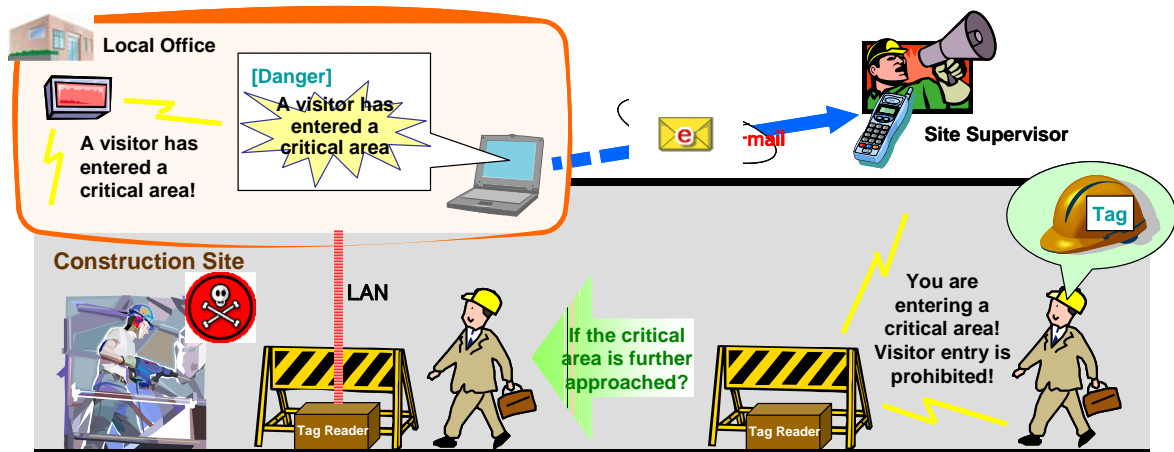


Figure 13-5 RFID Example

## Section 3 ESA Based Systems

## 14. System Design

The most important thing in implementing security in an IT system is access control, protecting assets (data, programs, hardware resources) from a variety of attacks. Assets can be protected by shielding them from the many types of external attacks, and by correctly controlling internal access.

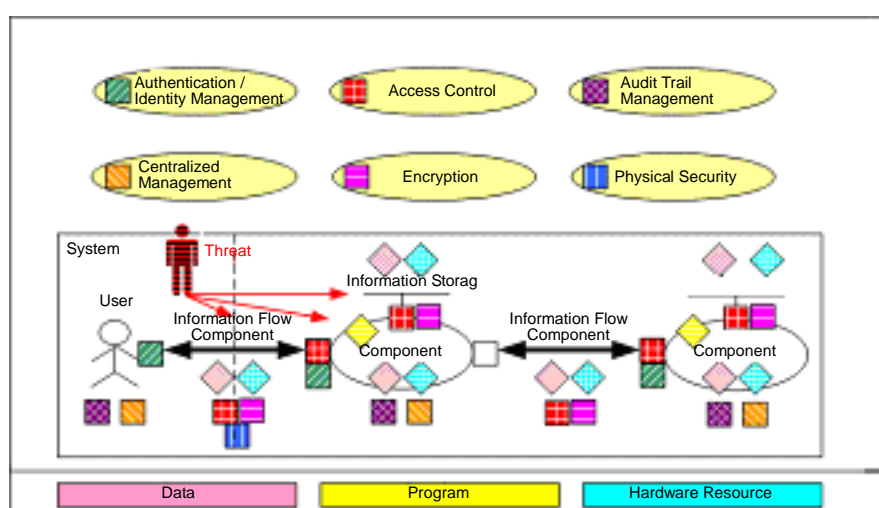
Methods must also be provided for evaluating whether or not that access control itself has been compromised by external or internal attackers.

Section 2 covered the basic concepts needed for the establishment of enterprise security architecture. This section uses the approach to architecture provided in section 2 to describe the basic approach to system design, and representative models used when doing so.










This section presumes, when implementing security functions in an IT system, that that IT system itself is physically protected. Please refer to Section 2, Chapter 13 "Physical Security" for details regarding physical security.

### 14.1. Security Function Implementation Model

IT systems can be considered as a conglomerate of resources (containing data or programs in a hardware resource) and transmission components, connected by some means. IT system access attempts can thus be controlled by implementing control measures for access attempts to individual resources, and control measures for access attempts to transmission components connecting resources. This is explained briefly in the diagram below.



**Figure 14-1 Resources and Security Functions**

"Figure 14-1 Resources and Security Functions " is a model which shows the relationships between resources and security functions in a general system. The four types of squares in the figure represent the following security functions: : Authentication / Identity Management, : Access Control, : Audit Trail Management, : Centralized Management, : Encryption, : Physical Security. The three diamonds represent the following assets: : Data, : Program, : Hardware Resource. The white triangle in the figure represents applications.

The "information processing component", "information flow component", and "information storage component" are modelizations of IT system design elements. The "information processing component" refers to the processing of data, and the hardware resources which perform this processing. It includes programs, servers, client PCs, and network equipment. The "information flow component" refers to the flow of data itself. It does not include cables, switches, or similar resources. The "information storage component" represents the locations where data is stored, and includes database servers and authentication servers.

In this model, before and after the flow processing component come authentication, identity management, and access control. Audit trail management is placed for each information processing component. Access control is always placed between the information processing component and information storage component, and the information flow component performs required encryption processing in accordance with the security policy.

If this model is obeyed, a user whose identity has been verified uses an information processing component client PC to access, via an information flow component network, a separate information processing component application server to perform business processes, storing information in an information storage component database (disk).

The ESA approach is to consider the six security functions for each resource, and between each resource. Security function implementation is performed as described in the procedure below. Please see Section 4. "Appendices" for details regarding risk and threat analysis.

#### 1. Asset Clarification

Assets to be protected are selected and clearly itemized. Threats are first determined for assets, and then countermeasures for those threats.

#### 2. Processing Flow Clarification

The processing flow for assets is clarified, specifying where on the IT system the assets reside, how they are processed, and where they are stored. This is effective in clarifying which security functions should be implemented where in each processing flow.

#### 3. Threat Clarification

Once the assets and their locations have been clearly itemized, the threats against those assets are determined. Determining the threats enables selection of countermeasures

against them.

#### 4. Security Function Placement for Each Resource and Between Each Resource

Countermeasures are decided for the threats identified in step 3. First, security functions for resources such as web servers and database servers are decided on. Next, security measures are decided for the segments between servers and resources. When assets span multiple resources, the security offered by a security function on one resource must carry over to the resource which the asset is passed to. This allows the security offered at the beginning to be maintained until the end.

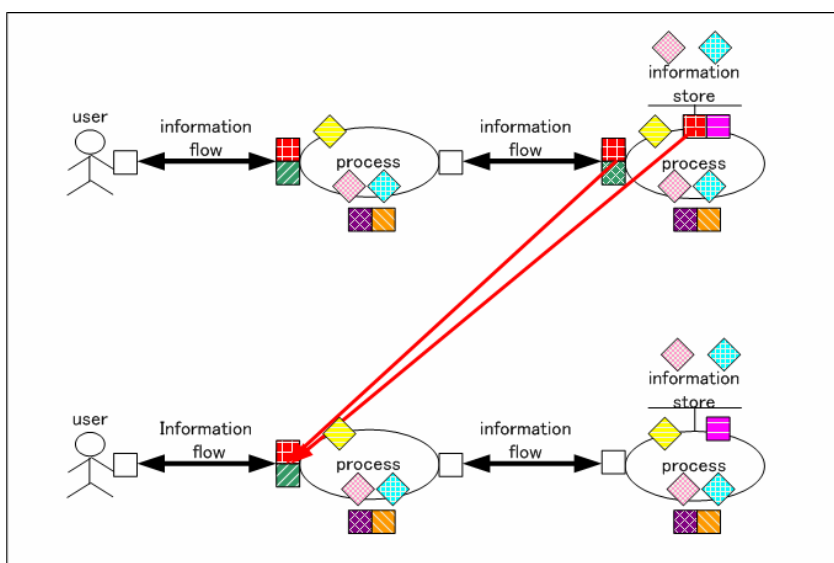
#### 5. Security Function Aggregation

Next, security functions decided in step 4 for resources and for the segments between resources must be checked for redundancy and unnecessary duplication. Unnecessary authentication functions and redundant access control functions within safe zones must be identified when possible, and their security functions aggregated. When aggregating these security functions, it is important to keep in mind the security requirements of the entire IT system, and to collect these security functions together without negatively impact the overall IT system. This is described further in "Aggregation and Aggregation Deployment" below.

### 14.2. Aggregation and Aggregation Deployment

Aggregation is the collecting of redundant features based on the security of zones created through the use of access filtering equipment such as firewalls.

Aggregation is performed using security functions and resources, such as the resources and security functions shown in Figure 14-1. For example, when a web server and an application server within the same secure zone transmit directly to each other, both servers making authentication requests to an authentication server is referred to as redundancy. In this case, aggregation can be performed by performing authentication with the authentication server via the web server, and handing the authentication results over to the application server. Aggregating functions and deploying them like this is called aggregation deployment.



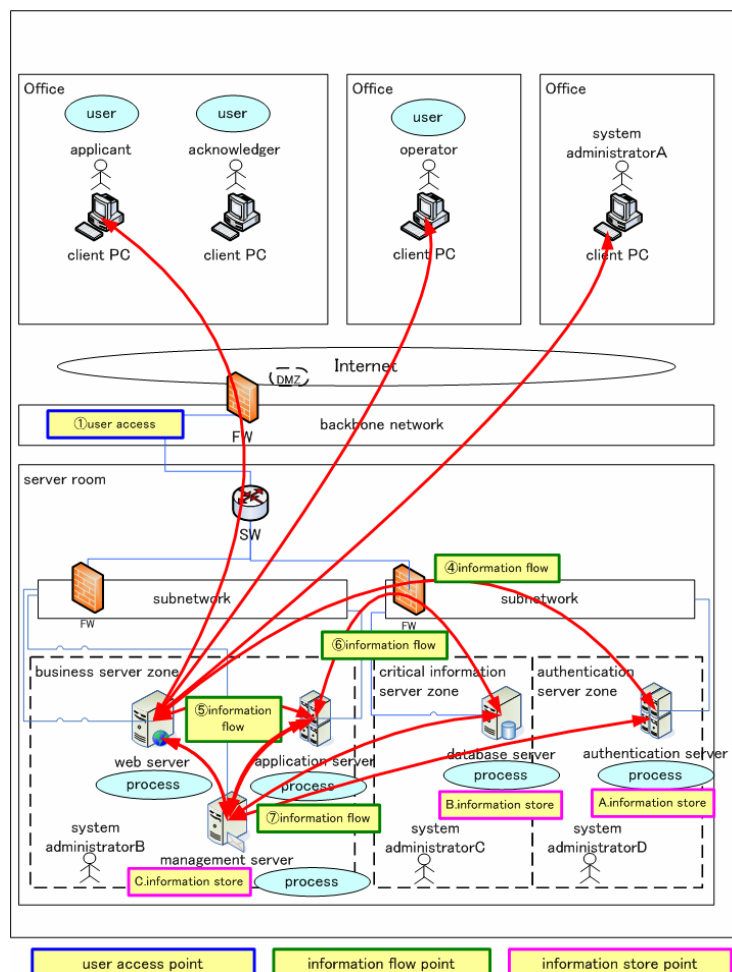
**Figure 14-2 Aggregation Deployment**

Let's look at another example. In the figure above, the three access control functions for the information processing components are aggregated in one location. This is based on the fact that the information processing components on the right and left are within zones secured by firewalls. As long as the information processing components are authenticated by each other, the security offered by the initial access control will be carried over from information processing component to information processing component. Aggregating the access control functions in one location does not affect the level of security. Generally, aggregating security functions results in improved operability, and decreased deployment and operation costs.

### 14.3. ESA Based Model Implementation Example

We have explained the basics of security function implementation based on the ESA approach. Next, we will look at specifically how to implement security functions from a resource and inter-resource perspective in a three-layer web system model.

The three layer web system is the core system configuration in the modern computing world, and also the configuration requiring the most security configurations. This is why the three-layer web system was selected as the first ESA based model. Future ESA based base models will add patterns in conjunction with aggregation procedures, supporting a wide variety of system configurations.

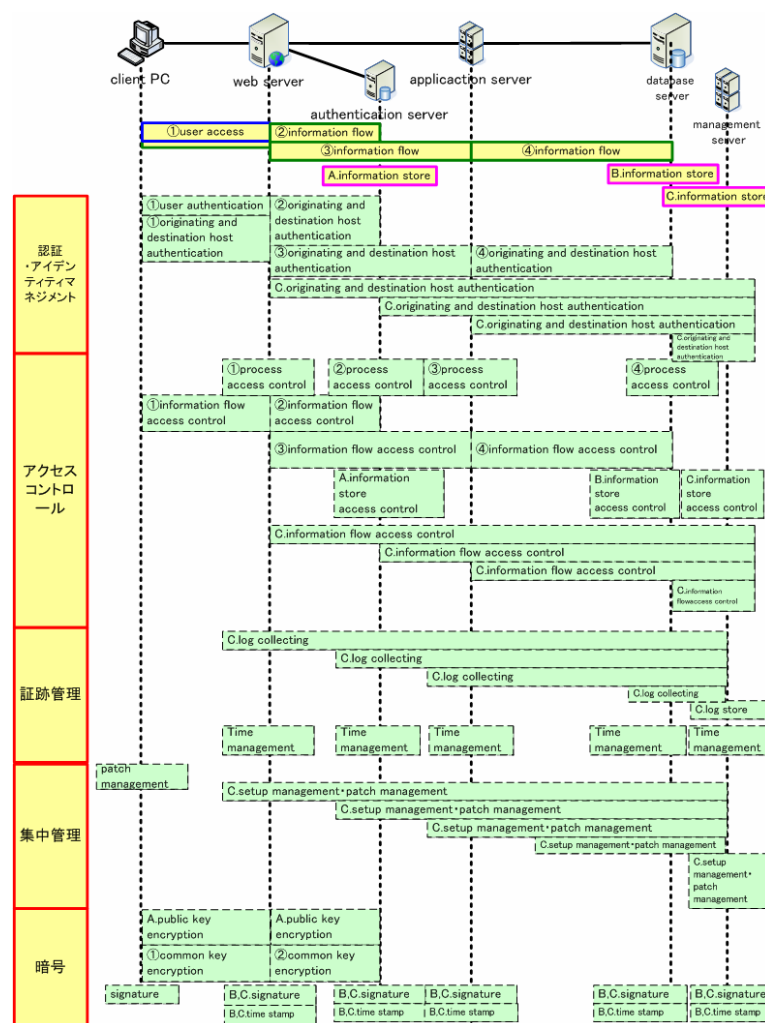


**Figure 14-3 3-Layer Web System Model**  
**(System Configuration / Access Relationship Diagram)**

Before looking at security functions for individual resources and their connections, first the access relationships between different resources within the system must be confirmed. In this system model, user terminals in offices and branches connect via the internet, through a company firewall, to company web servers, authentication servers, application servers, and database servers (in that order). The curved arrows indicate the flow of data. This model contains three zones: the business server zone, the confidential server zone, and the authentication server zone, requiring data to pass through a firewall whenever accessing a different zone, providing multiple levels of protection.

The figure is an overview of the security function items which should be implemented in a three-layer web system model. Details regarding the individual resources and inter-resource connections are provided in the following chapter.





**Figure 14-4 3-Layer Web System Model (Overview of Required Function Implementation)**

### 14.3.1. 3-Layer Web System Model Security Function Implementation Considerations

Below is a summary of the considerations made when implementing security functions in this model.

#### Authentication / Identity Management

- Authentication functions for authentication between resources are taken into consideration to provide security.
- The least necessary privileges are granted to users in order to prevent unauthorized use of the IT system.
- User roles and responsibilities are divided, and unauthorized activities prevented.
- User accounts are centrally managed in order to provide improved operability and security incident prevention.

### Access Control

- Access control for stored data is taken into consideration.
- Data manipulation by users (direct data manipulation, manipulation via applications, etc.) is taken into consideration.
- Access control for programs is taken into consideration.
- Access control for data flow is taken into consideration.
- Aggregation is taken into consideration for protected zones.

### Audit Trail Management

- Time synchronization for audit trail accuracy is taken into consideration.
- Signature and time stamp application is taken into consideration for audit trail legal admissibility.
- Audit trails are centrally managed for improved operability.

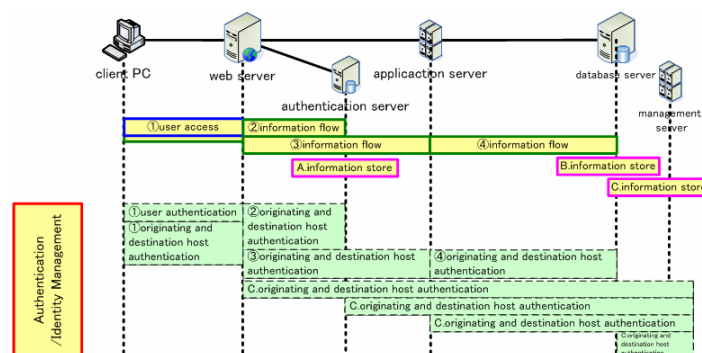
### Centralized Management

- Constant updating in order to correct any newly found vulnerability is taken into consideration.
- All changes performed in the IT system are objects of configuration management.

### Encryption

- Individual client PC encryption is not performed.
- User information sent when client PCs perform business activities is encrypted.
- User information sent from web servers to authentication servers is encrypted.
- Transmission between servers inside a secure zone protected by firewalls is not encrypted.

#### 14.3.2. Authentication / Identity Management Function Implementation



**Figure 14-5 Authentication / Identity Management Function Implementation**

### Client PC

This model stores all business assets on a database server. Data is not stored on client PCs. As such, client PCs do not need a strong authentication or identity management framework. However, in order to prevent usage by unauthorized parties, ID management functions to limit users are required.

### Connections Between Client PCs and Web Server

In order to prevent client PC spoofing, authentication is performed between accessing equipment and accessed equipment. To do this, SSL client authentication is used for transmission. SSL client authentication provides security for the transmission route, and prevents spoofing. SSL transmission can also be used for encryption, and is relatively inexpensive.

### Web Server

The only user accounts on the web server are administrator accounts. All user accounts used for business performance are centrally managed by the authentication server, and the web server receiving authentication requests from client PCs pass those requests on to the authentication server.

### Connections Between Web Server and Authentication Server

User account and authentication information received from client PCs are used to make an authentication request to an LDAP or other authentication server, and the authentication pass/fail information received from the authentication server is used for further processing.

### Authentication Server

If user account management is scattered, administrators are required for each server, and maintenance times will increase in direct relationship to the number of servers. Authentication information management will also become more complex, increasing the chances of security incidents. In order to prevent these problems, IT system user accounts are centrally managed by the authentication server. Division of roles and responsibilities is a cornerstone of security, so it is implemented thoroughly. Aggregation deployment is evident in the authentication process, where all authentication requests are received by the web server, and authentication results are returned to the web server. If an authentication request is successful, this result, as well as rights information for that user account, is returned to the web server. However, administrator accounts for each server are managed on each server.

### Connections Between Web Server and Application Server

Interconnection authentication is performed for the connection between the web server and application server.

Interconnection authentication uses IP address authentication between servers, based on the fact that web servers and application servers are both contained in the business server zone, and that programs are started on the application server by user accounts which have been authenticated by the authentication server. In order to implement aggregation deployment, server interconnection authentication implementation must be taken into consideration.

### Application Servers

User accounts on the application server are limited to application execution users and administrator accounts. Business user accounts are all centrally managed by the authentication server.

### Connections Between Application Server and Database Server

Interconnection authentication is performed for the connection between the application server and database server.

Interconnection authentication uses IP address authentication between servers, based on the fact that application servers and database servers are both contained in secure areas protected by firewalls, and that programs are started on the application server by user accounts which have been properly authenticated by the authentication server.

### Database Server

The only user accounts stored on database servers are the database user accounts used for data manipulation by connected application server programs, and administrator accounts. Data modification is performed by the application server. The database server is configured such that data manipulation cannot be performed.

### Operation Management Server

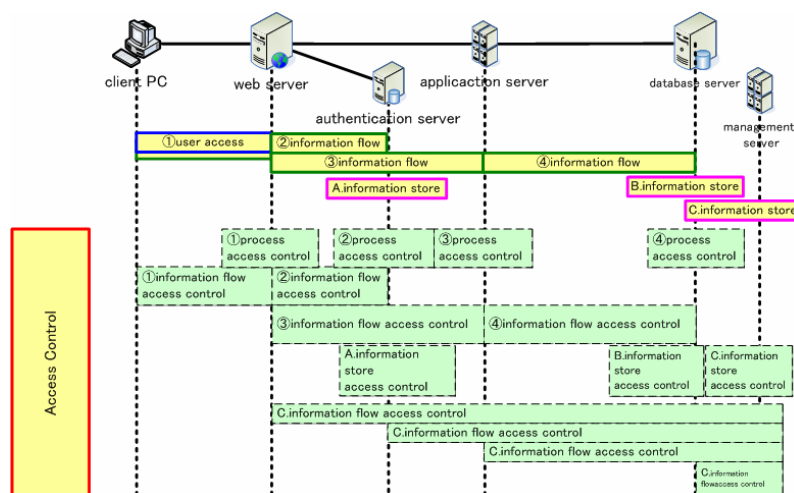
The only user accounts stored on operation management servers are the administrator accounts. All the user accounts used for operation purposes are centrally managed by the authentication server.

### Connections Between Each Server and Operation Management Server

Interconnection authentication uses IP address authentication between servers, based on the fact that individual servers and the operation management server are both contained in secure areas protected by firewalls, and that audit trails are sent by operation management user

accounts which have been properly authenticated by the authentication server.

### 14.3.3. Access Control Function Implementation



**Figure 14-6 Access Control Function Implementation**

#### Client PCs

Because information is not stored locally, file system write access is not strictly controlled.

#### Connections Between Client PCs and Web Server

In order to provide transmission security for client PC transmissions such as login requests and business application results transmission, it is important that transmission only be performed to the intended user. SSL client authentication is used to ensure this, with access from other parties controlled.

#### Web Server

Web server OS level access control uses discretionary access control in order to provide improved operability.

Web server access management objects include programs, business data being processed, logs, and administrator account information.

In order to prevent business application use and unauthorized operations by server administrators, business data modification, business application processing control, and log updating rights have been removed from administrator accounts.

#### Connections Between Web Server and Authentication Server

Transmission route access control is provided by authentication and identity management functions, and as such is not separately implemented.

#### Authentication Server

Authentication server OS level access control uses discretionary access control in order to provide improved operability.

Authentication server access management objects include programs, user account information, and administrator account information.

In order to prevent business application use and unauthorized operations by server administrators, user account information access and log updating rights have been removed from administrator accounts.

#### Connections Between Web Server and Application Server

Because the web server and application server both reside within the same business server zone, interconnection authentication is used between servers, and rights received as a result of authentication performed on the authentication server via the web server are passed on to the web server.

#### Application Server

Application server OS level access control uses discretionary access control in order to provide improved operability.

Application server access management objects include programs, business data being processed, logs, and administrator account information.

In order to prevent business application use and unauthorized operations by server administrators, business data modification, business application processing control, and log updating rights have been removed from administrator accounts.

#### Connections Between Application Server and Database Server

Because the business server zone and confidential server zone are both securely protected behind firewalls, interconnection authentication is used between servers, and rights received as a result of authentication performed on the authentication server via the web server are passed on.

#### Database Server

Database server OS level access control uses discretionary access control in order to provide improved operability.

Database server access management objects include business transaction data, business master data, logs, user account information, and administrator account information.

In order to prevent business application use and unauthorized operations by server

administrators, business data modification and log updating rights have been removed from administrator accounts.

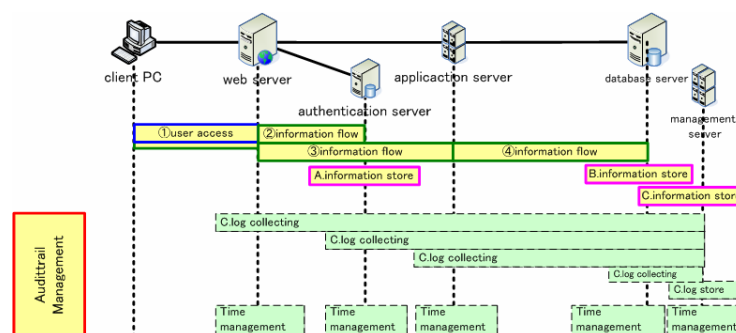
#### Operation Management Server

In order to prevent audit trail tampering, modification and deletion of collected audit trails are disabled for all accounts, including administrators.

#### Connections Between Individual Servers and Operation Management Server

Because all servers reside in secure zones protected by firewalls, interconnection authentication is used between servers, and rights received as a result of authentication performed on the authentication server via the web server are passed on.

#### 14.3.4. Audit Trail Management Function Implementation



**Figure 14-7 Audit Trail Management Function Implementation**

#### Client PCs

Startup logs, login authentication logs, and security auditing logs are collected.

Audit trails for business processing are centrally managed by the operation management server. Because client PCs do not perform business processing, there is no need to take logs.

#### Connections Between Client PCs and Web Server

Because transmission component logs are taken for the respective resources at both ends of the transmission segment, there is no implementation for the interconnection itself.

#### Web Server

The web server performs automatic time synchronization with an NTP server or other Japanese standard time server within the corporate network. The interval between synchronizations is based on average deviation results determined before system operation

begins.

Audit trail entries are made for control status assessment (C type), security incident detection (D type), and security tracking performance (T type) web server events. For details regarding which logs are obtained, please refer to Section 2 "Audit Trail Management".

Collected logs are digitally signed with a private key for server certificates, time-stamped, and transmitted to the operation management server via the log management function.

#### Connections Between Web Server and Authentication Server

Because transmission component logs are taken for the respective resources at both ends of the transmission segment, there is no implementation for the interconnection itself.

#### Authentication Server

The authentication server performs automatic time synchronization with an NTP server or other Japanese standard time server within the corporate network. The interval between synchronizations is based on average deviation results determined before system operation begins.

Audit trail entries are made for control status assessment (C type), security incident detection (D type), and security tracking performance (T type) application server events. For details regarding which logs are obtained, please refer to Section 2 "Audit Trail Management".

Collected logs are digitally signed with a private key for server certificates, time-stamped, and transmitted to the operation management server via the log management function.

#### Connections Between Web Server and Application Server

Because transmission component logs are taken for the respective resources at both ends of the transmission segment, there is no implementation for the interconnection itself.

#### Application Server

The application server performs automatic time synchronization with an NTP server or other Japanese standard time server within the corporate network. The interval between synchronizations is based on average deviation results determined before system operation begins.

Audit trail entries are made for control status assessment (C type), security incident detection (D type), and security tracking performance (T type) application server events. For details regarding which logs are obtained, please refer to Section 2 "Audit Trail Management".

Collected logs are digitally signed with a private key for server certificates, time-stamped, and transmitted to the operation management server via the log management function.





#### Connections Between Client PCs and Web Server

There are no centralized management related implementation points for the transmission component between client PCs and the web server.

#### Web Server

Vulnerability management is performed. Security patches are applied promptly in order to keep the server current.

The security patch application status is sent to the operation management server via the configuration management function.

#### Connections Between Web Server and Authentication Server

There are no centralized management related implementation points for the transmission component between the web server and authentication server.

#### Authentication Server

Vulnerability management is performed. Security patches are applied promptly in order to keep the server current.

The security patch application status is sent to the operation management server via the configuration management function.

#### Connections Between Web Server and Application Server

There are no centralized management related implementation points for the transmission component between the web server and application server.

#### Application Server

Vulnerability management is performed. Security patches are applied promptly in order to keep the server current.

The security patch application status is sent to the operation management server via the configuration management function.

#### Connections Between Application Server and Database Server

There are no centralized management related implementation points for the transmission component between the application server and database server.

#### Database Server

Vulnerability management is performed. Security patches are applied promptly in order to keep the server current.

The security patch application status is sent to the operation management server via the configuration management function.

#### Operation Management Server

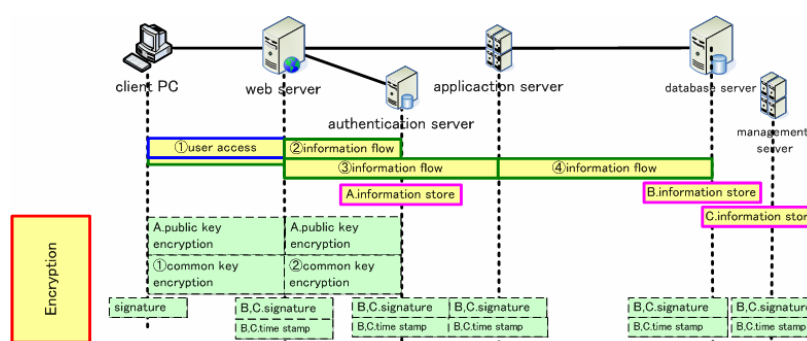
Vulnerability management is performed. Security patches are applied promptly in order to keep the server current.

The security patch application status is managed via the configuration management function.

#### Connections Between Individual Servers and Operation Management Server

There are no centralized management related implementation points for the transmission component between individual servers and the operation management server.

#### 14.3.6. Encryption Function Implementation



**Figure 14-9 Encryption Function Implementation**

#### Client PCs

Because client PCs do not store business data, encryption is not performed by individual client PCs. There is no need for hard disk encryption either. However, signatures are used because SSL client authentication is performed.

#### Connections Between Client PCs and Web Server

Encrypted transmission is performed using SSL client authentication in order to maintain the confidentiality of items entered onscreen and information obtained from the web system. When factoring in internal corporate access, transmission path encryption via SSL-VPN is used.

#### Web Server

In order to provide legal admissibility to audit trails sent to the operation management server, they are digitally signed and time stamped.

#### Connections Between Web Server and Authentication Server

Authentication information obtained by authentication requests issued by the client PC are sent to the authentication server. Encrypted transmission using LDAPS is performed when transmitting or receiving data.

#### Authentication Server

All user account information is encrypted.

In order to provide legal admissibility to audit trails sent to the operation management server, they are digitally signed and time stamped.

#### Connections Between Web Server and Application Server

Because the web server and application server reside within the business server zone, there is no danger of information leakage due to snooping, and thus encryption is not performed.

#### Application Server

In order to provide legal admissibility to audit trails sent to the operation management server, they are digitally signed and time stamped.

#### Connections Between Application Server and Database Server

Because the application server and database server are both secured by firewalls, and requests to the database server can only be performed by application server application users, encryption is not performed.

#### Database Server

The database server (including disks) resides within the confidential zone, so data encryption is not performed. However, in order to provide legal admissibility to audit trails sent to the operation management server, they are digitally signed and time stamped.

#### Operation Management Server

In order to provide legal admissibility to audit trails sent to the operation management server, they are digitally signed and time stamped.

#### Connections Between Individual Servers and Operation Management Server

The operation management server resides in the business server zone, so transmission paths are not encrypted.

We have described above the implementation of security functions based on the ESA

approach for the three-layer web system model.

It has traditionally been considered difficult determining what security functions to implement. This chapter has explained the concept of "aggregation deployment", and used the three-layer web system model to illustrate the actual implementation of these security functions, as well as important points to consider when doing so. Systems which perfectly match this system model can use the examples above as-is, but most systems will require customization and function expansion, or even feature system design that is completely different than the three-layer web model. However, regardless of the actual system structure, the approach to security policy compliant aggregation deployment explained with this model is a common fundamental aspect of security implementation.

In the future, we plan to develop ESA based models for a variety of system designs.

## 15. System Operation

### 15.1. System Operation Overview

When considering information security measures for an organization, in addition to the technical perspective described previously, it is also important to consider the management perspective. In order for information security management to effectively operate and maintain an IT system with security functionality, it must also indicate and manage the actions of the personnel and organizations involved.

Below are some frameworks which can serve as references when designing information security management. Please refer to Section 4 Chapter 16 "Representative Frameworks" for details regarding these frameworks.

Specifications regarding quality assurance requirements

- ISO 9000 Series<sup>22</sup>

Information security management standards, specific management measures, and practical standards

- ISO/IEC 27001<sup>23</sup>
- ISO/IEC 17799<sup>24</sup>, ISO/IEC 27002<sup>25</sup>
- JIS Q 27001<sup>26</sup>, JIS Q 27002<sup>27</sup>
- Information security management standards<sup>28</sup>, etc.

Specifications regarding personal information protection requirements

- JIS Q 15001<sup>29</sup>

Practical standards for overall IT control (IT governance)

- COBIT (Control Objectives for Information and related Technology)<sup>30</sup>
- System management standards and supplements<sup>31</sup>, etc.

<sup>22</sup> ISO 9001:2000 Quality management systems -- Requirements, etc.

<sup>23</sup> ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements

<sup>24</sup> ISO/IEC 17799:2005 Information technology -- Security techniques -- Code of practice for information security management  
<sup>25</sup> Scheduled for integration in ISO/IEC27000 series as ISO/IEC27002, based on ISO/IEC 17799:2005

<sup>26</sup> JIS Q27001 Information Technology - Security Technology - Information Security Management System - Requirements

<sup>27</sup> JIS Q27002 Information Technology - Security Technology - Code of Practice for Information Security Management

<sup>28</sup> Ministry of Economy, Trade and Industry - Information Security Management Guidelines

[http://www.meti.go.jp/policy/netsecurity/law\\_guidelines.htm](http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm)

<sup>29</sup> JIS Q15001 Personal Information Protection Management Systems - Requirements

<sup>30</sup> Please refer to the ISACA Information Systems Audit and Control Association Tokyo branch site

[http://www.isaca.gr.jp/homepage\\_j.htm](http://www.isaca.gr.jp/homepage_j.htm)

<sup>31</sup> Ministry of Economy, Trade and Industry "System Auditing Standards" and "System Management Standards - Supplement (IT Control Guidance for Financial Reporting) (Proposal)"

These frameworks describe their management items and management measures. However, they do not concretely address how to implement management measures in actual IT systems, how to implement their management items, how to operate management measures which have been implemented, or how to tie these to IT system information security management improvements. This chapter concerns the operation of IT systems which have implemented the management measures described in previous chapters.

## 15.2. Objectives of This Chapter

### 15.2.1. System Operation Issues

When implementing information security management, organizations may be faced with the problem of there being no management frameworks such as system operation advancement structures or approaches, or the actual contents of system operation required for the system being unclear. To help solve these problems, this chapter presents system operation frameworks and procedures from an IT service perspective, and operation procedures from a process perspective.

### 15.2.2. Benefits of This Chapter

This chapter presents requirements for effective IT system operation and maintenance from the twin perspectives of "business" and "IT service". This makes it possible to cover the IT system security functions and items necessary for system operation. This chapter also organizes information security processes, enabling requirement support for IT systems.

## 15.3. Overview of System Operation Process

### 15.3.1. Information Security from a Business Perspective

In order to think about how to operate the management measures in an IT system, IT system information security measures must be considered from a business perspective and matching operation perspective. It is also important to evaluate how information security has contributed to information security.

Individual organizations have their own objectives, and business processes exist in order to accomplish these objectives. Recently, business needs have relied increasingly on IT systems. With this has come an increase in the complexity of IT system information security demands.

It is important to remember that information security measures are not a goal, but a means for an organization to achieve its objectives. Information security can not be an impediment to an organization or its business profitability. In general, not all information and IT systems have the same value for an organization. Therefore, "the stricter, the better" is not necessarily true. Information security levels and severity must match the value of the

information and IT systems to which they apply. By balancing information security measures and their resulting costs, as well as balancing the value of information with the risk posed to the environment which handles it, an organization can start to implement appropriate information security measures and management.

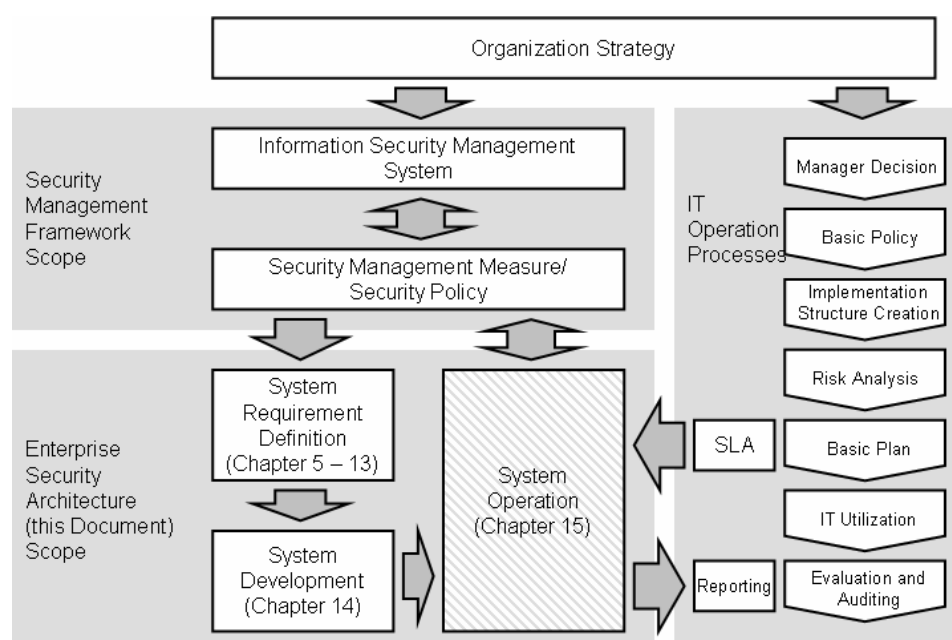
For some IT systems, implementing information security measures may serve as an important added value. By implementing appropriate information security measures and a quality and efficiency workflow, many business processes can be made to operate more reliably. This is an extremely valuable outcome. It is important to evaluate how the value created by information security measures has contributed to the business.

### 15.3.2. Position of System Operation

Actual system operation is based on an information security perspective derived from a business point of view. This chapter organizes the following in order to support the establishment of an ESA based system operation framework.

- Operations necessary for ESA "Control", "Plan", "Service Implementation and Provision", "Monitoring / Measurement and Evaluation", "Maintenance and Improvement", and "Reporting" processes.
- The relationship between the requirements of the operations necessary for each process and security function elements.

The role of this chapter is shown in Figure 15-1.



**Figure 15-1 Position of This Chapter**



### 15.3.3. System Operation Framework

This chapter treats information security processes provided by IT systems and their operations as part of a series of components which support business processes.

For example, ITIL<sup>32</sup>, a structural guideline concerning IT system operation and management operation, treats this series of components as "IT services", and, in order to connect them with business strategies, provides best practices via the process approach.

This chapter takes the processes described in ITIL's "security management" library into consideration in explaining the system operation framework<sup>33</sup> demanded by the ESA from an IT service perspective.

Security function requirements may vary based on the scale of an organization, the type of business it conducts, its atmosphere, and management system implementation status. In order to use this chapter effectively for IT systems and equipment based on these requirements, it is important to optimize the system operation framework described below to fit one's own organization and operation structure.

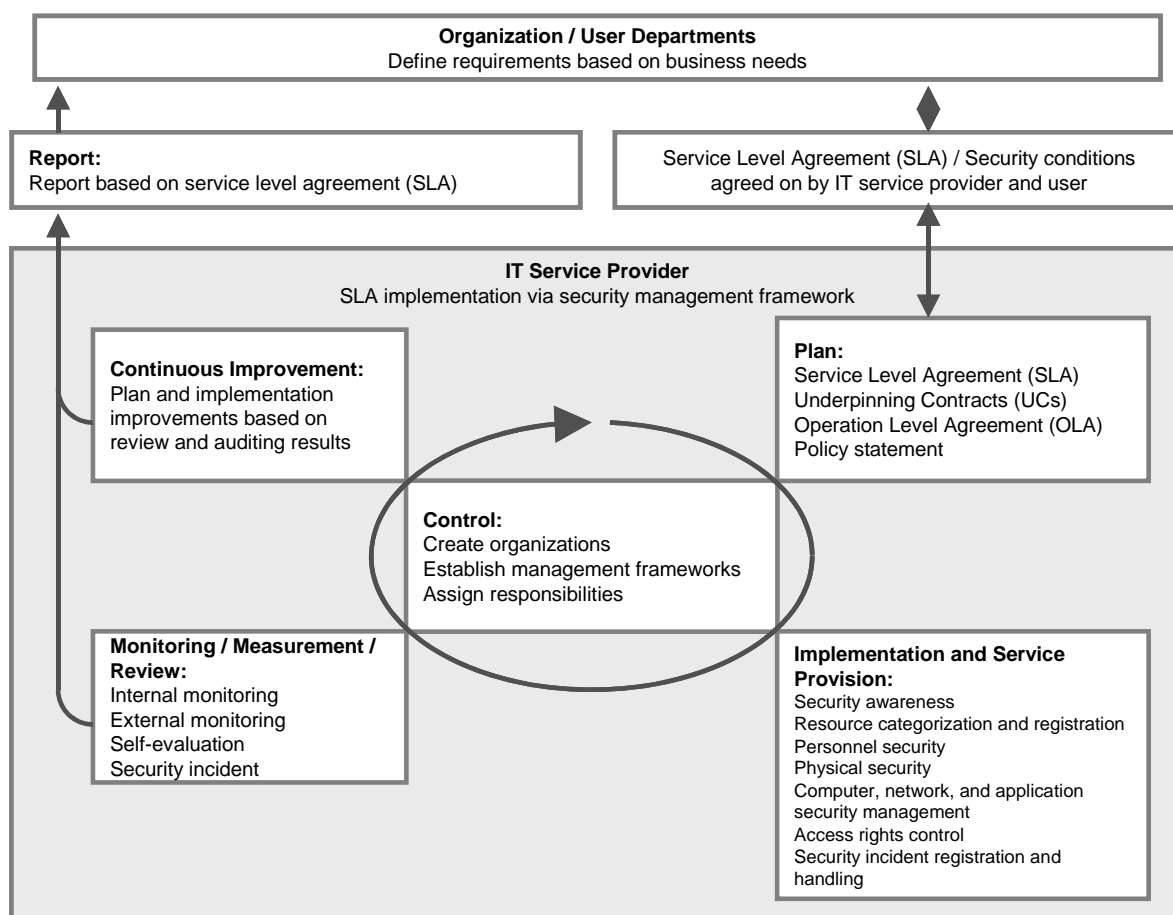
---

<sup>32</sup> For details regarding the IT Infrastructure Library, please refer to the ItSMF Japan site <http://www.itsmf-japan.org/itil/index.htm>.

<sup>33</sup> Framework: In this chapter, "framework" refers to the process structure and process relationships which can be applied generally to systems.

## 15.4. Overall Picture of System Operation Processes

Figure 15-2 shows overall processes for information security management from an information security measure perspective.



**Figure 15-2 Overall View of Security Management Process<sup>34</sup>**

First, we will define the relationship between IT service providers and service users. IT service providers can be IT service departments within one organization, or an outsourced external IT service provider. However, the differences between the two are minimal. Creating a Service Level Agreement (SLA)<sup>35</sup>, agreed on by both the internal IT service department and users departments, codifying service levels, can be effective for clarifying responsibilities. For the IT service provider, business condition based fundamental information security policies and risk analysis are the responsibility of the department using their services.

<sup>34</sup> Source: ITIL Security Management

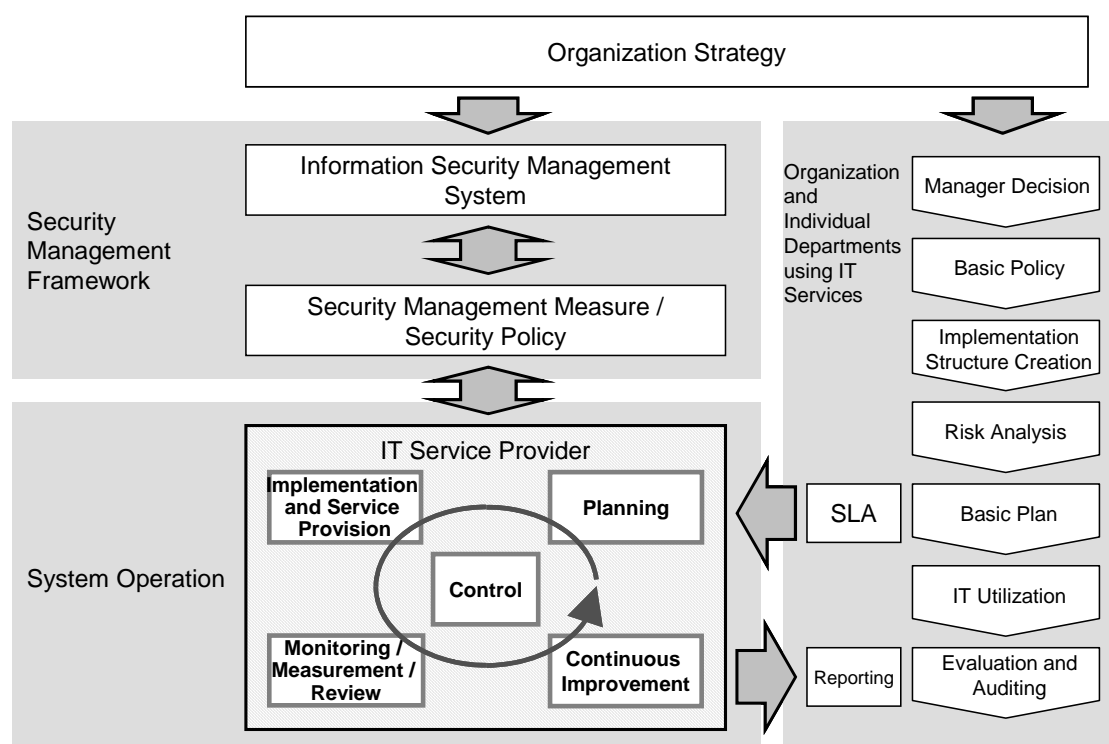
<sup>35</sup> A formal agreement supplied to the department using a service quantitatively defining the services provided. These quantitative definitions must be used in the establishment of metrics such as acceptable service thresholds, service provider objective values, and target values beyond those objectives.

The IT service provider can then implement planning processes based on the security requirements resulting from the fundamental information security policies and risk analysis results provided by the department that will be using the service.

Organizational and service user departmental processes are also important for information security management in IT environments. First, we will touch on processes related to organizations and departments using IT services. Next, we will provide an overview of information security management processes related to IT service providers.

#### 15.4.1. Processes Related to Organizations and Departments using IT Services

The diagram below shows a model of the processes related to organizations and departments using IT services.



**Figure 15-3 Information Security Management Model from a Business Perspective**

The main processes for organizations and departments using IT services are "manager selection", "fundamental organizational policy establishment", "promotion structure development", "risk analysis", "fundamental information security planning", "IT usage", and "evaluation and auditing".

Managers must be involved in information security. Information security requires investment both in organizations and in infrastructure, so proactive involvement by a manager serves as the actual launching point for information security management design. From here, the

fundamental information security policy, including promotion structures, responsibilities, and applied scopes, is decided. This fundamental information security policies clarify responsibilities, obligations, and rights. Based on the fundamental information security policy, a promotion structure is established.

The fundamental information security policy broadly describes "what" is protected "how", and "how much". It should contain the following specific information.

- A comprehensive guide to information security (overall awareness)
- A framework for establishing goals or indexes for the evaluation of activities
- Rules governing information security related activities
- Representative organization directives, regulations, and contracts
- Organizational structure for establishing and maintaining information security management
- Risk analysis guidelines (which assets and requirements to prioritize, etc.)

Information security environments can be affected by internal and external changes. Internal changes are those resulting from organizational decisions. External changes are those caused by the business process environment. These form issues which must be dealt with by information security management.

Environmental changes which require process adaptation include the following.

- Changes in actual business contents or business importance
- Physical changes (such as changing physical locations, etc.)
- Environmental changes
- IT usage related assessment changes
- Business domain changes
- Legal domain changes
- Hardware and software changes
- Legal requirement changes
- Threat changes
- New technology deployment

"Risk analysis" takes the business environment changes above into account when identifying risks to information security. This risk analysis not only clarifies the status and quality of current information security, but also clarifies what information security measures should be taken. That is, it presents the way things are, and the way they should be. There are a number of general methods for performing risk analysis. One example is described in Section 4, Chapter 17 "Risk Analysis Methodology (Example)".

The results of the risk analysis are used in creating a fundamental plan for changing the current state of information security to its ideal state. A service level agreement (SLA) based on this is then created in coordination with the IT service department.

In the "evaluation and auditing" process, the organization or departments using IT services review whether the information security measures that have been implemented are effective and functioning efficiently. Based on the results of this review, the "planning" and "implementation and service provision" processes are reviewed and reconsidered. The evaluation and auditing review results are also used in conjunction with the "auditing" process results obtained by the organization or departments using IT services in order to produce regular security improvement plans and to revise the service level agreement (SLA).

Evaluating the effectiveness and efficiency of information security measures is an especially important organizational and department responsibility, and establishing measurement standards (metrics) for this evaluation is an effective means to do so. When establishing these metrics, referring to COBIT, etc., can be effective.

#### 15.4.2. Information Security from an IT Service Perspective

The main processes in which IT service providers are involved are "control", "planning", "implementation and service provision", "monitoring, measurement and review", "continuous improvement", and "reporting". In this chapter, these processes have been broken down into smaller elements referred to as subprocesses. Requirements can be identified by looking at the actual operations involved in these subprocesses.

In the ITIL framework, the promotion structures and managers for each process are decided as part of the "control" process, based mainly on the fundamental information security policies and fundamental information security plans of the organization and departments using IT services.

**Table 15-1 "Control" Process Overview**

Item	Subprocess	Subprocess Contents
(1)	Information Security Organizational Structure	<input type="checkbox"/> Establishment and operation of information security committee <input type="checkbox"/> Establishment of information security promotion framework <input type="checkbox"/> Assignment of responsibilities <input type="checkbox"/> IT system related authorization process <input type="checkbox"/> Specialist support structure <input type="checkbox"/> Independent checking <input type="checkbox"/> Support for access by external users <input type="checkbox"/> External service contract

In the ITIL framework, operational level agreements (OLA)<sup>36</sup> and underpinning contracts (UC)<sup>37</sup> based on IT service provider policy statements, information security implementation plans, and service level agreements (SLA) are decided as part of the "plan" process.

**Table 15-2 "Planning" Process Overview**

Item	Subprocess	Subprocess Contents
(1)	Policy Statement	<input type="checkbox"/> Creation of IT service department policy statement
(2)	OLA	<input type="checkbox"/> OLA (Operation Level Agreement) definition and agreement
(3)	UC	<input type="checkbox"/> UC (Underpinning Contract) definition and agreement
(4)	Security Implementation Plan	<input type="checkbox"/> Profile definition <input type="checkbox"/> Security implementation plan creation

In the same way, the following, based on the information security implementation plan, are performed as part of the "implementation and service provision" process.

- Information categorization and allotment
- Implementation of security functions in IT system
- IT system operation management
- Education
- Security incident handling
- Regular monitoring

**Table 15-3 "Implementation and Service Provision" Process Overview**

Item	Subprocess	Subprocess Contents
(1)	Asset Categorization and Control	<input type="checkbox"/> Asset management responsibility <input type="checkbox"/> Asset categorization <input type="checkbox"/> Category guidelines
(2)	Human Resource Security	<input type="checkbox"/> Job description (JD) <sup>38</sup> <input type="checkbox"/> Selection <input type="checkbox"/> Confidentiality agreement <input type="checkbox"/> Education and training for all members <input type="checkbox"/> Security incident handling <input type="checkbox"/> Reporting of information security indicators and vulnerabilities <input type="checkbox"/> Disciplinary proceedings <input type="checkbox"/> Information security awareness improvement

<sup>36</sup> Operational Level Agreement (OLA): IT service provider internal document. Defines relationships between different fields within the organization. (From itSMF IT Service Management Glossary)

<sup>37</sup> Underpinning Contract (UC): Contract with external suppliers providing products and services which assist in provision of IT service to departments utilizing those IT services. (From itSMF IT Service Management Glossary)

<sup>38</sup> Job Description (JD): Document containing job contents agreed upon by all parties. (From itSMF IT Service Management Glossary)

(3)	Transmission and Operation Management	<input type="checkbox"/> Operation procedures and management responsibility <input type="checkbox"/> Operation procedure documentation <input type="checkbox"/> Security incident management procedures <input type="checkbox"/> Separation of roles and duties <input type="checkbox"/> Separation of development and operation environment <input type="checkbox"/> Outsourcing service management <input type="checkbox"/> Information handling and transfer <input type="checkbox"/> Network management <input type="checkbox"/> Network requirements
(4)	Access Control	<input type="checkbox"/> Access control maintenance and management <input type="checkbox"/> Responsibilities of departments using IT services <input type="checkbox"/> Network access control <input type="checkbox"/> Computer access control <input type="checkbox"/> Application access control <input type="checkbox"/> Control policy for antivirus measures <input type="checkbox"/> Monitoring and auditing of IT system access and usage

Internal auditing, external auditing, self-evaluation, and evaluation report creation are part of the "monitoring, measurement and review" process.

**Table 15-4 "Monitoring, Measurement and Review" Process Overview**

Item	Subprocess	Subprocess Contents
(1)	Evaluation	<input type="checkbox"/> Proper IT system usage <input type="checkbox"/> Confirmation of security policy and standard conformance <input type="checkbox"/> Confirmation of legal and regulatory item conformance <input type="checkbox"/> Confirmation of compliance with technical requirements <input type="checkbox"/> IT system auditing <input type="checkbox"/> Auditing tool protection

The "continuous improvement" process includes analysis of the evaluation report produced in the "monitoring, measurement and review" process, creation and implementation of security improvement plans, and reviewing of service level agreements (SLA).

**Table 15-5 "Continuous Improvement" Process Overview**

Item	Subprocess	Subprocess Contents
(1)	Evaluation Analysis, Planning and Improvement Activities, Input into SLA Revision	<input type="checkbox"/> Evaluation report analysis <input type="checkbox"/> Security improvement plan creation and implementation <input type="checkbox"/> Input into SLA revision

The "reporting" process consists of reporting to organizations and specific departments using

IT services. This includes implementation plans, regular implementation status reporting, monitoring reports, and reporting of special events.

**Table 15-6 "Reporting" Process Overview**

Item	Subprocess	Subprocess Contents
(1)	Reporting	<input type="checkbox"/> "Planning" related reporting <input type="checkbox"/> "Implementation" related reporting and regular reporting <input type="checkbox"/> "Evaluation" related reporting, and other reporting <input type="checkbox"/> Other events requiring special reporting

### 15.5. Concrete Subprocess Examples

We will now look at specific, concrete activities which make up these subprocesses. When designing operation structures, we recommend breaking them down as below in accordance with the subprocesses described above.

For example, one method is breaking down subprocesses into actual operation activities by comparing best practices such as ISO/IEC27002 and ITIL. This method is referred to as the base-line approach. The "Fujitsu Standard Security Policy 2007" supplement can also be used as a standard.

Here, we will provide an example of "computer access control" based on ITIL best practices.

#### 15.5.1. Computer Access Control

##### [Objectives]

- Prevent unauthorized access to information or IT systems in order to maintain information confidentiality.
- Prevent changes to information or IT systems before authorization has taken place.
- Protect information and IT systems from damage or destruction via unauthorized access.
- Prevent confusion within the standard operating environment.

##### [Specific Activities]

- Perform identification and authentication for all work stations and terminals.
- Enforce use of a standard login procedure which provides minimal information (for example, do not provide system types or organization name details).
- Always perform identification and authentication of users. For auditing purposes, processes performed by IT systems must be tie-able to actual personnel. Identification can be performed using passwords, smart cards, or authentication devices (hardware tokens).
- Forced alarm: For important IT assets, consider the implementation of a forced alarm. This would be useful in clarifying if an authorized user was performing an operation



because it was unavoidable.

- Automatic timeout: Use an automatic timeout function, which would automatically disconnect sessions and log users off of workstations if more than the specified period of time passed without any operations being performed.
- Usage period limitation: Limit the time that the IT system can be used to standard usage hours (for example, from 08:00 to 19:00).
- Perform access lockouts when more than a specified number of access attempts have failed.
- Perform strict login checking for users connecting externally, using methods such as authentication devices (hardware tokens), smart cards, challenge/response logins, etc.
- Use two element authentication when it is important to prevent impersonation and when accurate identification is essential.
- When physically providing authentication devices (hardware tokens) to personnel, always perform proper personnel identification first. If this is not performed, and authentication devices are provided to unauthorized parties, severe vulnerabilities will result.
- Choose the correct authentication method based on the degree of required confidentiality of the data being protected or the business being performed.
- Especially in the case of large scale organizations, establish automatic ID revocation procedures for when data or business utilization rights have been lost through retirement / quitting.
- Accounts which have not logged in for a long period of time must be frozen or deleted.
- Login and logout dates and times must be taken by authentication systems (or SSO systems) as part of audit trails.
- When using basic authentication, enforce the following password policy. This can be done through use of password policy management functions.
- 8 character or longer passwords
- Prohibit passwords containing only characters or numbers, or passwords consisting of repeated strings or simple sequences (require one or more special characters)
- Prohibit passwords which are identical with IDs, or which can be easily guessed based on the user
- Enforce regular password changes. Establish and automate a process for prohibiting use of the same password in successive generations.

By organizing the IT assets related to these subprocesses, as well as security functions and requirements, in the following table, we can see more clearly which items need to be considered for which activities.

## [Related IT Resources]

For example, for computer access control related IT assets, we have personnel, applications, and technology.

IT Resource	
✓	Personnel
✓	Applications
✓	Technology
	Facilities
	Data

✓ Applicable

## [Related Functions]

In the same way, "authentication and IDM" and "access control" are important related security functions. "Audit trail management" and "centralized management" supplement access control.

Security Function	
P	Authentication and IDM
P	Access control
S	Audit trail management
S	Centralized management
	Encryption
	Physical security

(P:) Primary, (S:) Secondary

## [Related Requirements]

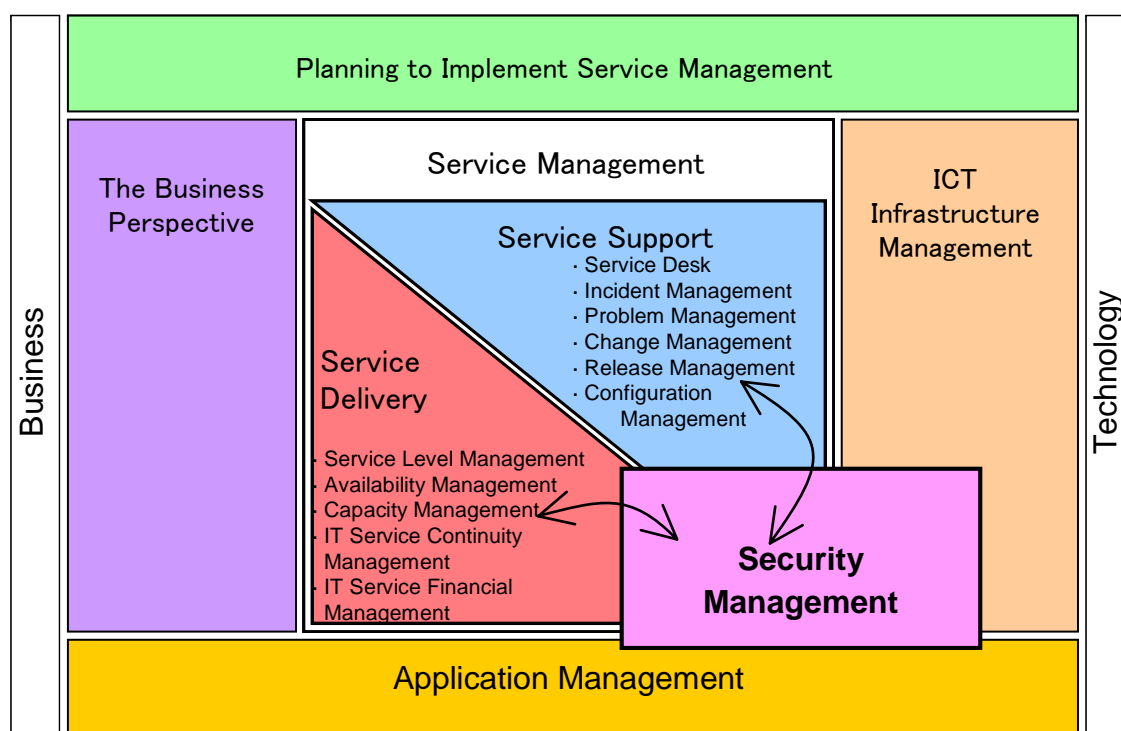
The main requirements for computer access control are confidentiality and integrity. Operation must take these requirements into consideration.

Security Requirements	
P	Confidentiality
P	Integrity
	Availability

(P:) Primary, (S:) Secondary

## 15.6. Relationship between IT Service and Other Processes

The relationship between the processes described in section 14.3.2 and the other processes necessary for IT service provision is important. This indicates that security must be considered for all processes involved in IT service provision. We will use the processes provided by ITIL, and the points regarding them which must be considered, as examples. The "centralized management" functions described in chapter 10 can be used for effective operation which factors in these points.



**Figure 15-4 ITIL Library Structure Plan (Position of Security Management)<sup>39</sup>**

Figure 15-4 shows the ITIL library structure and the position of security management within it. Security management is most closely related to the following service delivery and service support processes.

<sup>39</sup> Source: "IT Service Management", published by ItSMF Japan

Service Support	Incident management Problem management Change management Release management Configuration management
Service Delivery	Service level management Availability management Capacity management IT service continuity management

We will explain below how each of these processes are related to security management, as well as the contents of each process.

#### 15.6.1. Incident Management

Because security incidents frequently involve different procedures than standard incidents, it is essential that both can be identified and categorized. Incidents which may obstruct the satisfaction of SLA defined security requirements are categorized as security incidents. As such, incidents which are considered security incidents should be clearly defined within the SLA.

Security incidents tend to be urgent and have a great amount of impact, and the incidents themselves require confidentiality considerations, so it is important that contact procedures (such as organization internal level escalation procedures, et al) and incident entry contents be decided in advance, and the members of the organization made thoroughly aware of them. Security incident entry items may include the following.

- Incident number, incident submission date and time
- Incident occurrence date and time
- Detailed information regarding the person reporting the incident (including for which cases the reporter can be anonymous)
- Incident name
- Detailed incident contents
- Impact (including estimated losses)
- Urgency
- Department where incident occurred, and where it was detected
- Scope of incident effects (system, equipment, facility, etc.)
- Contact information for person reporting the incident
- Escalation status
- Resolution measures

When considering security incidents, the "Security Violation Detection (Type D)" audit trails described in chapter 9 "Audit Trail Management" are important. Information security incident management determines how these audit trails are handled.

### 15.6.2. Problem Management

The primary objective of problem management is the determination of the root cause of problems. If a security incident is recognized as a problem, it is important to begin problem resolution actions. It is important to narrow down the number of related parties, as security problem occurrence itself may be a strong blow to the organization.

It is also importantly to constantly check to ensure that problem and known error resolution measures and work-arounds<sup>40</sup> do not cause new security problems. When considering information security related problems, the "Control Status Assessment (Type C)" audit trails described in chapter 9 "Audit Trail Management" are important. "Security Tracking (Type T)" audit trail examination may also be required. Information security problem management determines how these audit trails are handled.

### 15.6.3. Change Management

Change management must take into consideration the security involved in daily operation. This is because normal changes can result in security related problems. As such, change advisory boards (CABs)<sup>41</sup> must include security managers and security managers from the departments using the IT services.

When changes involving security measures are planned, in addition to standard functionality tests, additional testing from a different perspective is needed. Normal functionality testing checks whether the function in question can be used as planned, but when testing a change involving security measures, in addition to checking the availability of the security functionality, one must also check whether there are functions which decrease the level of security offered.

### 15.6.4. Release Management

Release management controls the deployment of new software, hardware, and data transmission equipment versions. This process guarantees the following.

- The correct hardware and software are used.
- Hardware and software is tested before use.
- Deployment is properly authorized by change.

<sup>40</sup> Work-around: Incident and problem avoidance via temporary measures which allows customers to avoid negative effects of configuration items (CIs) (From itSMF IT Service Management Glossary)

<sup>41</sup> Change Advisory Board: Group which provides advice regarding change management (CM) regarding prioritization of group requests for change (RFCs) made by representatives who have the authority to perform business and technology based evaluations, as well as producing proposals for resource allocation necessary for change implementation, for all RFCs with large impacts. (From itSMF IT Service Management Glossary)

- Software used is legal.
- Software is virus-free, and is not infected when distributed.
- Software version numbers are known and entered in the configuration management database (CMDB)<sup>42</sup> by configuration management.
- Deployment is managed effectively.

It is important during testing and acceptance that security, based on SLA defined security requirements and measures, be considered.

#### 15.6.5. Configuration Management

Configuration management includes the ability to categorize configuration items (CIs)<sup>43</sup>, making it the process most closely connected with information security. CI categorization indicates necessary confidentiality, integrity, and availability. These categories are based on SLA security requirements, and categorization is performed by the department which uses the IT services. The SLA can define the security measures for each individual categorization level.

Categorization schemas should always be created in agreement with the structure of the department which uses IT services. However, in order to simplify management, when there are multiple departments which use the same IT system, a common categorization schema is recommended.

#### 15.6.6. Service Level Management

The primary objective of service level management is optimization of services in accordance with the SLA. Service level management includes a large number of security related activities, and security management has an important role in service level management. The primary activities in service level management are listed below.

1. Identification of security needs for departments using IT services. Because security needs are based on business profitability considerations, the determination of these security needs is the responsibility of the department using IT services.
2. Confirmation of the feasibility of the department's security requirements.
3. Proposals, deliberations, and definitions regarding SLA IT service security levels.
4. Identification, deliberations, and definitions regarding internal security requirements contained in the IT service OLA.

<sup>42</sup> Configuration Management Database: Database containing details regarding the attributes and history of each configuration item (CI), as well as details regarding important relationships between CIs. (From itSMF IT Service Management Glossary)

<sup>43</sup> Configuration Item: An IT infrastructure component. This also includes documents such as SLAs and RFCs. (From itSMF IT Service Management Glossary)

5. Monitoring of security evaluation metrics contained in the OLA.
6. Reporting regarding IT services provided.

For 1 to 3 above, security management processes form the basis for service level management. They also support service level management processes. 4 and 5 above are implemented as security management processes. Security management and other processes form the basis for 6 above. Service level managers and security level managers discuss and decide who actually performs which activities.

SLA definitions are normally based on general base level<sup>44</sup> security measures, but if the departments using IT services have additional security requirements, these must be clearly defined within the SLA as well.

#### 15.6.7. Availability Management

Availability management addresses the technical availability of elements which form the IT system. Availability quality is provided by reliability, including resilience to outages, maintainability, and serviceability. The availability management process is the process most directly related to security management. Most security measures provide confidentiality, integrity, and availability benefits, so availability management, and the IT service continuity management which will be discussed later, must function in concert with security management.

#### 15.6.8. Capacity Management

The primary objective of capacity management is the maximal utilization of IT system resources in alignment with the agreements made by the department using IT services in the SLA. IT system performance requirements are based on SLA defined quantitative and qualitative evaluation standards. Almost all aspects of capacity management affect availability, as well as security management.

#### 15.6.9. IT Service Continuity Management

The primary objective of IT service continuity management is the minimization of the impact of emergency situations to the level agreed upon by the department using the IT service. Not all emergency situations are necessarily disasters. The primary activities involved in IT service continuity management are the design and implementation of emergency situation plans and preventative measures. From a security perspective, IT service continuity management is tied to security management.

---

<sup>44</sup> This is usually referred to as a "baseline".

## 15.7. Summary

As this chapter has described, in order to operate and maintain an IT system with security functionality effectively, one must consider IT operation processes from a business perspective, and system operation processes from an IT service perspective.

There are some IT operation processes which should be implemented from the business perspective of organizations and departments using IT services, including managers. By tying together concrete security functions and required operation contents based on ITIL or other "IT Service" processes, system operation from an IT service perspective can cover, for example, the IT system security functions and system operation requirements that make up part of the management measures described in ISO27001. By organizing the relationships between information security processes and other IT service processes, support can be provided for the requirements of internal control, IT governance realization, and overall corporate information system optimization.

### [Reference Materials]

- ITILR Security Management

- "IT Service Management - Introduction to ITIL" itSMF

- "IT Service Management Glossary" itSMF



## Section 4 Appendices

## 16. Representative Frameworks

**Table 16-1 Representative Frameworks**

Name	Established by	Scope
ISO/IEC 27001	ISO/IEC	Requirements for information security management
JIS Q 2700 1	JISC	
Information Security Management Standard	Ministry of Economy, Trade and Industry	
ISO/IEC 17799:2005	ISO/IEC	Specific management measures and implementation standards for information security management
JIS Q 27002	JISC	
JIS Q 15001	JISC	Requirements for personal information protection
ISO/IEC 20000:2005	ISO/IEC	Requirements for IT service management
ITIL (IT Infrastructure Library)	British Office of Government Commerce	Specific implementation standards for IT service management
COBIT (4th Edition)	IT Governance Institute	Implementation standards for overall IT governance
System Management Standards and Supplement	Ministry of Economy, Trade and Industry	

### 16.1. ISO/IEC 27001, JIS Q 27001

ISO/IEC27001 is an international information security management system standard based on the British Standard BS7799-2. It covers information security requirements, with the objectives of maintaining and improving information security via management cycles such as risk analysis based management plan establishment and objective monitoring and reviewing of resource allocation and operation. This is standardized in Japan under the JIS Q27001 standard.

### 16.2. ISO/IEC 17799 (JIS Q 27002)

The ISO/IEC 17799 (JIS Q 27002) standard refers to the ISO/IEC 27001 (JIS Q 27001) standard, providing specific management measures and implementation standards for information security management.

### 16.3. Information Security Management Standard

This recursively summarizes the optimal implementation practices for information asset protection, based on ISO/IEC17799:2000 (currently ISO/IEC 17799:2005), and specifies information security related management and control items.

### 16.4. JIS Q 15001

This is a management system standard for personal information protection. It was revised in May, 2006 as JIS Q 15001:2006 "Personal Information Protection Management Systems", with an even deeper connection with the Private Information Protection Law. This standard includes all personal private information, regardless of how it is obtained, or whether it pertains to customers or employees. It is based on PDCA, and the privacy mark system is based on this standard.

### 16.5. ITIL (IT Infrastructure Library)

This is a framework composed of best practices related to IT service management. It contains a collection of actual IT operation knowledge and know-how, and is recognized as the de facto standard in Europe and North America.

ITIL is composed of the following seven documents.

- Service Delivery
- Service Support
- Security Management
- The Business Perspective
- ICT Infrastructure Management
- Applications Management
- Planning to Implement Service Management

The core of ITIL, the IT service management framework, is composed of the service delivery and service support documents above. Service delivery is composed of five processes for mid-term planning and improvement: "service level management", "availability management", "capacity management", "IT service continuity management", and "IT service financial management". Service support is composed of five processes focused on daily IT service operation and support: "incident management", "problem management", "change management", "release management", and "configuration management", as well as one function, the "service desk".

### 16.6. ISO/IEC20000:2005

This is an international standard based on the British BS15000 standard, based in turn on ITIL. It contains framework and evaluation standards for effective and efficient management of IT services by an organization. Management systems based on this standard can be used for

internal IT department deployment as well as external IT service provisioning deployment.

### 16.7. COBIT (Control Objectives for Information and related Technology)

This is a set of IT governance implementation specifications proposed by the Information Systems Audit and Control Association (ISACA) for use as organizational IT governance objectives. It divides the business processes of IT strategy development, system development, operation, and maintenance into 4 domains and 34 processes: "Planning and Organization (PO): 10 processes", "Acquisition and Implementation (AI): 7 processes", "Delivery and Support (DS): 13 processes", and "Monitoring and Evaluation (ME): 4 processes", and defines detailed IT control objectives for each process.

### 16.8. System Management Standard and Supplement

This, like COBIT above, is a standard for IT governance implementation specifications, created by the Ministry of Economy, Trade and Industry. It is composed of 5 categories and 287 items: "Information Strategy: 47 items", "Planning: 23 items", "Development: 49 items", "Operation: 73 items", and "Common Functions: 76 items". The supplement describes IT control concepts, manager evaluations, implementation guidance, and the like, for a variety of common hypothetical cases, with a focus on internal control related to financial reporting.

---

## 17. Risk Analysis Methodology (Example)

---

### 17.1. Risk Control

Risk management is an important concept in information security management. Information security risks must be defined and managed for any type of business or activity. ISACA defines risk management as:

"The definition and management (identification, analysis, evaluation, handling, and monitoring) of information security risks for achieving business goal goals"

### 17.2. Risk Management Overview

Risk management involves the clarification of vulnerabilities and threats pertaining to information assets used by a company in business activities, and the processes involved in implementing measures to decrease the risk levels to an acceptable level based on the asset value of the information resources affected. This concept is shown in the equation below.

"Total risk = threat x vulnerability x asset value"

The following risk measures are available:

- Termination of business activities accompanied by risk
- Transference of the risk to another party (insurance, outsourcing, etc.)
- Reduction of the risk (implementation of security controls and countermeasures)
- Risk acceptance

Generally, expenses incurred by countermeasures do not exceed the profits expected to result from those business activities. The following risk management structures are internationally known.

- Australian/New Zealand Standard on Risk Management (AS/NZS 4360)<sup>45 46</sup>
- United States NIST's Risk Management Guide for Information Technology System, Special Publication 800-30(SP800-30)<sup>47 48</sup>

---

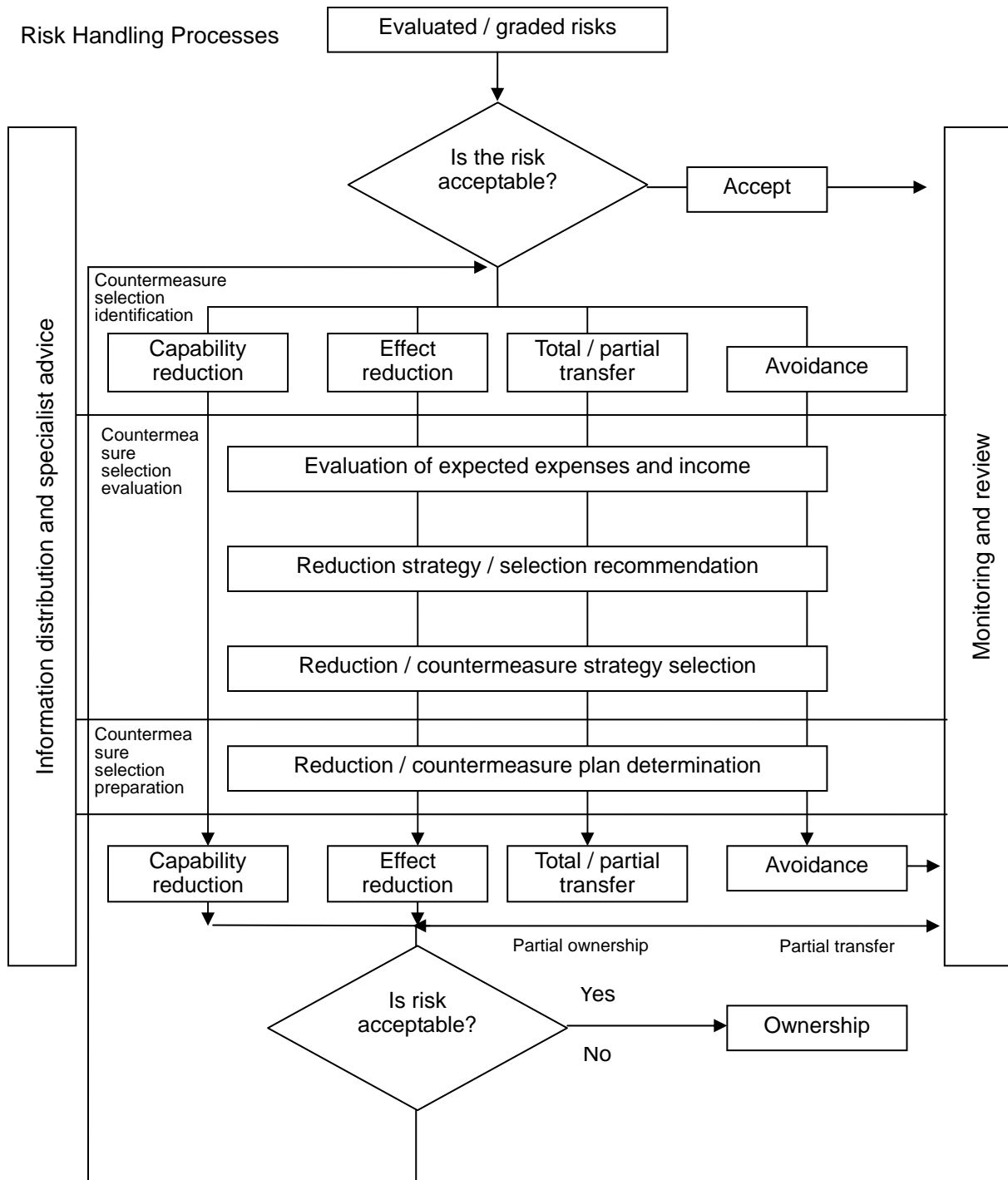
<sup>45</sup> <http://www.webstore.jsa.or.jp/webstore/Top/index.jsp?lang=jp>

<sup>46</sup> <http://www.riskmanagement.com.au/>

<sup>47</sup> <http://csrc.nist.gov/publications/nistpubs/index.html>

<sup>48</sup> <http://www.ipa.go.jp/security/publications/nist/>

The important elements in risk management are risk reduction, and risk handling processes. Risk handling processes are explained in the diagram below.



**Figure 17-1 Risk Handling Process (Source: AS/NZS:4360:1999)**

---

## 18. Risk Management Process

---

### 18.1. Plan Establishment

Risk management requires the establishment of a risk management plan, and the assigning of risk management responsibilities. This requires the attendance of representatives from important business departments, and the risk management plan must be led not from a technical but from a business direction. The following are defined in the risk management plan.

- Risk assessment goals and scope
- Risk control standards
- Risk control organization structure
- Risk evaluation method
- Risk management selection standards

### 18.2. Asset Assessment

The purpose of categorizing information assets is the clarification of evaluation standards when deciding protection measures appropriate to the value of the assets to which they apply, and the risk to those assets. Information classification is based on the confidentiality and importance of the information being classified. For each classification category, access rights, access right determination rights, and authorization rights must be clearly delineated. Generally, the following should be considered when classifying information assets.

- Classification depth (number of levels)
- Information asset location
- Who has the rights to determine classifications?
- How are classifications handled?
- How are classifications marked (how are they identified)?
- Who are the owners?
- Who has access rights?
- Who has the right to assign access rights?
- How are information assets transferred?

### 18.3. Risk Assessment

Risk assessment consists of threat and vulnerability evaluation, and risk evaluation based on these evaluation results.

## 18.4. Threat Evaluation

"Threats" refer to the latent damaging of information assets by means of a system vulnerability.

Ex.) Errors, malicious attacks, natural disasters, system shutdown, social engineering, and other acts by individuals or groups.

Threat analysis can be broadly divided into two approaches: the basic approach and the baseline approach.

## 18.5. Vulnerability Evaluation

Threats are caused by vulnerabilities. Below are the most common vulnerabilities.

Ex.) Software bugs, improper configuration, insufficient user security awareness, weak passwords, lack of redundancy, maintenance / operation problems.

## 18.6. Risk Evaluation

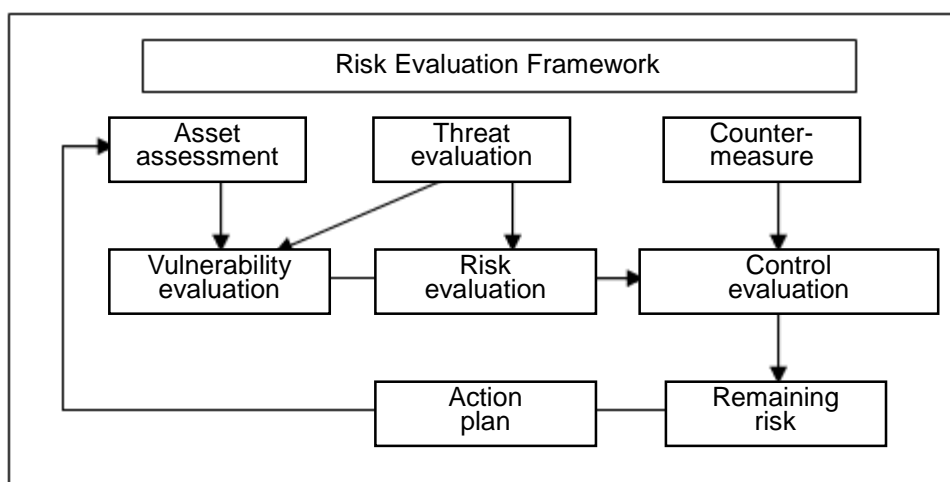
There are qualitative and quantitative methods of risk evaluation. Quantitative risk evaluation can be shown with the equation:

$\text{Risk evaluation value} = \text{predicted losses} \times \text{incident occurrence probability}$

Qualitative risk evaluation uses a level 3 or level 5 evaluation of effects for managed items for each type of risk based on degree of threat, vulnerability, and risk occurrence probability, and relative evaluation of risk size.

### Control Evaluation

The important processes in risk management are those of risk reduction and risk countermeasure processes. The risk countermeasure process is shown below.



**Figure 18-1 Risk Management Framework**



### 18.7. Remaining Risk

Risk reduction or prioritization is performed, and the acceptable risk level determined. The acceptable risk is authorized by a manager. The following points (from a risk reduction standpoint) must be considered when deciding on acceptable risk.

- Information security governance policy (security policy) conformance
- Whether measures / controls are excessive
- Whether there is any uncertainty in the risk assessment methodology
- Whether the results are cost effective

### 18.8. Action Plan

Action plans, including risk monitoring (including that of remaining risk) and escalation rules, are created. Risk management must handle changing threats and vulnerabilities, and as such risk management processes must be continuous and dynamic. As such, the following are necessary:

- Monitoring and review
- Reporting (escalation of critical security violations and issues to upper managers)
- Lifecycle process integration (change management, etc.)

### 18.9. Risk Reduction Methods

Risk reduction requires wide-ranging and inclusive consideration. Multilevel control, taking into account technical factors, organizational capability, and cost effectiveness, must be considered.

- Deterrent control
- Preventive control
- Detective control
- Corrective control

### 18.10. Information Asset RTO (Recovery Time Objectives)

It has become common knowledge that "information security is not perfect, and incidents will occur". In order to deal with this, RTOs (recovery time objectives) must be decided for information asset incidents as part of the risk evaluation environment. RTOs must be decided for all important information. RTOs are implemented via BIAs (Business Impact Analyses) integrated with business continuity plan creation.

---

## 19. Fundamentals of Quantitative Risk Analysis

---

### 19.1. Expected Value

The concept of the "expected value" in probability theory is an important concept which forms the foundation of quantitative risk analysis. Let us start by looking at this concept.

Let's consider a certain bet. A six sided die is cast once. If the die comes up 1, the bet is won, and you receive 600 yen. All other results are losses, and you do not receive any yen. What is the expected value of this bet?

The expected value is determined by comparing the possible return versus its probability. In this example, on average you will win 600 yen once for every 6 times the die is cast. A 1 in 6 probability is 1/6, so:

$$\text{Expected value} = \text{probability} \times \text{return} = (1/6) \times 600 = 600/6 = 100$$

That is, the expected value for this is 100 yen.

So what does the expected value mean? The expected value is the average return for each attempt. In this example, if this bet is repeated for a long period of time, the resulting return will be the equivalent of approximately 100 yen for each time the die was cast. For example, if the die is cast 1000 times, unless you are extremely lucky or unlucky, your final return will be somewhere in the neighborhood of 100 yen x 1000 die casts = 100,000 yen. This expected value provides a meterstick to use when deciding whether or not to make the bet. If, for example, it costs 200 yen to cast the die each time, over the long haul, you will have, on average, 200 yen (ante) - 100 yen (expected value) = 100 yen of loss.

Expected values can also be used for losses. For this same bet, from the point of view of the person paying off wins, there is a 1 in 6 chance of having to pay out 600 yen, so the expected value of losses is 100 yen. For losses, the formula can be rewritten as:

$$\text{Expected loss} = \text{probability} \times \text{loss}$$

This concept of expected value forms the cornerstone of quantitative analysis of risk.

### 19.2. Quantitative Determination of Risk

There are many ways to quantitatively determine risk, but the most common and instinctive is the use of the expected value of loss method. For example, if the probability of a certain building catching on fire is once per 100 years, and the average monetary loss due to a fire is 10,000,000 yen, then the risk of fire for that building can be calculated as:

$$\text{Risk} = \text{expected value of loss} = \text{probability} \times \text{loss} = 1/100 \times 10,000,000 = 100,000 \text{ (yen/year)}$$

That is, 100,000 yen per year. In this case, if insurance will cover all losses, then it worthwhile taking out insurance which costs less than 100,000 per year. This yearly expected value of loss

is generally referred to as "Annual Loss Expectancy", or ALE.

To use this method to quantitatively determine risk, you must know the probability of occurrence and the average losses for each risk. For earthquakes, fires, and other natural disasters, or for crimes, general statistics can be used as a foundation, but for many risks there are no such statistics, so determining accurate risk values can be difficult. When attempting to perform strict risk analysis, this often acts as an impenetrable obstacle.

Let us consider, then, instead of determining strict risk values, instead looking for general risk values for comparing different risks. Risks have an extremely large dynamic range. They range from daily activity levels of 10 or 100 yen to values equivalent to the budgets of entire nations, and range from risks which occur daily to those which occur only once every few hundred years. For example, the average yearly risk of a Japanese person being injured in a traffic accident is 0.0001, while the risk of being injured by a falling meteor is 0.0000000001. That is, the risk of being injured by a car is 1,000,000 greater. It doesn't make sense, then, to argue whether the chance of being injured by a meteor is 0.00000000011 or 0.00000000010. Either way, the risk of being injured in a traffic accident is far greater. When comparing something which is 10 or 100 times more or less likely, the difference of 0.1 or 0.2 is not really an issue.

Keeping this in mind, consider risk, then, from the standpoint of the number of digits. For example, when considering risks in the "10 yen", "100 yen", "1,000 yen", "10,000 yen", and "100,000 yen" categories, most individual risks will fall into one of the five. Fires, accidents, and other large risks would generally fall near the "100,000 yen" category, and insurance is used to move that risk. Considering risk from the standpoint of the number of digits allows comparison of risk without the need to determine exact values. This is how quantitative risk analysis can be performed without knowing concrete statistical values.

### 19.3. Risk Indicator Determination

Let us look at the "risk in terms of number of digits" concept from above as a formula.

Generally, the average loss value (V) for a risk can be written as:

$$V = a \times 10^x \quad (10^x \text{ means "10 to the } x \text{ power"})$$

The x represents the number of digits discussed above. If x is 1, then  $10^x$  is  $10^1$ , or 10, so V is "approximately 10 yen". If x is 3, then we have  $10^3$ , or 1,000, so V is "approximately 1,000 yen". The value a is a number between 1 and 10, so if a = 3 and x = 3, then V is  $3 \times 10^3 = 3,000$ , so "3,000 yen".

In the same way, the probability of a risk can be written as:

$$P = b \times 10^y$$

Probability values are expressed as numbers less than or equal to 1, so y is a negative number. b, like a, is a number between 1 and 10. If b=6 and y=(-3), then P is  $6 \times 10^{(-3)} = 0.006$ , or a

6/1000ths.

The expected value E for these risk, then is:

$$\begin{aligned}
 E &= V \times P \\
 &= (a \times 10^x) \times (b \times 10^y) \\
 &= a \times b \times 10^x \times 10^y \\
 &= ab \times 10^{(x+y)}
 \end{aligned}$$

ab covers the span between 1 and 100, averaging at 10. The main determinant for the number of digits in the risk expected value is the " $10^{(x+y)}$ " portion, and you can see that  $(x+y)$  basically controls the number of digits in the expected value. Thus, if you only want to obtain the number of digits in the expected value, all you need to do is add y, which indicates the number of digits in the probability, with x, the number of digits of loss.

Let's look at a specific example. First, let us define the loss value powers (exponents) as below.

Power x	Estimated loss
4	$10^4 = 10,000$ yen
3	$10^3 = 1000$ yen
2	$10^2 = 100$ yen
1	$10^1 = 10$ yen

Let us also define the probability of incurring this loss.

Power y	Estimated probability of occurrence
-1	$10^{(-1)} = 0.1$ times / year
-2	$10^{(-2)} = 0.01$ times / year
-3	$10^{(-3)} = 0.001$ times / year
-4	$10^{(-4)} = 0.0001$ times / year

If we make a table of these losses and probabilities, we get the following. The value at the intersection of a loss and a probability is the risk value for that set of conditions.

Risk (actual values)		Monetary Loss			
		10000	1000	100	10
Probability of Occurrence	0.1	1000	100	10	1
	0.01	100	10	1	0.1
	0.001	10	1	0.1	0.01
	0.0001	1	0.1	0.01	0.001

Let's rewrite this table using powers.

Risk (powers)		Monetary Loss			
		$10^4$	$10^3$	$10^2$	$10^1$
Probability of Occurrence	$10^{-1}$	$10^3$	$10^2$	$10^1$	$10^0$
	$10^{-2}$	$10^2$	$10^1$	$10^0$	$10^{-1}$
	$10^{-3}$	$10^1$	$10^0$	$10^{-1}$	$10^{-2}$
	$10^{-4}$	$10^0$	$10^{-1}$	$10^{-2}$	$10^{-3}$

Rewriting the above table using only the exponent values (for example, writing " $10^4$ " as "4") gives us the following table.

Risk (exponents only)		Monetary Loss			
		4	3	2	1
Probability of Occurrence	-1	3	2	1	0
	-2	2	1	0	-1
	-3	1	0	-1	-2
	-4	0	-1	-2	-3

As you can see, with this chart the risk value can be determined merely by adding the exponents for monetary loss and probability of occurrence. For example, if the monetary loss exponent is "4", and the probability of occurrence is "-1", the risk becomes "3", which is the same as  $4 + (-1) = 3$ . Writing this out as an equation gives us:

$$\text{Risk exponent} = \text{monetary loss exponent} + \text{probability of occurrence exponent}$$

Because some people may find it difficult to work with the negative values in the table, let us add 5 to each probability of occurrence, resulting in the following table. If we are just comparing relative values, there is no problem as long as we are adding the same value to all exponent values. This is the logical equivalent of changing the risk probability from "the probability of occurrence in a year" to "the probability of occurrence in 100,000 years". By doing this, we are able to immediately understand the results of a great number of risk analyses.

Risk (exponents)		Monetary Loss			
		4	3	2	1
Probability of Occurrence	4	8	7	6	5
	3	7	6	5	4
	2	6	5	4	3
	1	5	4	3	2

## 19.4. Courtney Method

Another method of risk analysis, the Courtney method, uses the same basic approach. The formula used in the Courtney method is defined below.

$$E = 10^{(P+V-3)} / 3$$

V: Expected losses due to occurrence of threat (exponent value of monetary value)

P: Probability of threat occurring (exponent of number of occurrences expected per 3,000 years)

E: Risk value (yearly)

This formula uses "per 3,000 years" for the probability of occurrence P, so to determine yearly risk values, the results must be divided by 3,000. The "/3" part of the Courtney formula divides the value by 3, and the exponent "-3" represents "dividing by  $10^3$ ", or "dividing by 1,000", so these parts of the formula serve to divide the risk value by 3,000.

$$\begin{aligned} E &= (10^{(P+V)}) / 3000 \\ &= (10^{(P+V)}) / (3 \times 10^3) \\ &= (10^{(P+V)}) \times 10^{(-3)} / 3 \\ &= (10^{(P+V-3)}) / 3 \end{aligned}$$

The main determinant of the value of E is the "P + V" section, and as we discussed earlier, the product of powers can be found by adding their exponents.

## 19.5. Approach to Vulnerability and Countermeasures

Vulnerabilities are inversely related to countermeasures. That is, vulnerabilities are the absence of sufficient measures. If we consider the fact that this affects risk values, then it must be possible to include this in the quantitative analysis. The table below is an example of that.

Vulnerability Index	Countermeasure Index	Affect on Risk	Affect to Index
-3	3	Estimated at 1/1000	-3
-2	2	Estimated at 1/100	-2
-1	1	Estimated at 1/10	-1
0	0	No effect	0

For example, when using vulnerability indexes, adding the vulnerability index to the risk index calculated based on the loss and probability results in the effect above to the risk. In this case, the method for determining the risk index is:

Risk index = Loss index + probability of occurrence index + vulnerability index.

In the same way, when using the countermeasure index, the countermeasure index value is subtracted from the risk index. As a result, the risk index formula becomes:

Risk index = Loss index + probability of occurrence index + countermeasure index

As you can see, elements which increase risk are added to the index, and those which decrease

risk are subtracted.

## 19.6. Applications

### 19.6.1. Basic Pattern (Courtney Method)

Variable	Representative Value	Index
Monetary Loss V	100,000 yen or less	1
	1 million yen	2
	10 million yen	3
	100 million yen or more	4
Probability of Occurrence P	Once every 300 years	1
	Once every 30 years	2
	Once every 3 years	3
	Once every 3 months (roughly 0.3 years)	4

The risk values for  $E = V + P$  then become the following.

Variable	Index	Risk Value (Yearly)
Risk Index E	2	Approx. 300 yen
	3	Approx. 3,000 yen
	4	Approx. 30,000 yen
	5	Approx. 300,000 yen
	6	Approx. 3 million yen
	7	Approx. 30 million yen
	8	Approx. 300 million yen

### 19.6.2. Including Vulnerabilities

The risk value is determined from the previous table using  $E = V + P + H - 1$ .

Variable	Representative Value	Index
Monetary Loss V	100,000 yen or less	1
	1 million yen	2
	10 million yen	3
	100 million yen or more	4
Probability of Occurrence P	Once every 300 years	1
	Once every 30 years	2
	Once every 3 years	3
	Once every 3 months (roughly 0.3 years)	4
Vulnerability H	Minimal	0
	Critical	1

### 19.6.3. Detailed Loss Values (1)

Variable	Representative Value	Index
Monetary Loss V	100,000 yen or less	1
	300,000 yen	1.5
	1 million yen	2
	3 million yen	2.5
	10 million yen	3
	30 million yen	3.5
	100 million yen or more	4
Probability of Occurrence P	Once every 300 years	1
	Once every 30 years	2
	Once every 3 years	3
	Once every 3 months (roughly 0.3 years)	4



$10^{0.5}$  = Approximately 3.1, so to raise the index by 0.5, the representative value would have to increase by a factor of 3.1.

Variable	Index	Risk Value (Yearly)
Risk Index E	2	Approx. 300 yen
	2.5	Approx. 1,000 yen
	3	Approx. 3,000 yen
	3.5	Approx. 10,000 yen
	4	Approx. 30,000 yen
	4.5	Approx. 100,000 yen
	5	Approx. 300,000 yen
	5.5	Approx. 1 million yen
	6	Approx. 3 million yen
	6.5	Approx. 10 million yen
	7	Approx. 30 million yen
	7.5	Approx. 100 million yen
	8	Approx. 300 million yen

#### 19.6.4. Detailed Loss Values (2)

Variable	Representative Value	Index
Monetary Loss V	100,000 yen or less	2
	300,000 yen	3
	1 million yen	4
	3 million yen	5
	10 million yen	6
	30 million yen	7
	100 million yen or more	8
Probability of Occurrence P	Once every 300 years	2
	Once every 30 years	4
	Once every 3 years	6
	Once every 3 months (roughly 0.3 years)	8

The indices of the previous example have been doubled. This is the equivalent of making the bottom index, instead of 10,  $10^{0.5}$ . The risk value table is the same as for the previous

example, so it has been omitted.

### 19.7. Example of Mistakes

In some quantitative risk analysis documents, even though the loss and probability values are clearly in index form (with an increase by a factor of 10 for each step), risk values are obtained by multiplying the indices. Expressed as a formula, this would be:

$$\text{Risk index} = \text{monetary loss index} \times \text{probability of occurrence index} \times \text{vulnerability index}$$

From a position of expected value theory, this is incorrect, and if we are determining expected values using indices, these must be added, not multiplied. Let's see how different our results are from when we use the correct equation:

$$\text{Risk index} = \text{monetary loss index} + \text{probability of occurrence index} + \text{vulnerability index}$$

First, let's look at a difference in absolute values. Let us assume that the loss value index, probability of occurrence index, and vulnerability index are all 3. Calculated properly:

$$\text{Risk index} = 3 + 3 + 3 = 9$$

That is, the risk is  $10^9$ , or approximately 10 billion yen / year. However, if we multiply instead, we get:

$$\text{Risk index} = 3 \times 3 \times 3 = 27$$

That is, the risk becomes  $10^{27}$ . This is 10 billion times the correct value of 1,000,000,000.

This also leads to incorrect results when comparing risks. For example, let us compare the risk values of the following two cases.

Case	A	B
Monetary Loss Index	2	4
Probability of Occurrence Index	2	1
Vulnerability Index	2	1

The total of the indices of both these cases is 6, meaning that the risk value of both cases is the same  $10^6 = 1$  million yen / year. However, if the indices are mistakenly multiplied, we reach different values.

$$\text{Case A: } 2 \times 2 \times 2 = 8$$

$$\text{Case B: } 4 \times 1 \times 1 = 4$$

The difference between these risk values is 4, that is, a mistake to the order of  $10^4$ , or 10,000. When multiplying indices, there is a tendency for a certain risk in a set of high risks to leap above even other unusually high risks. This prevents rational evaluation of risks. For example, prospect theory tells us that when the loss involved in a particular risk is very high, even if the probability of its occurrence is low, people tend to evaluate that risk as great. Correcting the effects of this psychological risk assessment is a worthwhile goal, but by multiplying the indices,

instead of correcting this trend, it is actually exacerbated.

### 19.8. Limits of Expected Value Based Quantitative Risk Analysis

We have discussed quantitative risk analysis using expected values, but the results of this analysis may not always be in agreement with the feelings of managers. One reason is the prospect theory mentioned earlier. Generally, if two risks carry the same expected value, even if the probability of occurrence is low, the risk which carries a great loss is felt to be a bigger risk. Another reason is that the possibility of risks changing is itself also a risk (volatility risk). That is, if the loss involved in a risk is low, it may be accepted even though the expected value is high. These ways of thinking about risk are not reflected in simple expected value comparisons, so expected values should not be thought of as absolute indices, but instead as one index to be used in risk evaluation.

## Fujitsu Enterprise Security Architecture

November, 2006

First Edition, Second Printing

April, 2007

Second Edition

Written by

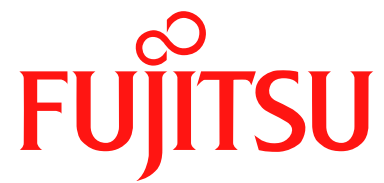
FUJITSU LIMITED Information Security Center    ESA Project

Edited and Published by

FUJITSU LIMITED Information Security Center

Fujitsu Solution Square, 1-17-25, Shin-kamata, Ohta-ku, Tokyo

Copyright © 2006,2007 FUJITSU LIMITED All rights reserved



THE POSSIBILITIES ARE INFINITE