TOPCIT

ESSENCE Ver. 3

Technical Field

04 Understanding Information Security

TOPCIT ESSENCE is published to provide learning materials for TOPCIT examinees.
The TOPCIT Division desires the TOPCIT examinees who want to acquire the necessary practical competency in the field of ICTto exploit as self - directed learning materials.

For more information about TOPCIT ESSENCE, visit TOPCIT website or send us an e-mail.

As part of the **TOPCIT ESSENCE** contents feed into authors' personal opinions, it is not the TOPCIT Division's official stance.

Ministry of Science, ICT and Future Planning
Institute for Information and Communications Technology Promotion
Korea Productivity Center

Publisher TOPCIT Division
+82-2-398-7649 www.topcit.or.kr helpdesk@topcit.or.kr

Date of Publication 1st **Edition** 2014. 12. 10.
2nd **Edition** 2016. 02. 26.
3rd **Edition** 2020. 02. 26.

TOPCIT

ESSENCE Ver. 3

Technical Field

04 Understanding Information Security

TOPCIT ESSENCE Ver. 3

Technical Field

04 Understanding Information Security

CONTENTS

CONTENTS

CONTENTS

I. Concept of information security

▶▶▶ Subject

Understanding the concept of information security

▶▶▶ Recent trends and major issues

IT-related technologies, such as the popularization of the cloud, promotion of big data, and the artificial intelligence industry, are gradually advancing, as well as full-scale development of the IoT industry. Various convergence technologies and services are also emerging. However, as information security technology is not being applied to keep pace with this, various incidents of security infringement, using new technology and convergence technology, are expected to increase. As a result, various security technologies and security services need to be urgently developed for the information security of new technologies and convergence technologies. Therefore, we need to understand the concept of information security, which becomes the foundation.

▶▶▶ Learning objectives

To be able to explain the concept of information security.

To be able to explain the goal and importance of information security.

▶▶▶ Keywords

Information security, administrative/technical/physical information security, confidentiality, integrity, availability, non-repudiation, authentication, access control

✚ Preview for practical business

Assistant manager Kim, working for company A has overseen the development, deployment, and maintenance of Java source programs. He used to check web pages and servers on a regular basis.
In this process, he should ensure the availability of numerous source codes that he is managing, and he should manage the performance and capacity to ensure the availability of the server, so that the applications can work properly. He should also take technical protection measures, like encryption, to maintain the confidentiality of customer information that is saved by the application.
He is trying to ensure confidentiality, integrity, and availability of business information. Let's take a closer look at the concepts and goals of information security.

01 Overview of information security

A) Overview of information security

① Concept of information security

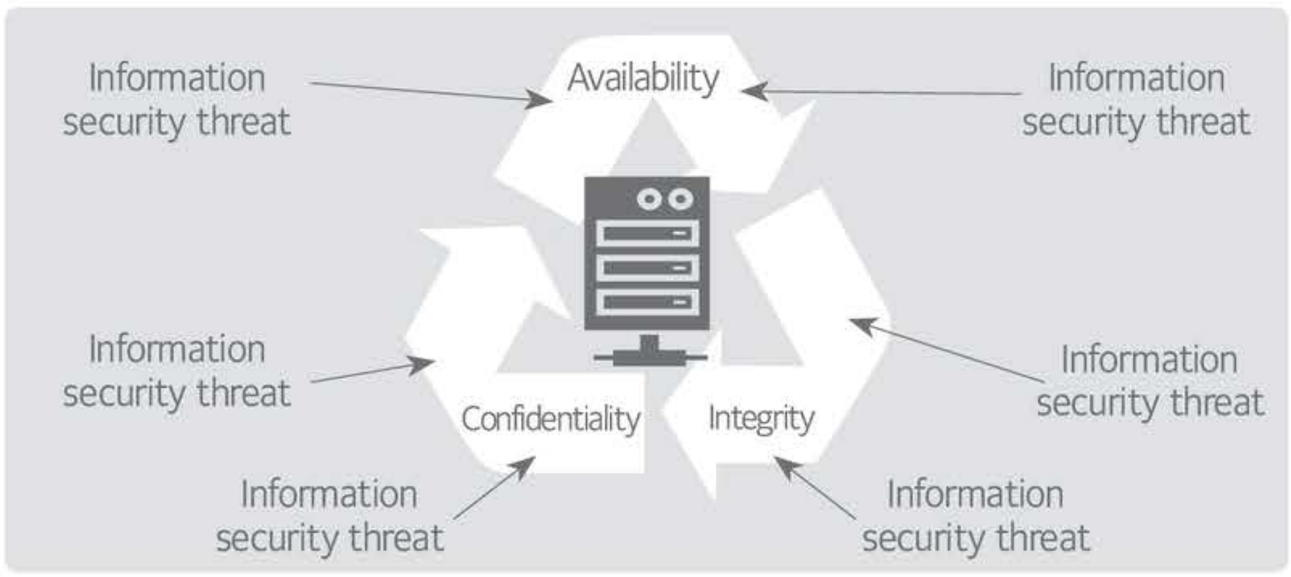
Information security refers to protecting information administratively, physically, and technically in order to prevent damage, alteration, and leakage of information while being collected, processed, stored, and transmitted information.

② Need for information security

The need to guarantee privacy and prevent crimes on the Internet is gradually increasing. Concerns about the leakage of major domestic technologies and information are also increasing, due to globalization, as the entire world is connected through the Internet.

③ Goals of information security

The three goals of information security are confidentiality, integrity, and availability. Efforts should be made to administratively, physically and technically ensure these attributes.



[Figure 1] Three goals of information security

- Confidentiality means that the original information is not exposed to unauthorized users while being stored and transmitted.
- Integrity means that the original information is maintained while sending and receiving it, without illegal creation, modification, or deletion.
- Availability means that authorized users can access and use the requested information when necessary.

02 Basic terms of information security

A) Authentication

Authentication refers to a method of verifying whether the information exchanged between the sender and receiver, who are the subjects of the information, has not been altered or deleted, and whether the subjects (sender and receiver) are legitimate.

B) Non-repudiation

Non-repudiation refers to security technologyto prevent the repudiation after receiving and sending a message, by verifying the fact of message receiving/sending. Non-repudiation can be classified into the following three categories:

① Non-repudiation of origin

Non-repudiation of origin refers to the prevention of the sender's claim that the message was not received after actually receiving the message.

② Non-repudiation of delivery

Non-repudiation of delivery refers to the prevention of the receiver's claim that the message was not delivered after actually sending the message.

③ Non-repudiation of receipt

Non-repudiation of receipt refers to the prevention of the receiver's claim that the message was not received after actually receiving the message.

C) Cryptography

Cryptography is largely classified into cryptographic techniques and encryption protocol techniques.

① Cryptographic techniques

Cryptographic techniques can be divided into the symmetric key cryptosystem, in which the encryption key and the decryption key are the same,while in the public key cryptosystem, the encryption key and the decryption key are different, depending on whether the encryption key and the decryption key are the same.

② Cryptographic protocols

Cryptographic protocols refer to the protocols that use cryptographic techniques. As a protocol means a series of finite phases where more than 2 persons participate to achieve a certain purpose, the cryptographic protocol should prevent repudiation by a participant, or a third party, to ensure a certain purpose of the concerned cryptographic protocol (authentication, confidentiality, integrity, non-repudiation, etc.), as well as the meaning of each message.

D) Digital signature

A digital signature is the method of providing both data integrity and signature authentication, by performing a hash operation on a specific document, using the signature's private key. Signing the entire message is very inefficient because the public key operation should be performed on all message blocks repetitively. Therefore, an electronic signature can be efficiently generated by calculating a hash value for the message, then signing on that value. Although the signature is on the hash value, instead of on the message itself, it is recognized as a genuine signature for the message because finding another message with the same hash value is difficult.

E) Hash function

A hash function, or hash algorithm, is a mathematical function that converts a random string of various sizes into a short hash value (hash code) of fixed length, then outputs it. That is, the function compresses an input string of a random length into a string with a fixed, short length.

Unlike an encryption algorithm, the hash function does not use a key, therefore providing the same output for the same input. Thanks to this property, the hash function can be used for integrity verification, which can detect an erroneous or altered input message.

F) Malware

Malware is an abbreviation of malicious software and refers to software designed to perform malicious actions

against computers, file systems, or networks. Malware can be classified into the following types:

① Worms

Malware that runs independently. This malware replicates itself and spreads to other computers.

② Viruses

Viruses refer to malicious codes that are inserted into the code of another independent program, then make the program perform malicious behavior and spread on its own.

③ Trojan horse

A program with hidden codes. Although it looks like a normal program, malicious code is executed when the user executes the program.

G) Major security solutions

① Firewall

A firewall refers to a security solution installed between the public network and the private network to protect the private network from the outside. In general, there are two types of firewalls. The first type is a packet filtering gateway, which determines whether to pass the packet, based on a series of rules. The second type is a proxy server that provides authentication to specific hosts to access a private network and allows them to pass the packet. However, a method with increased security is also used, which combines these two methods.

② Intrusion Prevention System (IPS)

A security system that blocks intrusions in real time by detecting unauthorized and abnormal behaviors for the target system (network detection area), and by distinguishing detected illegal behavior. It can be assumed that the characteristics in the common area between the average area of the behavior of the intruder, and that of the behavior of the authorizer, make intrusion detection difficult. The intrusion detection system is built first, along with a firewall, when implementing a general security system. The purpose of building the intrusion detection system includes real-time detection and blocking of illegal activities, such as hacking, and defense against attacks performed by using the packet, allowed by the firewall.

③ Virtual Private Network (VPN)

A technology that enables to safely use access control, authentication, and confidentiality services, like a private network when using a public network, without building a physical private network between remote sites. IPSec and SSL are the representative technologies for implementing a VPN. The VPN can be implemented in a dedicated system, router, or firewall.

④ Single Sign On (SSO)

Single sign on enables the user to access another site without a separate authentication procedure after logging in on one site. In general, different systems and sites manage their user information separately. However, it is necessary to link user information on occasion. In this case, SSO can be used for the integrated

authentication of multiple systems, based on the information of one user.

⑤ Web Application Firewall (WAF)

Located in front of the web server, this security solution monitors incoming traffic with the HTTP/HTTPS protocol and blocks malicious attacks detected against the web application, such as the SQL Injection attack or XSS attack, before it reaches the web server.

⑥ Network Access Control (NAC)

When at the endpoint, when a user computer attempts to access the internal network for the first time, the system checks whether the accessing user computer complies with various security policies, such as network user authentication, anti-virus program installation, etc., and controls network access according to the pre-defined security policy, when security policies are not observed.

⑦ Wireless Intrusion Prevention System (WIPS)

The WIPS automatically detects and blocks access from unauthorized wireless devices by continuously monitoring the wireless LAN operated of a specific organization, and it improves the stability of wireless LAN and enables integrated management. The WIPS provides a function of detecting and blocking an intrusion attempt using an unauthorized AP or user device in the exposed wireless network.

⑧ Enterprise Security Management (ESM)

ESM is designed to provide a consistent and intuitive administrator and user interface by integrating security management functions modularized by function and product. This security solution aims to build an integrated security management system for all systems, according to standard policies, by building an efficient, policy-oriented, and systematic security management system.

⑨ Security Information Event Management (SIEM)

The SIEM solution establishes an early warning and monitoring system for intelligent threats, which provides correlation analysis and forensic functions in the vast information of big data, by extending the role of the existing ESM from the security domain to the entire enterprise, and by adding corporate compliance response functions, so that those threats can be traced later, instead of only collecting and analyzing logs.

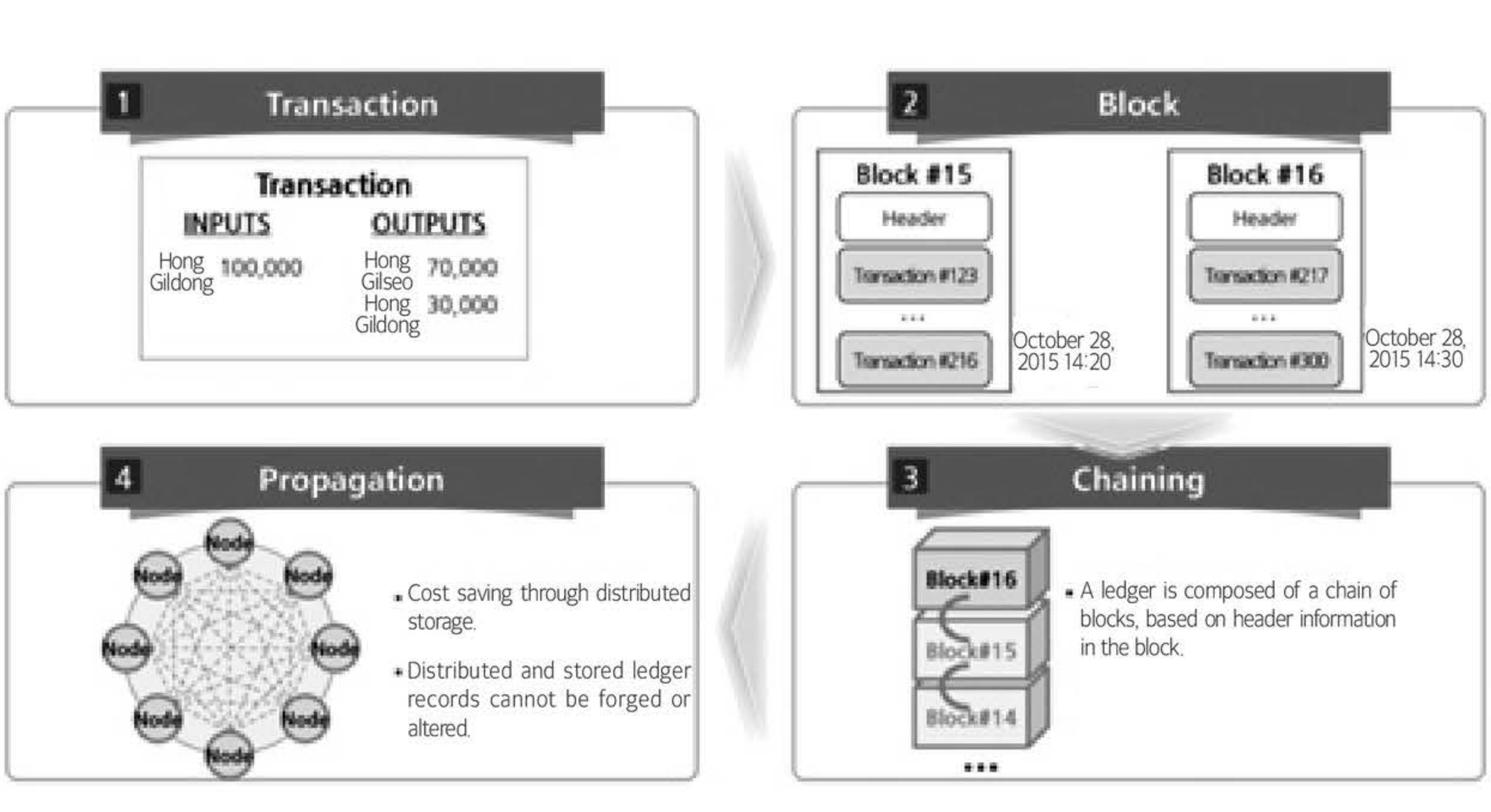
03 New technical terms of information security

A) Blockchain

The Bitcoin cryptocurrency system and all transactions occurring in the network are recorded in one public ledger, distributed, and stored in a single ledger. Blockchain is a distributed ledger and is designed with a structure that enables network participants to store and verify data. When transactions occur, transactions that have occurred for a certain period of time (10 minutes) are collected to create a block, in order to verify transaction information, then the blocks are sequentially connected to form a chain. That's why it is called a

blockchain.

A copy of the transaction ledger is distributed among network members. Whenever a new transaction occurs, the transaction is verified by the consent of the members. The blockchain uses a P2P network method instead of depending on the existing centralized system. Therefore, it is not necessary for a transaction broker to intervene. As a result, the efficiency and transparency of transactions are increased, and transactions can be made faster and safer, at a low cost. In addition, as transaction information based on the blockchain cannot be forged and altered, transaction reliability increases, and transaction information can be easily traced.



[Figure 2] Conceptual diagram of the blockchain

B) FIDO (Fast Identity Online Alliance)

FIDO was established in July 2012 to set the technical (De facto) standard for the authentication method, using biometrics in the online environment. The FIDO standard separated local user authentication in the user device from remote authentication performed by the service provider's server.

① FIDO 1.0

Even though FIDO 1.0 is similar to existing biometric authentication, it provides two authentication methods: the UAF (Universal Authentication Framework) protocol that does not store the user's personal information on the server, and the U2F (Universal 2nd Factor) protocol that improves security using two-factor authentication.

② FIDO 2.0

FIDO 2.0 provides a convenient authentication and payment environment using bio-information, instead of the password in the PC and web environment. It is expected that more biometric authentication devices will be installed in PCs and laptops, and various device authentication methods, using the smartphone as a key, can be provided. FIDO 2.0 is a universal authentication technology standard that is developed to provide the FIDO clients and ASM on the platform. Here, the platform largely means the operating system platform, including

Windows and Android, and the web platform based on the web browser. FIDO server, RP server, and RP client are the components that should be provided by the server. Therefore, if they are regarded as a part of the server, the standard protocol is not needed anymore. Therefore, FIDO 2.0 does not use the UAF protocol, but exchanges messages, using its own protocol defined by the server. The FIDO client, which was provided as an Android app in the existing FIDO 1.0, will be provided as an API by the operating system, or as a JavaScript API by the web browser.

C) Network segregation and network linking

Network segregation refers to network blocking, which separates the business network from the external network in order to block illegal access from the external Internet network and to prevent the leakage of internal information. There are two types - physical network segregation and logical network segregation.

<Table 1> Physical network segregation and logical network segregation

Item	Physical network segregation	Logical network segregation
Operation method	Physical segregation of the business network and internet network (using 2 PCs)	Logical segregation using virtualization or other methods (using 1 PC)
Introduction cost	High (additional PC, network installation)	Low (depending on the installation environment)
Security	High security (basic segregation)	Low security (vulnerabilities occur)
Efficiency	Low efficiency (work environment)	Easy to manage (applying security policies)
Detailed method	2 PCs, multi-PC, network switching device	Server-based, PC-based

D) Fraud Detection System (FDS)

The FDS is a system that detects suspicious transactions and blocks abnormal financial transactions by comprehensively analyzing device information, access information, and transaction details used in electronic financial transactions. Pattern analysis is the core engine of the FDS because the usual transactions of the user are analyzed, and abnormal behavior is detected when an action that violates the analyzed pattern is taken. The FDS has the following functions.

① Information collection

The FDS collects user media environment information and accident type information by collecting information on user information and behavior.

② Analysis and detection

The FDS detects abnormal behavior by analyzing various correlations by user type and transaction type, and by testing the pattern, based on the analysis of abnormal behavior, using the collected information.

③ Response

The FDS blocks an illegal transaction by blocking the transaction or by requiring additional authentication when abnormal behavior is detected.

E) Quantum cryptography

Quantum cryptography is a cryptographic technology that utilizes the characteristics of mechanics. Unlike existing cryptosystems that are based on mathematical complexities, quantum cryptography is based on the characteristics of quantum. A quantum cannot be copied or returned to its original state. Due to these properties, the receiver can detect an eavesdropping attempt when a third party measures the quantum for eavesdropping because its state is changed if measured.

F) Trusted Platform Module (TPM)

The trusted platform module (TPM) is a standard established by the TCG (Trusted Computing Group), an international industry standard organization, to overcome the limitations of security technology that only operates with software. This module provides a strong security environment that stores important data that requires security in a secure space separated by hardware, such as the encrypted key, password, digital certificate. It ensures that key management, encryption processing, etc., are only handled inside the security device. The latest TPM 2 was released in September 2016, which includes the Mobile Trusted Module (MTM).

G) Re-identification

De-identification is the process or method of converting data in such way that an individual cannot be identified. Re-identification is the process or method of identifying an individual from the de-identified data by combining, analyzing, and processing it with other information. Personal information may be disclosed, due to intentional or accidental re-identification, while collecting information from SNS or websites, like search engines, or while companies that handle personal information, such medical and financial institutions, are analyzing data. Recently, as big data is being used in various fields, there is concern that personal information may be leaked indiscriminately due to re-identification.

H) EU-GDPR

EU-GDPR is the personal information protection law of the EU (European Union) that took effect from May 25, 2018. Since administrative measures, such as penalties, may be imposed if the law is violated, Korean companies need to pay attention so as not to violate this law. The EU has enacted the General Data Protection Regulation to protect personal information and to provide opportunities for the utilization of personal information at the same time, using the concept of general personal information, anonymous information, and pseudonym information.

Major changes to the GDPR are as follows:

① Enforcement regulation (imposition of penalties)

Whereas the previous EU Directives were the regulation at the recommendation level, the GDPR is quite different, in that it is a mandatory regulation that all member states must comply with. (Penalties are imposed if violated.)

② Extra-territorial scope

The GDPR applies not only to the company operating a business site in the EU, but also to the companies that process the personal information of EU residents in overseas countries through e-commerce, etc.

③ Increased responsibilities

The increased responsibility of the enterprise, such as the designation of the Data Protection Officer (DPO), and the increased rights of the information owner, such as the right to data portability, have been added.

II. Fundamental technologies for information security

▶▶▶ Subject

Understanding cryptography, authentication technique, and access control

▶▶▶ Recent trends and major issues

The seriousness of the problems caused by the expansion and development of the cyber world are increasing day by day. Even Windows and anti-virus patch programs are sometimes distributed after infection with a virus or alteration. From the viewpoint of information security, various security threats can be actively responded to by ensuring confidentiality and integrity. Confidentiality is based on the concept that data should be viewed only by authorized and legitimate users who hold the right to access the data, whereas integrity is based on the concept that data should be the original data without forgery or alteration. Therefore, it is very important to individually or collectively ensure confidentiality and integrity in information security, by applying them while considering the characteristics of each piece of data.

▶▶▶ Learning objectives

To be able to explain the concept of ciphers and classical ciphers to support confidentiality.

To be able to explain private key encryption and public key encryption algorithms.

To be able to explain the hash function to support integrity.

To be able to explain the hash function to support integrity.

To be able to explain the electronic signature and public key infrastructure (PKI) for secure transactions.

To be able to explain authentication techniques and authentication methods to control access.

▶▶▶ Keywords

Encryption algorithm, private key encryption, public key encryption, hash function, authentication, digital signature, PKI, access control, cryptographic protocol, DES, AES, RSA, ECC, hash collision, public certificate, multi factor authentication, session key

✚ Preview for practical business Managing information safely

Assistant manager Kim, working for web application program development company A, has been in charge of developing, deploying, and maintaining Java-based source programs. He should check the web pages and servers on a regular basis when processing his work. However, he is not safe from various security threats that are becoming diversified and intelligent by regular check only.

He also should exchange source programs with partners while doing his work and should ensure that those source programs are not disclosed to other competitors.

In such a situation, confidentiality must be ensured so that a large number of source programs, managed by Kim, are not disclosed to unauthorized third parties during storage or transmission. To do this, let's see what steps Kim should take, and how to apply the concept of confidentiality in practice.

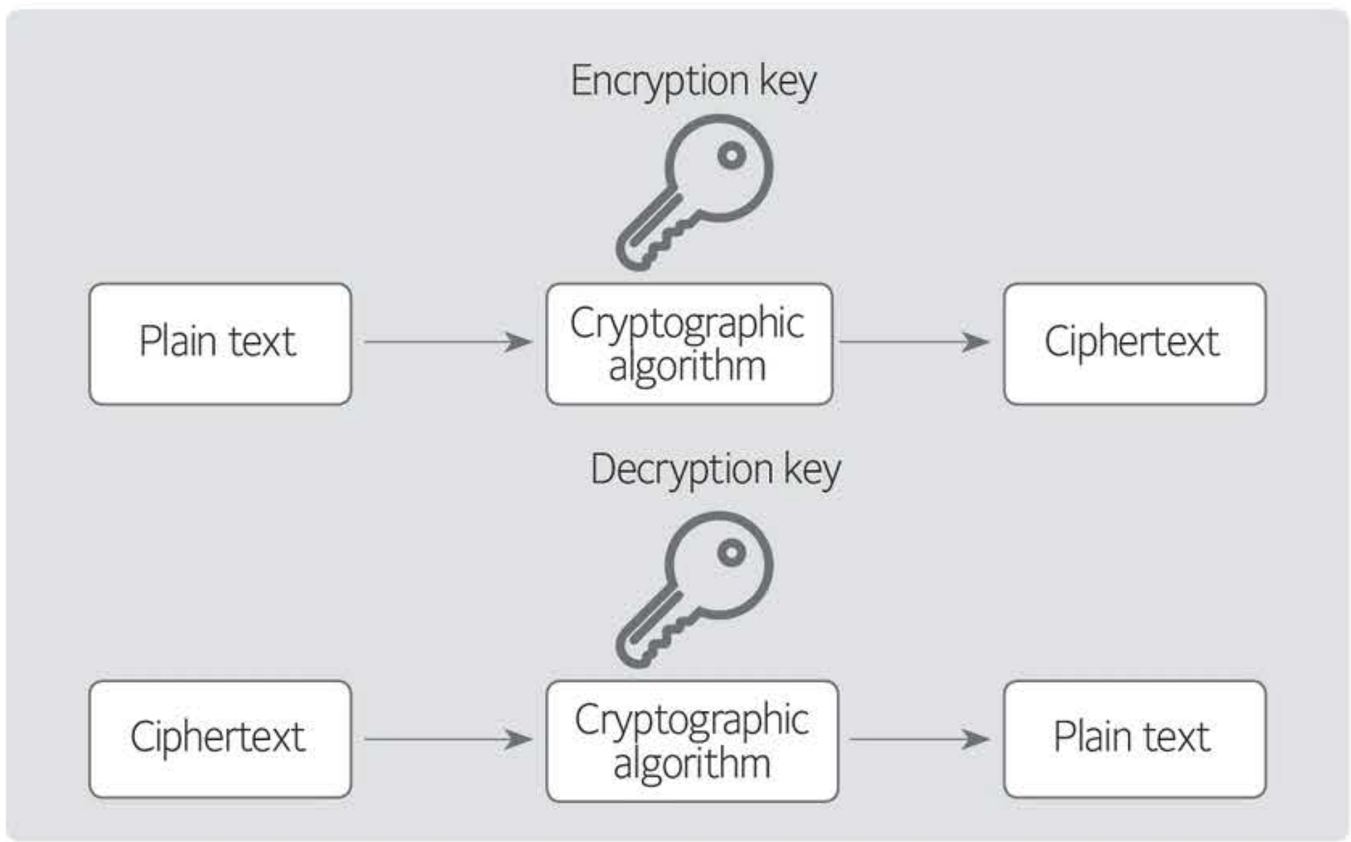
01 Cryptographic techniques

A) Concept of a cipher

Encryption is the process of converting plain text, which can be seen by anyone, into an incomprehensible form of ciphertext. Decryption is the process of converting ciphertext back into plaintext, so that it can be understood. These two processes are called cryptography. The mathematical function used in these two conversion processes is called a cryptographic algorithm. The cryptographic algorithm uses a key to perform encryption and decryption. In short, encryption is an important means to obtain confidentiality, which is one of the three main goals of information security.

B) Encryption and decryption

Encryption is the process of converting plain text into a form (ciphertext) that cannot be recognized by a third party, whereas decryption is the reverse process of encryption. That is, decryption is the process of restoring converted ciphertext back into plaintext.



[Figure 3] Encryption and decryption

Initially, encryption was mainly used for military purposes. However, it is used to protect a variety of important information with the development of information,communication, and Internet technology.

C) Classification of cryptographic techniques

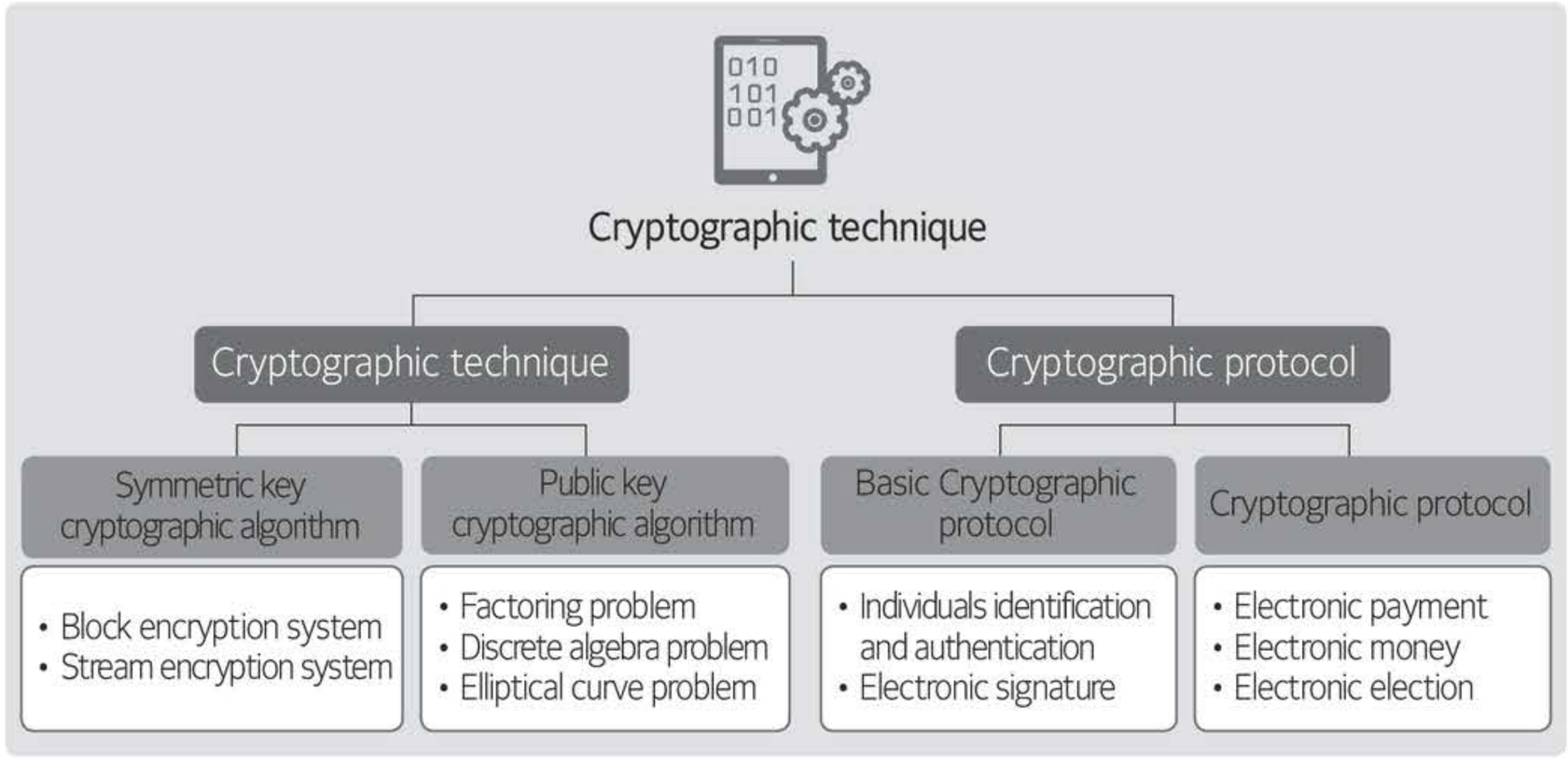
Cryptographic techniques are classified into the cryptographic technique and cryptographic protocol technique.

① Cryptographic techniques

Cryptographic techniques can be divided into the symmetric key cryptosystem, in which the encryption key and the decryption key are the same, and the public key cryptosystem, in which the encryption key and the decryption key are different, depending on whether the encryption key and the decryption key are the same.

② Cryptographic protocols

Cryptographic protocols refer to the protocols that use cryptographic techniques. As a protocol means a series of finite phases in which more than 2 persons participate to achieve a certain purpose, the cryptographic protocol should prevent repudiation by a participant, or a third party, to ensure a certain purpose of the concerned cryptographic protocol (authentication, confidentiality, integrity, and non-repudiation, etc.), as well as the meaning of each message.

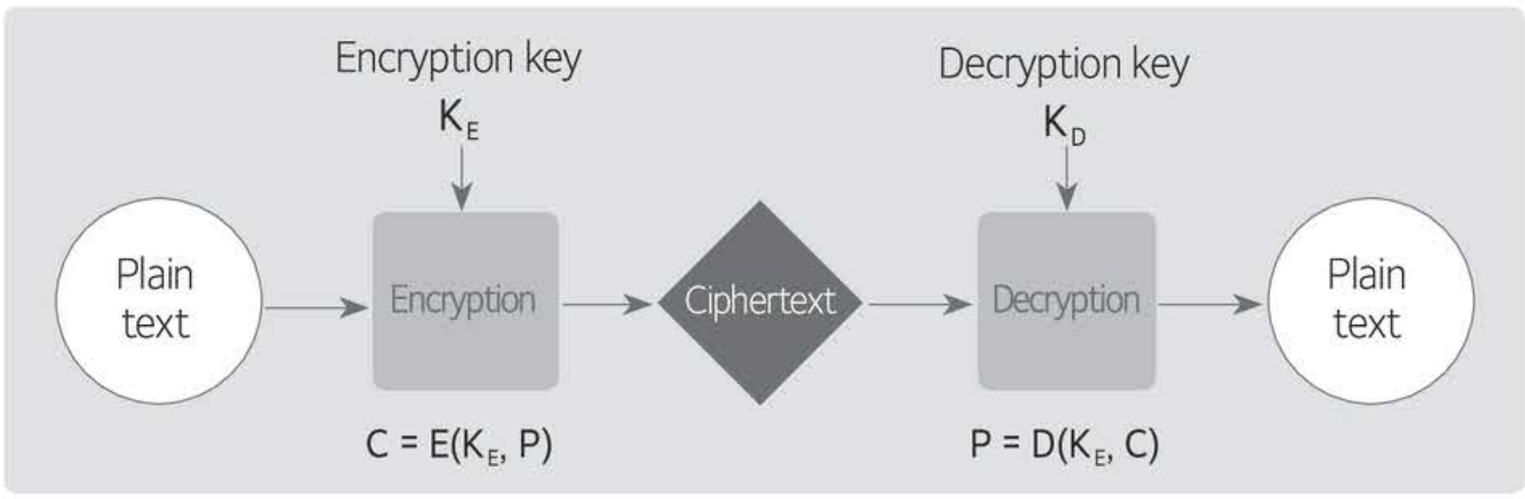


[Figure 4] Classification of cryptographic techniques

D) Cryptographic algorithm and cryptosystem

① Cryptographic algorithm

The cryptographic algorithm that uses an encryption key can be described as [Figure 5]. In the figure, P is plain text, E is the cryptographic function, and K(KE, KD) is the key value. As in the public key method, the encryption key and the decryption key can be different. In that case, keys are expressed KE and KD respectively. Since ciphertext is generally transmitted over the communication line or network that is not secure, the sender and receiver can ensure confidentiality by transmitting the result of encrypting the plaintext.



[Figure 5] Cryptographic algorithm

The receiver tries to send plaintext P, which can be seen by anyone, to the other party. The sender generates ciphertext C from plaintext P using the encryption key KE and the cryptographic algorithm E,then delivers it to the receiver. In general, we cannot understand ciphertext C without knowing the decryption key, which is called computational impossibility. Here, the computational impossibility means that we can understand the contents of the plaintext, even though we don't know the decryption key, if infinite time is used. The attacker attempts to understand the contents of the plaintext using various methods. The legitimate receiver can understand plain text P that the sender has initially intended to send, by receiving ciphertext C sent by the sender and converting it using the decryption key KD and decryption algorithm D.

② Cryptosystem

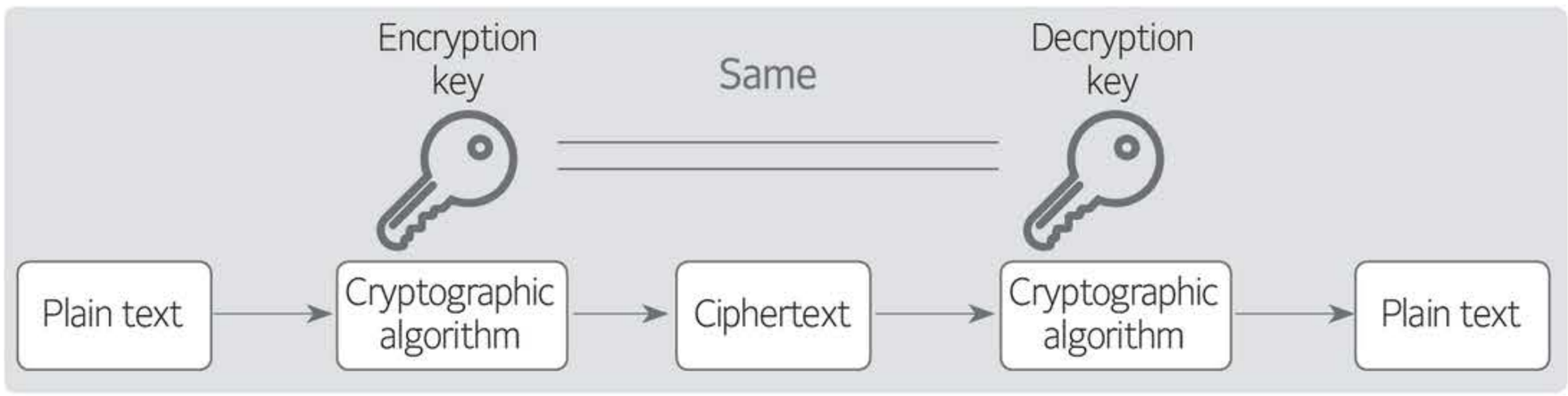
All the elements that are needed for a series of encryption and decryption processes are called a "cryptosystem". The cryptosystem should generally meet the following requirements:

- Encryption and decryption should be effectively performed by the encryption key.
- A cryptosystem should be easy to use.
- Security should be performed by the encryption key, rather than by a cryptographic algorithm.

E) Private key encryption and public key cryptographic algorithm

① Private key cryptographic algorithm

The secret key encryption algorithm has the advantage that the encryption key used for encryption and the decryption key used for decryption are the same, and that the length of the key may be short, and the speed of encryption and decryption operations is fast.



[Figure 6] Private key cryptographic algorithm

However, it is difficult to share the key if the distance between the sender and the receiver is long. If there are many other parties who require encrypted communication, it is quite burdensome to generate and maintain different keys. It is called a private key encryption system, in the sense that the key should be kept and managed in secret.It is also called a conventional encryption system, in the sense that it is commonly used.
The private key encryption system is still widely used, even though it is difficult to share the key, because the cryptographic algorithm is composed of a combination of substitution and transposition, enabling fast operations. In addition, this system is divided into the block cipher and the stream cipher, as shown in Table 2, depending on the plaintext processing method.

<Table 2> Comparison of the block cipher and the stream cipher

Item	Block encryption	Stream encryption
Operating method	Plaintext is divided into fixed size inputs, called blocks, and each block is encrypted.	Plaintext is encrypted in bits.
Strengths	Easy to implement	Low risk of error spread Easy to implement in a mobile communication environment
Shortcomings	High risk of error spread Initial values should be set.	Slow execution time Malicious attackers can easily modify the content.

• Block cipher algorithm

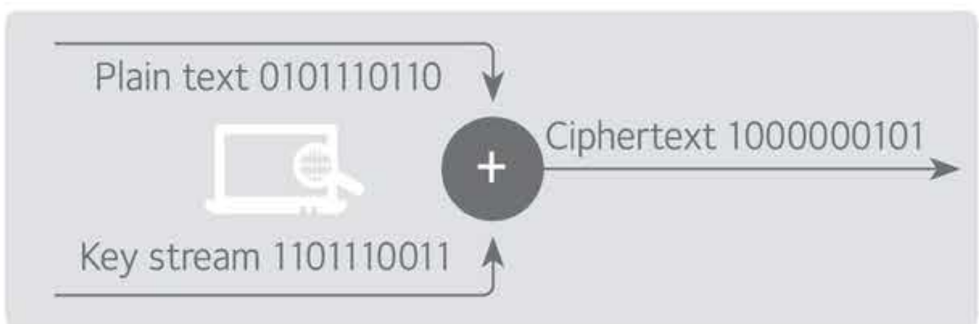
The block cipher algorithm performs the encryption and decryption process, using the cryptographic algorithm that transforms fixed size input blocks into fixed size output blocks using a secret key. The block cipher algorithm includes Feistel Network, DES (Data Encryption Standard), AES (Advanced Encryption Standard), IDEA (International (Data Encryption Algorithm), SEED, and ARIA. <Table 3> shows major attack techniques against the block cipher system.

<Table 3> Block cipher attack techniques

Attack technique	Contents
Differential attack	The differential attack is a method of attack on the selected plaintext. This attack technique finds the key used for encryption by using the bit difference of the ciphertext blocks, which corresponds to the difference of two plaintext blocks.
Linear attack	The linear attack is a method of attacking plaintext. This attack technique finds the encryption key by properly linearizing a nonlinear structure inside a cryptographic algorithm.
Brute force attack	An attack technique that finds the encryption key by comparing plaintext and ciphertext by using all possible encryption keys used for encryption.
Statistical analysis	An attack technique that decrypts ciphertext using all known statistical data, including statistical data on the frequency of each word used in ciphertext.
Mathematical analysis	An attack technique that decrypts ciphertext using mathematical theories, including statistical methods.

• Stream cipher algorithm

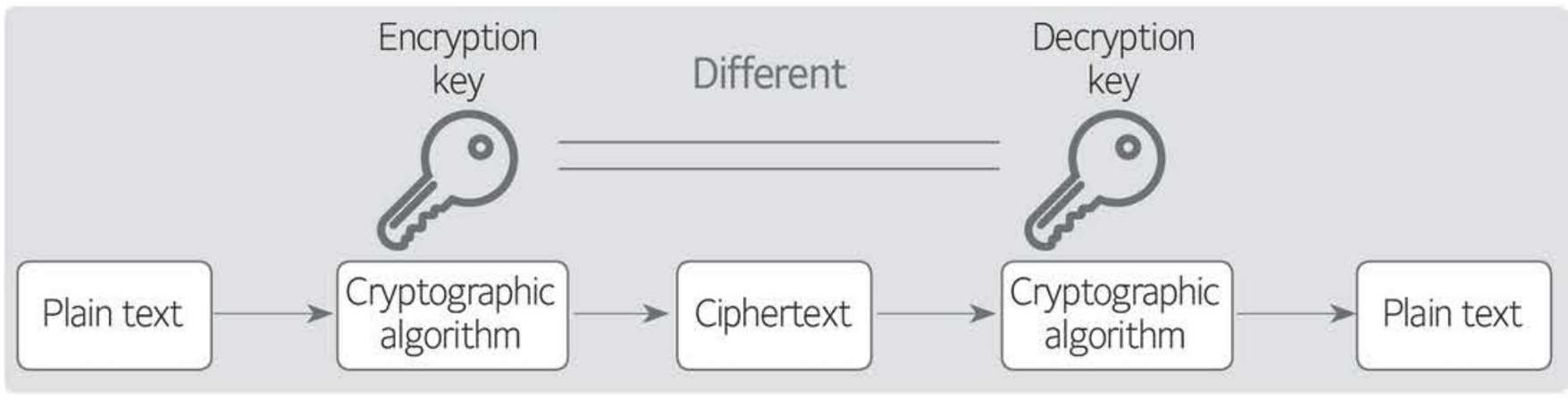
A stream cipher is a method developed mainly in Europe. Unlike block ciphers that perform encryption and decryption in blocks, ciphertext is created by the bitwise XOR operation of the plaintext bit string, and the bit string of the key, as shown in [Figure 7]. RC4 is a representative stream cipher, and there are other algorithms, such as A5/1 and A5/2.



[Figure 7] Stream cryptographic algorithm

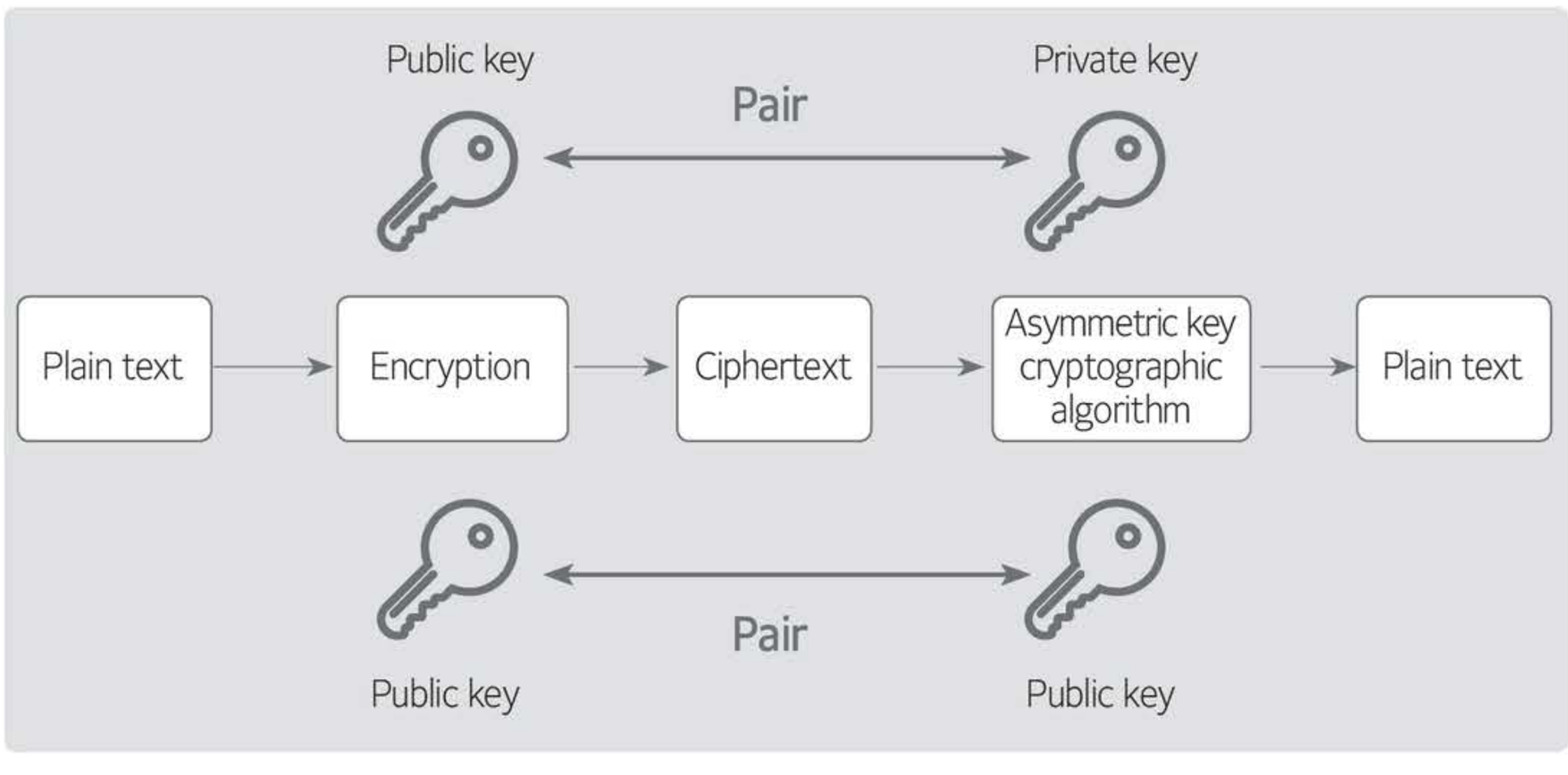
② Public key cryptographic algorithm

The public-key cryptographic algorithm became the important element of modern ciphers, since the introduction of the concept of the public key cipher by Diffie and Hellman in 1976, and the development of a practical public key cryptographic algorithm, called RSA, in 1978.



[Figure 8] Public key cryptographic algorithm

Unlike the private key encryption, the sender and receiver use different keys to establish secret communication, as shown in [Figure 8]. The sender encrypts data, using the receiver's public key, and sends the result over the network. The receiver decrypts the encrypted data, using the private key that matches the receiver's public key, to restore the plain text.



[Figure 9] Key mechanism of the public key cryptographic algorithm

The public key encryption system has the advantage of establishing secure communication using the cryptographic algorithm, even though the key is not shared with other users. Each user discloses the key that will be used to send data to them (called a public key), and has the key that can decrypt the information encrypted by their public key (called a private key). Therefore, it has the characteristic that anyone can encrypt information, but only those who have a private key corresponding to the public key can decrypt the information. For example, when there are 'n' users in the network environment, a total of 2n keys are required across the network because each user holds two keys (a public key and a private key). Each user must hold

only two keys, that is, their own private key and a public key.
The public key cipher has the advantage of being used for various authentication functions and secure key exchange, because only each user knows their private key corresponding to the public key, which can be checked by everyone. RSA (Rivest, Shamir and Adleman), ElGamal, and ECC (Elliptic Curve Cryptosystem) are the representative public key cryptographic algorithms.

• RSA

The RSA public key cryptosystem is used for encryption and authentication. The safety of this system is based on the difficulty of factoring a large integer. RSA has the characteristic that ciphertext for the same message is always the same, because no random numbers are used in the encryption process. Since the safety of the RSA system depends on prime number p and q, the prime number selection conditions are important.

• ElGamal

ElGamal was proposed in 1984 by Stanford University cryptographer, T. ElGamal, and is the first public key cryptographic algorithm, based on the difficulty of the discrete algebra problem. When a message is encrypted with ElGamal, its length is doubled. However, different ciphertext is created each time, even though the same message is encrypted because random numbers are used for encryption, which is a great advantage from the perspective of information security.

• ECC

The Elliptic Curves encryption system is based on the discrete logarithm problem on the elliptic curve. Since its safety is high and its speed is fast, it draws attention as a new public key encryption system. For example, it is known that a 1024-bit key of RSA and a 160-bit key of elliptic curve cipher have the same level of security. In addition, the ECC system is suitable for the encryption of mobile communication, such as a mobile phone with limited power supply.

③ Comparison of the private key cryptographic algorithm and public key cryptographic algorithm

<Table 4> shows the result of comparing the private key encryption system and the public key encryption system.

<Table 4> Comparison of the private key cipher and public key cipher

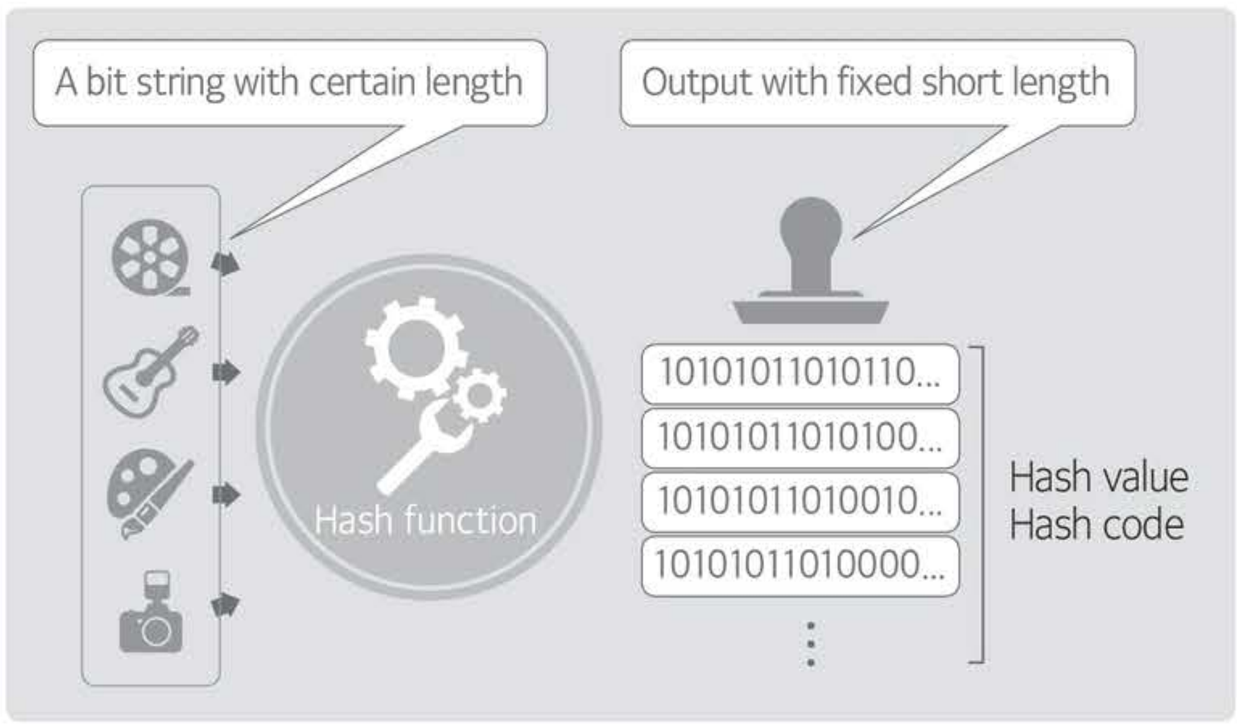
Item	Private key cipher	Public key cipher
Key relationship	Encryption key = decryption key	Encryption key ≠ decryption key
Encryption key	Private	Public
Decryption key	Private	Private
Algorithm	Public	Public
Number of keys	n(n-1)/2	2n
Number of keys to be managed per person	n-1	1
Encryption speed	High speed	Low speed
Authentication (digital signature)	Complex	Simple
Strengths	Fast encryption/decryption time Short key length	Easy key distribution. Fewer number of keys to manage. Used in various fields, such as authentication.

Shortcomings	The number of keys to manage increases as many as the number of users. The key changes frequently.	Slow encryption/decryption time. Long key length. The key does not change frequently.

F) Hash function

① Concept of the hash function

A hash function, or a hash algorithm, is a mathematical function that outputs a short hash value (hash code) with a fixed length from random data of various sizes, as shown in Figure 10. That is, the hash function compresses an input string with a random length into a string with a fixed, short length. For example, HAS-160 (Hash Algorithm Standard 160), SHA-1 outputs a 160-bit result.



[Figure 10] Hash function

The cryptographic algorithm uses keys, but the hash function does not use keys. Therefore, the same input always produces the same output. The hash function with this characteristic is used to verify the integrity that detects the error in or tampering of the message by extracting the unalterable evidence value for the input message.

② Properties of the hash function

Since the operating algorithm of the hash function is simple, it is easy to calculate h(x), when function h and input x are given, and system resources, such as a CPU and memory, are consumed relatively less. Also, the hash function should have the basic properties described in <Table 5> from the aspect of stability.

<Table 5> Basic properties of the hash function

Property	Characteristics
Pre-image resistance	• When y is given, it is difficult to find x where h(x)=y.
2nd pre-image resistance	• Given h(x)=y, it is difficult to find x where h(x')=y (however, x≠x').
Collision resistance	• It is difficult to find x and x' (however, x≠x') where h(x)=h(x')

The hash function is widely used in the security field because of its characteristic that the original text cannot be

restored using the hash value. That is, the original text cannot be restored through computation using the hash value.
Therefore, the hash function is mainly used to safely store sensitive data, such as the password, buta bypass attack can be made using hash collision, which outputs the same output for two different input values.

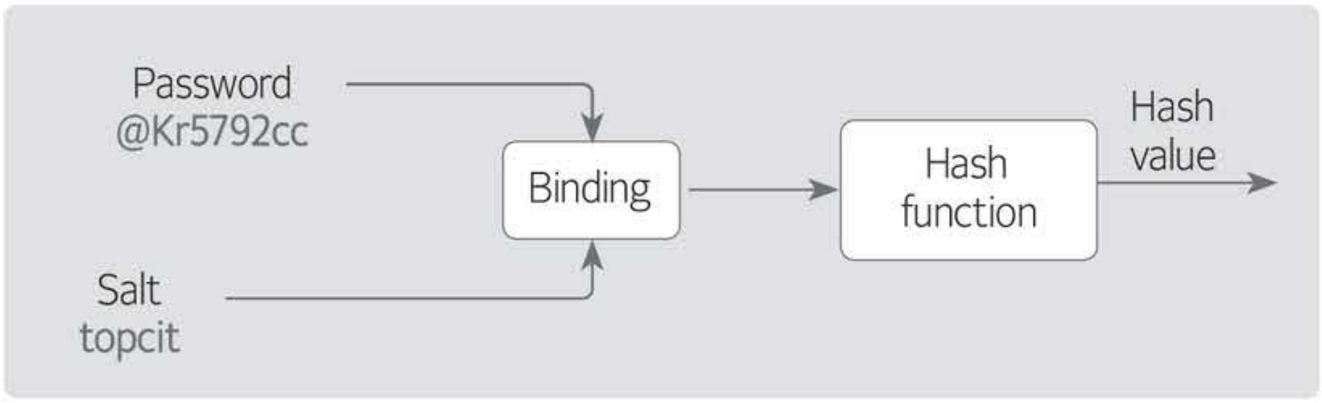
③ Types of hash functions

- MD5(Message Digest Algorithm 5)
  MD5 is a 128-bit hash function used for testing the integrity of the program or file. It was designated as RFC 1321 of the IETF. However, it is recommended to use a safer algorithm like SHA-2 for hashing purposes, because several important defects were found.
  MD5 is frequently used for saving a password. The result of hashing a password with MD5 is saved. Therefore, a server operator or a third party cannot know the original password using the hash result value of the password only stored in the system. If the user correctly inputs the password, the same hash value is returned, confirming that the password is correct.

- SHA (Secure Hash Algorithm)
  MD5, which was developed from SHA, means a set of interlinked hash functions. It was first designed by the National Security Agency (NSA) in 1993,and it was designated as the national standard in the U.S. It is also called SHA-0 to distinguish the first function from the functions designed later. SHA-1, a variant of SHA-0, was announced two years later. Subsequently, four more variants were released, such as SHA-224, SHA-256, SHA-384, and SHA-512. These are called SHA-2 as a group. Currently, SHA-3, which is completely different from SHA-1 and SHA-2, is under development, and it was confirmed as SHA-3 in 2012.
  SHA-0 and SHA-1 have a hash value of 160 bits, and SHA-224/256/384/512 provide a hash value of 224/256/384/512 bits, respectively. In addition, it is recommended to use a hash function of SHA-256 or higher for safety. On the other hand, an attack on SHA-2 has not yet been reported, but there is a possibility of an attack because SHA-2 functions use a method similar to that of SHA-1.

④ Supplementing hash functions

Salt is an arbitrary bit string that is added when a hash function generates a hash value. Salting is to generate a hash value by adding a bit string to the original message. For example, a hash value can be created by adding salt “topcit” to the password “@Kr5792cc”.
as shown in [Figure 11].



[Figure 11] Hash function and salt

When the salting method is used, an attacker cannot check whether the password matches the salted hash

value, even though the attacker finds the hash value of the password "@Kr5792cc". In addition, if different salts are used for each user, the hash values of the users who use the same password are generated differently, which significantly improves the problem of the possibility of recognition.
The hash values of the salt and password can be stored in the server database, then, when the user logs in, the input password can be checked by hashing it. It is known that to make salt and digest difficult to guess, all passwords should have their own salt, and the salt length should be 32 bytes or more.

⑤ Utilizing hash functions

• Integrity verification method

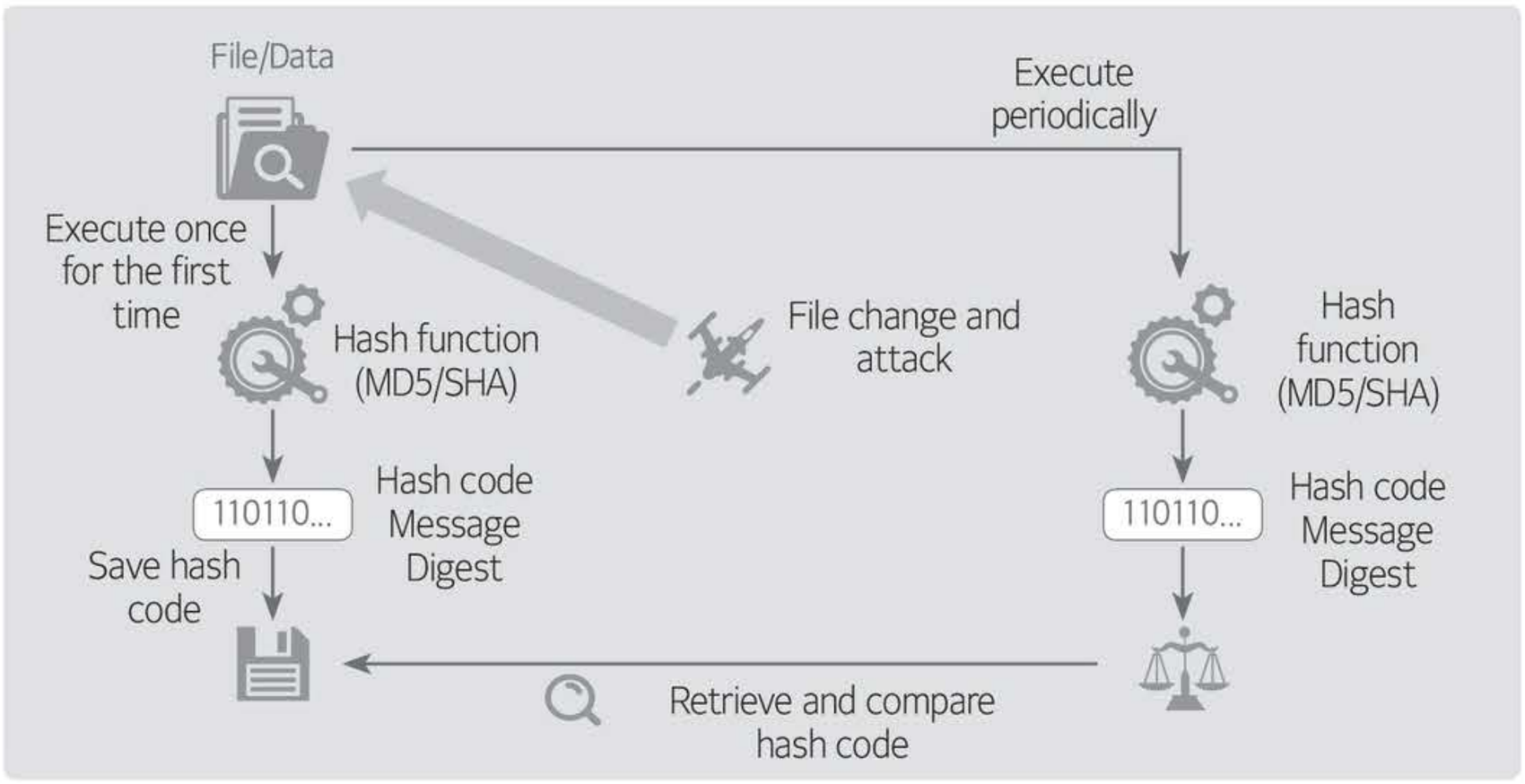
Integrity verification methods in servers or network security, are divided into the method of detecting an error that occurs while transmitting data, and the method of preventing unauthorized modification, as shown in <Table 6>. A checksum and cyclic redundancy check (CRC) are used to test integrity when an error occurs during data transmission. The checksum method, a type of duplicate test, tests integrity by adding data to obtain a checksum, converting it into a certain bit value, then adding it to the message.
CRC is mainly used as a method of verifying transmission data errors in the communication system, such as the Internet. A checksum is calculated at the sending side, based on polynomials that are easy to detect and corrected errors, and it is sent after adding it to the header. Then, the receiving side verifies integrity by calculating the checksum again, based on the same polynomial and comparing it with the received checksum.

<Table 6> Integrity verification method

Cause of change	Solution
Data transmission error	• Checksum • CRC ✔ Used for verifying data ✔ Generating numeric values with fixed length
Unauthorized change	• Hash function ✔ MD5 - Expansion of CRC - Supplementing MD2~4 - 128-bit hash function - Recommended to use SHA-1 ✔ SHA-1 - MD5 replacement and extension - Security protocol, used by programs ✔ SHA-2 - Commonly referred to as SHA265~512 - Attack methods are available against SHA1.

• File integrity

To ensure integrity when sending files on the Internet or posting them on a website, assistant manager Kim secured a method of verifying that files are not tampered. To do so, he also sends, or posts hash values that are calculated by the hash function. He also decided to manage the alteration status as shown in [Figure 12]. He makes a list of important source files managed by the server, and stores the hash value for each file, then compares the hash value in the file list with the original hash value on a regular basis.



[Figure 12] Server file integrity check

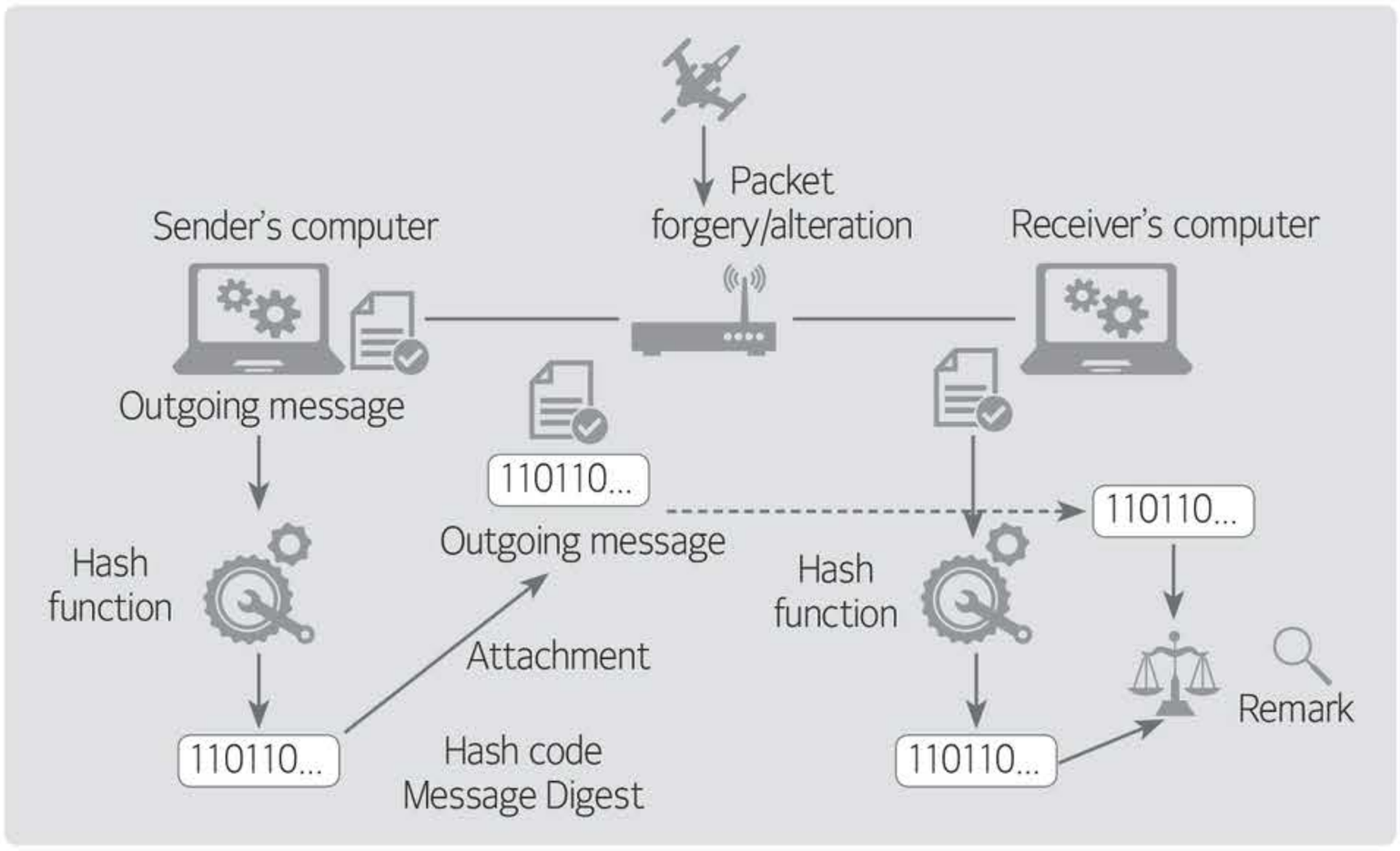
However, a security incident that has occurred between the check period cannot be detected by checking integrity periodically. The shorter the integrity check period, the better. However, if the number of files increases, creating and comparing hash values for each file increases the server load. Therefore, it's not an effective method.

Introducing an integrity check technique that can detect an error at the kernel level in real time, is an alternative to the periodic integrity check method. That is, it is more effective to only run an integrity check once and check file alteration in real time whenever the file is executed or loaded into the memory to check whether the file has been tampered. In this way, loading the tampered executable file into memory can be prevented without constantly causing a CPU load.

- Integrity during transmission

  The integrity of the message transmitted over the network is also an important security issue. A hacker can intercept and alter the transmitted message as shown in [Figure 13]. To check the integrity of the transmitted message, the sender creates a hash value for the message and transmits it along with the message. Upon receipt of the message, the receiver checks the integrity of the message and, if tampered, ignores the message.

  The hash function can be used in the form of a message authentication code (MAC), if authenticating the identity of the sender is not needed, and only the integrity of the data that has not been tampered during transmission is needed. When the sender calculates the hash value using the message as an input, it becomes a message authentication code. If this message authentication code is sent together with the message, the receiver can be confident that the message has not been tampered during transmission.



[Figure 13] Checking the integrity of the transmitted file

- Encryption based on the password
  Both the hash function and encryption are techniques of hiding the password effectively. However, there is a difference, in that the encryption algorithm can encrypt the unencrypted plaintext and then decrypt it again, whereas the hash function cannot find the original value of the hash function using the result value.
  The hash function can be used for password-based encryption (PBE). In PBE, the hash value, which is obtained by entering the result of combining the password and salt (random number generated using a pseudo-random number generator) into the hash function, is used as an encryption key. Attacks against the password can be prevented using this method.

- Electronic signature
  The hash function can be used for digital signatures. A digital signature is a method of providing both data integrity and the signature's authentication by performing a hash operation on a specific document, using the signature's private key. Signing the entire message is very inefficient because the public key operation should be repetitively performed on all message blocks. Therefore, an electronic signature can be very efficiently generated by calculating a hash value for the message and signing on that value. Although the signer signed the hash value, instead of the message itself, this signature is recognized as a genuine signature for the message because finding another message with the same hash value is difficult.

02 Authentication technology

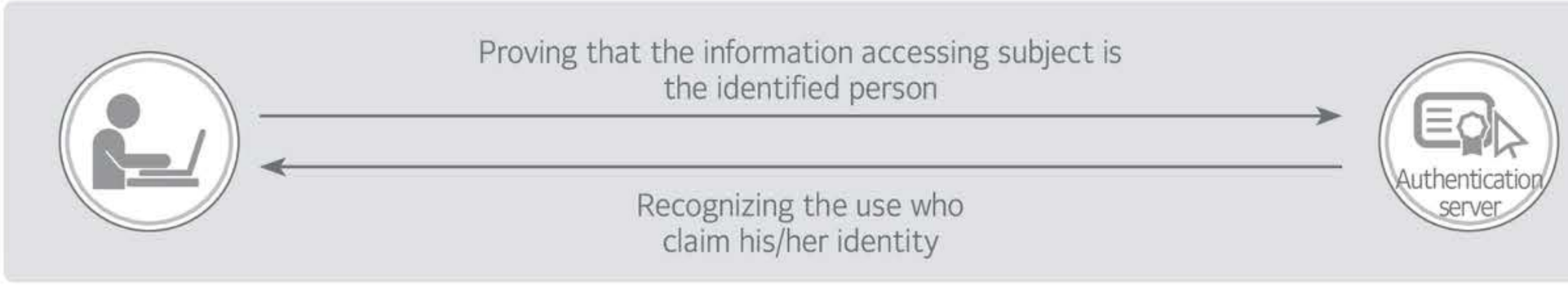
A) Concept of authentication

Authentication refers to a method of verifying whether the information exchanged between the sender and receiver, who are the subject of the information, has not been altered or deleted, and whether the subject

(sender and receiver) is legitimate. That is, authentication can be divided into message authentication and user authentication.

① User authentication

User authentication refers to a function that enables the user to prove their identity to the other party over the network. Given this, a third party should not be able to disguise as the user.



[Figure 14] User authentication

User authentication, also known as identification, is used to verify the identity of a user when logging in to a server, and to grant the authority of using information services. Servers should require the remote user to go through a strict authentication procedure because the remote user can perform all the privileges as the user in question, once authenticated.

② Message authentication

Message authentication is to check whether the contents of the transmitted message have the original information and are not altered or modified. An electronic signature can be used to verify that the transmitted message has not be altered, and to identify the sender at the same time.

B) Type of authentication methods

Authentication can be performed by using the user's knowledge, the user's object, or the user's physical characteristics.

① Knowledge-based authentication

This method is based on the user's information ("What you know"), and uses various means, such as a PIN (Personal Identification Number), password, account number, etc.

② Ownership-based authentication

This method is based on the user's possessions ("What you have"), and uses various means, such as anOTP (One Time Password), smart card, card key, etc.

③ Presence-based authentication

This method is based on the user's body or characteristics of their body ("What you are"), and uses various means, such as iris recognition, fingerprint recognition, voice recognition, and face recognition.

C) Type of authentication technologies

① Password authentication

• Overview of password authentication

The user sets the password in advance. After that, the user is authenticated by comparing the password entered during authentication, with the set password. Although this authentication technology is the most widely used, it requires careful attention when using it because it is the most insecure as shown in [Figure 15].

[Figure 15] Vulnerabilities of the password authentication method

• Password policy

When creating a password, it should have at least 8 digits by combining uppercase letters, lowercase letters, numbers, and special characters. The user should be able to remember the password easily, but the attacker should have difficulty guessing it.

Passwords should not be saved in plaintext, but should be saved using a hash function, rather than a two-way encryption algorithm. The authentication system should limit the number of failed login attempts.

• Attack techniques against the password

Attack techniques against the password include brute force attacks, dictionary attacks, Trojan horses, direct access to the password file, social engineering techniques, etc.

• Countermeasures against password attacks

Various countermeasures can be implemented, such as using a password generator, limiting the number of login failures, changing passwords periodically, using an intrusion detection system (IDS) to detect dictionary attacks and brute force attacks, implementing security awareness training, using an OTP, etc.

② One Time Password (OTP) authentication

• Concept of the OTP

An OTP is one of the methods used by the authentication system to authenticate users. This authentication technology uses a one-time password generator that generates and inputs a one-time password for each session.

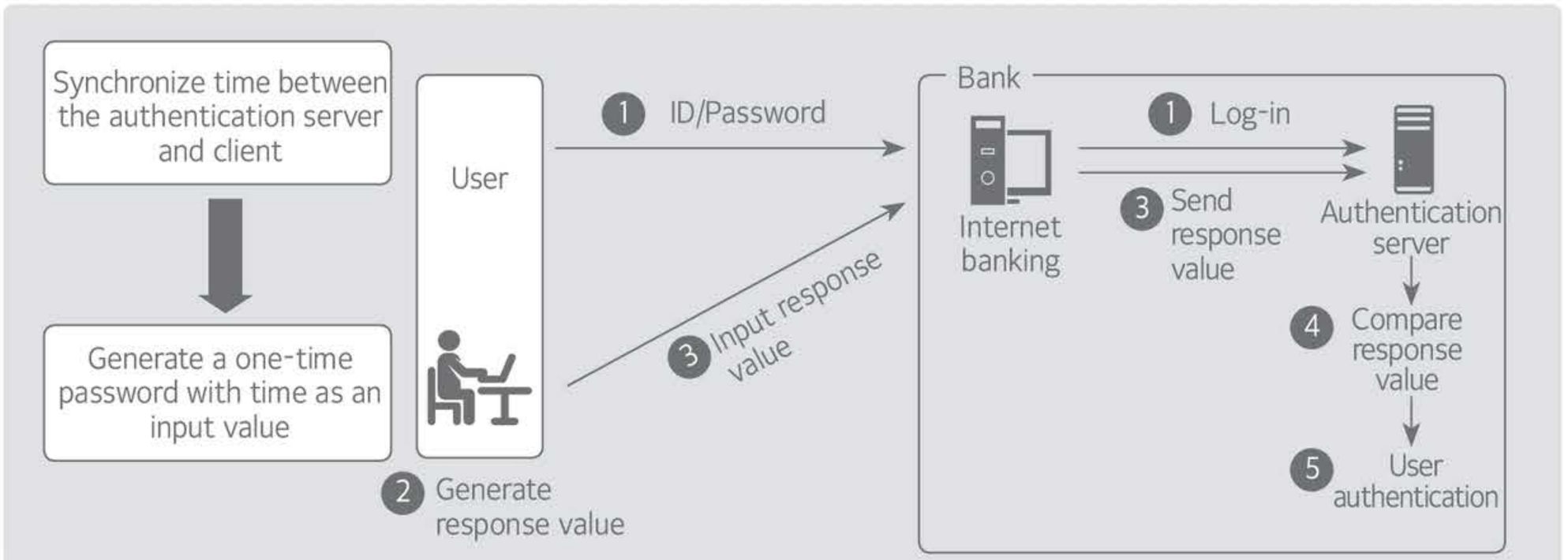
• Type of OTPs

The OTP can be largely classified into the synchronous and asynchronous types, as shown in <Table 7>.

<Table 7> Type of OTPs

	Item	Contents
Synchronous	Challenge-response	An authentication server generates a random number and sends it to the client, and the client generates a one-time password using the random number as an input value.
Asynchronous	Time-synchronous	The authentication server and the client are synchronized, and a one-time password is created by using the time as an input value.
	Event-synchronous	The authentication count record is shared with the authentication server, and a one-time password is created by using the authentication count as an input value.

[Figure 16] shows the OTP operating procedure of the time-synchronous type.



[Figure 16] Operating procedure of the time-synchronous type

③ Biometric authentication

• Concept of biometric authentication
Authentication technology to extract the measurable physical or behavioral features of a person, using an automated sensor, and to use it as a means of authentication.

• Characteristics of biometric authentication
Universality: Each person must have the characteristic used by the system.
Distinctiveness: The characteristic must be distinguishable.
Acquisition: The characteristic can be measured and quantified from the sensor.
Permanence: The characteristic must not change or modify during the human life.
Accuracy: The characteristic that requires authentication precision, regardless of environmental changes.
Acceptability: The acquisition phase should not be intrusive and the system should be user-friendly.

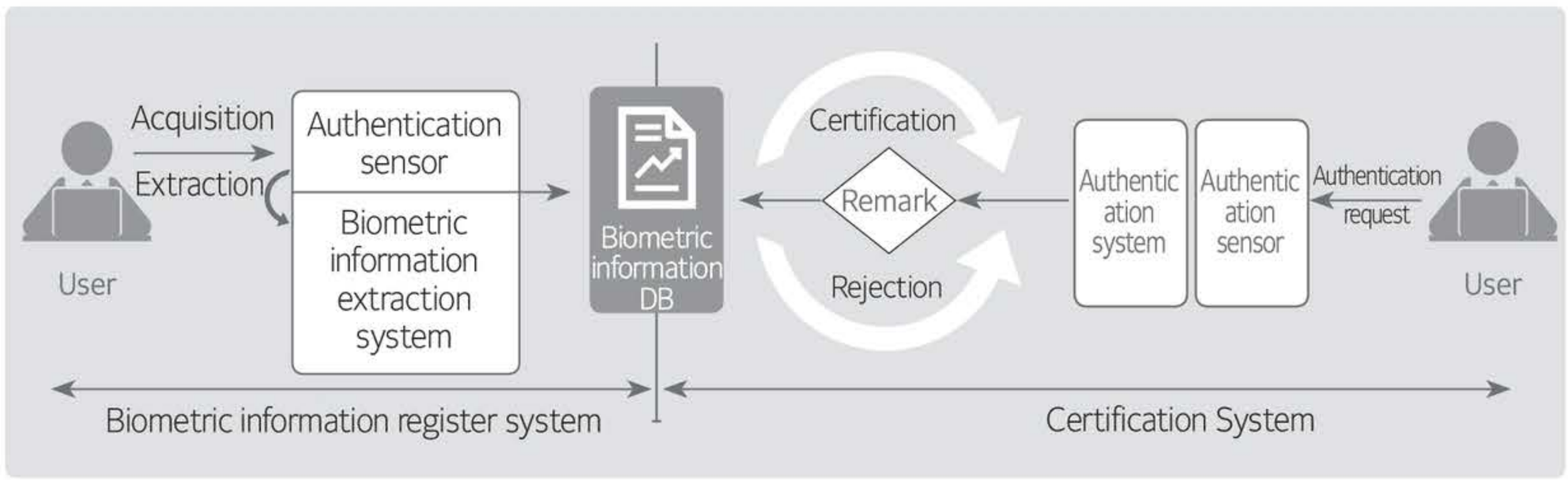
• Types of biometric authentication
As shown in <Table 8>, the types of biometric authentication can be divided into a method using body information and a method using behavioral characteristics.

<Table 8> Types of biometric authentication

Item	Type	Description
Body	Fingerprint	Semiconductor, optical, and mixed types are available. Fingerprint recognition occupies the largest market share.
	Iris	Iris scanning recognition is very accurate and fast, but it requires an expensive biometric system.
	Face	A face contains and provides recognition information, and is the most natural authentication method.
	Vein	Vein recognition checks the vein shape to recognize the pattern.
	DNA	DNA is the most accurate authentication method.
Behavior	Signature	Since a signature has a certain pattern, it can be identified not only by the final signature form, but also by a kind of trajectory of hand movement.
	Voice	Voices are frequently used by physical access control applications.

• Process of biometric authentication

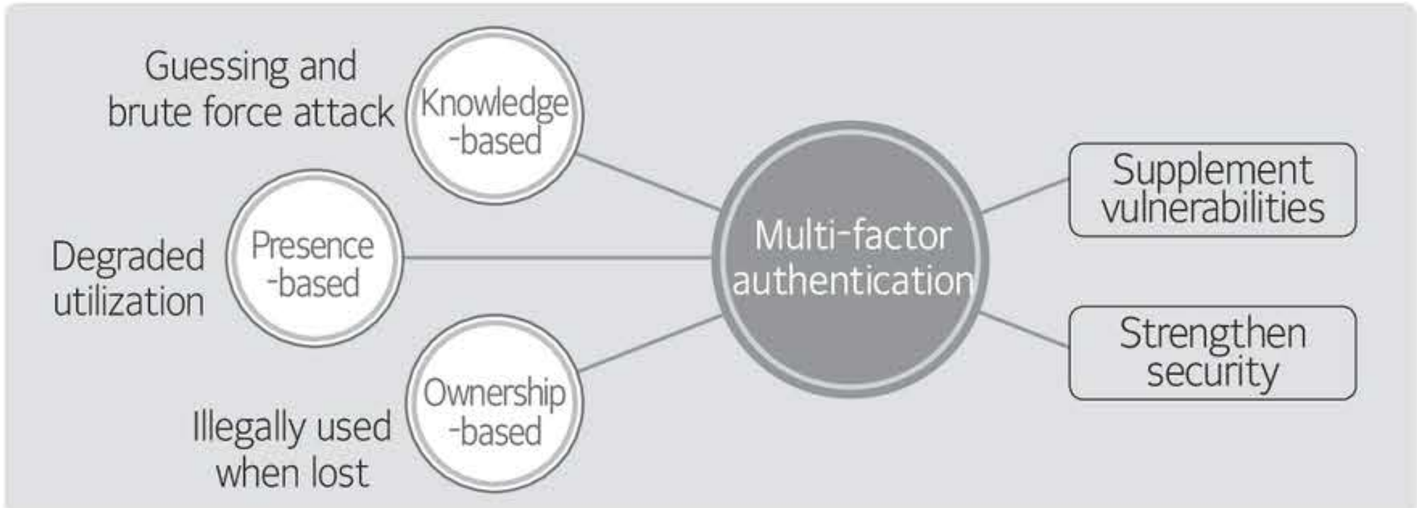
As shown in [Figure 17], the biometric authentication system consists of a “biometric information registration system” and a “biometric authentication system”. The user’s biometric information is stored in the biometric database in advance, and authentication is performed by comparing the data saved in the biometric information database, with the biometric information extracted from the user.



[Figure 17] Process of biometric authentication

④ Multi-factor authentication

As shown in [Figure 18], multi-factor authentication is a method of improving the security of authentication by combining multiple authentication technologies to supplement the weakness of a single authentication method.



[Figure 18] Concept of multi-factor authentication

To implement a more powerful multi-factor authentication system, it is desirable to mix and use various authentication technologies, based on knowledge, ownership, and presence, such as OTP + fingerprint recognition.

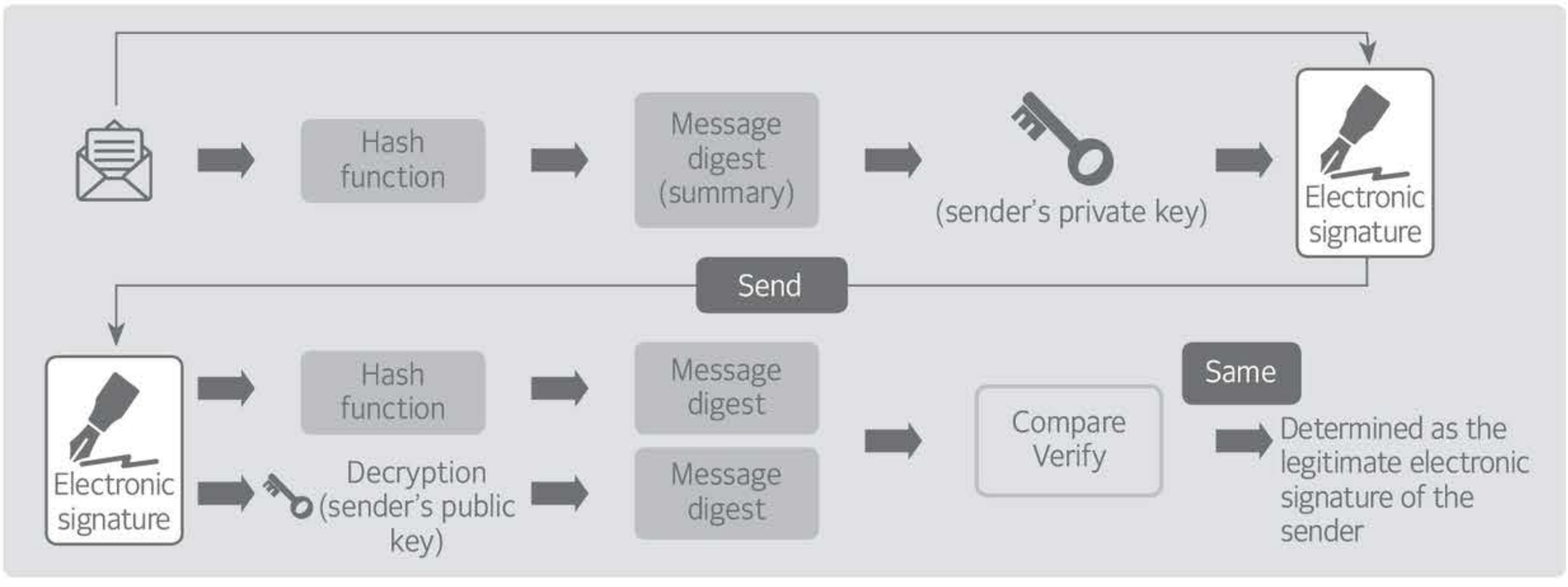
D) Electronic signature

① Concept of the electronic signature

An electronic signature is a technology that enables the user to sign on an electronic document using the authentication function of encryption technology, as shown in [Figure 19]. The effect of an electronic signature can be obtained by authenticating the identity of the signer, by using the authentication function of the public key cryptographic technique, while authenticating an electronic document to be signed at the same time.

The basic assumption of the public key encryption system is that the user (owner) will securely and secretly keep the private key (secret key), which becomes a pair of the public keys. If a certain signing operation is performed using the private key in this environment, it can only be performed by the user who has the private key, and the result can be recognized as the user's signature.

The sender sends a message using public key cryptographic techniques, together with an electronic signature, which is the result of encrypting the message digest (hash value of the message) with the private key. Then, the receiver checks the sender authentication, non-repudiation, and message integrity, by comparing the result of decrypting the sender's message, using the received electronic signature with the message digest value that was calculated by using the received message.



[Figure 19] Concept of the electronic signature

② Requirements for a secure digital signature algorithm

- Forgery prevention: Anyone other than a legitimate signer shouldn't be able to forge the signature.
- User authentication: The signer should be identifiable from the electronic signature.
- Non-repudiation: The signer should not be able to deny that the signer has signed the document.
- Alteration prevention: A signed document should not be changeable.
- Reuse prevention: A signature for one document cannot be reused as a signature for another document.

③ Operation of the electronic signature

The operation of the digital signature consists of six phases as shown in <Table 9>.

<Table 9> Operation procedure of the electronic signature

Order	Description
Phase 1	The sender generates a message digest, a fixed-length string, by applying a hash algorithm to the message to be sent.
Phase 2	The sender creates an electronic signature by encrypting the created message digest using the sender's private key.
Phase 3	The sender sends a message and digital signature to the receiver.
Phase 4	The receiver extracts the message digest generated by the sender, by decrypting the received digital signature using the sender's public key.
Phase 5	The receiver generates a new message digest by applying the same hash algorithm as the sender to the received message.
Phase 6	The receiver compares the message digest received from the sender, with the receiver's message digest. If they are the same, it is regarded as the electronic signature of the legitimate sender.

E) PKI (Public Key Infrastructure)

① Definition of PKI

PKI is an infrastructure for managing the public key, which is an essential element for encryption and authentication required for secure transactions. This infrastructure safely distributes encryption and decryption keys, as well as certificates that provide information security services. PKI is a network structure of objects that sets up and provides policies, means, and tools, which makes the use of certificates and encrypted communication easy in various application fields that require secure communication, such as information system security and electronic commerce.

② PKI components

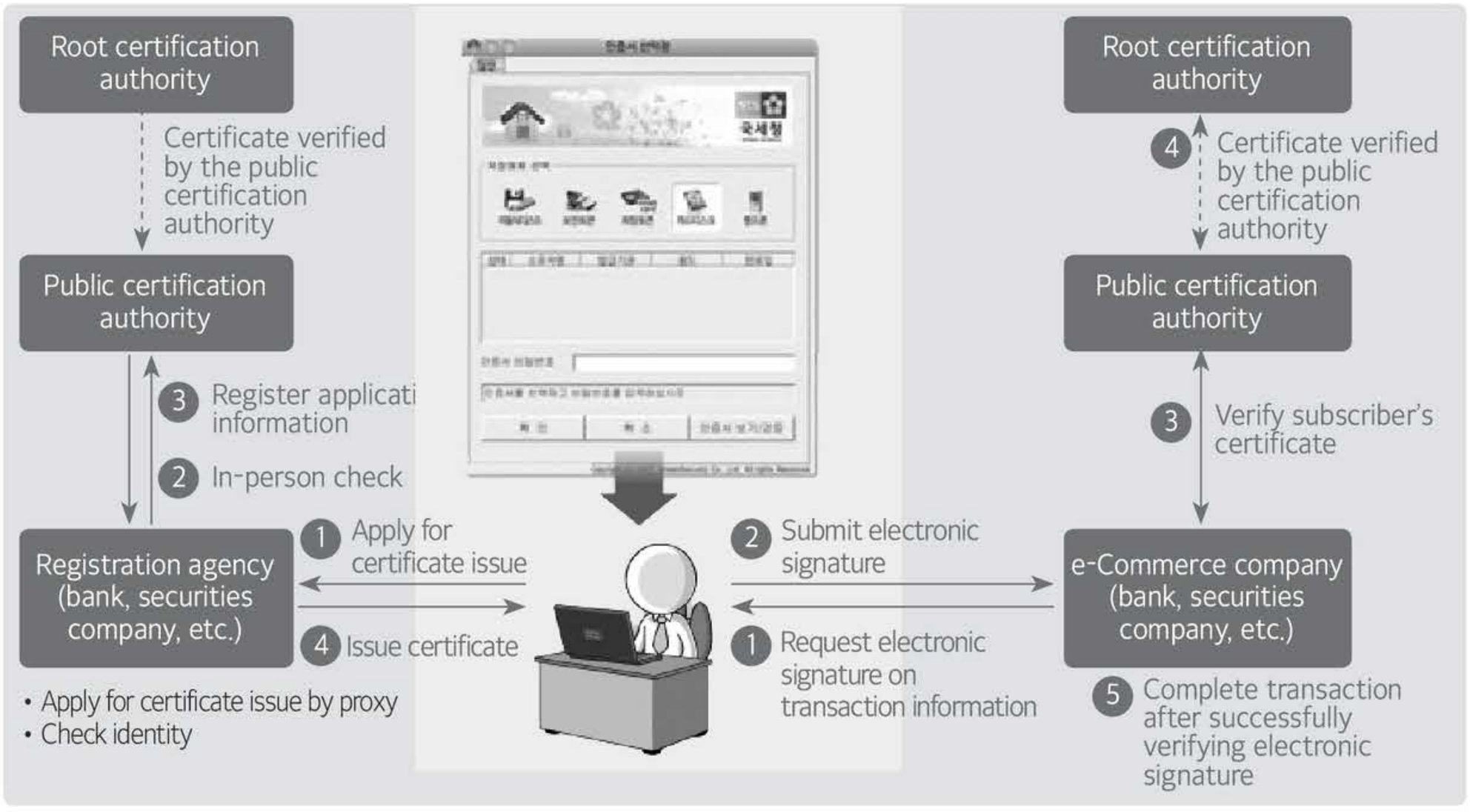
As shown in <Table 10>, the PKI is composed of the policy approval authority (PAA), policy certification authority (PCA), certification authority (CA), registration authority (RA), and public certificate.

<Table 10> PKI components

Composition	Details
Policy approval authority (PAA)	Creating and setting up policies and procedures comprehensively used for PKI (Ministry of Security and Public Administration)
Policy certification authority (PCA)	Establishing detailed policies for the policy approved by the PAA (Korea Internet & Security Agency)
Certification authority (CA)	Issuing user's public key certificates and managing the list of revoked certificates (Korea Information Certificate Authority, Koscom, Korea Financial Telecommunications and Clearings Institute, Korea Electronic Certification Authority, KTNET)
Registration authority (RA)	Doing business for certification authorities and receiving public certificate registration applications (banks, securities companies)
Certificate holder	The owner of the public key certificate who receives a certificate, and signs and encrypts electronic documents.
User	A user who verifies the authentication path and electronic signature, using the public key of the certification authority.
Public key certificate and CRL repository	Using the certificate standard that complies with the X.509 v3 standard. An electronic file that proves the relationship between the electronic signature verification key and the key owner. A CRL repository to manage the list of revoked certificates

③ PKI operation

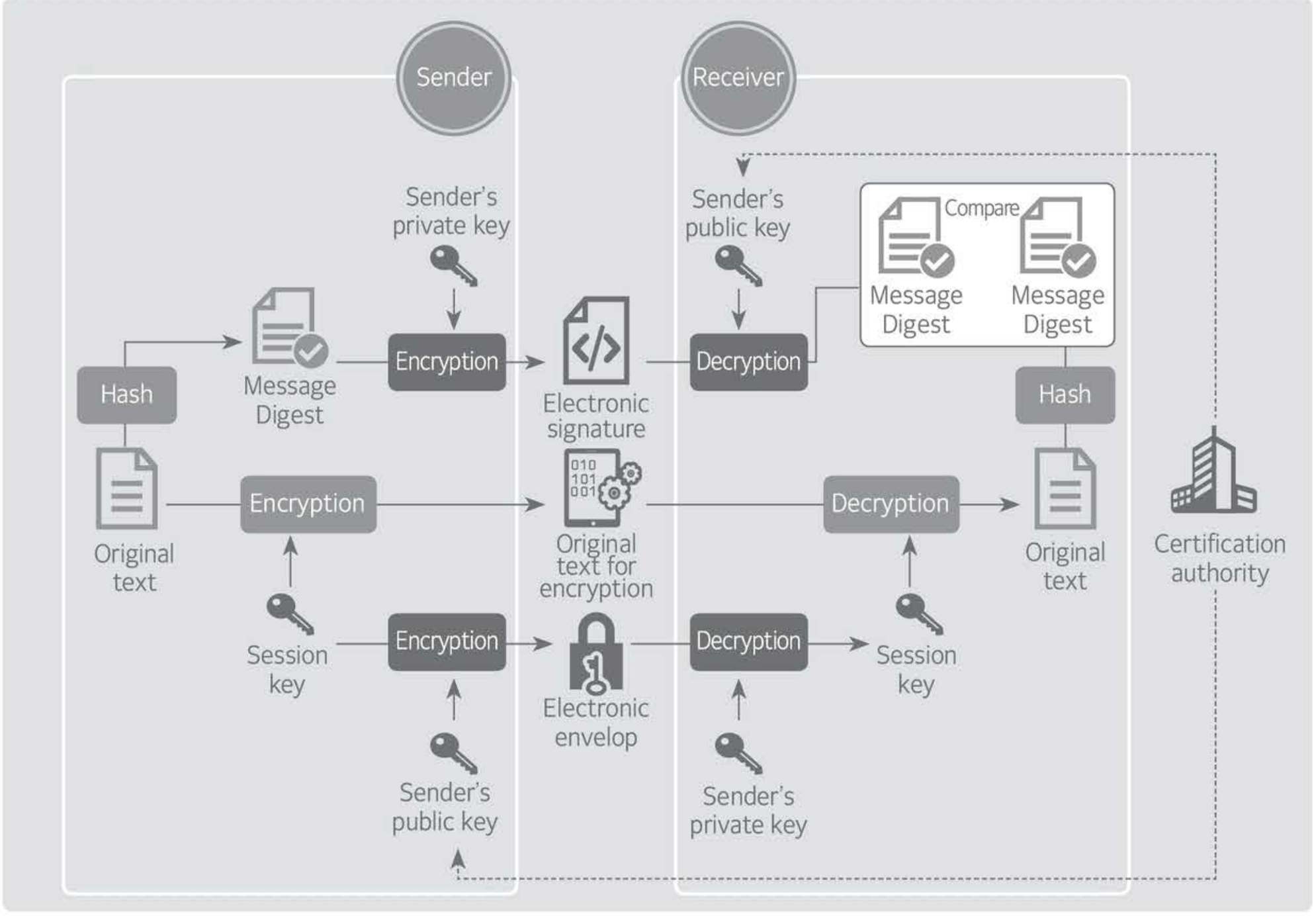
When the user requests certificate issuance to the RA after applying for subscription and checking identity at the RA branch, the RA sends the issuance and registration request information to the CA. The CA issues a private key signed with the CA's private key, and posts it to the directory server,then sends it to the user, via the RA. The user stores the issued certificate in a hard disk or a removable disk of a PC and uses it in financial transactions and electronic commerce. At this point, financial institutions verify the certificate by contacting the public CA. [Figure 20] shows the participants of the PKI and the workflow between them.



[Figure 20] Participation factors and workflow of the PKI

④ Electronic signature and encryption in PKI

[Figure 20] describes the process for user authentication and message confidentiality, and <Table 11> describes the main operation steps of the sender and receiver in the PKI environment,which is when both the sender and the receiver operate the public certificate encryption system. The session key in [Figure 21] is a one-time secret key, generated by the sender, to apply the secret key system to the message. The sender encrypts this key, using the public key of the receiver,to safely transmit it. This encrypted session key is called an electronic envelope.



[Figure 21] Electronic signature and encryption processing procedure in the PKI

<Table 11> Operation steps of the sender and receiver

Item	Order	Description
Sender	Phase 1	Creating a message digest by applying a hash algorithm to the original message
	Phase 2	Encrypting the created message digest, with the sender's private key, by applying a public key cryptographic algorithm (generating an electronic signature)
	Phase 3	Encrypting the original message, with a session key, by applying the private key cryptographic algorithm
	Phase 4	Encrypting the session key used for encryption, with the receiver's public key (e-envelope)
Receiver	Phase 1	Generating a message digest, by decrypting a document that is electronically signed with the sender's public key
	Phase 2	Extracting the session key, by decrypting the encrypted session key, with the receiver's private key
	Phase 3	Decrypting the encrypted original text using the extracted session key
	Phase 4	Creating a message digest, by applying a hash algorithm to the decrypted message
	Phase 5	Comparing the two generated message digests

⑤ Public key certificate

Public key certificates are X. Public key certificates are issued by a public CA by complying with the X.509 standard. Public certificates include the NPKI certificates, which are used by the public for financial transactions and e-commerce transactions, and the GPKI certificate, which are used by administrative agencies for administrative work.

The public certificate encryption system began to be advanced in 2011, and the length of the digital signature key of the RSA algorithm has been increased from 1,024 bits to 2,048 bits.The hash function was replaced by SHA-256 (a hash function producing a 256-bit value), instead of SHA-1 (a hash function producing a 160-bit value). <Table 12> shows the main contents included in the NPKI certificate.

<Table 12> Main contents of the public key certificate

Contents	Description
Version	Version of the certificate format
Serial number	A unique integer value that represents the certificate serial number of the issuing CA
Algorithm identifier	A signature algorithm OID (Object Identifier) used to generate the certificate
Issuer	The DN (Distinguishing Name) of the CA that issued the certificate
Period of validity	The validity period of the certificate. The start and expiration dates are represented in seconds.
Subject	The DN of the certificate owner.
Public-key information	The subject's public key and the identifier of the algorithm that will use this key.
Signature	Signed with CA's private key.

⑥ Method of verifying the validity of the certificate

- CRL (Certificate Revocation List)

  CRL refers to the list of certificates revoked by the CA. The list contains the serial number, the revocation date, and the reasons for revocation. According to RFC 3280, the certificate can be permanently revoked or temporarily held. The CRL should be periodically downloaded from the CRL distribution point. If the download cycle is too long, a revoked certificate can be used. If the cycle is too short, the overhead increases each time the certificate is used.

- OCSP (Online Certificate Status Protocol)

  This protocol makes up for the shortcomings that the CRL should be periodically updated. When the user attempts to gain access, the OCSP protocol immediately answers the validity of the certificate by requesting certificate status information in real time. The protocol is defined in RFC 6960, and generally uses a server configured with the HTTP.

03 Access control technology

A) Overview of access control

① Concept of access control

Access control refers to the task of controlling who can access a system, and which task the user can perform when the user interacts with the system. Specifically, access control consists of three parts: identification, authentication, and authorization.

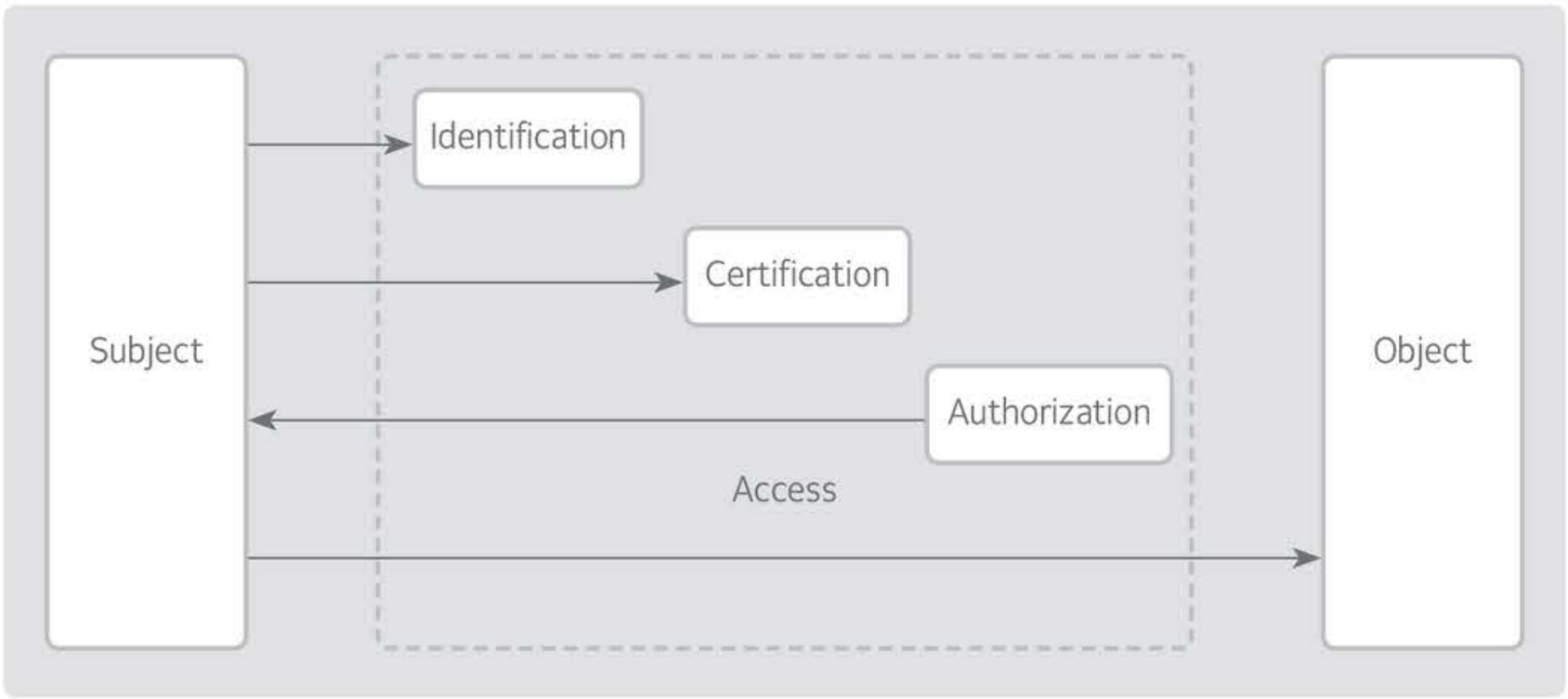
- Identification
  A process of identifying a subject using its unique token, that is, a process where the system identifies the subject. (e.g., ID, employee card, biometrics)

- Authentication
  A process where the subject verifies its identity to the system, that is, a process where the system acknowledges the user who claims his/her identity (e.g., password (knowledge-based), certificate (ownership-based), OTP (ownership-based), biometrics (presence-based)).

- Authorization
  A process when the system controls the task and object, which can be performed and accessed by the authenticated user (e.g., mandatory access control, discretionary access control, role-based access control).

② Access control performing procedure

An object can be accessed only when the right to access is obtained through the authorization process after identification and authentication.



[Figure 22] Procedure for performing access control

B) Access control policy

The system security policy is the high-level instructions for designing and managingthe access control system. In general, the policy is the expression of the basic principles, desired by the organization, to protect target system resources. That is, the access control principle defines the subject (who), time (when), location (where), object (what), and behavior (how) that can be accepted or refused. The access control principle, which limits the scope of access, can be divided into the following two basic policies:

① Minimum privilege policy

This policy is called the "need-to-know" policy. System subjects should use the minimum amount of information that is needed for their activities. This policy has the effect of applying strong control over object access. However, sometimes this policy may impose excessive useless limitations on the legitimate subject.

② Maximum privilege policy

This policy is based on the principle of maximum availability that is applied to increase the benefits of data sharing. That is, this policy can be effectively applied to the case when no special protection is needed, due to the high reliability of data exchange with the user.

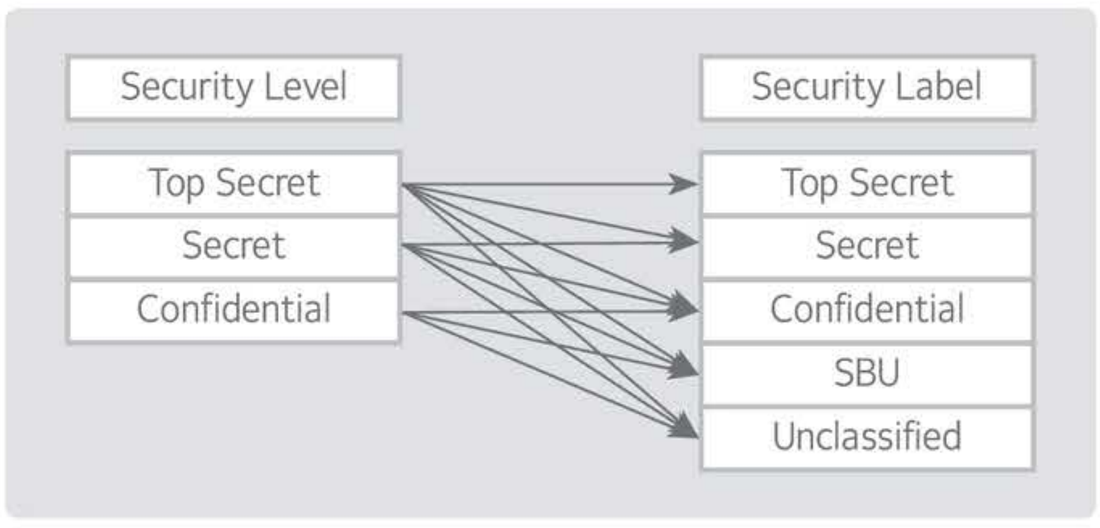
C) Types of access control policies

This policy is designed to implement an access control system that only allows authorized users to access information resources.

Representative access control policies include mandatory access control, a discretionary access control policy, and a role-based access control policy.

① Mandatory Access Control (MAC)

A security level is given to the subject and a security label is given to the object. Then, it is determined whether the subject in question can access the object, according to the predetermined rule. This policy is mainly used for military purposes. A strong security system can be maintained, but its management efficiency is deteriorated.

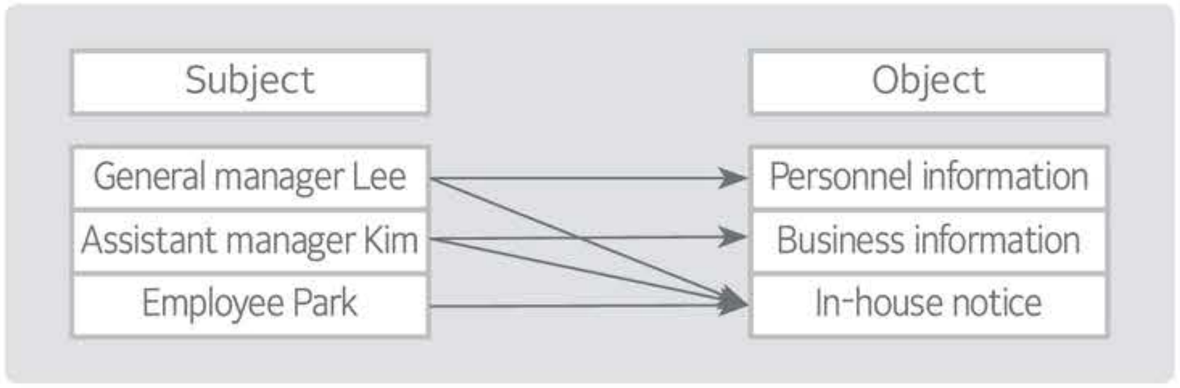


[Figure 23] Mandatory access control

② Discretionary Access Control (DAC)

Access to an object is controlled by the identity of the subject's account or the account's belonging group.

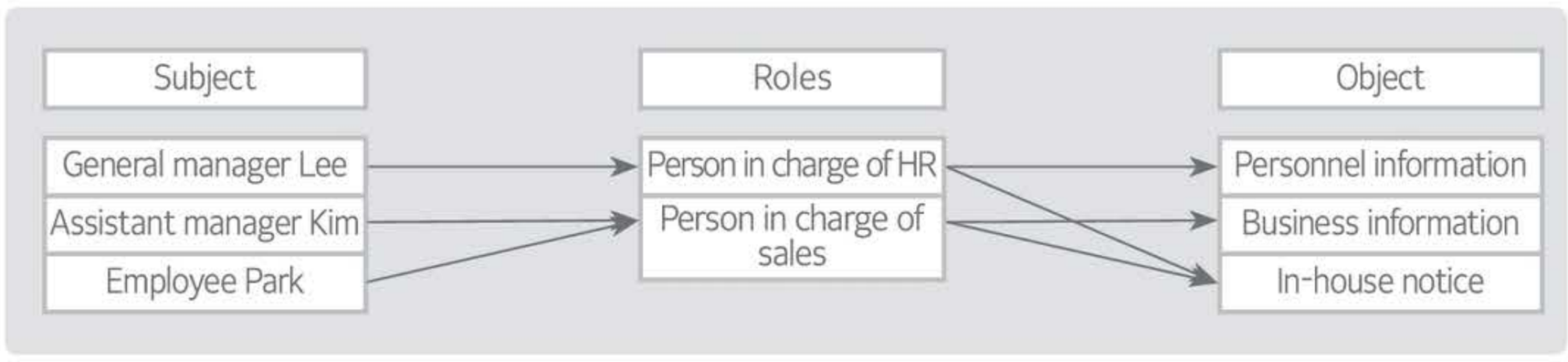
The owner of the object determines access permission. This policy is mainly used for the system access control of Unix or Linux systems.



[Figure 24] Discretionary access control

③ Role-Based Access Control (RBAC)

The administrator defines roles in advance and maps the object that can access each role. Then, a role is given to the subject for access control. This policy can be used by organizations or systems with frequent changes. Management efficiency can be improved, but security can be degraded.



[Figure 25] Role-based access control

D) Access control mechanisms

① Access control matrix

Subjects and objects are represented in rows and columns, and each entry in the matrix represents access rights. All relationships between the subjects and the objects are managed in a matrix. Since it is inefficient to search a matrix to access a specific resource, it is divided into a capability list and an access control list for easy management.

		Object			
		Object 1	Object 2	Object 3	Object 4
Subject	User A	Read, write	Read	Read, write	No access
	User B	Read, write	Read, write	Read, write	Read, write
	User C	Read	No access	No access	No access
	User D	Read, write	Read, write	No access	No access

[Figure 26] Access control matrix

② ACL(Access Control List)

The access rights of the subject are managed based on the object. The list corresponds to the column of the access control matrix.

③ CL (Capability List)

Based on the subject, the rights to access the object are managed in a linked list format. The list corresponds to the row of the access control matrix.

④ SL (Security Label)

SL refers to a set of security attribute information assigned to an object.

E) Access control models

① Bell-Lapadula model

The first mathematical model that was designed, with the support of the U.S. Department of Defense, as an access control model (MAC policy) based on compulsory policies. This model emphasizes confidentiality. It puts emphasis on secret leakage prevention, rather than illegal information destruction or alteration, and it prevents information from flowing from the high level to the low level.

② Biba model

A model designed to guarantee integrity, which is the shortcoming of the Bell-Lapadula model (however, confidentiality is not guaranteed). This model deals with integrity as an item that is accessed by the subject.

③ Clark and Wilson model

A model designed for commercial use with a focus on integrity. This model assumes that alteration prevention can be more important than secret disclosure prevention, depending on the characteristics of the information, when handling the security requirements of the application. In this model, only programs can access the object all the time.

④ Chinese wall model (Brewer-Nash)

A model that blocks the flow of any information that causes a conflict. This model prevents conflicts of interest and applies the concept of task separation to access control.

III. Latest information security technology

▶▶▶ Subject

Understanding the latest information security threats and response technologies

▶▶▶ Recent trends and major issues

New types of cyber-attacks emerge, such as the combination of cyber-attacks and social engineering techniques, and cyber convergence attacks, by combining various cyber-attack technologies, etc. Accordingly, the security threats of the financial IT environment are gradually becoming more intelligent, advanced, and diversified. As IoT and big data emerge as core technology that can influence the competitiveness of companies and countries in the future,a specific plan for applying security is urgently requiredto fully promote those technologies.

▶▶▶ Learning objectives

To be able to explain the latest information security threats and countermeasures.

To be able to explain information security technology for responding to security threats in a cloud environment.

To be able to explain information security technology for responding to security threats in a big data environment.

To be able to explain information security technology for responding to security threats in a web/mobile environment.

▶▶▶ Keywords

APT, smishing, spear phishing, ransomware, “fileless” attack, Malvertising, IoT security, security by design, privacy by design, cloud security, hypervisor infection, virtual machine attack, virtual machine portability, independence between VMs, hypervisor detection technique, VM detection technique, PPDM, personal information de-identification, pseudonymization, aggregation, categorization, data masking

✚ Preview for practical business Latest information on security threats and response technologies

Recently developed home appliances, such as refrigerators and TVs, were hacked in company A. Many customers who have purchased those products, have reported an incident of receiving millions of spam emails to the customer center. On the other hand, IoT security breach incidents occur in company B. Smartphones that they have recently developed and launched were infected with a malicious app, which remotely controlled the vehicle electronic control device through a wireless communication network.

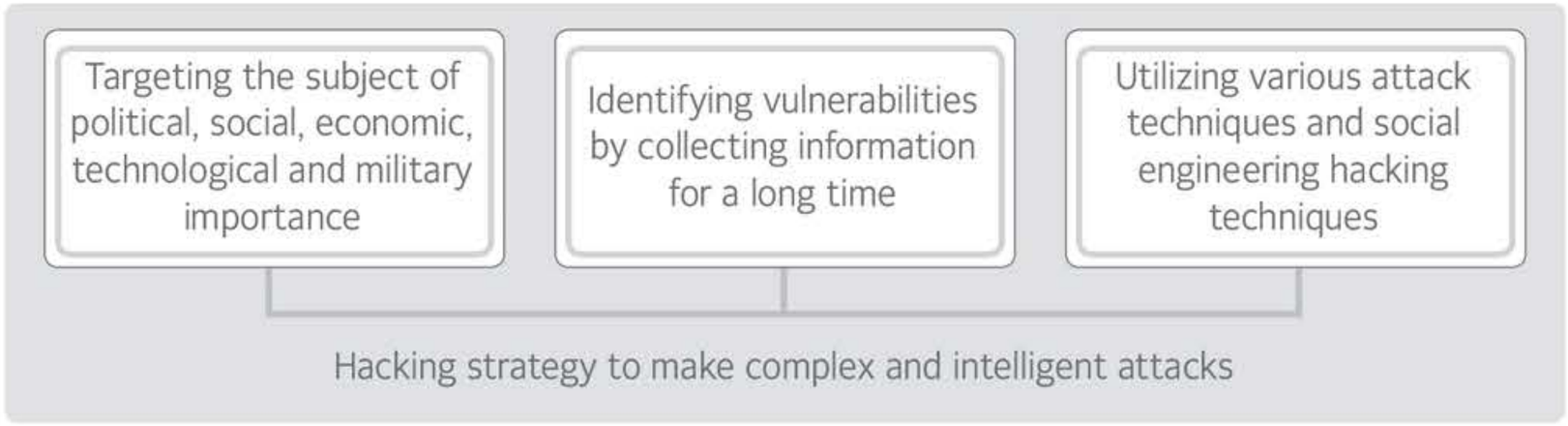
As described, numerous products with the latest technology are released, and various attempts are being made to hack those products.

In this section, we will learn the type of the latest information security threats and available countermeasures.

01 Latest information security threats

A) APT (Advanced Persistent Threat) attacks

① Concept of the APT attack



[Figure 27] Concept of the APT attack

② Procedure of the APT attack

An APT attack is made through several processes, such as infiltration, search, collection, and leakage stages.

- Stage 1: An attacker infects vulnerable systems or employee PCs with malware.
- Stage 2: The attacker infiltrates the internal network using malware.
- Stage 3: The attacker collects information on the infiltrated internal system and infrastructure and prepares for attacks.
- Stage 4: The attacker steals important information from the vulnerable system to destroy the system and make a DoS attack.

③ Cases of the APT attack

- In Korea, the computing network of financial institution N was paralyzed in 2011, due to data deletion by hacking.
- The information of 1.75 million customers was leaked, due to the hacking of financial institution H.
- The information of 35 million customers was leaked, due to the hacking of portal company N.

④ Countermeasures against the APT attack

<Table 13> Countermeasures against the APT attack

Countermeasures	Contents
Strengthening security management, operation, and education	• Analyzing the overall security threat of the organization and reorganizing the security system, by analyzing various vulnerabilities, based on the analysis of the target security system. • Management is required, including continuous management, constant security control, and regular mock hacking, with a focus on the security management organization for continuous operation.
Endpoint security	• The endpoint is the primary target of the APT attack, and malware can infiltrate into the endpoint using media, such as the Internet, e-mail, SNS, messenger, P2P, USB, etc. • OS security update, security software installation and operation, and application control based on the whitelist are needed.

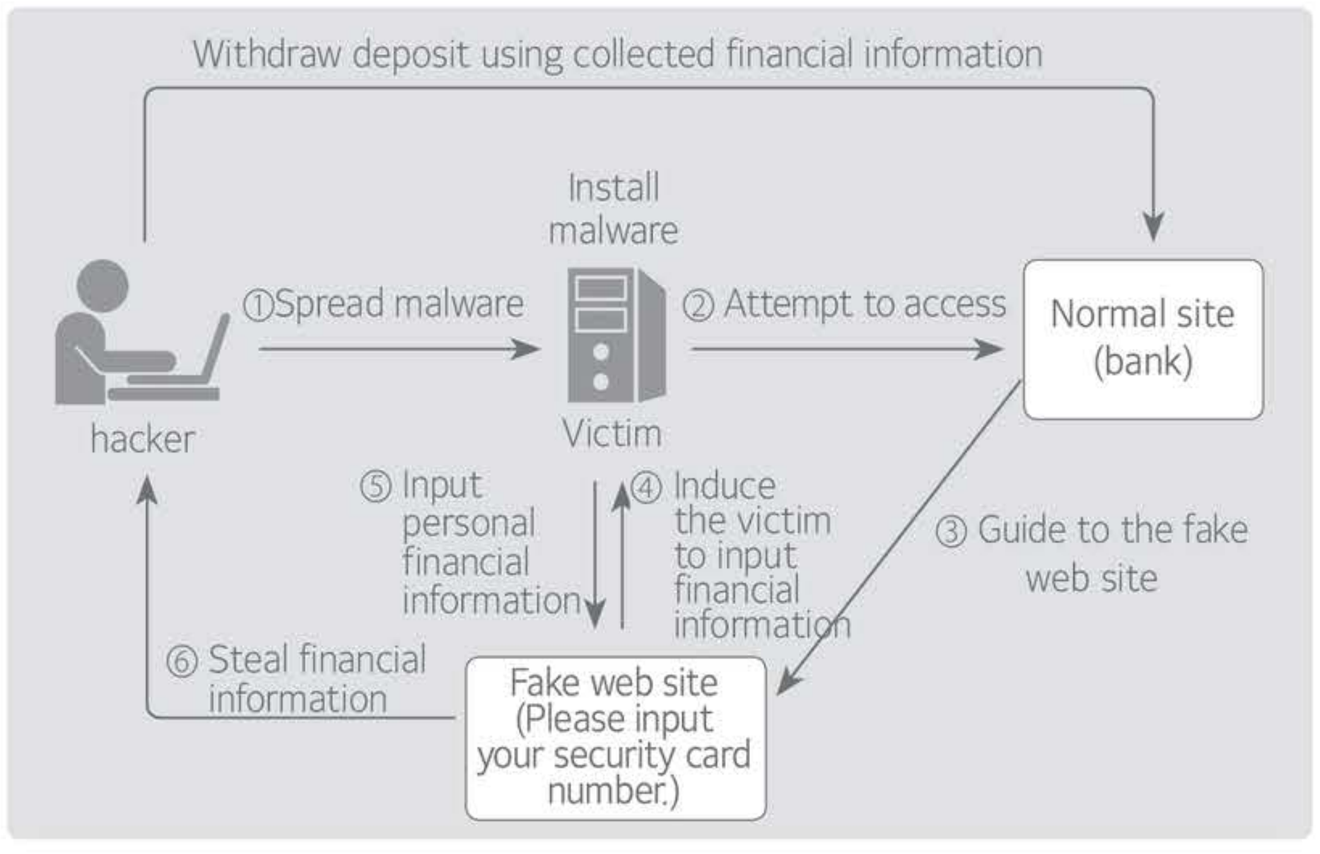
Access right management	• Management of access rights to important information, minimization of access rights, and subdivision of information rights, according to the importance of the information. • Person and device authentication, strategic management of rights, and automatic allocation and collection of rights for the information of high importance.
Important information encryption and DLP	• Encrypting data before saving, as the ultimate goal of the APT attack is data. • Solutions, such as DLP (Data Loss Prevention), are needed to be introduced, because information can be leaked in various ways, depending on the storage type of the important information.

B) Pharming

① Concept of a pharming attack

A pharming attack refers to scamming that causes illegal financial fraud or personal information leakage, by stealing financial information or access information when the user accesses the web site of the financial company or portal. The user is automatically guided to the pharming (fake) site, due to the altered host file (C:\windows\system32\drivers\hosts) or the altered "Favorites" of the web browser in the PC that is infected with the malicious code.

② Procedure of performing the pharming attack



③ Countermeasures against the pharming attack

- Strengthen the security level by clicking the [Internet Options] menu of the web browser and selecting the [Security] tab.
- Keep the anti-virus program up-to-date and check for malware infection on a regular basis.
- Frequently check whether the PC host file (C:\windows\system32\drivers\hosts) is forged or altered.

C) Qshing

① Concept of Qshing

Qshing is a compound word of "QR code" and "fishing" of personal information and financial information. This

attack technique induces users to connect the malicious link or infect the user's device directly using a QR code.

② Procedure of the Qshing attack

Infecting the user's smartphone with a malicious code so that the user is connected to a fake financial site (phishing site), even if the user accesses a normal financial site → Inducing the user to install a malicious app by showing a QR code on a fake financial site, as if additional authentication is required → Stealing personal information, such as the security card, phone numbers, and text messages, using the malicious app and manipulating the mobile environment, such as blocking text message reception and call forwarding service set-up. → Causing financial damage, such as small amount payments, money transfers, etc.

③ Combining Pharming and Qshing

It was found that malware is evolving into a form that combines pharming, targeting the Internet banking of the existing PC, and Qshing, targeting the financial information of the smartphone.

④ Response to QR code-related attacks

Keep the security of application software, such as an anti-virus program, a web browser, etc.,up to date to prevent damage caused by QR code-related malware. In addition, disable the "Allow Installation from Unknown Sources" option in the smartphone toprevent the malicious app from being installed through QR codes.

D) Smishing

① Concept of the smishing attack

Smishing is a compound word of SMS and phishing. Smishing is a fraudulent technique that exploits the small amount payment service of the smartphone, by using a text message that disguises a free coupon or an event winning, as smartphones become popular and various financial services, such as small amount payments, are increased.

② Procedure of performing the smishing attack

[Figure 28] Procedure of performing the smishing attack

③ Countermeasures against the smishing attack

- Refrain from clicking a web site link in a promotional text message with an unknown source.
- Check the correct domain URL when accessing the website link included in a text message.
- Install a smishing blocking app.

- Cancel download/installation when an app is installed without consent.
- Delete illegal apps, using the app management menu, if installed.
- Check the mobile phone billing details if smishing damage is expected (communication service company or payment agency).

E) Spear phishing

① Concept of spear phishing

An attacker sets key personnel working in the company (those who access confidential data, critical systems, etc.) as an attack target, rather than the system or network of an organization with well-established information security systems. The attacker sends spear phishing emails, based on the collected information on the target, in the attack preparation stage. After acquiring the device authority of key personnel, using social engineering techniques, the attacker hijacks account information (ID, passwords, etc.) by monitoring the device for several months or by control major systems and networks using remote control tools.

② Countermeasures against spear phishing

Awareness and response training on spear phishing should be implemented for key personnel, such as security managers, web server operators, end users, etc. In particular, web server operators should prepare countermeasures, such as the detection of malicious code distribution, operation of the web firewall, and web server security measures. For application programs and operating systems, security vulnerabilities should be continuously monitored, and security patches should be periodically applied.

F) Cryptojacking

① Concept of cryptojacking

Cryptojacking is a compound word of cryptocurrency and hijacking. Hackers mine virtual money using the users' PC. An attacker infects a user's PC with malware to mine cryptocurrency, by consuming the infected PC, or hacks and infiltrates into a website and inserts a malicious script (JavaScript) to mine cryptocurrency.

② Countermeasures against cryptojacking

- Keep the anti-virus program up-to-date and check for malware infection on a regular basis.
- Use browser extensions, such as AntiMiner, NoCoin, MinerBlock, etc.
- Block malicious sites, such as coinhive.com, using an IP firewall or writing detection rule script in security equipment (IDS/IPS).

G) Ransomware

① Concept of ransomware

Ransomware is a compound of ransom and software. Ransomware disables the system or encrypts data to demand money, by taking said system or data hostage. Ransomware became popular since the first ransomware AIDS in 1989. Ransomware became a serious social issue after the distribution of the Korean version of CryptoLocker in 2015. If the attacker's demand is not accepted within the specified period, ransom

can increase, and infected systems and encrypted data may be unavailable or deleted.

② Major characteristics of ransomware

- Since ransomware uses a private key encryption system, the encryption key and the decryption key must be the same. If multiple keys have been used for encryption, batch decryption is impossible, or it takes a lot of time, because multiple keys should be used for encryption.

- Demanding payment by virtual currency like Bitcoin
  Even if the requested amount is paid in full, there is no 100% guarantee for decryption. An attacker may demand payment by virtual currency, such as Bitcoin, in exchange for the decryption of the encrypted file. However, even if the requested amount is paid, full recovery is impossible.

- Once ransomware has made a successful attack, modified variants are continuously created.
  Variants with different infection paths and attack methods constantly appear, such as CryptoLocker, Cryptowall, and CryptXXX.

③ Procedure of the ransomware attack

Accessing to the infection path → Downloading ransomware to a PC and executing ransomware → Searching for encryption targets (document files, images, etc.) and encrypting them→ Demanding money for decryption

④ Countermeasures against ransomware

- Keeping all actives programs up to date
  Malware infection attacks using software vulnerabilities are increasing, such as Windows operating systems, Internet browsers, such as Internet Explorer, Chrome, Firefox, etc., and programs used in a PC (Hangul, MS Office, Adobe, Java, etc.). In particular, the “zero-day attack” is increasing,which uses the vulnerability as soon as an operating system or software vulnerability is discovered. Therefore, the operating system and all active programs should be kept up-to-date, and security updates should be applied immediately.

- Installing the latest anti-virus program on the PC and smartphone
  Basically, anti-virus programs should be installed to protect the PC or smartphone safely from malware. Furthermore, anti-virus engines should be updated on a regular basis, and automatic updatesare recommended. In addition, users sometimes need to check whether the anti-virus program is properly performing in real-time and with periodic checks, and whether anti-virus engines are updated regularly. The anti-virus program should always be updated to the latest version because modified variants of malware may appear, or new types of malware may appear.

- Setting the pop-up blocker
  Hackers use adware to register fake advertising sites that distribute malware in the user’s PC. The software download site distributes adware to users, and users access the fake advertising site using the adware. Then, the user’s PC is infected with malware. That’s why users have to block the advertising pop-up windows using a pop-up blocker in the Internet web browser.

- Refraining from distributing e-mail addresses and periodically changing account passwords
  You should refrain from distributing your e-mall address because hackers can send e-mails that contain

malware or e-mails for spear phishing attacks using your distributed e-mail addresses. In addition, it is necessary to change the account password periodically, because hackers can send e-mails for spear phishing to the recipients saved in the e-mail address book, if the e-mail account is hacked.

- Backing up important data regularly
  Important data should be backed up regularly because important documents and files cannot be read or used if encrypted after infection with ransomware. Anti-virus programs may prevent infection with malware or they may remove malware, butthey cannot decrypt the encrypted documents. Therefore, important documents or files should be backed up regularly to a separate external storage device and stored in a safe place.

H) Drive by download attack

Recently, malware is distributed using a drive-by download method that infects the user PC with malware as soon as the user accesses a malicious web site while surfing the web, instead of attacking a vulnerable service through a network. Malware distribution, using the drive-by download method, can infect a user's device without the user's knowledge, andit can infect multiple users at the same time, using the web server accessed by multiple users as an attack medium. The user PC infected with malware in this process can cause secondary damage, such as the DDoS attack, spam e-mail sending, and theft of personal information, without the user's knowledge in the same way.

I) "Fileless" attack without malware installation

Generally, when an attached file is executed or a malicious executable file is clicked, an external attacker invades the system and infects it with malware. Fileless attacks do not execute a file, but mainly use a vulnerability in a web browser to infect malware when a user clicks a link to a malicious site. This attack technique uses PowerShell*, which is installed through Windows 7, and command utility (WMIC)**, which is a Windows management tool, to make an attack. Such an attack may be difficult to detect using an anti-virus tool because software is not installed on the user's PC.

* PowerShell: A task-based shell and scripting language, specifically designed for system management. PowerShell is used to easily control and automate the management of Windows OS and application programs.

** WMIC (Windows Management Instrumentation Command): A system command input tool for Windows management, provided by Windows.

J) Malvertising

Malvertising is a compound word of malware and advertising. Malvertising is a technique of distributing malware using online advertising. The malvertising technique inserts malware by spreading advertising into the normal online advertising network or web site. Online advertising provides the best environmental conditions for spreading malware because it displays the topics that can attract the attention of visitors, or it is posted on the site with a high number of visitors. In addition, the risk of malware infection increases exponentially in online advertising, because it is linked with numerous normally operated websites and can easily distribute malware in large quantities, even if an attacker does not directly hack each website.

02 Security trends related to the latest information technology

A) IoT security

① Overview on IoT security

Security is a core technology that must be provided to promote IoT technology and to create new services. As the number of devices connected to the Internet increases, the number of attack targets and threat elements also increase. In particular, security technology is indispensable for IoT devices and communication technologies that are applied to healthcare services or industrial facility control services, because an injury can occur beyond simple economic damage, if the security of the service is breached. In addition, when ordinary things around us are connected to the Internet, the range of concerns about personal information leakage or privacy invasion increases. It is also obvious that the level of breach will increase beyond comparison with the present.

Security and privacy protection systems should be considered from the design and development phase of the IoT device and service. In addition, it should be possible to block potential security threats in advance in the IoT device deployment and installation phase. Potential security threats and vulnerabilities should be checked, and security should be applied throughout the entire lifecycle of the IoT device, such as the setup, operation, and execution phase, when the device is actually used, and during the destruction phase.

② Applying security to the design/development phase of the IoT device

- Security by design

  A method should be considered that can reduce the weight of the IoT device while minimizing the misuse of information and device, such as confidentiality, integrity/authentication, and availability, considering the low power/low performance characteristics of the IoT device. The IoT service should provide a method of managing device access rights, end-to-end communication security, and providing integrity/authentication that is suitable for the service operating environment for the IoT device and information. The application of software security technology and hardware security technology should be actively reviewed, and standard security technology, with proven safety, should be used.

- Privacy by design

  The privacy protection methodology of the user should be applied to the IoT device and IoT service operation policy by default. The method of encrypted transmission, anonymous storage, and integrity/authentication application should be included in the privacy information collected by the IoT device. The IoT service should include the method of de-identification, access control/authentication, confidentiality, and secure storage of collected privacy information. IoT service providers should guarantee transparency to the maximum by visualizing the operation policy, including the scope and period of privacy information use, to the user.

③ Applying and verifying the secure S/W and H/W development technology.

Secure coding, software and application security verification, and secure hardware device should be used when designing and developing IoT products and services.

• Application of secure coding

Secure coding should be applied to prevent security vulnerabilities that may exist from the source code implementation phase, regardless of the IoT device. Software developed in Java and C/C++ should utilize secure coding guides prepared in advance. Languages without a guide must verify the security quality of the source code, based on international standards, and must use a separate analysis tool and methodology.

• Verifying software security

When using various software to improve the productivity and quality of products and services during IoT product and service development, security measures against the presently known security vulnerabilities should be verified, and security patches must be applied. The guideline procedure should be performed to verify the countermeasures against known security vulnerabilities, and the known vulnerabilities should be searched and responded to using reference sites.

• Using secure hardware devices

IoT devices require various levels of security strength, depending on the type of application service. IoT devices have various hardware security vulnerabilities, such as the side channel attack, firmware code extraction, and key value extraction, because those devices are mainly installed in the environment that can easily be exposed to attackers. For this reason, various hardware security techniques, such as firmware/code encryption, execution code domain control, and reverse engineering prevention techniques, should be used to strengthen hardware security. It is necessary to appropriately apply these techniques according to the application environment of the IoT device.

• Converging software security technology and hardware security technology

When converging software security technology and hardware security technology, confidentiality and integrity functions should be provided for the transmitted data, by establishing a safe secure channel between software security technology, and hardware security technology, based on a trusted approach (one-way and two-way authentication).

④ Security by system component to provide IoT services

• IoT network

Security requirements that are suitable for the communication/network access protocol, mainly used by the IoT service, should be applied.

• Dedicated IoT protocol

Security vulnerabilities need to be eliminated when linking between protocols. The security requirement for the data transmission protocol that is standardized by the IoT standard organization, should be applied.

• IoT platform

The IoT platform security requirements, defined by the proven standard organization, should be applied.

• Service model

Various security requirements and legal/regulatory matters, related to security, should be applied for

each service.

B) Cloud security

① Overview of cloud security

Concerns about cloud security begin with the fact that the exact location of the stored data cannot be easily understood, and the data is accumulated, due to the characteristics of the cloud. In particular, when using a public cloud, the question of whether storing sensitive data on the cloud, which is an external storage space, is correct in terms of reliability and stability, is becoming an obstacle to cloud adoption and spread.

② Threats of cloud security

- Hypervisor infection
  If the hypervisor in the virtualization system, which is essential to run the cloud service, is vulnerable, several virtual machines (VMs) using the hypervisor can be damaged at the same time.

- Attack against the virtual machine
  As the users' virtual machines are interconnected, there is an attack path from an internal virtual machine to another virtual machine, such as packet sniffing, hacking, DDoS attack, and malware spread.

- Attacker tracking
  It is difficult for existing network security equipment (firewall, IPS, IDS, etc.) to detect attacks and intrusions against the inside of the virtualized machine, because it is not easy to identify and trace an attacker in the virtual environment.

- Portability of the virtual machine
  Since virtual machines can be easily transported between physical platforms in the virtualization, there is a possibility that malware can spread easily, as the virtual machine infected with malware is ported to another physical platform.

③ Countermeasures against cloud security threats

- Protecting incoming and outgoing data
  The confidentiality of incoming and outgoing data should be maintained by using TLS, SSH, VPN, etc. for security issues that may occur when sending user data to the cloud server through the Internet.

- Encrypting data when storing data
  Data should be encrypted before storing it in the cloud storage, and at least AES-256 and a secure cryptographic algorithm should be used.

- Access and authentication
  A secure access and authentication mechanism should be applied, the administrator password should be changed periodically, and access control policies, such as 2-factor, should be established and observed.

• Securing independence between VMs
A system should be protected by utilizing the strengths of a VM's virtual network security against the threat to the shared repository and shared network to the maximum extent, and complete isolation between the VMs accessed by users should be provided.

• Attack and intrusion detection
Attacks and intrusions should be detected by applying the hypervisor type detection technique, which analyzes the internal state of each virtual machine and detects intrusions using the hypervisor, and the VM type detection technique, which is an agentless virtual security detection technique.

C) Big data security

① Overview of big data security

As big data is introduced at a rapid rate, the risk of personal information leakage is also increasing because an enormous amount of customer information is collected and concentrated. Unlike existing data types, big data extensively collects and analyzes sensitive personal information, such as credit information, location information, and behavior information. Therefore, the scope and scale of a leakage incident are inevitably enlarged if it occurs. Hence, security should be ensured most of all to spread the use of big data in the financial sector. The safe management of big data by lifecycle, from big data collection to destruction, is important.

② Security threat and response by the phase of the big data lifecycle

• Big data collection phase
If the data of a specific individual is to be collected, the individual's personal information should be de-identified if it is not allowed by the law or agreed to by the owner in advance.
When collecting big data using active data collection technologies, such as Chukwa, Scribe, and Flume, the owner of the data to be connected should consent, and access controls should be applied to the data. When using passive data collection technologies, such as Web Robot or Web Crawler, robot exclusion standards should be complied with.

• Big data storage and management phase
Data should be encrypted using a cryptographic technique suitable for data distribution and replication, technical and physical access controls should be applied, and data should be de-identified through data filtering before being stored.

• Data processing and analysis phase
Data anonymization techniques, such as K-anonymity, L-diversity, and differential privacy, should be used to de-identify data in the processing and analysis phase. Sensitive information should be processed in an encrypted state, using order preserving encryption, operation preservation encryption, etc. In addition, privacy should also be protected when mining big data, by using the Privacy Preserving Data Mining (PPDM) technique, etc.

• Data destruction phase

When destroying big data, the characteristics of the distribution and replication environment of big data should be considered, and it should be completely destroyed in an unrecoverable way. In addition, a management system for monitoring the data destruction is needed in terms of internal control.

③ Overview of personal information de-identification

• Concept of personal information de-identification

De-identification refers to processing that makes it difficult to identify a specific individual, even if individually identifiable information in data is combined with other information, by deleting some of or all such information, or by replacing some information with other attributed information.

• Targets of personal information de-identification

De-identification targets information that can identify an individual by him/herself, and information that can be easily combined with other information to identify an individual, even if the information alone cannot identify that individual.

• Personal information de-identification techniques

Big data de-identification techniques include pseudonymization, aggregation, data reduction, data suppression, and data masking.

<Table 14> Personal information de-identification techniques

Processing technique	Detailed technology	Main content
Pseudonymization	Heuristic anonymization, K-anonymization, encryption, exchange method	A technique that makes it difficult to identify individuals, by replacing important identifying elements in personal information, with other values.
Aggregation	Aggregation, sub-aggregation, Rounding, rearranging data	A technique that shows the total value of data to prevent the identification of individual data values.
Data reduction	Simple anonymization by deleting attribute values, partially deleting attribute values, deleting data rows, and removing identifiers	A technique that removes unnecessary values, or values that are important for identifying individuals, among the values configured in the data set,according to the purpose of data sharing and opening.
Data suppression	Data suppression, random rounding method, range method, control rounding	A technique that prevents the identification of individual data values, by converting data values into category values.
Data masking	Adding random noise, replacing with space	A technique that prevents the identification of key personal identifiers, which is highly likely to contribute to the identification of an individual in combination with open information.

④ Major personal information de-identification technologies and utilization methods

• Heuristic pseudonymization
A method of hiding values corresponding to the identifier, based on several pre-defined rules, or hiding personal information by processing it at the discretion of the data handler. This technique can be applied to a variety of personal information, such as the name, user ID, department (company) name, institution number, address, credit rating, mobile phone number, zip code, e-mail account, etc.

• K-anonymity
A method of disclosing data by keeping k or more data that have the same attribute value in order to prevent a privacy violation by keeping the number of values, which can be held by the designated attribute, over a certain level. This method can be applied to personal information, such as age, height, address, zip code, department (company), etc.

• Aggregation
A method of reducing sensitivity by aggregating data into a group or part (total, average, etc.), if the collected information contains sensitive personal information. This method can be applied to personal information, such as age, height, income, credit card use amount, etc.

• Data suppression
A method of converting specific personal information data into an average or category value to hide it. This method can be applied to personal information, such as age, height, disease, etc.

• Adding random noise
A method of preventing the exposure of identification information by adding noise, such as random numbers, to sensitive personal identification items. This method can be applied to personal information, such as the resident registration number, user ID, name, date of birth, height, age, etc.

D) Mobile security

① Security threats and countermeasures in the mobile environment

Smartphones, which are equipped with a user-oriented mobile PC platform,provide voice calls, wireless Internet connections using mobile communication and Wi-Fi, web browsers, and multimedia content services. Open OS allows users to freely install various apps on their devices. This open web environment of smartphones causes security threats, which become an issue.

② Security threats in the smart and mobile environment

• Security vulnerabilities, due to jailbreaking and rooting
• Threats of smart device theft and loss
• Malware infection and app forgery and alteration
• Sniffing and session hijacking through an illegal AP

③ Countermeasures against security threats in the mobile environment

<Table 15> Countermeasures against security threats in the mobile environment

Threat	Countermeasures
Threat factors of the device	• Encrypting application program codes and data • Applying theft and loss prevention solutions • Applying security updates and running an anti-virus program regularly
Threat factors of memory	• Applying anti-virus technology and memory hacking prevention technology • Applying personal information leakage prevention solutions
Threat factors of web services	• Applying app forgery and alteration prevention solutions • Blocking illegal apps, by applying electronic signature technology
Threat factors of networks	• Blocking illegal APs • Applying location information protection and data encryption technology • Applying a personal firewall and VPN

IV. Security management system and standard

▶▶▶ Subject

Understanding security management systems and standards

▶▶▶ Recent trends and major issues

The ISMS (Information Security Management System) certification system, which is a domestic information security management system, was mandated on February 18, 2013. A total of 126 certificates were issued in 2013 once ISMS certification became mandatory, and the number of certification issues has increased remarkably when compared to the total of 151 cases issued for 11 years, since 2002. The number of companies that voluntarily received certification increased in 2014 and 2015, in addition to the mandatory companies.

▶▶▶ Learning objectives

To be able to explain the concept of the information security management system.

To be able to explain personal information protection.

To be able to explain standards related to information security.

▶▶▶ Keywords

Information security management system, information security management process, information protection measures, certification screening criteria, control items, ISO27001, risk identification, risk assessment, quantitative technique, qualitative technique, baseline approach, detailed risk approach, expert judgment method, combined approach, individual Information, collection, use, storage, provision, consignment, destruction, uniquely identifiable information, personal information processing system, collection, consent to use, OWASP top 10, CWE, SANS top 25

✚ Preview for practical business **Security management system and standard**

Assistant manager Kim has continuously check if there is a problem in the information security management system, by operating it for two months after installation and has improved it through internal audits.
Since then, he applied for the certification screening of the information security management system and received certification, then decided to confirm that the certification is valid for three years and that the information security management system will be maintained every year through a follow-up screening.
Let's review what the information security management system that he has installed and operated is, as well as the available risk management methods and related certification systems in detail.

01 Information security management system

A) Overview of the information security management system (ISMS)

① Concept of the information security management system

The information security management system refers to a system that manages information security measures in order to maintain the confidentiality, integrity, and availability of information assets. It continuously manages and operates various processes, such as information security system development, countermeasure implementation, operation, monitoring and review, and improvement, based on risks.
Enterprises can quickly respond and minimize damage when security breach incidents occur, by implementing comprehensive information security measures by building and operating the information security management system.

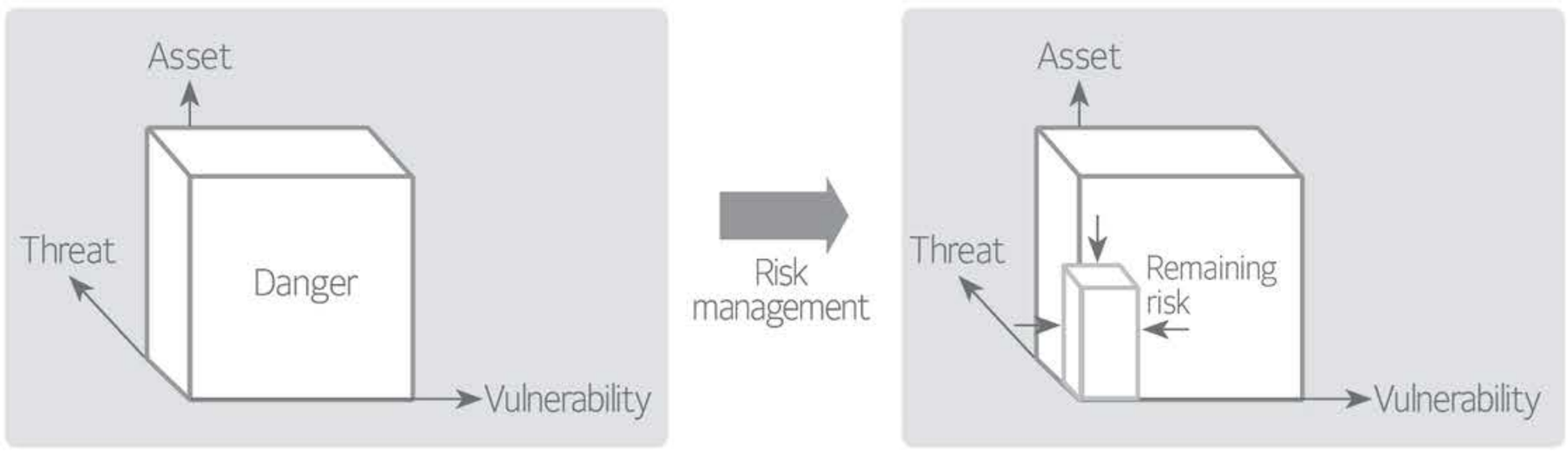
② Composition of the information security management system

As shown in [Figure 29], the information security management system consists of the establishment of the management system, risk management, management system operation, and management system inspection and improvement.

[Figure 29] Composition of the information security management system

B) Risk management

As shown in [Figure 30], risk management is a series of processes that estimates values, by identifying information assets managed by an organization, identifies risks from the legal, administrative, physical, and technical aspect by assets, and by preparing effective protection measures against the risk that exceeds an acceptable degree of assurance (DoA)[1].



[Figure 30] Risk management

1 DoA: Degree of Assurance

① Risk identification

- A risk means the possibility that an unexpected situation occurs and affects (damages) an organization, and can be expressed as a function of assets, threats, and vulnerabilities. The value of each information asset should be estimated, and risks of each asset should be identified during the risk identification process.

② Risk assessment

- The scope of risk analysis should be selected based on the scope of the information security management system, according to the business, organizational, locational, asset, and technical characteristics during the risk assessment process.
- For efficient risk analysis, a quantitative or qualitative method should be selected, depending on whether the risk can be quantified or not. Alternatively, the baseline approach, detailed risk approach, or combined approach should be selected, depending on the approach.

③ Risk assessment method

- Risk assessment method depending on risk quantification

<Table 16> Quantitative technique vs. qualitative technique

Item	Quantitative technique	Qualitative technique
Characteristics	• Used when the scale of damage can be measured in monetary units. • Past data approach, mathematical formula approach, probability distribution estimation method	• Since the scale of damages cannot be measured, it is expressed as an interval (e.g., H:3, M:2, L:1) or a variable. • Risk analysis method based on the experience and knowledge of the analyst. • Delphi method, scenario method, ranking method.
Strengths	• Cost-effectiveness analysis and budget planning are easy because quantified data is used. • Calculation is logical because a mathematical method is used.	• Used when estimating information that cannot be quantified. • Easy to understand terms. • Analysis does not take long.
Shortcomings	• Difficult to obtain accurate quantification values. • Mathematical calculation takes much time and effort.	• Room for the abuse of subjective judgment. • Cost-effectiveness analysis is difficult.

- Risk assessment method depending on the approach.

<Table 17> Risk assessment method depending on the approach

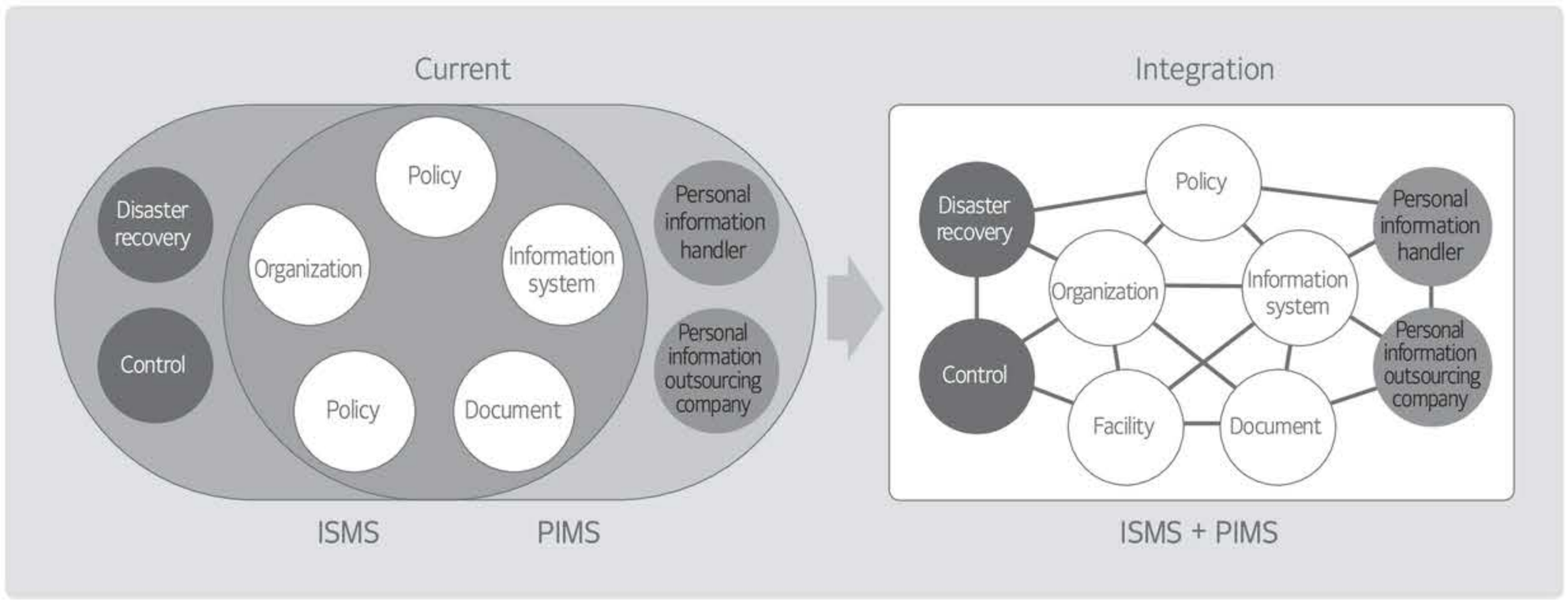
Item	Contents
Baseline approach	• Setting the basic level of information security for all systems and establishing protective measures to achieve the basic level. • Less time and costs are required. Protective measures that are basically required by all organizations can be selected. • Applying security control for each department in the organization, which is lower or higher than the proper security level, since the characteristics of the organization are not considered.
Expert judgment method	• Risk analysis based on expert knowledge and experience, not the standardized method. • Cost effective in small organizations. • Objective assessment is difficult because there is no structured approach.

Detailed risk approach	• Determining the level of risks after measuring asset values and asset risk level and analyzing vulnerabilities. • Appropriate protective measures can be established within the organization. • Professional knowledge, time, and efforts are needed.
Combined approach	• Major systems or high-risk systems are identified and "detailed risk approach" is applied, and the "baseline approach" is applied to other systems. • Time and efforts can be efficiently utilized by quickly establishing security strategies. • Resources can be wasted if the application target of two methods is not clearly set.

C) Information security and information security management system (ISMS-P)

① Overview of ISMS-P

The certification system is integrated so that the existing information security management system (ISMS) and the personal information security management (PIMS) can be systematically protected in a single system.

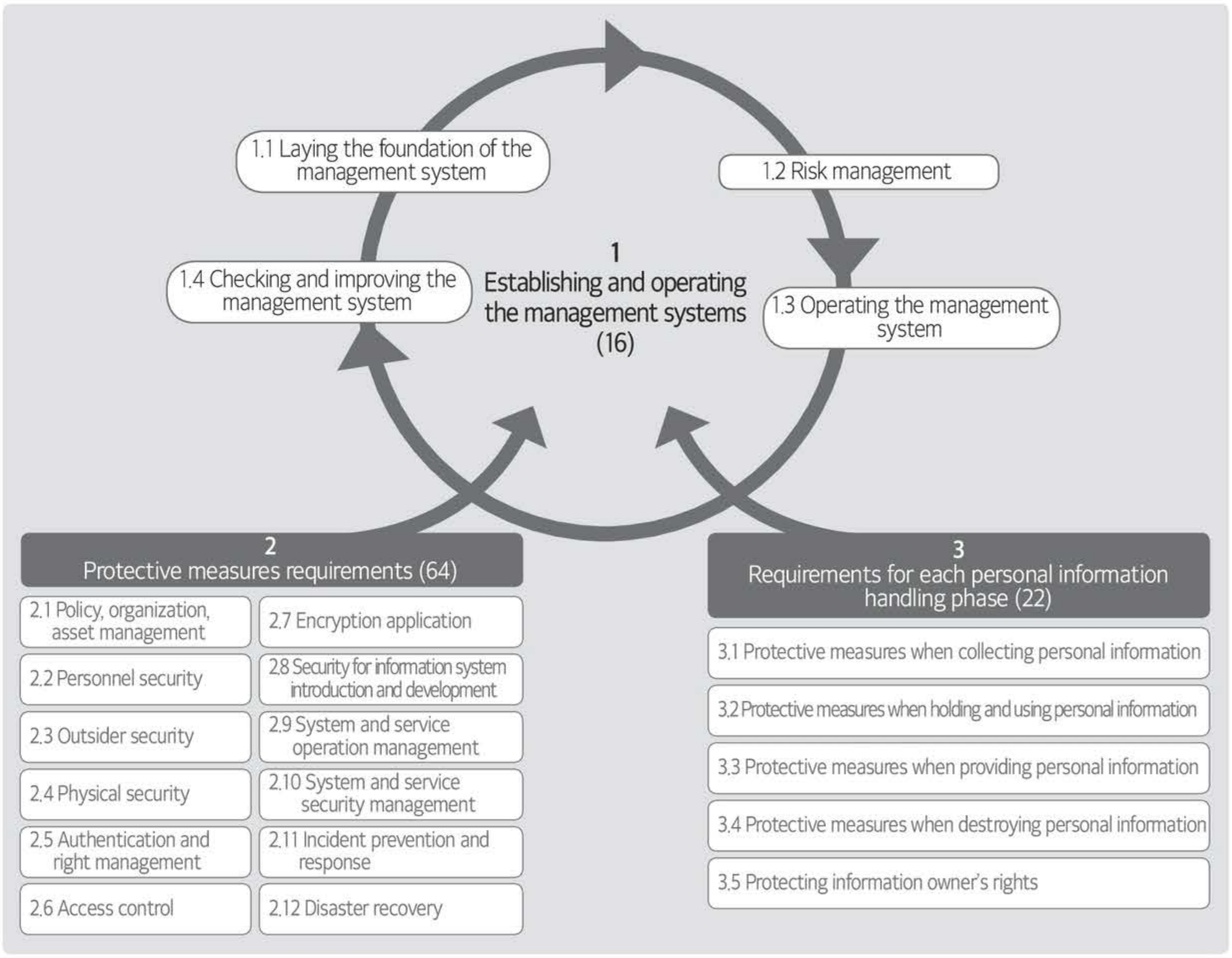


[Figure 31] Overview of ISMS-P

(Source: https://isms-p.kisa.or.kr)

② Composition of ISMS-P

ISMS-P consists of 102 certification criteria items, including the establishment and operation of 16 management systems, 64 protective measures requirements, and 22 requirements for each personal information processing stage.



[Figure 32] Composition of ISMS-P

(Source: https://isms-p.kisa.or.kr)

02 Personal information protection

A) Privacy policy

① Reflecting the method of obtaining consent when collecting personal information

When obtaining consent to personal information collection, consent details should be presented before the user enters personal information, and the user should be able to accept or reject.

When obtaining consent to information collection, the purpose of collecting and using personal information, the items of personal information to be collected, the period of personal information retention and use, and the disadvantages in case of rejection should be presented to the users.

② Reflecting the method of personal information destruction

When the retention period of collected personal information has expired, or the purpose of use has been achieved, personal information must be destroyed, without delay, in an irrecoverable way. If the personal information must be retained according to other laws and regulations, it must be stored separately from personal information that is currently in use.

To store separately, a separate database can be generated and stored, or data can be stored in a physically separated server. The access rights of the general personal information database should be set differently from the personal information database that is stored separately, in order to prevent unnecessary access, inquiries, and leakage.

③ Access control on the personal information processing system

Those who handle personal information should control unauthorized access by limiting the access rights, in order to prevent illegal access and breach incidents to the personal information processing system, and to detect illegal attempts to leak personal information by analyzing the connected IP addresses. The access control method includes ACL (Access Control List), firewall, and free intrusion detection system (Snort).

④ Applying encryption when storing and transmitting personal information

- Encrypting personal information to prevent illegal exposure or forgery/alteration, when storing it in the personal information processing system or transmitting it through the network.
- Storing passwords after one-way encryption to prevent decryption.
- Developing a system by including the feature that can provide a temporary password or reset the password, since the password cannot be decrypted when lost.
- Storing uniquely identifiable information, such as the resident registration number, passport number, driver's license number, and foreign registration number, and bio information, such as fingerprint, iris, voice, handwriting, etc., after encryption with a secure encryption algorithm.
- Applying encryption systems, such as SSL/TLS to the personal information transmission section.

⑤ Managing the logging and storage of access records and changes to rights

Those who handle personal information should retain and manage the access record of the personal information system for at least 6 months. Access records are the data that can check for illegal access by generating log files, which keep track of personal information input/output and modification, data access details, etc.

03 Information security standards and related systems

A) ISO 27001:2013

ISO 27001:2013, an international standard for information security management systems and certification systems, enables the applicant to receive existing quality management certification (ISO 9001), environmental management certification (ISO 14001), etc. together with ISO/IEC 27001 and 27002 (ISMS2.0), which are

certifications in the information security sector. As shown in <Table 18>, the checklist in the annex has been changed from 133 control items in 12 fields, to 114 items in 14 fields.

<Table 18> ISO 27001 control fields

ISO/IEC 27001:2013 2.0	
Control field	Number of control items
Information security policy	2
Information security organization	7
Asset management	10
Personnel security	6
Physical and environmental security	15
Communication security	7
Access control	14
Acquiring, developing, and maintaining the information system	13
Managing information security accidents	7
Managing business continuity	4
Compliance	8
Supplier relationship	5
Password control	2
Operational security	14
Sum	114

B) OWASP TOP 10

The OWASP Top 10 - 2017 is primarily based on over 40 sets of data submitted by companies specializing in application security, and on the survey on more than 500 persons in the industry. The data encompasses the vulnerabilities collected from hundreds of organizations as well as more than 100,000 real-world applications and APIs. The Top 10 items are selected and ranked, according to the prevalent data, which is compensated with the estimated value of the possibility, detectability, and level of impact of the attack. [Figure 33] shows the OWASP 2017 version, compared to the previous version in 2013.

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 - Injection	→	A1: 2017 - Injection
A2 - Broken authentication and session management	→	A2: 2017 - Broken authentication
A3 - Cross Site Scripting (XSS)	↘	A3: 2017 - Sensitive data exposure
A4 - Insecure direct object references (merged with item A7)	U	A4: 2017 - XML external entities (XXE) [New]
A5 - Security misconfiguration	↘	A5: 2017 - Broken access control [Merged]
A6 - Sensitive data exposure	↗	A6: 2017 - Security misconfiguration
A7 - Missing function level access control (merged with item A4)	U	A7: 2017 - Cross Site Scripting (XSS)
A8 - Cross Site Request Modulation (CSRF)	☒	A8: 2017 - Insecure deserialization [New, Community]
A9 - Using known vulnerable components	→	A9: 2017 - Using components with known vulnerabilities
A10 - Unvalidated redirects and forwards	☒	A10: 2017- Insufficient logging and monitoring [New, Community]

[Figure 33] OWASP TOP 10 2017

(Source: https://www.owasp.org/images/b/bd/OWASP_Top_10-2017-ko.pdf)

C) CWE(Common Weakness Enumeration)

CWE is a classification system that MITRE, which is an affiliate of the U.S. Department of Defense with the support of the National Cyber Security Division within the Department of Homeland Security, classifies software weakness items, based on the view, category, vulnerability, and complex elements. (http://cwe.mitre.org)

D) CWSS (Common Weakness Scoring System)

CWSS is a scoring system for determining the relative importance of various vulnerabilities in architecture, design, code, or implementation in software, which can be important security issues of software.

E) CVE (Common Vulnerabilities and Exposures)

While CWE is a classification system for common vulnerabilities, CVE is a list of security vulnerabilities discovered over time. It can be seen as a record history of discovered security vulnerabilities, managed by the identification system of “CVE-Year-Sequence”.

F) CVSS (Common Vulnerabilities Scoring System)

CVSS is an open framework used to assess and identify security vulnerabilities. It consists of three metric groups: basic metric group, temporary metric group, and environmental metric group. The result, calculated by the three metric groups, becomes the overall score of the vulnerability and the priority of the vulnerability.

G) SANS (SysAdmin, Audit, Networking, and Security) Top 25

SANS top 25 is the list of the most serious programming errors that cause software vulnerabilities in three categories, including the management of unsafe and dangerous resources between components, and content related to the use of inappropriate security countermeasures. This list is created by the MITRE and SANS associations, based on CWE.

V. Application security

▶▶▶ Subject

Managing applications safely!

▶▶▶ Recent trends and major issues

It is analyzed that most cyber-attacks exploit software security vulnerabilities. Accordingly, the importance of application security is also highlighted. Understanding and applying secure coding to practical businesses are important, in order to safely develop an application.

▶▶▶ Learning objectives

To be able to explain security weaknesses and security weaknesses remaining in software.

To be able to understand the concept, technique, and lifecycle of secure coding.

To be able to explain secure coding in major languages and mobile environments.

▶▶▶ Keywords

Secure coding, security weakness, security vulnerability, secure SDLC

✚ Preview for practical business

Recently, company A is building a website that strengthens security, due to the vulnerability of personal information, and is considering secure coding to improve security.

1) The company is trying to apply secure SDLC.
2) The customer and the development company consider secure coding in the requirement definition stage.
3) The company considers secure design when designing analysis, from the perspective of architecture.
4) Developers review their codes in the development phase and the quality control department performs a third-party security check.
5) The company considers secure coding diagnostic tools for review in the operation and maintenance stage.

However, developers are having difficulty in the development process, due to the lack of understanding on secure coding and the lack of training on security vulnerabilities.
Let's review secure coding that should be applied throughout the development lifecycle to build an application with strong security.

01 Need for securing coding

A) Need for secure coding

It was analyzed that about 70% of cyber-attacks exploit the security vulnerability of software itself. It was also analyzed that modification costs can be reduced by tens of times, compared to the cost of modification after the product release.

Accordingly, removing security vulnerabilities in the software development phase is highlighted as an effective method before releasing the product, to prevent and respond to cyber-attacks.

Secure coding is a defensive programming technique that reduces software vulnerabilities and hacking risks, by removing security weaknesses in the software development lifecycle (SDLC).

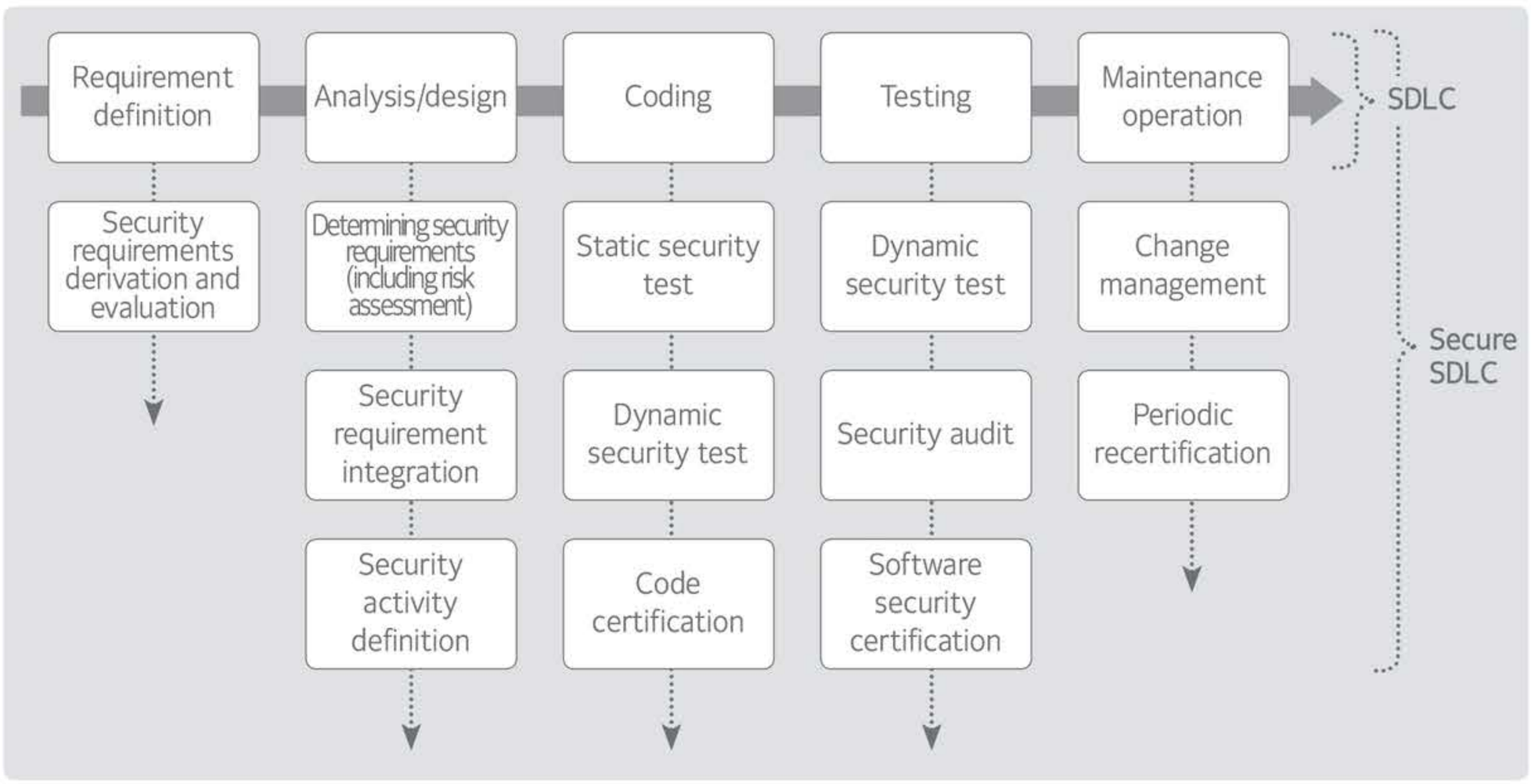
02 Main content of secure coding

A) Software security weakness and security vulnerability

① Weakness: Errors occurring in the design and implementation phase, such as software defects, errors, and bugs. Software weakness can cause software vulnerabilities. A representative example is the Common Weakness Enumeration (CWE).

② Vulnerability: An error in software that can be accessed and used by hackers, by accessing the system or network. Hackers can exploit this accessible security weakness. An example is the Common Vulnerabilities and Exposures (CVE).

B) Secure SDLC



[Figure 34] Secure SDLC

① Phase of secure SDLC requirement definition

A phase that defines security objectives, according to the characteristics of the project and software, and analyzes security weakness and impact, according to the potential threat. Security requirements for software development are derived in this phase.

② Secure SDLC analysis/design phase

A phase that designs security architecture and security requirements in the entire architecture design process. Developer training is implemented, and security test plans are designed in this phase in order to build a safe security system.

③ Secure SDLC coding phase

Coding rules are defined by checking the weaknesses and strengths of the used programming language from a security perspective. The static unit test of the developed code is conducted, and compliance with the predefined secure coding rules are verified. When a commercial package is used, security vulnerability content and action details found in the package are checked.

④ Secure SDLC testing phase

A dynamic unit test is conducted on the developed program, and the usability of the security applied application is tested. Matters to improve security are derived and applied, by checking the vulnerability of the infrastructure and application program, independently of the system.

⑤ Secure SDLC maintenance phase

When modifying codes, according to the software change management procedure, impact on security is evaluated, vulnerabilities are checked periodically, and matters to improve security are derived and applied.

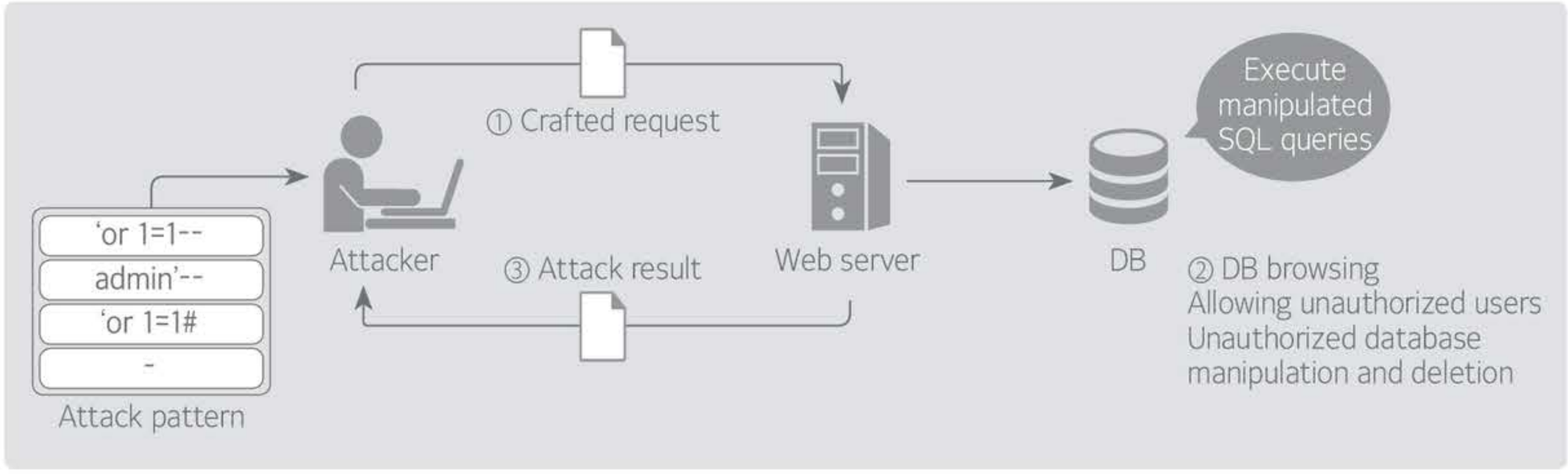
03 Major secure coding techniques

A) Major secure coding techniques for Java

① Secure coding techniques for responding to the SQL injection attack

- Attack overview

If the validity of the data entered in the web application program, linked with the database, is not verified, an attacker can read or manipulate information from the database by inserting an SQL statement into the input form and URL field. The SQL injection attack refers to this security vulnerability.



[Figure 35] SQL injection security vulnerability

- Coding technique:
  Uses a method that transfers the compiled query statement (constant) to the database, using the Prepared Statement object, etc. When using Prepared Statement, filter special characters and query reserved words that are used for the database query. When using a framework, such as Struts and Spring, use the module that verifies the external input values and security module, according to the circumstances.

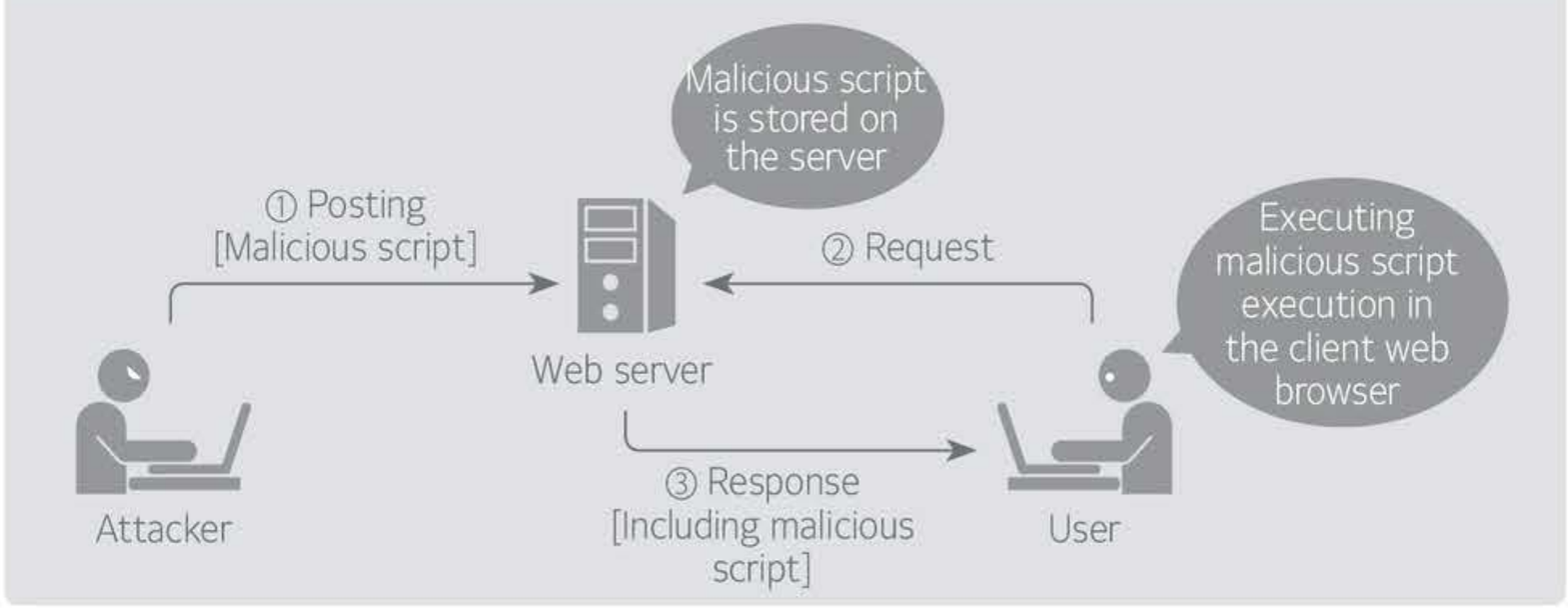
<Table 19> Code example

Unsafe code	String gubun = request.getParameter("gubun"); ..... String sql = "select b_gubun " + " , a.idx " + " , a.b_id " + " , date_format(a.w_date, '%Y-%m-%d') " + " , a.pwd " + " , a.content " + " , b.idx " + " , a.security " + " from board a left outer join tail b on a.idx = b.b_id " + " where b_gubun = '" + gubun + "' "; Connection con = db.getCon(); Statement stmt = con.createStatement(); ResultSet rs = stmt.executeQuery(sql);
	The value of "gubun", which is entered from the outside, is used to create an SQL query, without any verification. In this case, if a' or 'a' = 'a is entered as the value of "gubun", the conditional clause is changed to b_gubun = 'a' or 'a' = 'a', and the structure of the query is changed. Then, all the contents of the "board" table are retrieved.
Safe code	String gubun = request.getParameter("gubun"); ..... String sql = "select b_gubun " + " , a.idx " + " , a.b_id " + " , date_format(a.w_date, '%Y-%m-%d') " + " , a.pwd " + " , a.content " + " , b.idx " + " , a.security " + " from board a left outer join tail b on a.idx = b.b_id " + " where b_gubun = ? "; Connection con = db.getConnection(); PreparedStatement pstmt = con.prepareStatement(sql); pstmt.setString(1, gubun); ResultSet rs = pstmt.executeQuery();
	The PreparedStatement object that receives a parameter should be created as a constant string, and the parameter should be set with the setXXX method to prevent eternal input from changing the structure of the query statement.

② Secure coding technique for responding to the Cross Site Scripting (XSS) attack

• Attack overview:

An attacker can insert a malicious script into a web page to induce the user to execute it. For example, if an unverified external input is used to create a dynamic web page, it can cause an attack, such as information leakage, because inappropriate script is executed with the rights of the person who views the transmitted dynamic webpage.



[Figure 36] XSS security vulnerability

• Coding technique:

Special characters such as <>& “, should be replaced with < > & " using a character conversion function or method, in order to prevent script insertion into the external input value. If a bulletin board allows HTML tags, allowed HTML tags should be created as a whitelist to support only those tags.

<Table 10> Safe coding example

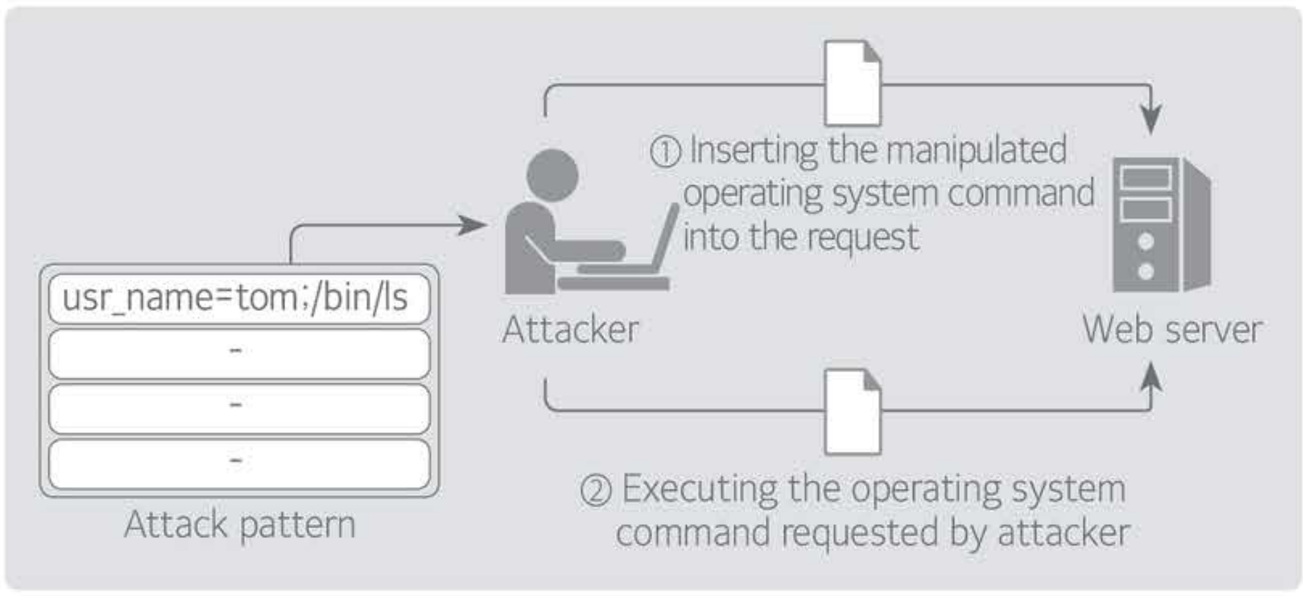
Safe code	String name = request.getParameter(“name”);
	if(name != null)
	{
	name = name.replaceAll(“<”, “<”);
	name = name.replaceAll(“>”, “>”);
	name = name.replaceAll(“&”, “&”);
	name = name.replaceAll(“\“\””, “"”);
	
	}

	Strings related to script in the “name”, which is entered by the user, should be filtered and converted.

③ Secure coding techniques for responding to the OS command injection attack

• Attack overview:

If the user input, that has not been properly verified, is configured and executed as part or all the operating system commands, unintended system commands may be executed, which may improperly change the rights or negatively affect the system operation.



[Figure 37] OS command injection security vulnerability

• Coding technique:
An application program should be configured in a way that system commands are not transferred to the inside of the server through the web interface. The value received from the outside should not be used as an internal system command, without verification. If a command is generated or selected according to external input, the values required for command generation should be specified in advance and selected, according to the external input.

<Table 21> Code example

Unsafe code	public static void main(String args[]) throws IOException {
	if (args.length == 0) {
	System.err.println("Please input the name of the program to execute.");
	return;
	}
	// All programs passed as a parameter can be executed, because there is no limit in the program to be executed by the program concerned.
	String cmd = args[0];
	Process ps = null;
	InputStream is = null;
	InputStreamReader isr = null;
	BufferedReader br = null;
	try {
	ps = Runtime.getRuntime().exec(cmd);
	is = ps.getInputStream();
	isr = new InputStreamReader(is);
	br = new BufferedReader(isr);
	String line = null;
	while ((line = br.readLine()) != null) {
	System.out.println(line);
	}
	}
	... (Appropriate exception handling and resource release handling) • • •
	}

	Programs are executed using the Runtime.getRuntime().exec() command, and the argument value received from the outside is used to create the command. However, an attacker can execute any programs, because the program concerned does not restrict the program that can be executed.

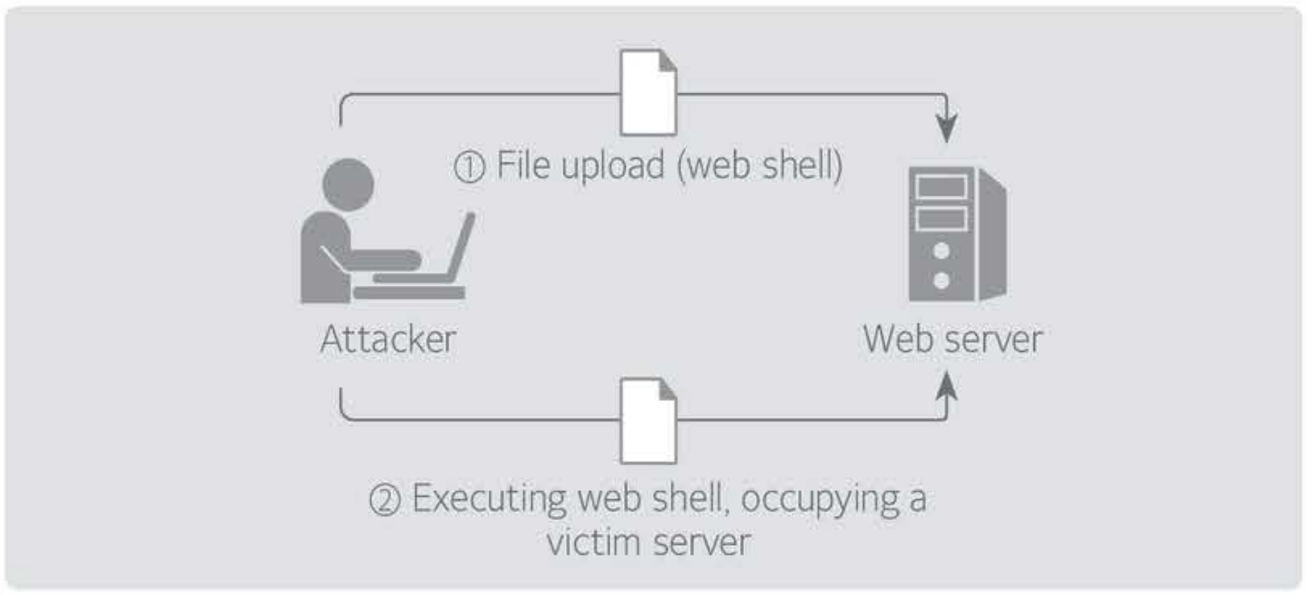
Safe code	public static void main(String args[]) throws IOException {
	// The program that can be executed by the application concerned is limited to Notepad and Calculator.
	List<String> allowedCommands = new ArrayList<String>();
	allowedCommands.add("notepad");
	allowedCommands.add("calc");
	if (args.length == 0) {
	System.err.println("Please input the name of the program to execute.");
	return;
	}
	
	String cmd = args[0];
	if (!allowedCommands.contains(cmd)) {
	System.err.println("Not an allowed command.");
	return;
	}
	Process ps = null;
	InputStream is = null;
	InputStreamReader isr = null;
	BufferedReader br = null;
	try {
	ps = Runtime.getRuntime().exec(cmd);
	.....

	An array of predefined parameters should be created, and appropriate parameters should be selected, according to the external input. The possibility of using an inappropriate external input as a command should be removed.

④ Secure coding technique for responding to the "unrestricted upload of dangerous files" attack

- Attack overview:

  "Unrestricted upload of dangerous files" is a security weakness that can control the system by executing internal commands or connecting with the outside, if a script file (asp, jsp, php file, etc.), that can be executed on the server side, can be uploaded, and the attacker can manually execute this file through the web.



[Figure 38] "Unrestricted upload of file with dangerous type" security vulnerability

- Coding technique:

  Allow the upload of the file with the extension allowed by the whitelist only. Also remove execute attribute, if the file execution status can be set.

<Table 22> Code example

Unsafe code	…… String filename = file.getOriginalFilename(); // Do not check the extension of the upload file. File uploadDir = new File("/app/webapp/data/upload/notice"); String uploadFilePath = uploadDir.getAbsolutePath()+"/" + filename; /* Below is the file upload routine. */ ….
	If the validity of the file to be uploaded is not checked, an attacker can upload or send a dangerous file.

Safe code	……
	// Check the extension of the uploaded file using the white list method
	if (filename != null) {
	if (filename.endsWith(".doc") || filename.endsWith(".hwp") ||
	filename.endsWith(".pdf") || filename.endsWith(".xls")) {
	/* File upload routine below */
	// When saving the file, change the file name to a format that cannot be guessed by external users
	……

	Uploading is restricted if the extension of the uploaded file is not allowed when it is checked. When saving the file, the file name entered from the outside is changed.

B) Major secure coding techniques for C language

① Secure coding techniques for responding to the memory buffer overflow attack

• Attack overview:

The memory buffer overflow attack occurs when reading or writing data to a location beyond the allocated memory range, that is allocated by the program using contiguous memory space. As the memory buffer overflow causes program malfunction, or execution of malware, an attacker can obtain the rights to control programs.

• Coding technique:

When the program uses a memory buffer, a proper buffer size should be set, and the program should be controlled to read and write, within the set range of memory. In particular, if the string is not terminated with a null character when saving it, unintended results may occur. Therefore, a null character must be inserted into the buffer range, so the string can be terminated with a null character.

<Table 23> Code example

Unsafe code	…typedef struct _charvoid {
	char x[16];
	void * y;
	void * z;
	} charvoid
	void badCode() {
	charvoid cv_struct
	cv_struct.y = (void *) SRC_STR;
	printLine((char *) cv_struct.y);
	/* The pointer y is overwritten due to the use of sizeof(cv_struct) */
	memcpy(cv_struct.x, SRC_STR, sizeof(cv_struct));
	printLine((char *) cv_struct.x);
	printLine((char *) cv_struct.y);
	}

	This program copies a specific string to the individual field of a pointer structure. The program causes a buffer overflow that overwrites the contiguous memory space pointer y, due to the data size sizeof(cv_struct), which is incorrectly calculated. Also, incorrect results can be obtained when referring to a string, because the program has not added a terminating character to the copied string.

Safe code	typedef struct _charvoid {
	  char x[16];
	  void * y;
	  void * z;
	} charvoid
	
	static void goodCode() {
	  charvoid cv_struct
	  cv_struct.y = (void *) SRC_STR;
	  printLine((char *) cv_struct.y);
	  /* Change to sizeof(cv_struct.x) to prevent the overwriting of pointer y */
	memcpy(cv_struct.x, SRC_STR, sizeof(cv_struct.x));
	  /* Insert a null character to end with a string */
	cv_struct.x[(sizeof(cv_struct.x)/sizeof(char))-1] = '\0';
	  printLine((char *) cv_struct.x);
	  printLine((char *) cv_struct.y);
	}

	To make a code secure, first, modify the code in a way that only the index within the allowed range is used, by using sizeof(cv_struct.x), which calculates an exact string, because a string copy is limited to the field value x within the struct. Second, since the copied string should have the correct null information, the last index of the array cv_struct.x, which has the copied value, should be calculated and padded with a null character.

② Secure coding techniques for responding to the format string insertion attack

• Attack overview:

This security weakness could occur if the value entered from the outside is not verified and used as the format string of the input/output function. An attacker can attack a vulnerable process, or read or write memory content, by using the format string. As a result, the attacker can obtain the rights of the vulnerable process and execute random code.

• Coding technique:

When using the function that uses a format string such as printf() and snprintf(), the user input value should not be used as a format string, or included in format string creation. When using the user input value for the function that uses a format string, a structure that enables the user to change the format string should not be used.

<Table 24> Code example

Unsafe code	void incorrect_password(const char *user) {
	  static const char msg_format[] = "%s cannot be authenticated.\n";
	  size_t len = strlen(user) + sizeof(msg_format);
	  char *msg = (char *)malloc(len);
	  if (msg == NULL) {
	  /* Error handling */
	  }
	  int ret = snprintf(msg, len, msg_format, user);
	  if (ret < 0 || ret >= len) {
	  /* Error handling */
	  }
	fprintf(stderr, msg);
	  free(msg);
	  msg = NULL;
	}

	msg is vulnerable to format string insertion because it contains an unreliable user input and is passed as a format string argument, when fprintf() is called.

Safe code	void incorrect_password(const char *user) {
	static const char msg_format[] = "%s cannot be authenticated.\n";
	size_t len = strlen(user) + sizeof(msg_format);
	char *msg = (char *)malloc(len);
	if (msg == NULL) {
	/* Error handling */
	}
	int ret = snprintf(msg, len, msg_format, user);
	if (ret < 0 || ret >= len) {
	/* Error handling */
	}
	if (fputs(msg, stderr) == EOF) {
	/* Error handling */
	}
	free(msg);
	msg = NULL;
	}

	The example uses fputs(), instead of fprintf(), to output msg as stderr, without treating is as a format string.

C) Major secure coding techniques for Android-Java

① Secure coding technique for responding to the attack against the component that can be accessed from the outside

• Attack overview:

If android: exported="true" is set in the manifest.xml file for the component of the Android application, intent can be transferred to the component, from outside, to activate it. In this case, system security can be breached, because the company starts execution in an unintended situation.

• Coding technique:

It is desirable to not give the access rights to the component to the outside.

<Table 25> Code example

Unsafe code	<manifest xmlns:….> <application android:icon="@drawable/icon" android:label="@string/label"> <service android:name=".syncadapter.SyncService" android:exported="true"> …. </application> </manifest>
	Since the attribute value of the SyncService service is set to android:exported="true", a security vulnerability may occur when the component is started from outside.
Safe code	<manifest xmlns:….> <application android:icon="@drawable/icon" android:label="@string/label"> <service android:name=".syncadapter.SyncService" android:exported="false"> …. </application> </manifest>
	If the Android:exported property is set to "false" or the setting is removed, the attribute becomes "false" and access from the outside is blocked.

② Secure coding techniques for responding to the access control pass attack, using the shared ID

• Attack overview:

If the android: sharedUserId attribute is set for the manifest tag in the Manifest.xml file, other application programs can access the information of the program by using the same ID and signature. Due to this weakness, the integrity and security of the program may be intentionally and unintentionally breached.

- Coding technique:
  It is desirable to not set a shared ID.

<Table 26> Code example

Unsafe code	<manifest xmlns:android="http://schemas.android.com/apk/res/android" Package="com.example.android.apis" android:versionCode="1" android:versionName="1.0" android:sharedUserId="android.uid.developer1">
	Since the android:sharedUserId attribute is set for the manifest tag in the Manifest.xml file, other applications with the same shareduserId tag value and application program signature can access all the data of this program.
Safe code	<manifest xmlns:android="http://schemas.android.com/apk/res/android" Package="com.example.android.apis" android:versionCode="1" android:versionName="1.0"> <!-- Delete android:sharedUserId="android.uid.developer1". -->
	Prevent the risk of data leakage or inappropriate access, due to the shared ID, by not setting the android:sharedUserId attribute for the manifest tag in the Manifest.xml file.

VI. Data Security

▶▶▶ Subject

Managing database safely!

▶▶▶ Recent trends and major issues

An amendment to the Personal Information Protection Act, which mandates the encrypted storage of the resident registration number, passed the National Assembly plenary session on February 28, 2014. The content of the amendment is that the personal information handlers, who keep the resident registration number, are obligated to encrypt the resident registration number in order to minimize damage if the personal information is leaked. Matters concerning the targets of encryption and application timing of each target are determined by Presidential Decree, considering the size of the personal information processing and the impact of leakage. However, its implementation is delayed, because enormous costs are required to encrypt the social security number, risk of failure, and concern about rapid performance degradation after encryption. Recently, there has been a spike in interest in database encryption, due to these trends and issues.

▶▶▶ Learning objectives

To be able to explain database security requirements.

To be able to explain control elements for database security.

To be able to select a database for encryption and apply cryptographic techniques.

▶▶▶ Keywords

Virtual tables (views), database access control, API method, plug-in method, TDE method, master key, key life cycle, HSM (Hard Security Module), random number generator

✚ Preview for practical business

Since the database collects and stores a large amount of data, from personal information, to corporate confidential information, it is an important asset to protect for an organization, in addition to being a key target for attackers. Therefore, database access control and encryption policies should be established, and countermeasures should be prepared to identify various security threat elements of the database and safely protect important data from these security threats.

Company A decided to come up with access control and encryption measures to safely manage the database and requested consulting by submitting the following requirements to the consulting company:

1) Company A experiences frequent organization and business changes. Therefore, the company needs a database access control system that can be flexibly applied to such changes.
2) Company A should encrypt uniquely identifiable information, within the period stipulated by the law, in accordance with the revision of the Personal Information Protection Act.
3) Company A should thoroughly analyze the impact of encrypting uniquely identifiable information in order to prevent system failure and performance degradation.

Therefore, let's review the database access control system that is desirable for company A, and the methods for encrypting uniquely identifiable information and matters to consider.

01 Overview of database security

A) Overview of database security

① Three principles of database security

Database security means taking administrative, physical, and technical protection measures in order to secure confidentiality, integrity, and availability from the threat of leakage, change, or destruction of organizational database information.

In the past, the performance of DB was emphasized, but safe management and data protection is becoming especially important in recent years, which proves that the value of data is increasing with the advancement of IT services. Since the database collects and stores a large amount of data, from personal information, to corporate confidential information, it is an important asset to protect for an organization, and a key target for attackers.

<Table 27> Three principles of database security

Three principles of security	Details	Implementation plan
Confidentiality	• Blocking the leakage of information stored in the database • Only the authorized person accesses the database to view information	Database privilege management Database encryption
Integrity	• Only authorized person can change database information	Database privilege management
Availability	• Ensuring continuous and uninterrupted database services	Database redundancy

② Need for database security

• Database security for sustainable management

Recently, personal information leakage incidents have occurred in succession, such as H capital, S portal, N game company, K telecom, etc., which emphasize the necessity of database security. Database security is a prerequisite for sustainable management because enormous economic loss, along with a decline in customer trust, can threaten the foundation of a business, if database information is leaked.

• Database security for responding to regulations

Recently, the importance of database security has been emphasized because it is mandated by related laws, such as the Personal Information Protection Act, the Information Communication Network Act, the Electronic Financial Transaction Act, etc., in addition to the importance of personal information protection.

B) Database security threats and responses

① Database security threats

Database security threats can be caused by a variety of factors, but general database security threats to the organization can be classified into the following four:

<Table 28> Database security threats

Security threat	Description
Web security threats	Illegal information acquisition by unauthorized external users, using the SQL injection attack or web shell execution, after uploading a file.
Vulnerable identification and authentication	Making repetitive authentication attempts to obtain the legitimate user's identity or acquiring the authorized user's identity, using social engineering techniques, etc.
Data leakage	Acquiring illegal information by stealing unencrypted data and by decrypting the encrypted data.
Misuse of cryptographic modules	Decrypting ciphertext, using unreliable cryptographic modules and an inappropriate cryptographic mode.

② Countermeasures against database security threats

There are access controls, views, and cryptographic techniques to cope with database security threats.

<Table 29> Countermeasures against database security threats

Item	Details	Case
Access controls	Allowing only authorized users to access the database and preventing unauthorized users from accessing the database itself.	Account management MAC, DAC, RBAC
Views	Limiting access to the permitted data only among the entire database, using views.	CREATE VIEW
Encryption	Saving important data after encrypting with one-way and two-way cipher algorithms.	SEED, AES SHA-256

02 Database access control

A) Database access control policy

① Discretionary access control (DAC) policy

A method of controlling access to objects, based on the subject or the identity of the group to which the subject belongs. On object owner determines access permission.
e.g.,) The owner of the table can grant or revoke the privilege to another person.

② Mandatory access control (MAC) policy

Access to an object is controlled, based on the owner's rights to the confidential object.
e.g.,) Allowing only the database administrator to access the system catalog.

③ Role-based access control (RBAC) policy

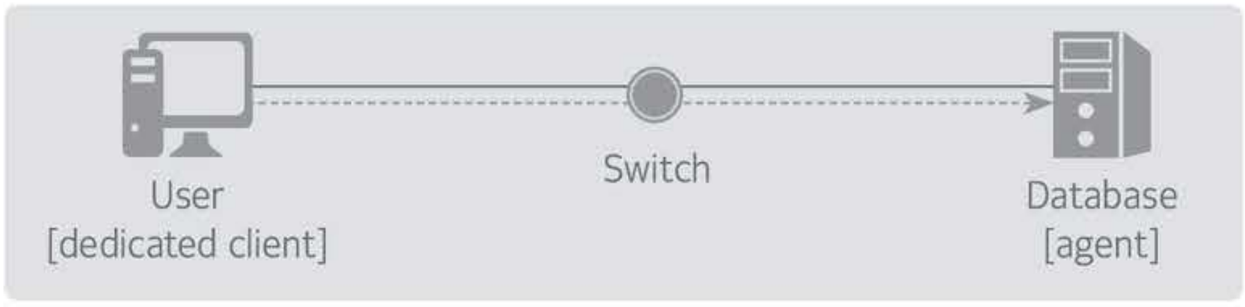
The central administrator controls the relationship between the subject and object, and decides on access to the resource, based on their roles in the organization.

e.g.,) Defining DBA roles and granting RBA roles and necessary privileges to a specific person.

B) Method of controlling access to the database

① Agent method

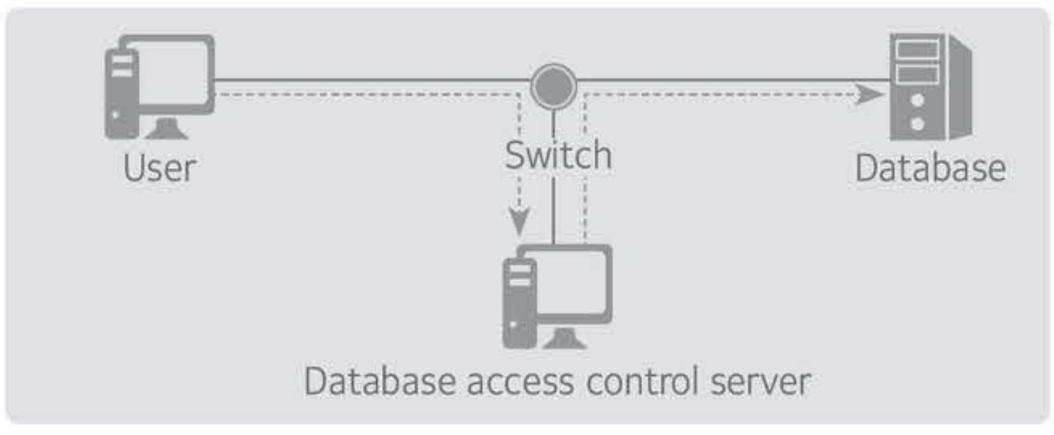
A method of accessing a database, using a dedicated client for database access, after installing an agent with the access control and logging function in the database server itself. This method can implement strong access control, but it can cause performance degradation of the database server, due to the traffic therein.



[Figure 39] Database access control by the agent method

② Gateway method

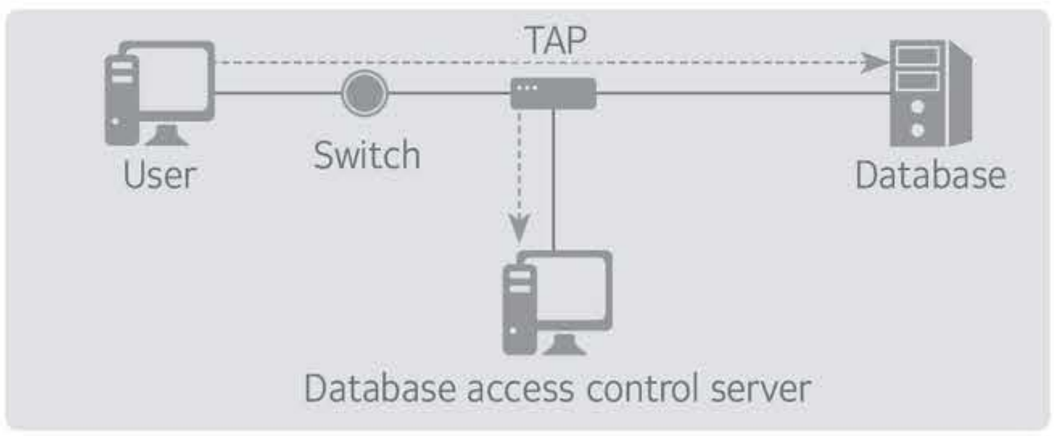
A method of passing all database server connection requests through the database access control server (proxy server). This method provides the most powerful access control function. As the database access control server can be configured in redundancy, work is not affected, even when a failure occurs.



[Figure 40] Database access control by the gateway method

③ Network sniffing method

A method of analyzing and logging network packets, using TAP equipment, etc. There is no need to install a separate agent between the database server and client, and a system can be built, without any load on the network. However, it is not easy to fundamentally block the damage to the data integrity caused by improper alteration.



[Figure 41] Database access control by the network sniffing method

④ Hybrid method

To compensate for the shortcomings of each method, a hybrid method of mixing each method is commonly used to control database access. The hybrid method is used in the form of agent + gateway method, gateway + network sniffing method, agent + gateway + network sniffing method.

03 Database encryption

A) Considerations when applying database encryption

When applying database encryption, data column to encrypt, encryption algorithm to use, impact of encryption on performance, and encryption key management method should be considered.

<Table 30> Considerations when applying database encryption

Matters to consider	Description
Encryption target and method	Selecting the data designated by domestic laws and regulations and other important data
Cryptographic algorithm	An algorithm, recommended by cryptography research institutes at home and abroad, should be applied. A one-way algorithm (SHA-256 or higher) should be applied to passwords, and a two-way algorithm (SEED, ARIA, AES, etc.) should be applied to other information.
Search and performance	When applying encryption, performance, such as index maintenance, should be considered. Also, a method of applying partial encryption, etc. should be considered.
Encryption key management	Encryption/decryption keys and master keys should be safely managed, from its generation, to its destruction.

B) Target and method of database encryption

Data, designated by domestic laws and regulations, and other important data should be selected as an encryption target first. The database information to encrypt, in accordance with each law and regulation, includes passwords, bio information, resident registration numbers, passport numbers, driver's license numbers, foreign registration numbers, credit card numbers, account numbers, transaction logs, etc. Different encryption methods are required, according to the characteristics of information, and a database should be encrypted/decrypted, using a cryptographic algorithm that fits each characteristic.

<Table 31> Target and method of database encryption

Item	Target	Encryption method
Common	Passwords	Storage after one-way encryption
Personal Information Protection Act	Passport numbers	Storing after encryption, with a secure two-way cipher algorithm
	Driver's license numbers	
	Foreign registration numbers	
	Resident registration numbers	
	Bio information	

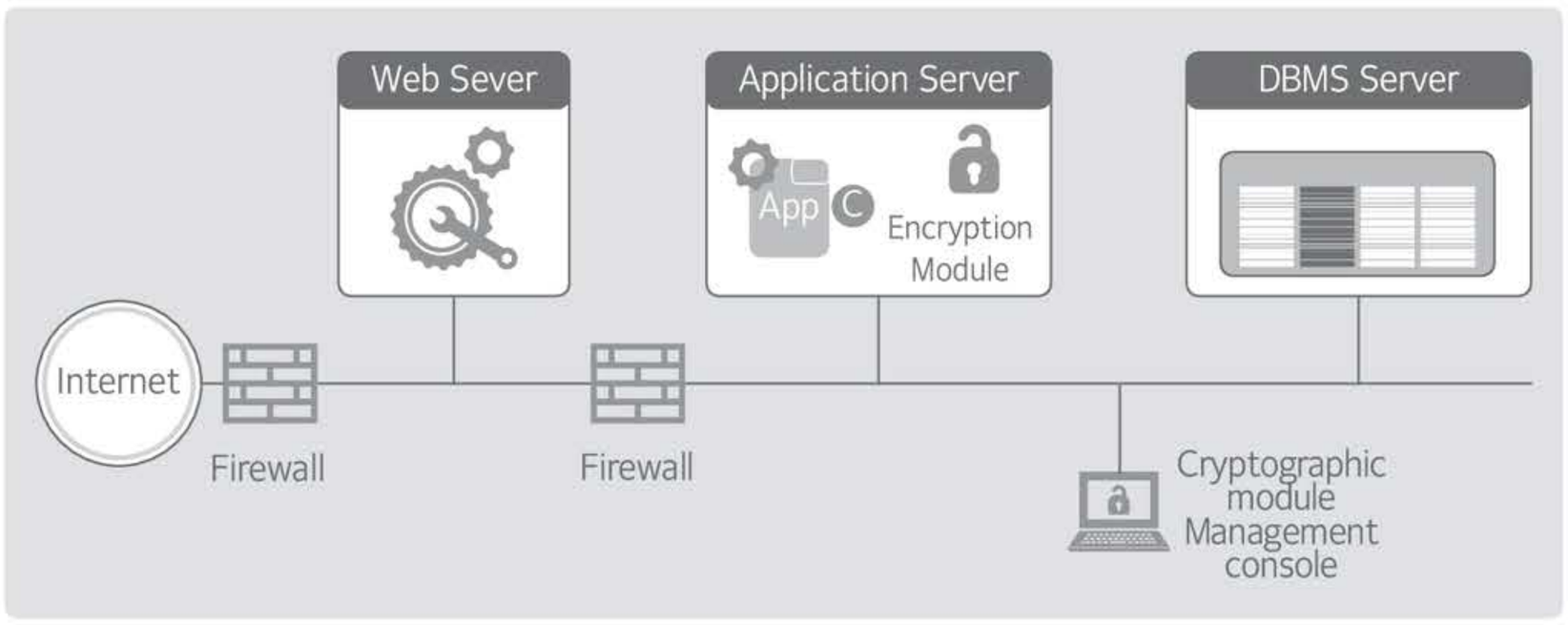
Information and Communication Network Act	Resident registration numbers	Storing after encryption, with a secure two-way cipher algorithm
	Account numbers	
	Bio information	
Electronic financial supervision regulations	Transaction logs	Storage after encryption

C) Types of database encryption

There are various types of database encryption, such as the API type, plug-in type, TDE type, and hybrid type or proxy type, that combines the API and plug-in type.

① API method

API type database encryption performs encryption/decryption by installing an encryption/decryption module inside an application program server. It requires the modification of multiple application programs, and data is transmitted after encryption between the AP server and database server. There is a low possibility that a load is created in the database server, but a load is likely to be created in the AP server.

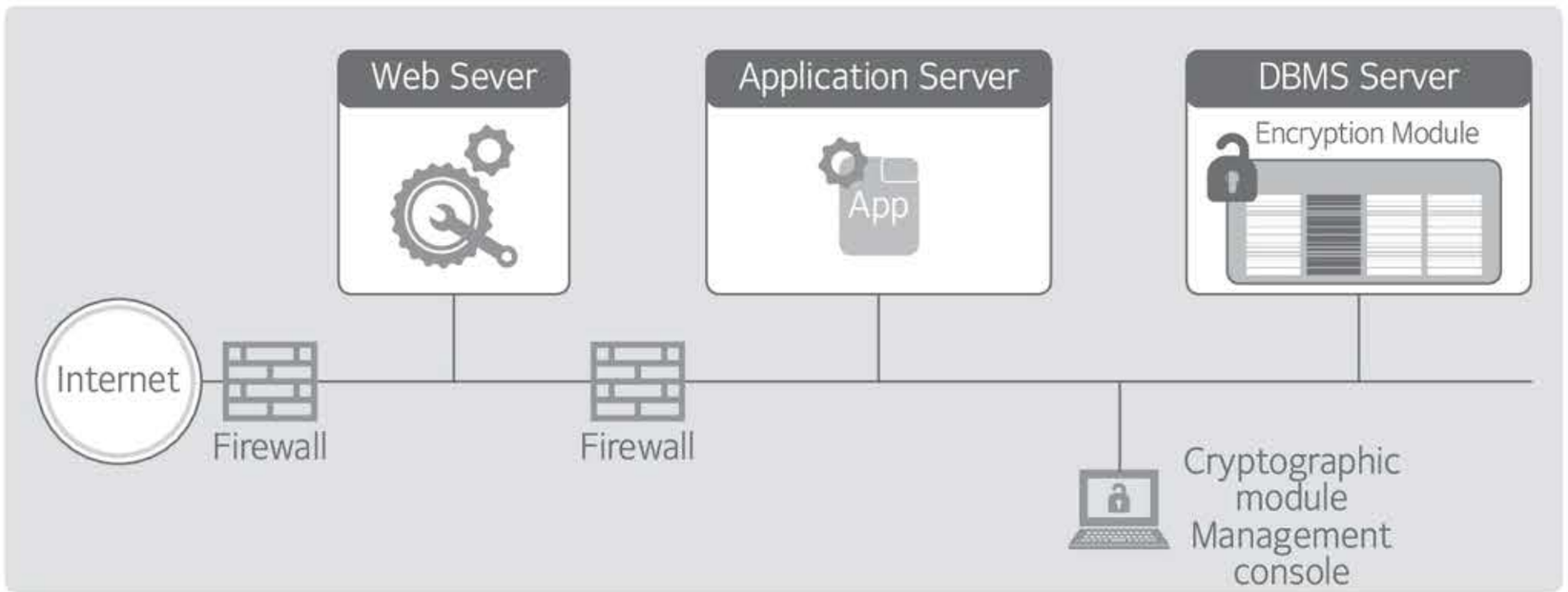


[Figure 42] API type database encryption

If the application program is easy to modify and the performance of the database server is poor, it is recommended to select this type, as data is transmitted after being encrypted through the network.

② Plug-in type

When the plug-in type is used, the encryption/decryption module is installed inside the database server in order to perform encryption/decryption. A load on the database server may be created and data is exchanged between the AP server and database server in plain text when it is encrypted/decrypted.

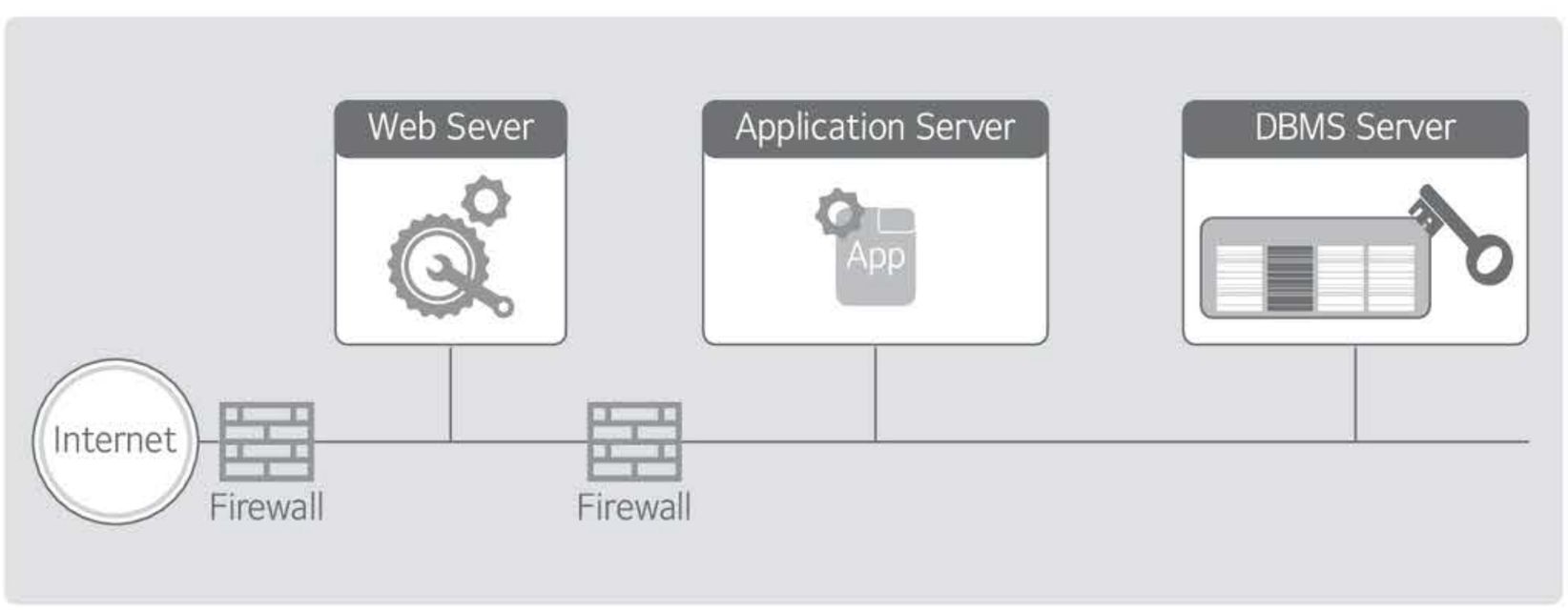


[Figure 43] Plug-in type database encryption

It is recommended to select this type when database performance is good, and the application program is difficult or impossible to modify.

③ TDE method

A method of using the built-in or optional encryption/decryption function of the database. This type can be supported, depending on the DBMS type and version. There is no modification to the application program because encryption/decryption is performed at the DBMS kernel level. However, this type may not be supported, depending on the DBMS type or version. The selection of this type can be considered when introducing a new DBMS.



[Figure 44] TDE type database encryption

D) Applying database encryption

The concepts of a one-way cipher algorithm and a two-way cipher algorithm can be applied to the database as follows:

① Application of a one-way cipher algorithm

Original data extraction by computation should be made impossible, using a hash cipher algorithm (one-way cipher algorithm), and a cryptographic hash function, above SHA-256, is generally used.
Currently, there are two cases when the one-way cipher algorithm should be applied: when data is saved in plain text in the existing database, and when an insecure hash cipher algorithm, such as MD5 or SHA-1, is used.

• When data is stored in plain text

If passwords are stored in plain text and the hash cipher algorithm is applied only to passwords, they may be vulnerable to dictionary attacks, such as Rainbow attacks. Therefore, the SALT value, which is a random string, should be added to the user's password, and the hash cipher algorithm should be applied. Then, the SALT value should be stored in a safe place.

If the password is stored in plain text

EmpNum	LastName	FirstName	Password(plain text)
10001	KIM	NAMIL	1234
10002	LEE	YOUNGPYO	god
10003	CHA	DORI	angel

Input : Password + SALT → SHA-256 → Ciphertext (hash value)

Storing the salt in a safe place

EmpNum	LastName	FirstName	Password(SHA-256)
10001	KIM	NAMIL	03ac674216..
10002	LEE	YOUNGPYO	11043a8795..
10003	CHA	DORI	C9d751a1a..

[Figure 45] When data is stored in plain text

• If an insecure hash cipher algorithm is used

If an insecure hash cipher algorithm, such as MD5 or SHA-1, is used, the previously stored hash value should first be converted into a double hashed value, by applying the SHA-256 hash cipher algorithm, before storing it. Then, the data of the successfully logged-in user should be gradually converted into a single hash value, using SHA-256, before storing it. At this time, the login success time should be used, or a separate column should be added in order to check whether the data has a single hash value or a double hash value.

If an insecure hash cipher algorithm is used

EmpNum	LastName	FirstName	Password(MD5)
10001	KIM	NAMIL	930e1c89..
10002	LEE	YOUNGPYO	347ed2f4..
10003	CHA	DORI	ed6f836d..

Input: Ciphertext (hash value) + SALT → SHA-256 → Ciphertext (hash value)

Converting into a single hash value using SHA-256 for successfully logged-in users only

EmpNum	LastName	FirstName	Password(SHA-256)
10001	KIM	NAMIL	03ac674216..
10002	LEE	YOUNGPYO	11043a8795..
10003	CHA	DORI	C9d751a1a..

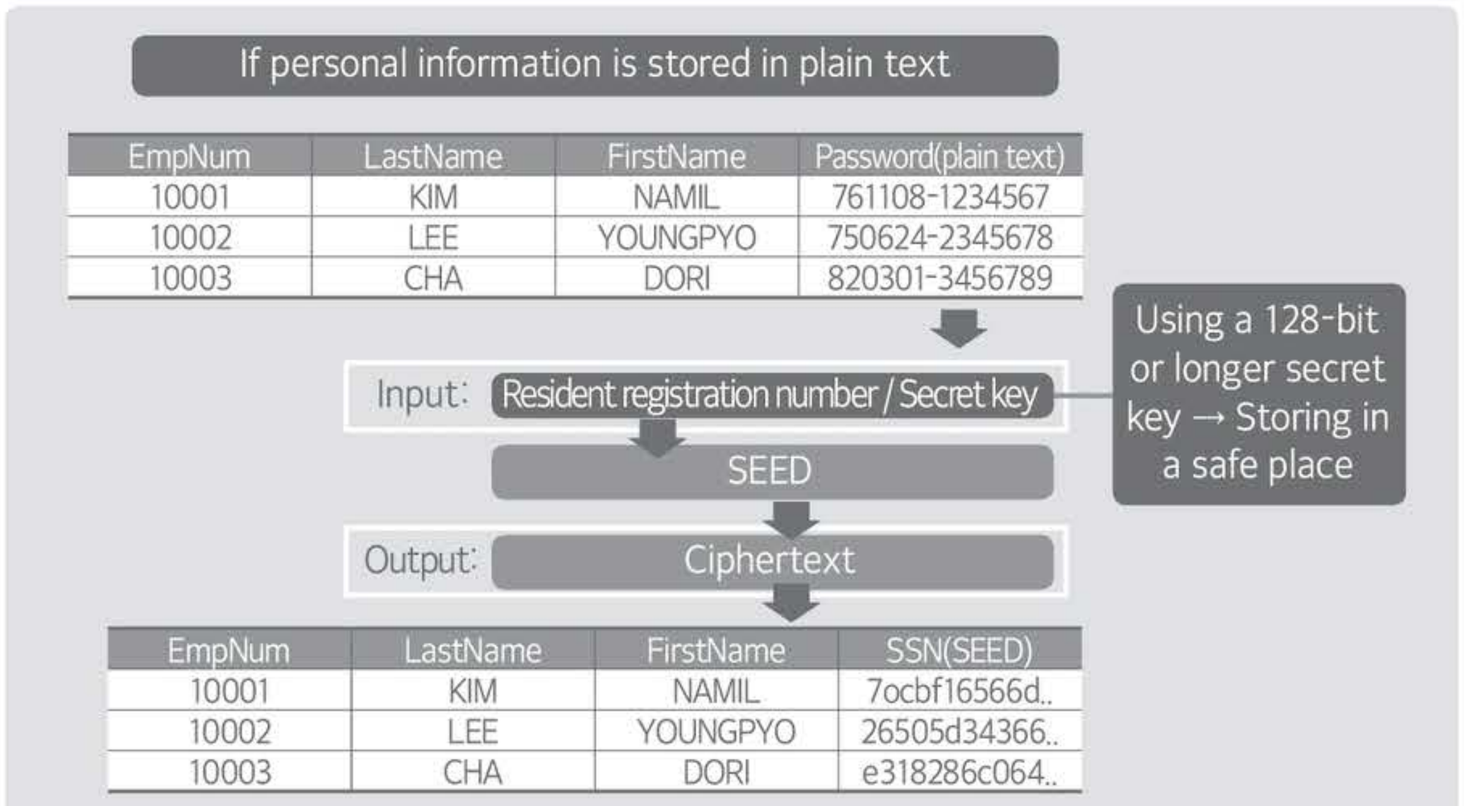
[Figure 46] If an insecure hash cipher algorithm is used

② Application of a two-way cipher algorithm

Data, such as personal information, should be encrypted and decrypted using a two-way cipher algorithm. Secure block cipher algorithms, such as SEED, ARIA, and AES (Rijndael), are generally used.
Currently, there are two cases when the secure block cipher algorithm should be applied: when data is saved in plain text in the existing database, and when an insecure cipher algorithm, such as DES or 3-DES, is used.

• When data stored is in plain text

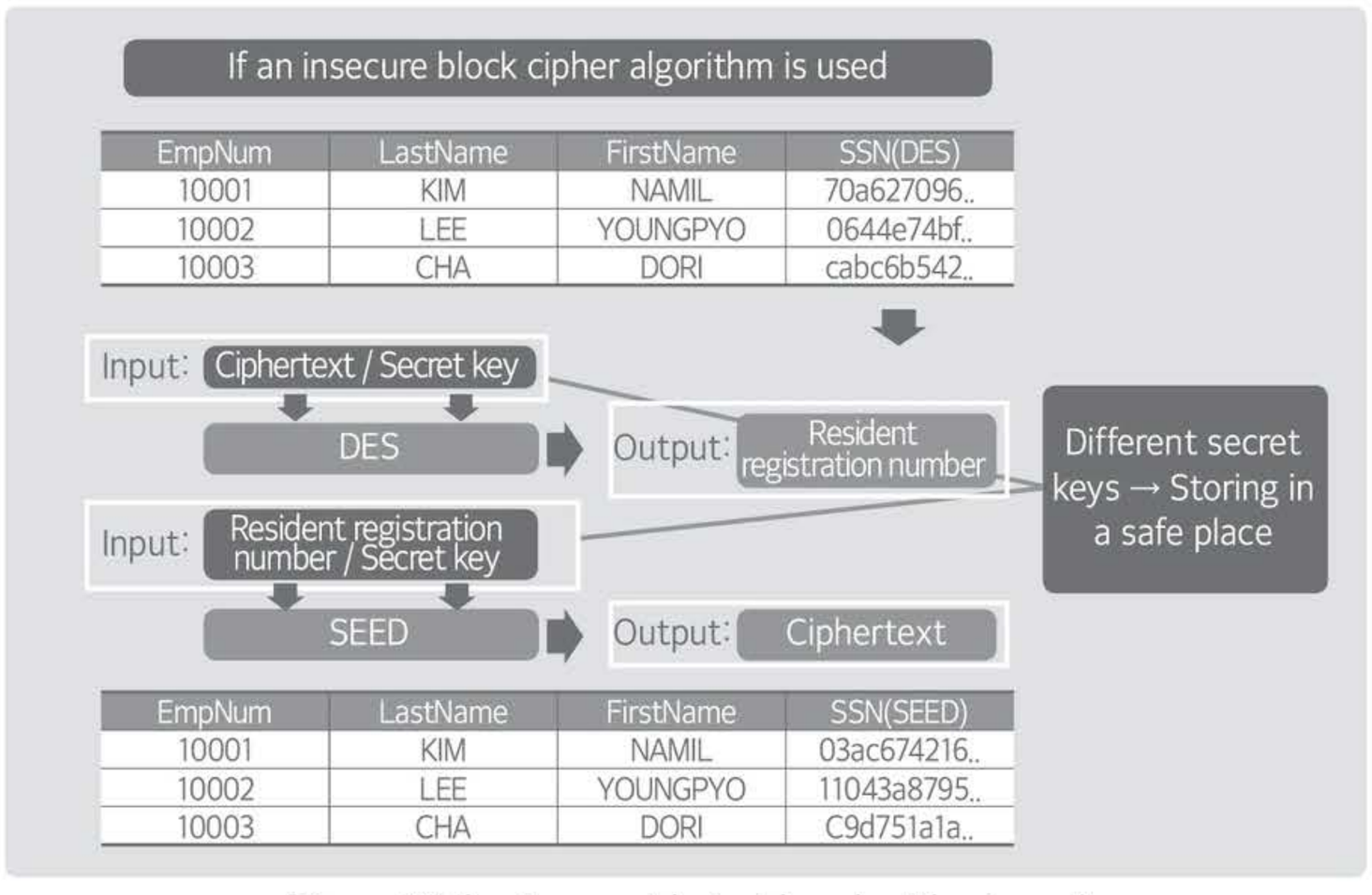
When personal information is stored in plain text, it should be encrypted and stored, using a 128-bit or higher secret key, and the used secret key should be stored in a separate safe place.



[Figure 47] When personal information is stored in plain text

• If an insecure block cipher algorithm is used

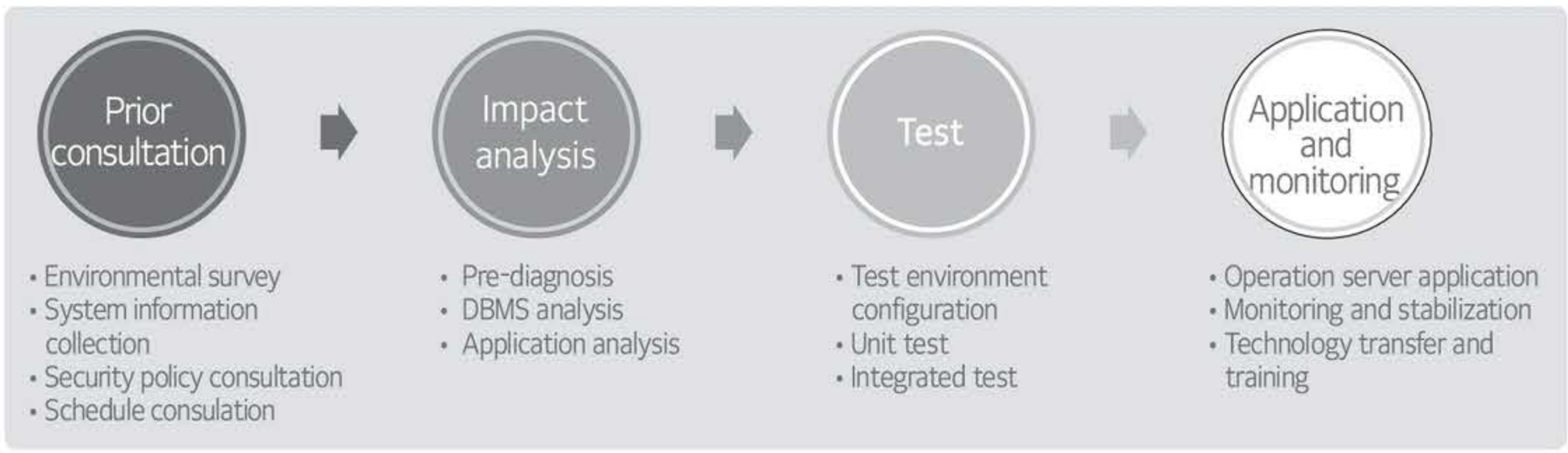
If an insecure block encryption algorithm, such as DES or 3-DES, is used, the existing encrypted data is decrypted, using a batch job processing method, then encryption is performed, using a secure block encryption algorithm.



[Figure 48] If an insecure block cipher algorithm is used

E) Procedure of applying database encryption

A database is encrypted with the procedure of [Figure 49], which consists of prior consultation, prior impact analysis, test verification, build, and stabilization.



[Figure 49] If an insecure block cipher algorithm is used

① Prior consultation for encrypting a database

All stakeholders participating in the project should consult on necessary matters in advance to share necessary information in advance, such as the database to be encrypted to apply the database application security, the applicable environment, the security policy, etc., before applying security to the DB application.

② Analyzing the impact of database encryption

In this phase, the operational server is monitored and the impact on the application and DBMS is analyzed, before applying security to the database application.

This phase is one of the most important phases in applying security to database applications. Before applying encryption to the operating system, it is necessary to perform encryption pre-diagnosis, such as extracting encryption targets and encryption-related SQL queries in advance, running performance tests on the test system, etc. Overall, the DBMS and application are analyzed in order to analyze the impact on changes in performance and system resources after encryption.

• Selecting an encryption target

The encryption target should be determined by searching the tables and columns of the entire operating DBMS to extract the columns needing to be encrypted.

• Analyzing query statements

The amount of data extracted when executing query statements and the time of query statement execution should be analyzed, and the query statement expected to need optimization should be selected, by extracting all query statements used in all operating DBMS.

• Analyzing DBMS

The resources used by the DBMS, such as CPU, memory, and storage, should be checked, and the appropriate level of additional resources, that are required when applying encryption, should be calculated.

• Analyzing applications

The application modules that are affected by the application of encryption should be extracted, and the

common modules that are additionally required to apply encryption, as well as application logic that needs to be changed should be analyzed. Then, the application module that needs to be optimized should be selected.

③ Testing database encryption

Business tests, such as applications, are conducted in this phase, after applying encryption, by creating the same test environment as the database application operating environment. The problems that can occur when migrating to an operating environment, should be identified by running tests. Migration to the operational environment should be prepared by resolving all issues. All applications and all query statements should be tested.

④ Applying and monitoring database encryption

Database application security should be applied to the operating environment in this phase, by synthesizing the items verified in the test phase. Encryption should be applied to data, and source code that was modified in the test and verification phase, and optimized query statements should be reflected. Issues that were identified in the test phase should be resolved and applied to the operating environment. It should be continuously monitored and checked whether any errors occur in the applied applications and query statements, and whether applications are running properly.

04 Database encryption key management

A) Type of database encryption keys

If the encryption/decryption key is leaked, the encryption is not effective. Therefore, the encryption key should be redundant (encryption/decryption key and the master key), according to the principle of key redundancy, so that only authorized persons can access it.

<Table 32> Database encryption key

Type	Description
Encryption/decryption key	A key used to encrypt data, and to decrypt the already encrypted data.
Master key	A key used to store and distribute the encryption and decryption key after encryption.

B) Management methods by encryption key lifecycle

① Key generation stage

An encryption/decryption key should be generated using a safe random number generator, and an algorithm with proven stability should be used for the encryption key derived from user input.

② Key distribution stage

Security should be maintained when distributing keys, by encrypting the encryption keys using an asymmetric key cipher algorithm, so that only the authorized person can access the keys.

③ Key storage stage

Encryption keys should be stored using the hardware storage method, such as a separate key management server or an HSM (Hard Security Module), instead of hardcoding the encryption key into the application program, saving as a file in the file system, or storing the encryption key inside the DBMS.

④ Key use stage

The database administrator and security manager should apply the principles of "granting least privilege and separation of duty", and they should only allow authorized persons to access or modify the master key.

⑤ Key backup and recovery stage

Backup and recovery procedures for the encryption key should be prepared to recover it when lost or damaged, and the encryption key should be backed up periodically, according to the key backup policy.

⑥ Key replacement stage

The security of the encryption key should be maintained by replacing it periodically, according to the internal policy of the organization. Before replacing the encryption key, data should be decrypted with the existing encryption key, and a new encryption key should be created. Then, the data should be encrypted again.

⑦ Key destruction stage

When the encryption key is lost or damaged, the data should be decrypted using the encryption key that has been backed up by the administrator, according to the procedure stipulated by the organization policy. A new encryption key should be generated, and the data should be encrypted with the generated key again. Then, the lost or damaged encryption key should be destroyed.

VII. System Architecture Security

▶▶▶ Subject

Managing systems safely!

▶▶▶ Recent trends and major issues

Recently, the number of attacks targeting the system, such as the server, is increasing, using APT attacks. Accordingly, the importance of system security is also increasing together with network security, such as the firewall and intrusion detection system. In particular, efforts should be made to strengthen access control to the system, security settings, and account management, in order to respond to the hijacking of system administrator's rights or inappropriate access of internal users to information security resources.

▶▶▶ Learning objectives

To be able to apply security settings to the Windows system.

To be able to apply security settings to the UNIX and Linux system.

▶▶▶ Keywords

Account and password management, shared folder management, service security, password crack, UMASK, daemon, anonymous FTP, secure FTP

✚ Preview for practical business

All systems of major domestic broadcasting companies and financial companies were paralyzed, due to exposure to cyber terror, on March 20, 2013. The internal computer networks of 3 broadcasting companies and 4 financial companies were down all at once, around 2 pm on this day, and serious confusion occurred. As computer networks at similar institutions were down at the same time, the police suspected a high possibility of cyber terror and began an investigation. The Korea Communications Commission announced that the incident was caused by malware, distributed by the update management server (PMS), and the extent of the damage was so enormous that it was difficult to estimate.

Financial company A, a hacking victim, analyzed three major causes of hacking damage:

1) The administrator PC was not secure enough and servers could be accessed from the IP address, other than that of the administrator.
2) Security patches were not applied properly, and authentication of the updated server was weak.
3) Default passwords were used, and the use of unnecessary commands were not restricted.

Let's learn how to set security, according to the system characteristics, to effectively respond to cyber-attack damage, such as in the case of company A, and how to manage systems safely, based on such understanding.

01 Windows system security

A) Overview of Windows system security

Windows systems are widely used as PC operating systems, and they require security management in various areas, such as account and password management, access control, system security, service security, monitoring, and other security management.

<Table 33> Windows system security

Item	Detailed item
Account and password management	• Checks related to accounts (unnecessary accounts, accounts with an administrator privilege) • Checks related to passwords (vulnerable passwords, encryption, automatic account locks in case of password error, maximum password usage period, etc.)
Access control	• Access control setting checks (shared folders, remote registry access, automatic screen locks, etc.)
System security	• Privilege setting checks (system directory privilege, Windows account privilege, system utilization rates, etc.)
Service security	• Service shutdown (unnecessary service, terminal service, anonymous FTP, SNMP settings, etc.)
Monitoring	• System audit policies, log record settings, etc.
Other security management	• Security settings, scheduling details, anti-virus use status, and latest patch checks

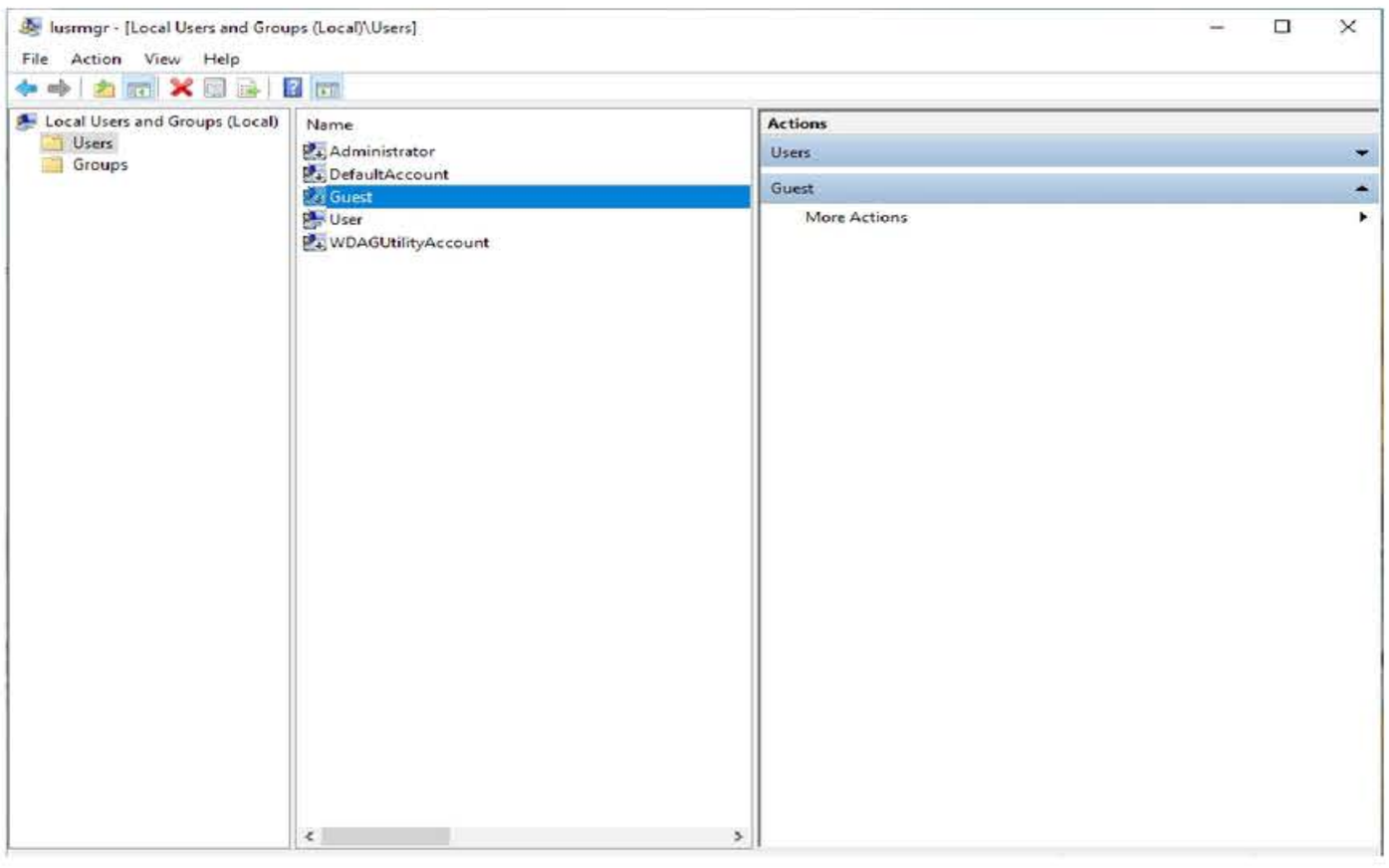
B) Account and password management

① Deleting guest accounts and unnecessary accounts

Restrict the use of the guest account. If access by unspecified individuals is required, general user accounts, not guest accounts, should be created and used. Execute lusrmgr.msc (local users and groups) and delete guest accounts and unnecessary accounts.

• How to delete unnecessary accounts

Input lusrmgr.msc into the search programs and files box, by selecting [Start], and delete guest accounts and unnecessary accounts from local users and groups.



[Figure 50] Deleting unnecessary accounts

② Setting account lockout

The account lockout policy should be checked and set to respond to the brute force attack or password crack attack, by setting account locks, according to the number of logon failures, in the security policy settings to improve system security.

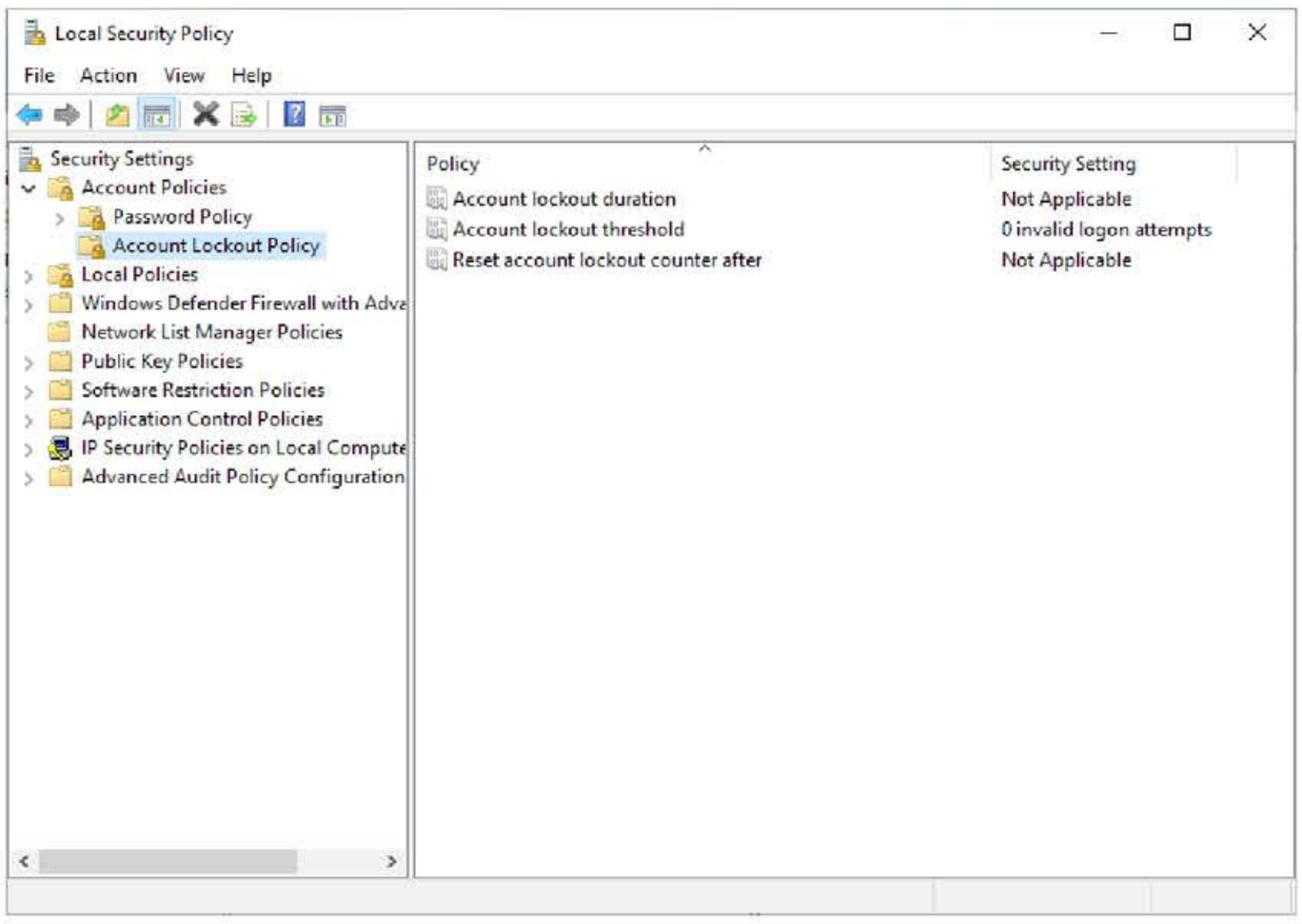
It is desirable to set "Account lockout duration" to 60 minutes, "Account lockout threshold" to 5 times, and "Reset account lockout counter after" to 60 minutes in Account Lockout Policy.

• How to set account lockout

Input secpol.msc into the Search programs and files box by selecting [Start].

Click the "Account Lockout Policy" sub-menu under the [Account Policies] menu.

Set "Account lockout duration", "Account lockout threshold", and "Reset account lockout counter after".



[Figure 51] Setting account lockout

C) Access control

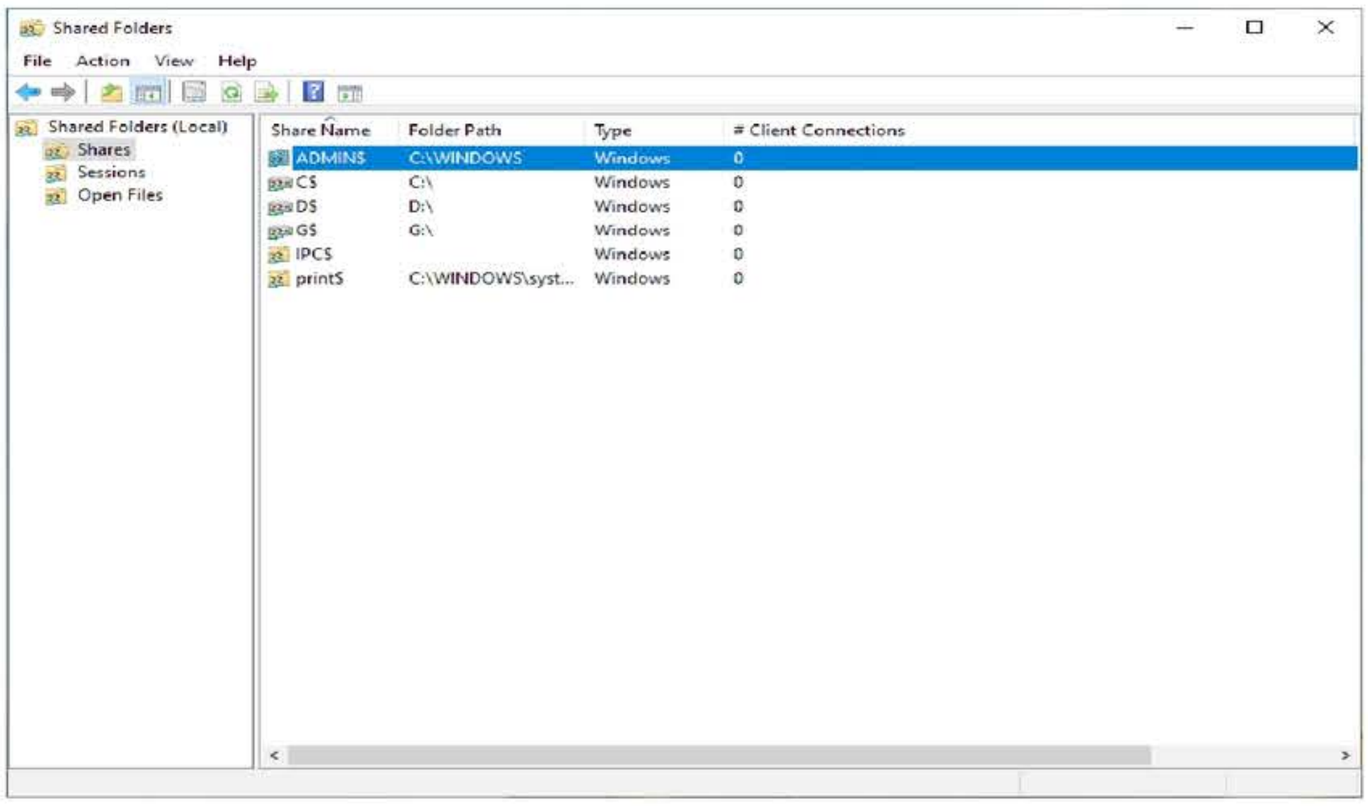
① Checking unnecessary shared folders and stopping sharing

Since malware and viruses may spread through unnecessarily shared folders, unnecessary shared folders should be removed. If a shared folder needs to be used, only authorized users should be allowed to access the shared folder. Also, check the shared folder using fsmgmt.msc and stop sharing if unnecessary.

• How to stop sharing unnecessary shared folders

Input fsmgmt.msc into the search programs and files box by selecting [Start].

Check unnecessary shared folders and stop sharing if sharing is not necessary.



[Figure 52] Stop sharing unnecessary shared folders

D) System security

① Turning off automatic administrator logon in Windows

If the automatic logon function is used, an attacker can check the login account and password in the Windows registry, using hacking tools. Therefore, the automatic logon function must be disabled by setting the AutoAdminLogon value in the Windows registry to "0".

- How to turn off automatic administrator logon in Windows
  Input regedit into the Search programs and files box by selecting [Start], and
  Set the AutoAdminLogon value in the HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon entry to "0".
  If there is a "DefaultPassword entry", delete it.

② Checking startup programs

Startup programs include the programs that are executed when the computer boots. However, malware can copy its code in this folder so that it is executed when the computer starts. Therefore, delete any unauthorized or unnecessary programs from the Startup programs.

- How to delete startup programs
  Input msconfig into the search programs and files box by selecting [Start].
  When the System Configuration dialog box opens, click the Startup tab.
  Check for unauthorized or unnecessary programs and click the check (√) mark on the program to remove and then, click the [OK] button.
  When a pop-up window appears, prompting that the computer needs to be restarted, click the [Restart] button.

E) Service security

① 2.5.1 Stopping unnecessary startup services

Unnecessary services should be stopped, because unnecessary system services can be installed and executed by default, and these services can become a security vulnerability in the system, or they can waste system resources. It is recommended not to use the service installed by default, or the services that are not used for a specific purpose. The system administrator should accurately identify the purpose of the target system and remove unnecessary services.

- How to stop unnecessary startup services
  Input services.msc into the search programs and files box by selecting [Start].
  Stop the unnecessary service on the list and change "Startup type" to "Disabled".

F) Checking the terminal service

Remote Desktop Services is a tool used to manage remote servers. However, if a weak password is used or access control is not adequate, it can be exploited as a hacking tool. Therefore, it should be checked whether unnecessary Remote Desktop Services is used or not. If Remote Desktop Services is used, the encryption level should be set to "Medium" or higher.

02 Unix-like system security

A) Overview of Unix-like system security

Unix-like operating systems, which are widely used as server operating systems, include Unix and Linux-like operating systems. Security management is needed in various areas, such as account and password management, access controls, system security, service security, monitoring, and other security management.

<Table 33> Unix-like system security

Item	Detailed item
Account and password management	Checks related to accounts (unnecessary accounts, accounts with a root privilege)
	Checks related to passwords (vulnerable passwords, encryption, automatic account locks in case of password error, maximum password usage period, etc.)
Access control	Access setting checks (access by the approved PC/user, remote access encryption, session end time, etc.)
System security	Privilege setting checks (user environment settings, key directories and files, boot scripts, etc.)
Service security	Service shutdown (unnecessary service, NFS settings, anonymous FTP, SNMP settings, etc.)
Monitoring	Log recording settings, CPU/file system use rate check
Other security management	Access warning message, scheduling content, latest patch checks

B) Account and password management

① Deleting unnecessary accounts

In many cases, accounts created by default when installing the OS or package, use the default password. Accounts that are not deleted by the system as well as suspicious accounts should be deleted, because they can be exploited for the password guessing attack. In general, system accounts that do not require login should be prohibited from logging in.

• How to delete unnecessary accounts
  # userdel [lp | uucp | nuucp | *Account to be deleted*] on SUN/HP-UX.
  # rmuser [lp | uucp | nuucp | *Account to be deleted*] on AIX.

② Checking the account that uses a vulnerable password

In general, if a password that is easy to guess is set for an account, unauthorized users can access the system. A password should be set using a combination of 8 or more letters, numbers, and special characters that are not the same or similar to the account name.

• How to check the account that uses a vulnerable password method:
  Check the password, using a password cracking tool, such as "john the ripper".
  Create a password.txt file in the same directory as the john script.
  Copy the contents of the password encryption file /etc/shadow (/etc/passwd for HP-UX), paste it into the password.txt file, and input john password.txt.

C) Access control

① Allowing access to authorized systems only

The Inetd daemon executes the Internet service daemon, which is an internal program registered in /etc/inetd. conf, when requested by the external network. If the access rights of inetd.conf(xinetd.d) are incorrectly set, unauthorized persons can register a malicious program in this file and execute it with root privileges. Therefore, include those who will be allowed to access in the /etc/hosts. allow and include those who will be denied in the /etc/hosts. deny file.

② Setting session idle timeout

If timeout is not set for a session that is not in use, it may cause problems, both in confidentiality and availability. Therefore, the connected session should be set in a way that it is blocked from the server in question, if not used for a specified period of time.

• How to set session idle timeout
  Add "TIMEOUT=300" (stop sessions if not used for 300 seconds) to the "/etc/default/login" file.
  Add "TMOUT=300, export TMOUT" to the /etc/profile or .profile file in HP-UX, AIX, and Linux.

D) System security

① Setting privileges to the user's default configuration file

The /etc/profile file is a login script for setting the default use environment of all the log-in users. If the access right of the /etc/profile is incorrectly set, unauthorized users can cause a breach incident by changing the user environment, using various methods. Therefore, remove the writing privilege for the /etc/profile from the users, other than the root (bin).

• How to remove other users' privileges of the /etc/profile file:

```
# ls -al /etc/profile
# chown root /etc/profile
# chmod o-w /etc/profile
```

② Setting umask

To check the umask setting details of the current user, run the "umask" command at the command prompt. The umask value should be set to "027" or "022". If the umask value is set to "027", a file is created with the access rights of "rw-r-----", and if the umask value is set to "022", a file is created with the access rights of "rw-r--r--". Therefore, the umask value should be set to "022" so as not to allow unnecessary access.

• How to set umask:

In SUN, uncomment the UMASK option in the /etc/default/login file and set it to 022. For other UNIX operating systems, add "Umask 022" in the .profile.

E) Service security

① Stopping unnecessary services

If unnecessary service ports are open, it can cause security vulnerability. Therefore, unused services should be removed. <Table 34> shows a list of daemon services and service ports that should be checked for stopping.

<Table 34> List of daemon services and check ports

Item	Detailed item
Echo (7)	Simply sends the received message again.
Ehargen (19)	A service that returns a string of random length.
Finger (79)	Outputs user information.
Nntp (119)	Network News Transfer Protocol (NNTP) - a standard service that can create a discussion group on the Internet.
Netbios_Dgm (138)	NetBIOS datagram that is used to broadcast to the service, host, group, or all of the above.
Ldap (389)	A service for accessing the directory service.
Ntalk (518)	A service that enables a chat between different systems.
Ldaps (636)	LDAP over SSL
Nfsd (2049) - NFS	NFS server daemon service when not in use.
Discard (9)	A service that discards the received data of the random user.
Time (37)	The TCP version of the RFC 868 time server used by the Rdate daemon.
Sftp (115)	Ftp over SSH
Ntp (123)	Network Time Protocol (ntp) synchronizes time between the client and server.
Netbios_Ssn (139)	NetBIOS session service used to send and receive actual data, using network sharing, etc.
Printer (515)	Used to spool in a remote printer.

Uucp (540)	Used to copy files between different Unix systems and send commands to be executed in different systems.
Ingreslock (1524)	Ingre database lock service
Dtspcd (6112)	A daemon service to control the subprocess of the desktop.
Daytime (13)	Daytime is a daemon that displays the current time and date in ASCII format when responding to the client's query.
Tftp (69)	File transfer protocol
Uucp-path (117)	Uucp path service
Netbios_ns (137)	NetBIOS name service used to identify a resource on the network.
Bftp (152)	Binary File Transfer Protocol
Talk (517)	A user connects the system remotely and can start a chat session with a user who has logged into another system.
Pcserver (600)	ECD integrated PC board server used to make RPC related attacks.

② Restricting the use of anonymous FTP and using Secure FTP

Anonymous FTP allows a malicious user to obtain information about the system. Since various attacks can be made if writing permission is set in the directory, the use of anonymous FTP should be restricted by setting it in such a way that only necessary users can gain access. Also, secure FTP should be used, rather than FTP with weak security.

When using general FTP by using anonymous FTP or by setting up an account, there are security vulnerabilities, such as the transmission of user authentication information, in plain text without encryption, and security vulnerabilities of the FTP protocol itself. That is, FTP can acquire account privileges by exploiting the authentication vulnerability of the account login and by applying a brute force attack or a sniffing attack. Therefore, when creating an FTP program for sending and receiving a file, an SFTP server should be installed and an SFTP client program should be written.

• How to apply SFTP using Java

The SFTP open-source library is used to create a SFTP client program using Java. Download and install Commons-Net library from the Apache open-source project site (http://commons.apache.org/proper/commons-net/), then write a SFTP client program as follows:

```
// Import libraries
import org.apache.commons.vfs2.FileObject;
import org.apache.commons.vfs2.FileSystemOptions;
import org.apache.commons.vfs2.Selectors;
import org.apache.commons.vfs2.impl.StandardFileSystemManager;
import org.apache.commons.vfs2.provider.sftp.SftpFileSystemConfigBuilder;
// FTP connection and file download
   StandardFileSystemManager manager = new StandardFileSystemManager();
   String sftpUri = "sftp://" + userId + ":" + password +  "@" + serverAddress + "/" +
    remoteDirectory + fileToFTP;

FileObject localFile = manager.resolveFile(file.getAbsolutePath());
   FileObject remoteFile = manager.resolveFile(sftpUri, opts);
   remoteFile.copyFrom(localFile, Selectors.SELECT_SELF);
```

• How to apply SFTP using C

The SFTP open-source library is used to create a SFTP client program using C. Download and install Libssh2 library from the libssh2 site (http://www.libssh2.org) and create a SFTP client program as follows:

```
// Include libraries
#include "libssh2_config.h"
#include <libssh2.h>
#include <libssh2_sftp.h>
// FTP connection and file download
session = libssh2_session_init();
libssh2_userauth_password(session, username, password);
libssh2_sftp_open(sftp_session, sftppath, LIBSSH2_FXF_READ, 0);
libssh2_sftp_read(sftp_handle, mem, sizeof(mem));
```

VIII. Understanding Network Security

▶▶▶ Subject

Understanding network security!

▶▶▶ Importance of practical business

High

▶▶▶ Recent trends and major issues

The Internet is growing rapidly, with the advancement of wired and wireless communication technology, which has already deeply penetrated into our lives in all aspects of politics, economy, and society. The Internet is changing everything around us by promoting a new paradigm shift.
It is now developing into the Internet of Things (IoT). However, when we try to use the Internet in our real life, such as for remote medical treatment and e-commerce, there are still several restrictions. Among those restrictions, security-related issues are most important and urgent. The most essential technology to protect internal information assets from various network security threats, include the firewall, virtual private network (VPN), and intrusion detection system (IDS).

▶▶▶ Learning objectives

- To be able to classify the concepts and type of attacks through the network, and to explain how to respond.
- To be able to describe network security technology and major solutions.
- To be able to explain the wireless LAN security standard (IEEE.11i) and security technology.
- To be able to explain the principle and application of SSL (Secure Socket Layer).
- To be able to explain and utilize security types and principles by application layer protocol.

▶▶▶ Keywords

Firewall, Virtual Private Network (VPN), SSL, traffic attack, denial of service (DOS) attack, Intrusion Detection System (IDS), IPSec, transmission mode, tunnel mode, sniffing, spoofing, key management, NAT, DMZ, WLAN, IEEE 802.11i, 4-way handshake, OWASP top 10, anonymous FTP

✚ Preview for practical business Building a secure network using the firewall and DMZ

Company A is a small and medium-sized company that utilizes a network connected to 90 computers. Currently, the company has 126 public IP addresses (211.82.50.0/25), one router (211.82.50.126/25), a switch, a database server, and a web server, respectively. In this situation, assistant manager, Kim, was instructed to introduce a firewall to configure the external, internal, and DMZ network, in order to increase a network security level. Let's learn how to build a secure network under the following conditions.

- Set private IPs (192.168.1.0/24) for 90 internal PCs and the database server.
- Place the web server in the DMZ area, while keeping the existing address (211.82.50.1/25).
- Subnet the external network and DMZ network into two existing IP bands (211.83.50.0/25).
- Use only one router, one firewall, and two switches.

01 Overview of network security

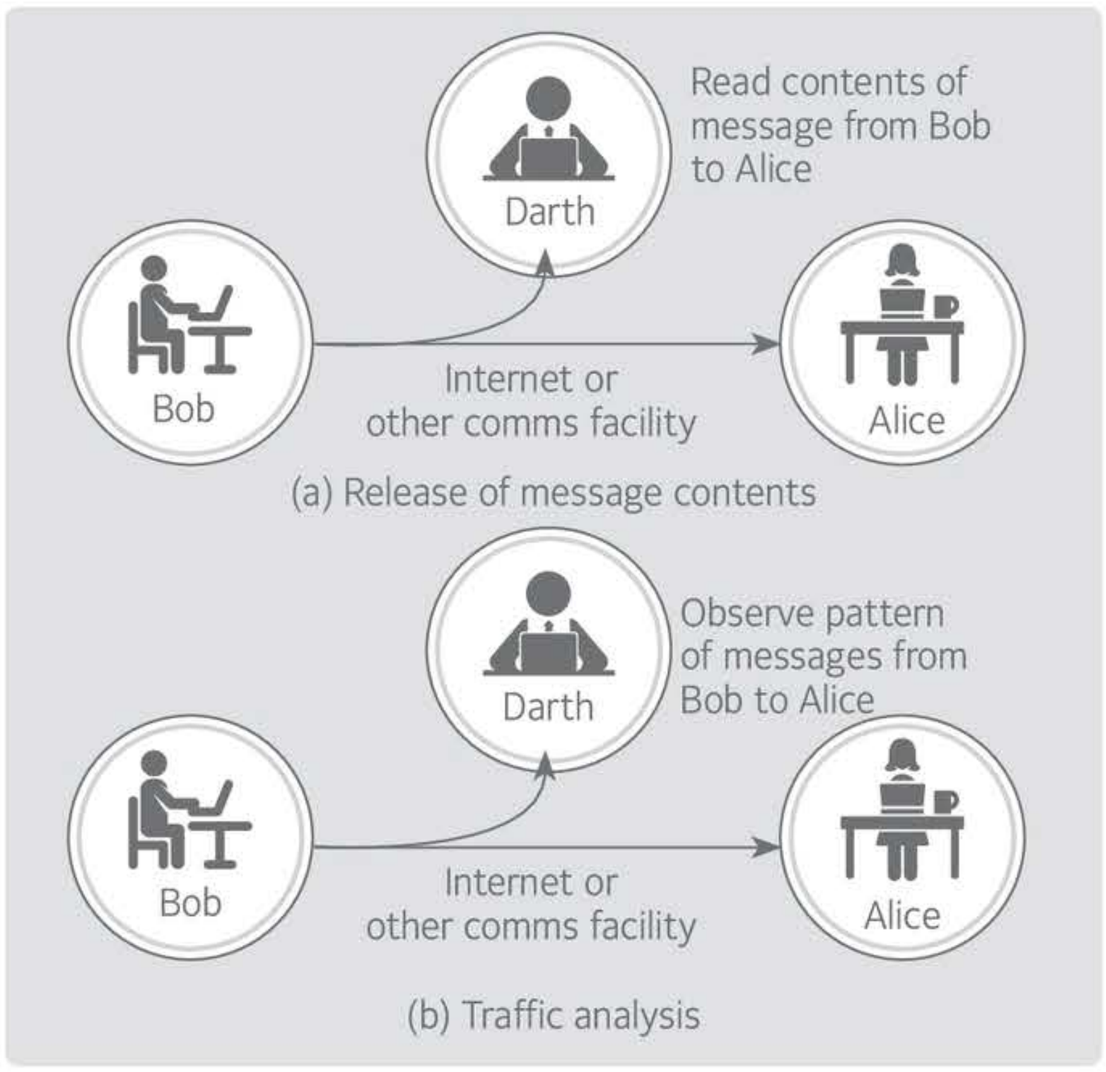
A) Concept of network security

① Type of security attacks

X.800 divides security attacks into passive attacks and active attacks. A passive attack means that an attempt is made to obtain and exploit system information, but system resources are not affected. An active attack aims to change system resources and affect system operations.

- Passive attack

  A passive attack refers to the eavesdropping or monitoring of transmitted data and is attempted to obtain the transmitted data. As shown in [Figure 53], passive attacks include message content disclosure and traffic attack. Traffic attacks can also be made against encrypted data transmission for confidentiality. This attack estimates the nature of communication by observing the number and length of message exchanges.
  The passive attack has the characteristic that it is difficult to detect, because the attack does not change data. Therefore, prevention is more important than detection.

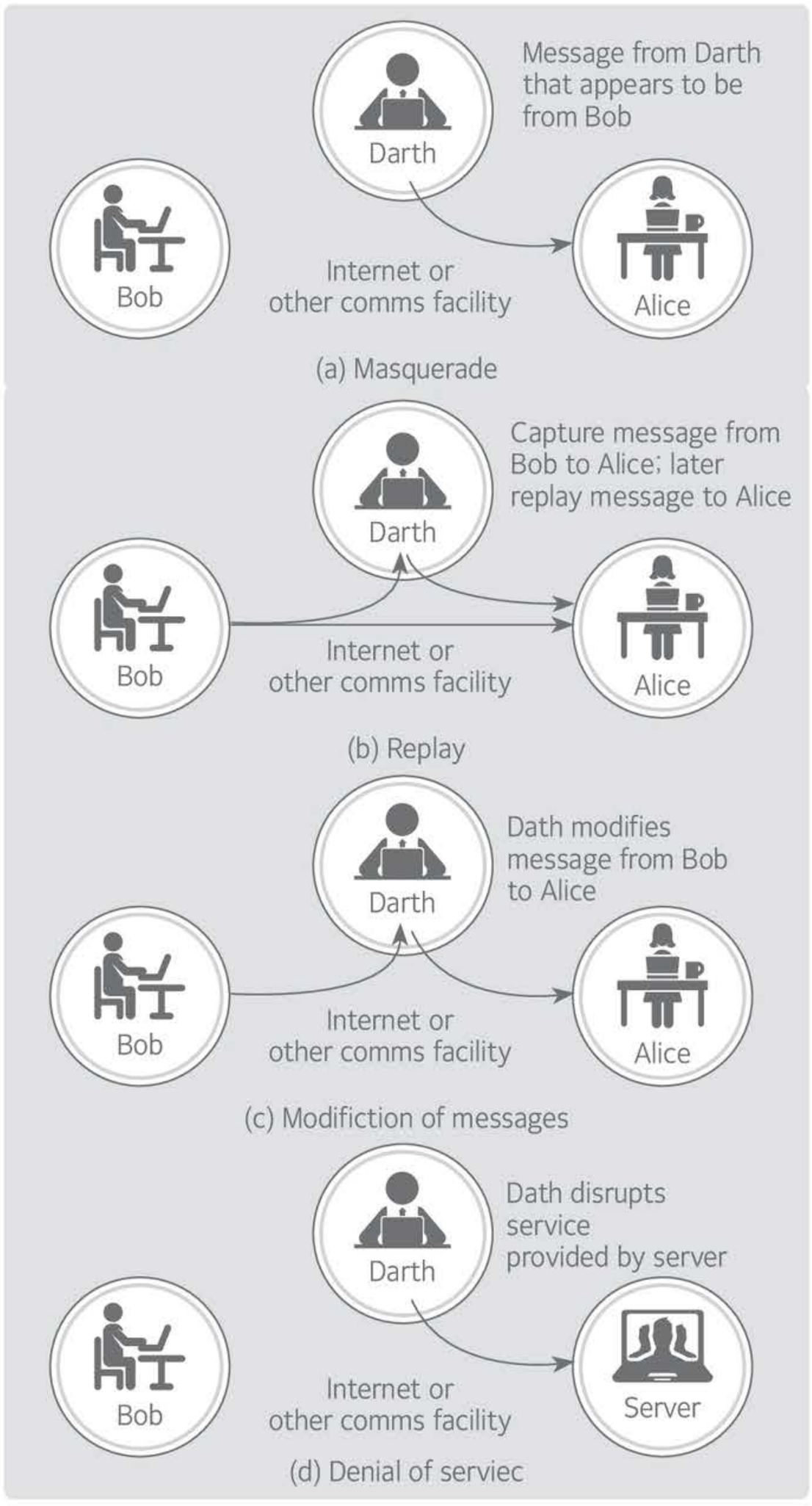


[Figure 53] Passive attack
(Source: W. Stallings, Cryptography and Network Security - Principles and Practice, Prentice Hall, p.17)

- Active attack

  An active attack can be classified into masquerading, replay, modification of message, and denial of service (DOS) attack, which entail the illegal modification of transmitted data or the creation of false data.
  Masquerading occurs when one entity pretends to be another. In general, the masquerading attack is made together with one of the other active attack types.
  The replay attack acquires one message, by using an inactive attack method, and sends the message again to obtain unauthorized results.

The modification of message attack obtains unauthorized results by illegallychanging parts of legal messages, delaying message transmission, or changing the message sequence.
The denial-of-service attack interferes the normal use or management of communication equipment (specific computer or network). This attack is generally called a DoS attack. Most of these attacks are made against a specific target.
The active attack has characteristics that are opposite to the passive attack. It is very difficult to prevent active attacks completely, because all communication equipment and communication lines cannot be physically protected at all times. Response to active attacks aims to detect an attack and recover from the collapse or delay, due to such an attack.



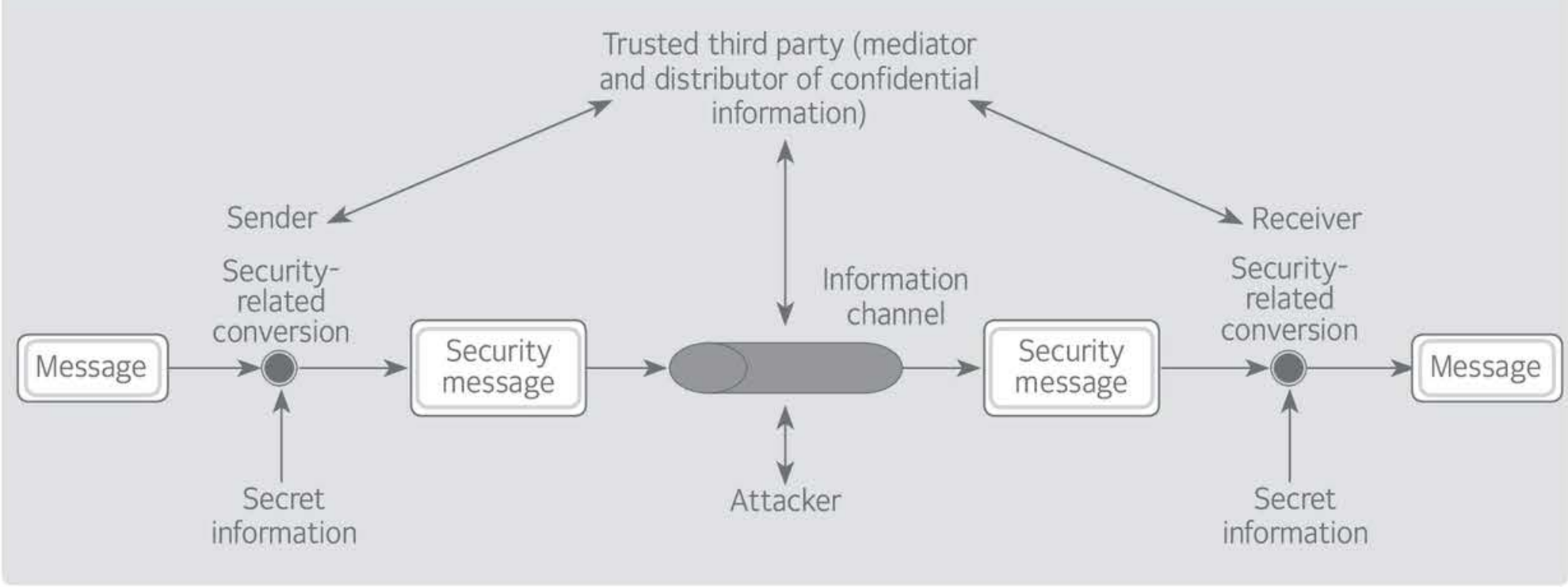
[Figure 54] Active attack
(Source: W. Stallings, Cryptography and Network Security-Principles and Practice, Prentice Hall, p.18, 19)

② Network security model

A computer network consists of communication objects, such as computers and communication systems (a set of transmission devices and communication lines). The computer network exists to support data transmission between the sending computer and receiving computer, regardless of the distance.
[Figure 55] is an abstract expression of network communication elements from the perspective of security. A single message is sent from the sender to the receiver through a network, like the Internet. Two communication subjects should cooperate with each other to exchange messages in this process. A logical information channel (a path consisting of numerous communication devices is allocated between the sending computer and the receiving computer, which is used to transfer data) is established by setting the Internet path between the message source and destination, negotiating between the two communication subjects.
If transmission data needs to be protected from attacks on confidentiality and authentication, corresponding security measures are started. All mechanisms for security should include the following two elements:

- Conversion, related to the security of the data to be sent, belongs to this. For example, encryption that mixes messages to prevent attackers from understanding the message or adding a code (hash code), based on the message content to identify the sender, belong to this.

- For example, encryption keys belong to this, which are used to convert the message (confidential information shared by two communicating subjects that is unknown to the attacker) before sending it, and to convert it again after receiving the message.



[Figure 55] Network security model

(Source: W. Stallings, Cryptography and Network Security - Principles and Practice, Prentice Hall, p.25)

A trusted third party may be needed for secure transmission. For example, a third party may distribute secret information, such as encryption keys, to both communication subjects to prevent attackers from knowing it or may mediate a dispute when it occurs.
A general network security model should meet the following four basic conditions when designing a specific security service:

- Design should be an algorithm design that performs conversion related to security. An attacker should not be

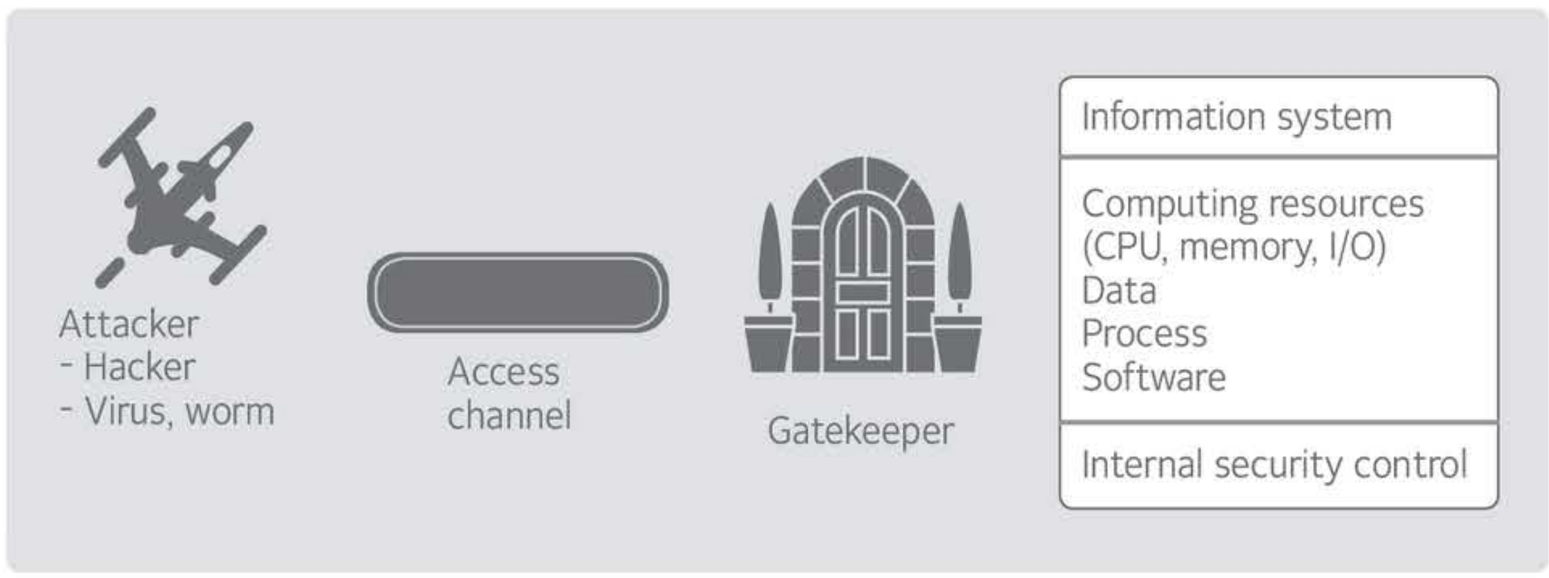
able to destroy the purpose of conversion in the design.

- Secret information, to be used by the conversion algorithm, should be created.
- A method for distributing and sharing confidential information should be developed.
- A security algorithm for a specific security service and a protocol, to be used by the two communicating entities that will use secret information, should be designated.

③ Network access security model

An attacker tries to infiltrate into the information system to damage it or to destroy or steal personal information. In addition, malware, such as a virus or worm, can infect the information system through the network.

Security response techniques against such unwanted access can be divided into two categories, as shown in [Figure 56]. The first category is the method of denying access to the information system, except for the authorized users, using the gate keeper function. The log-in procedure using a password falls into this category. Once accessed by the user or software, the second-phase response is performed by the internal security control function. An intrusion detection system (IDS) that monitors the activity status of an information system and detects an intruder can be selected as the representative method of performing internal security control.

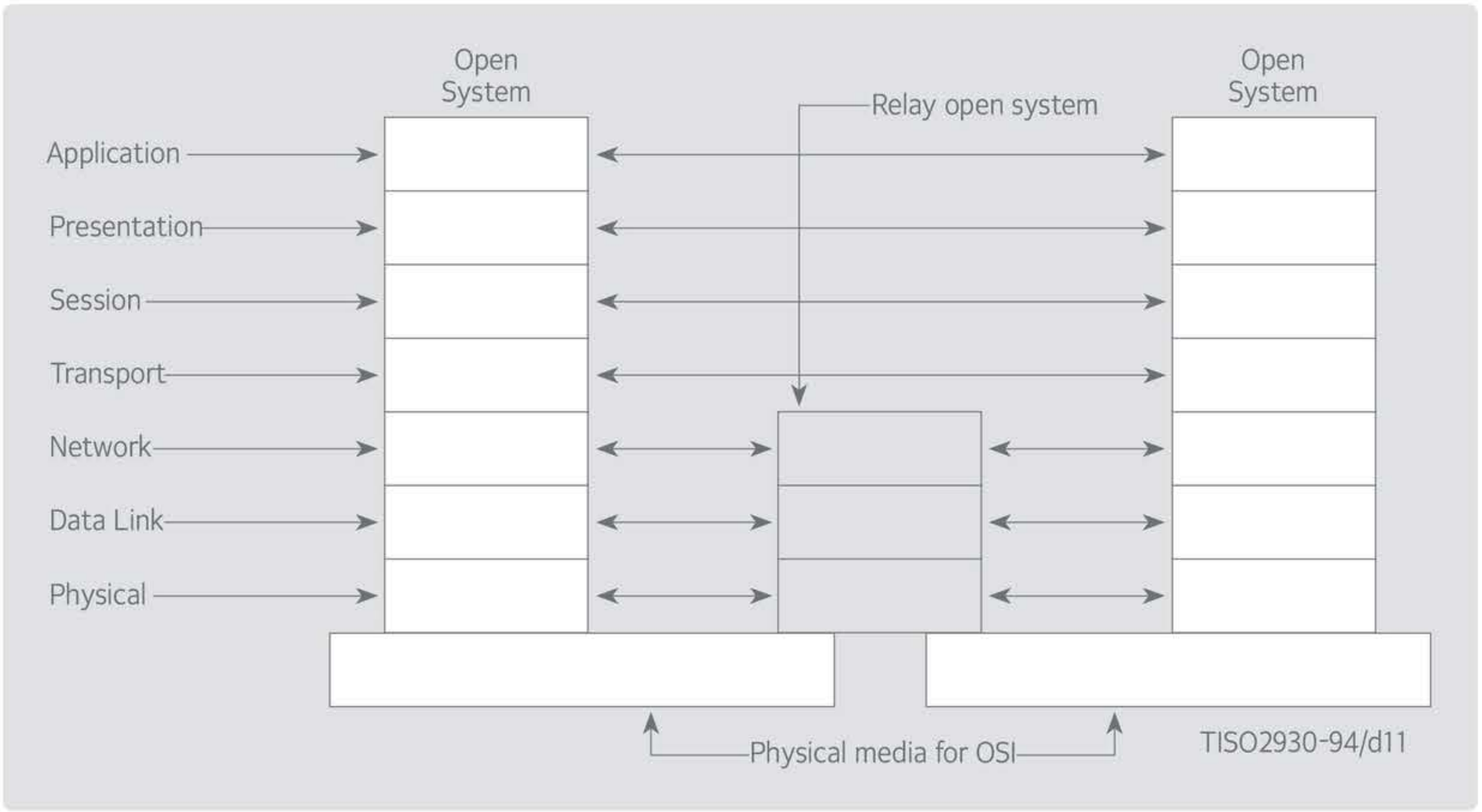


[Figure 56] Network access security model
(Source: W. Stallings, Cryptography and Network Security-Principles and Practice, Prentice Hall, p.26)

B) Communication protocol layer and security

① OSI 7-layer reference model and TCP/IP protocol layer structure

[Figure 57] shows the OSI (Open System Interconnection) 7-layer reference model, described in the ISO/IEC 7498-1:1994(E) standard document, which indicates the interconnection structure between open systems.



[Figure 57] OSI 7-layer reference model

<Table 35> shows the protocols and functions corresponding to each layer of the OSI 7-layer reference model.

<Table 35> Protocols and functions of each layer of the OSI 7-layer reference model

Layer	Protocol	Function
Application layer	HTTP, SMTP, SNMP, FTP, Telnet, SSH, DNS, etc.	Provides services, such as user interface, e-mail, and database management, to users.
Presentation layer	JPEG, MPEG, XDR, etc.	Converts transmitted data using a common presentation method.
Session layer	TLS, RPC, NetBIOS, etc.	Manages communication sessions. Sessions between communication devices are established, maintained, and synchronized.
Transport layer	TCP, UDP, SCTP, etc.	Perform data transmission and error control between the source and destination (end-to-end) process.
Network layer	IP, IPX, ICMP, X. 25, ARP, OSPF, etc.	Responsible for transferring packets, from the source, to the destination host, in multiple network environments.
Data link layer	Ethernet, Token Ring, wireless LAN, etc.	Transfers frames from one device to another, without errors.
Physical layer	Radio wave, coaxial cable, UTP, optical fiber, etc.	Converts bits into signals and transmits them using physical media.

The structure of the TCP/IP used for the ARPANET reference model that appeared earlier than the OSI 7-layer reference model and is composed of three layers, as shown in [Figure 56].

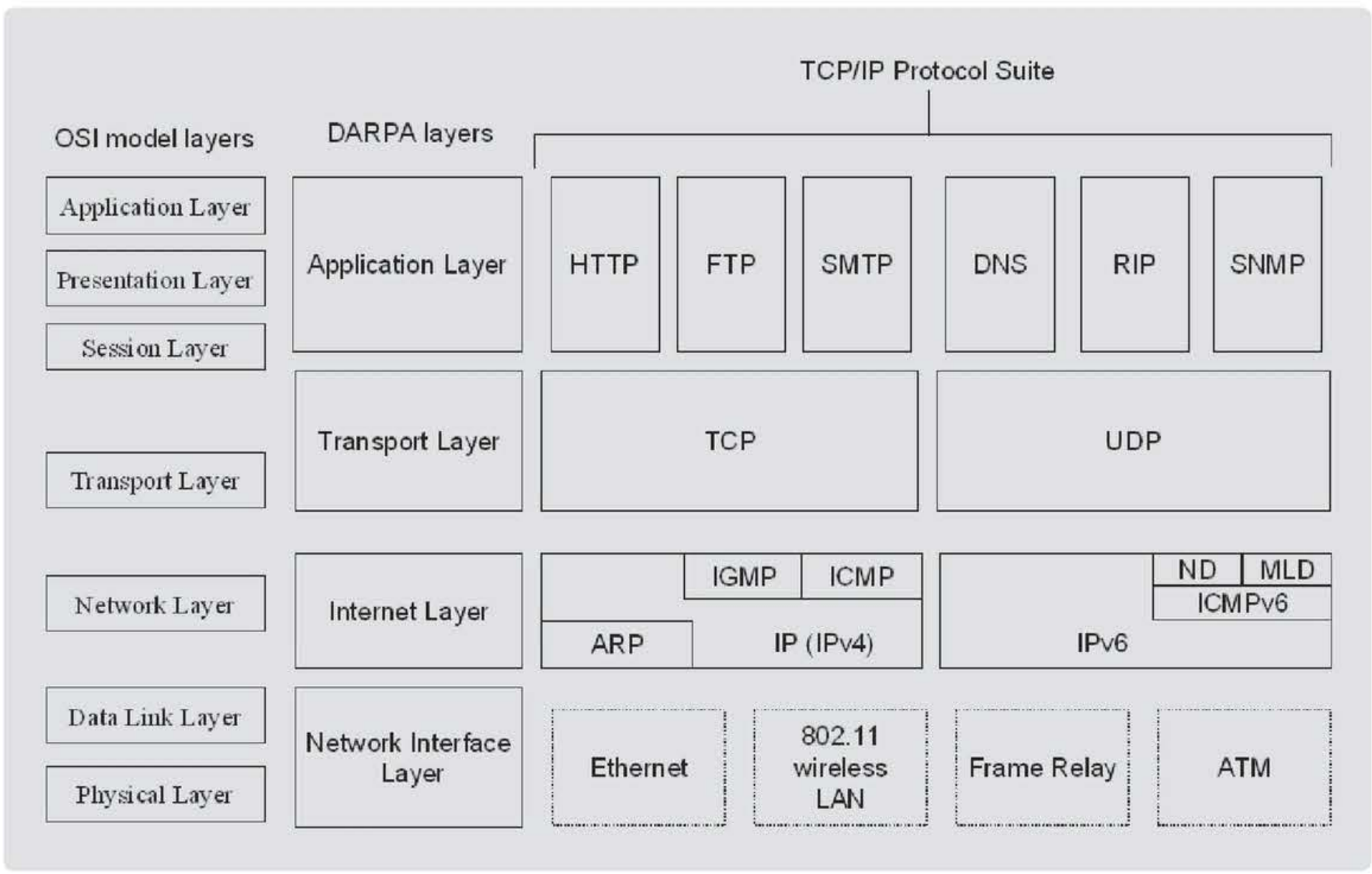
- Application layer: Provides application services, including web (HTTP), DNS, Telnet, FTP, e-mail sending/receiving (SMTP/POP3/IMAP4), etc. This layer runs using the services provided by the lower layer and the

transport layer. The concept of this layer includes, not only the application layer, but also the presentation layer and the session layer of the OSI reference model.

- Transport layer: Also known as the host-to-host transport layer. This layer manages data exchange between virtual ports that are managed by the application program, such as the TCP, UDP, and SCTP protocol. This layer corresponds to the transport layer of the OSI reference model.

- Internet layer: Also known as the network layer, this layer manages the addressing and routing functions, and it corresponds to the network layer of the OSI reference model.

The network interface layer in [Figure 58] is not a concept that is dependent on the structure of the TCP/IP protocol. It is also referred to as a network access layer. The network interface layer is randomly selected by the network interface layer and practically transfers TCP/IP packets through a physical medium, such as IEEE 802.3 Ethernet or IEEE 802.11 Wi-Fi. This layer includes the functions of both the data link layer, which manages the MAC function of the OSI 7-layer reference model, and the physical layer that defines electrical signals.



[Figure 58] TCP/IP protocol layer

② Security function by layer

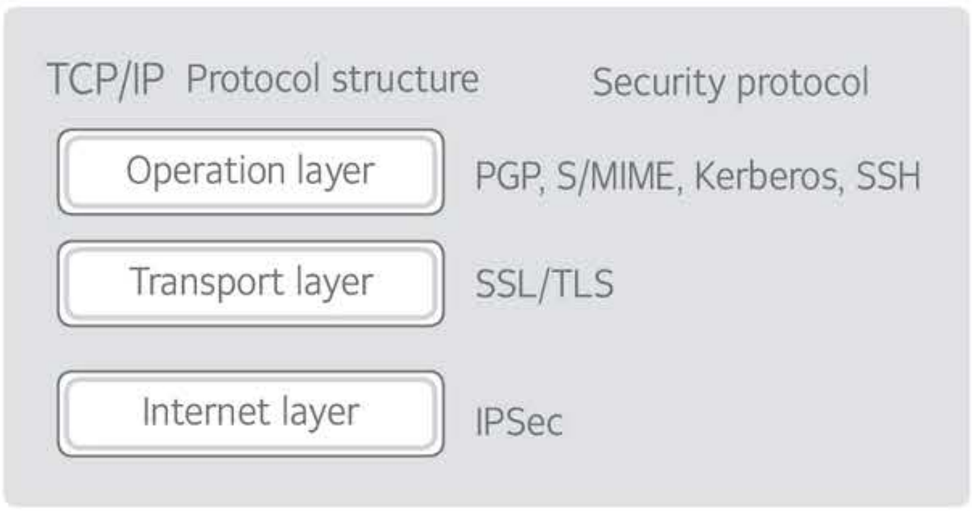
Since the purpose of designing the TCP/IP protocol structure lies in free information exchange, the concept of security is not considered in the design process. As TCP/IP is used as the core protocol of the Internet, and the application, like e-Commerce, is developed or used, protocols with security functions are added to

the structure of the TCP/IP protocol. [Figure 59] shows security protocols by layer, based on the OSI 7-layer reference model.

- Security protocols related to the application layer
  There are various security protocols related to the application layer, such as PGP and S/MIME that provide e-mail security function, Kerberos that provides authentication functions, and SSH (secure shell) that supports secure remote access, etc.

- Security protocols related to the transport layer
  SSL (Secure Socket Layer)/TLS (Transport Layer Security) is a protocol that acts above the transport layer, which provides the secure transport layer services to the application layer. TLS is the Internet Engineering Task Force (IETF) standard for SSL, and it provides end-to-end security and data integrity.

- Security protocols related to the Internet
  The IPSec (IP Security) protocol that acts above the Internet layer, which provides security features, such as authentication and encryption, to the Internet layer. This protocol is used to implement VPN services.



[Figure 59] Security protocols by layer

C) Types of network attacks and countermeasures

① DoS attack

The DoS attack disturbs the normal operation of a specific server by causing various types of load. It is an attack on availability, one of the security services. Typical DoS attacks include land attacks, ping of death attacks, Syn flooding attacks, and Boink attacks.

- Land attack
  An attack that sends a packet to the target, by making the IP address of the source and destination identical to the attacker's IP address. Server operation fails, due to serious failure in the IP protocol stack because the host that receives the packet falls into an infinite loop of receiving and sending the packet.
  This attack can be responded to by blocking packets whose source IP address is the same as the server's IP address, among the packets flowing into the network, using a router or packet filtering tool.

- Ping of death attack
  When an attacker makes an ICMP packet that much larger than the normal size and sends it, the packet is divided into many small fragments and transmitted to the attacking network. Accordingly, the attack target

system must process all those small packets. As a result, it takes a lot more load than the normal Ping command, and the performance of the system is degraded.
This attack can be responded to by blocking ICMP protocols, which sends the Ping command, using a firewall and other devices.

- Syn flooding attack
  Syn flooding attacks exploit the vulnerability that half-open connection can establish during the 3-way handshaking process (TCP connection setup process). The system, under this attack, can no longer accept connection requests from outside. Therefore, normal services cannot be provided. Not only Windows systems, but all systems that provide TCP-based services on the Internet (for example, web server, FTP server, mail server, etc.), can be damaged by this attack.
  This attack can be responded to by reducing the waiting time of the SYN reception status in the target system, or by installing an intrusion prevention system.

- Boink attack
  The Boink attack is a DoS attack that modifies Boink. Assuming that the packet size is 100 bytes, 1 is sent as the sequence number (which is the byte number) of the first packet. After that, 101 is sent as the sequence number of the next packet, and 201 is normally sent as the next packet. Then, 2002 is abnormally sent as the 20th packet, and 101 is normally sent as the 21st packet. Then, 2002 is abnormally sent as the 22nd packet, and so on. As a result, the overload of repeatedly sending and combining packets is applied to the attack target system.
  The countermeasures against this attack are similar to those against the ping of dead attack or Syn flooding attack.

The DDoS (Distributed DOS) attack is the evolved type of the DoS attack. The DDoS attack is a DoS attack that has multiple attack sources.

② Sniffing attack

Sniffing is based on the concept of eavesdropping, etc., and is also known as a passive attack. All systems connected to the Internet, that is, LAN, have an IP address (layer 3 address) and a MAC (medium access control) address (layer 2 address) implemented in a network interface card. Since every MAC address on the Internet has a different value, each system can be uniquely identified.
All hosts on the same LAN share the same communication line. Therefore, computers on the LAN can view all the communication traffic of other computers.
Due to this characteristic, network interface cards (commonly referred to as LAN cards) have a filtering function that ignores a frame without its own MAC address. This filtering function ensures that only traffic with its own MAC address can be received.
However, users can set the function that enables all traffic to be viewed, using the LAN card in case of special circumstances, which is called promiscuous mode. Sniffing is an attack that eavesdrops on all traffic on a specific LAN, by setting the LAN card to promiscuous mode.
When a LAN uses a switch, traffic is sent to a specific destination computer. Therefore, even if the LAN card is set to promiscuous mode, traffic of other destinations cannot be received. In this case, sniffing can be performed using the method of switch jamming, ARP redirect, ICMP redirect, MAC spoofing, etc.

Since all sniffers eavesdrop on the network by setting their LAN cards to promiscuous mode, a system running a sniffer program can be detected by periodically checking if a specific host is set in promiscuous mode. Ping, ARP, DNS, or induction method can be used for detection.

③ Spoofing attack

Spoofing is the act of disguising and can apply to anything related to communication, such as the IP address, host name, port number, MAC address, etc. A spoofing attack technique is used to attack other target systems by disguising its own identification information. The spoofing attack is used for other attacks, such as packet sniffing, DoS attack, and session hijacking.

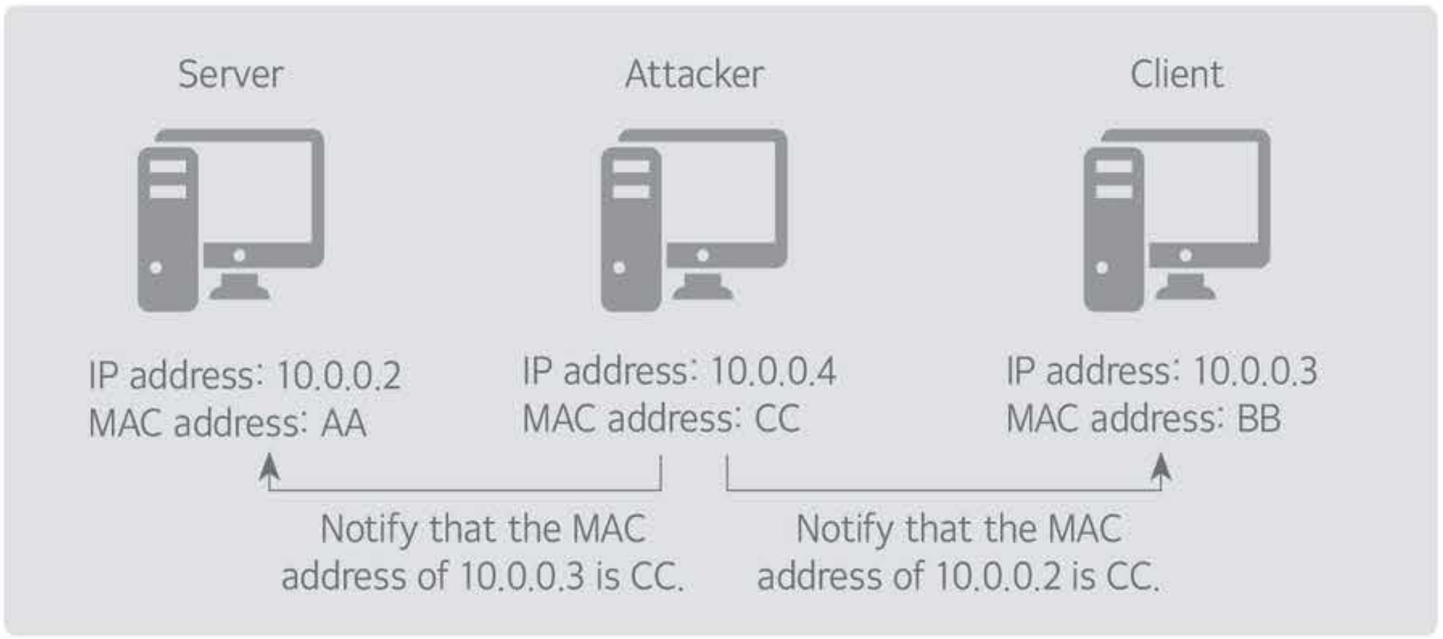
• ARP spoofing

The ARP protocol maps IP addresses and MAC addresses, whereas ARP spoofing attacks trick MAC addresses.

As shown in [Figure 60], the attacker first informs the client of the fake MAC address "CC", corresponding to the server (address: 10.0.0.2) and notifies the server of the fake MAC address "CC", corresponding to the client (address: 10.0.0.3).

Since an attacker notifies its own MAC address to the other communication party (server and client computer), both the sever and the client send packets to the attacker.

After the attacker reads the packets received from the server and the client, the server normally sends the packets that the server sends to the client, and the packets that the client sends to the server. (As a result, the attacker can obtain the contents of the communication between the server and the client.)



[Figure 60] ARP spoofing
(Source: Yang Daeil, Introduction to Information Security, Hanbit Media, p. 156)

There are no fundamental countermeasures against ARP spoofing, because it's the problem of the TCP/IP protocol structure itself. However, the change of the MAC address can be prevented by setting the attributes of the ARP table, using the arp command to prevent the change of the ARP table. To use this method, the setting command should be executed every time the system is rebooted.

• IP spoofing

An IP spoofing attack hacks the host by changing its IP address. That is, an attacker steals the IP address of other users and illegally obtains the rights to log on or others.

Two systems, A and B, that are in a trusted relationship in the network environment can use a service that enables the user to log into system B using the system A account, which is called trust authentication. Authentication is performed by the trust service on the network, based on the network address, not the password. That is, the server stores the trusted client IP addresses and allows log-in without an ID and password, if the client with the saved IP address requests log-in.
To respond to IP spoofing, it is recommended not to use trust authentication, except under special circumstances.

- DNS spoofing
  If an attacker takes control of the DNS server of a certain domain, the user can be connected to the system designated by the attacker, because the user finally obtains that IP address even though the user intended to obtain the IP address of the other system. That is, the attacker sniffs the DNS, designated by the user, to request address translation and traffic from the higher-level DNS site that gives the response, and it passes the IP address of the attacker's intended site as the final response.
  To respond to DNS spoofing, the IP address of the important access server can be registered in the host file, so the IP address can be obtained without querying the DNS server. However, it is realistically impossible to register and manage the IP addresses of all servers.

02 Security protocols and security solutions

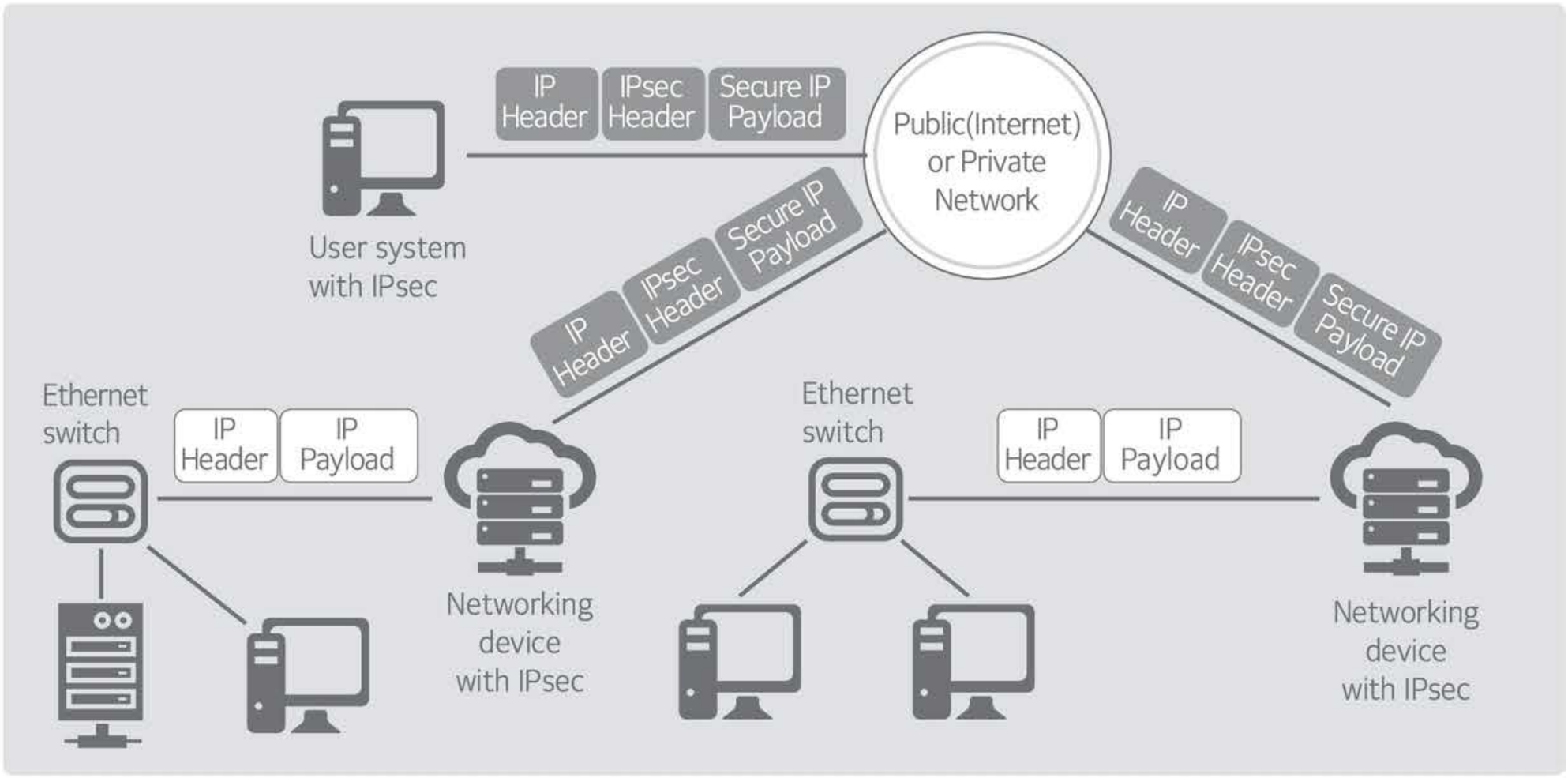
A) IPSec

① Concept

The IPv4 (Internet Protocol version 4) has no authentication function and is vulnerable to attacks, such as eavesdropping or packet alteration. IPsec (Internet Protocol Security) was developed to make up for the security vulnerability of IP. IPSec provides security functions to all application programs because it supports the safe operation of the IP, by providing encryption and authentication services to the IP by packet unit. IPsec encompasses three functional areas: authentication, confidentiality, and key management. It is optional in Ipv4, but implemented as a basic function in IPv6.

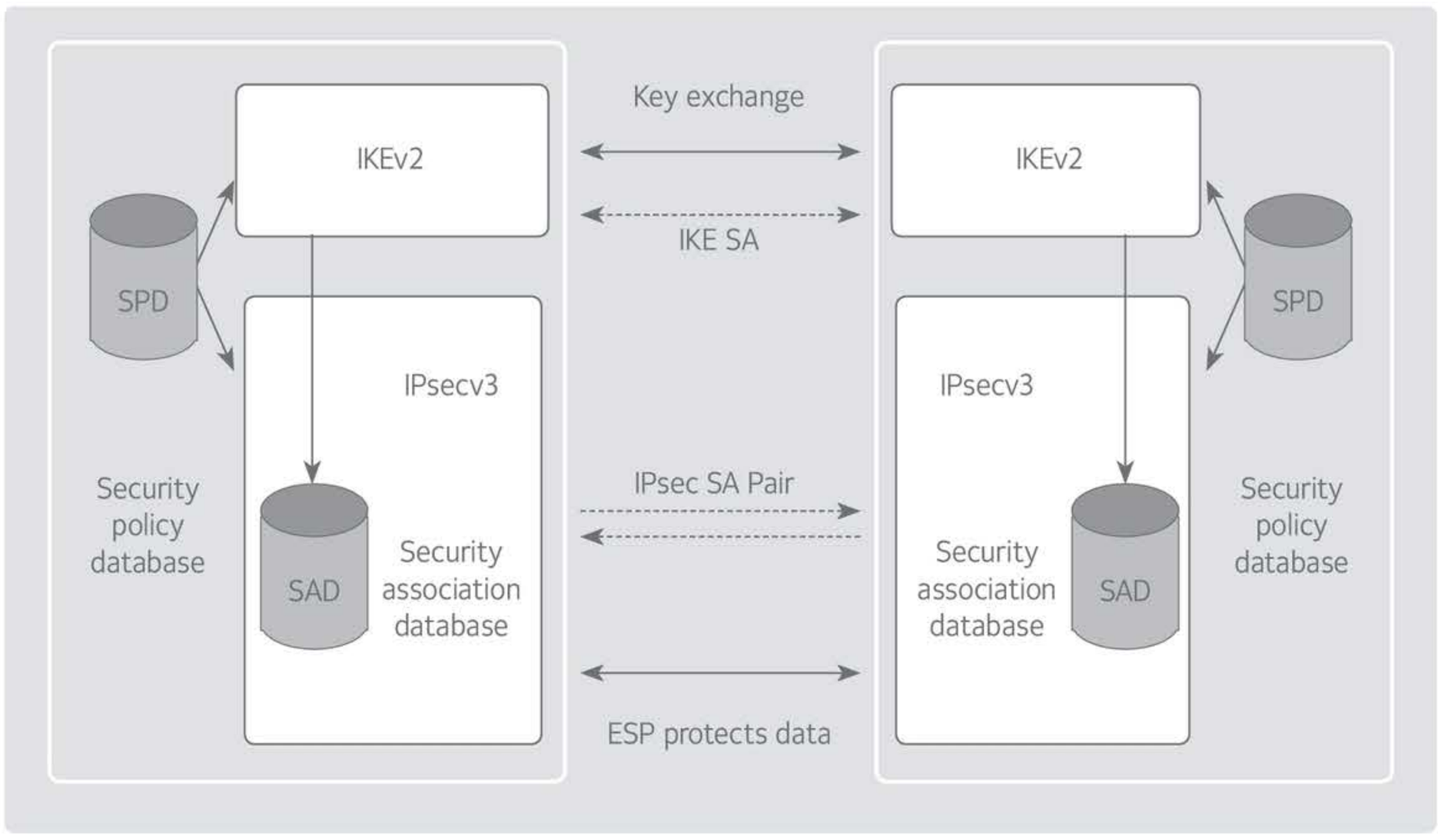
② Composition and operation

[Figure 61] shows that when an organization uses the LAN distributed in several places, IP traffic is transmitted within the LAN, but outgoing traffic of the LAN is transmitted using IPSec protocol for safe communication. The IPSec protocol runs on the device, such as the router or firewall, which is transparently visible to the computers on the LAN.



[Figure 61] IPSec operation
(Source: W. Stallings, Network Security Essentials, Pearson, p.272)

[Figure 62] shows the structure of IPSec. IPSec is largely composed of Internet Key Exchange (IKE) for Security Association (SA) negotiation, a repository of Sas - Security Association Database (SAD), Security Policy Database (SPD) that stores security policies that define how IP traffic is associated with a specific SA, AH (Authentication Header) protocol, providing an actual authentication service, and the Encapsulating Security Payload (ESP) protocol, providing authentication and encryption services.



[Figure 62] IPSec structure
(Source: W. Stallings, Network Security Essentials, Pearson, p.276)

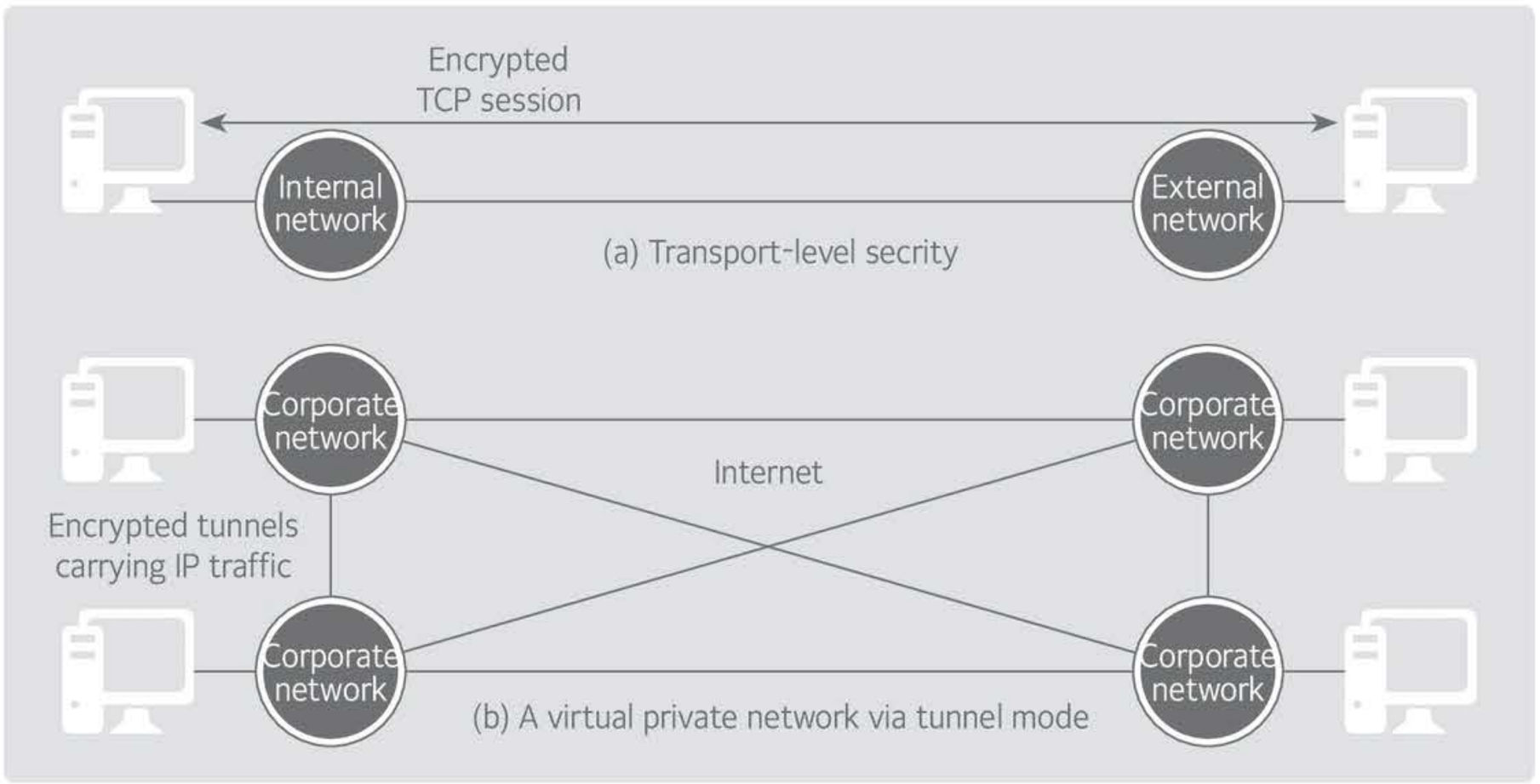
• Transport mode and tunnel mode

AH and ESP support transport mode or tunnel mode. As shown in [Figure 63], IP headers do not change and only the payload of the IP datagram is encrypted in transport mode, whereas all IP datagrams are encrypted and transmitted as the payload of a new IP packet in tunnel mode. In general, the router plays a proxy role of IPSec in tunnel mode.

The transport mode is mainly used to protect the upper layer protocol, which is the payload range of the IP datagram. For example, it is used to protect TCP fragmentation or ICMP packets. IPSec in transport mode operates right above the IP layer. ESP encrypts the IP payload, but it does not encrypt the IP header in transport mode, and authentication is optional. AH only authenticates the IP payload and selected parts of the IP header in transport mode.

Tunnel mode protects all IP datagrams. To this end, an "external" IP datagram that has a new external IP header is created. No router can inspect the internal IP header while this datagram is transported. For this reason, the IP datagram can be transported to the external network, through a conceptual tunnel, using tunnel mode.

ESP in tunnel mode encrypts all internal IP datagrams, including the internal IP header, and authentication is optional. AH in tunnel mode authenticates all internal IP datagrams and selected parts of the external IP header.



[Figure 63] Encryption of transmission mode and tunnel mode
(Source: W. Stallings, Network Security Essentials, Pearson, p.285)

• Security Association (SA)

To establish secure communication with the other party, using IPSec, authentication and encryption algorithms to be used by two communication entities, as well as encryption keys, are needed. The security algorithm and key information should be exchanged and saved before full-scale communication, and the records of this information are called SA. Since there are many SAs in one system, SAs are identified by the security parameter index (SPI), which is given randomly, and a destination IP address. Since one SA is needed

for secure communication in one direction, two SAs are needed for two communication entities in order to establish two-way communication.
<Table 36> shows the communication process between system A and B, while the SA is stored. It is assumed that system A initiates communication in this table.

<Table 36> Communication phase in the IPSec environment

Sequence	Description
Phase 1	System A finds the SA of system B by searching for its own SAD in order to establish secure communication with system B.
Phase 2	Check the encryption key and algorithm to be used, using the SA information of system B, encrypt the IP datagram to be transported using them, and insert a SPI into the IPSec header and send it to system B.
Phase 3	Check the encryption key and algorithm to be used using the SA information of system B, encrypt the IP datagram to be transported using them, and insert a SPI into the IPSec header and send it to system B.
Phase 4	Upon receiving the encrypted IP datagram, system B searches for the corresponding SA in its SAD using the SPI and source address A in the IPSec header.
Phase 5	Check the encryption key and algorithm to be used in the information of the corresponding SA and decrypt the IP datagram in the received packet using them.

• IKE
Key management of IPSec includes the cryptographic key determination and distribution function. Four keys are needed for communication between two applications. That is, a pair of the sending and receiving keys is needed for integrity and confidentiality.
Let IKE create and store the SA through secure authentication between two applications to enable IPSec communication by exchanging messages. IKE defines procedures and packet formats to establish, negotiate, modify, and remove the SA.

③ Utilization

Implementing VPN and IPSec, using IPSec, also provides security for application layer services, such as secure remote access, e-commerce security, etc.

B) SSL

① Concept

SSL is a protocol developed by Netscape's Hickman in 1994 and standardized by the Internet Engineering Task Force (IETF) after the SSL version 3.0 and named as TLS (Transport Layer Security). Most web browsers support SSL. The SSL protocol is positioned between the application layer and the transport layer in the TCP/IP protocol structure. The protocol is designed to use TCP to provide reliable end-to-end secure services. Even though SSL can be used in various application layer protocols, it is actually most widely used by the HTTP application. When HTTP uses SSL, it is called HTTPS.
The two important concepts of SSL are connection and session.

• SSL connection: SSL connection refers to transport providing appropriate services. A connection in SSL is a peer-to-peer relationship and is temporary, and all connections are associated with one session.

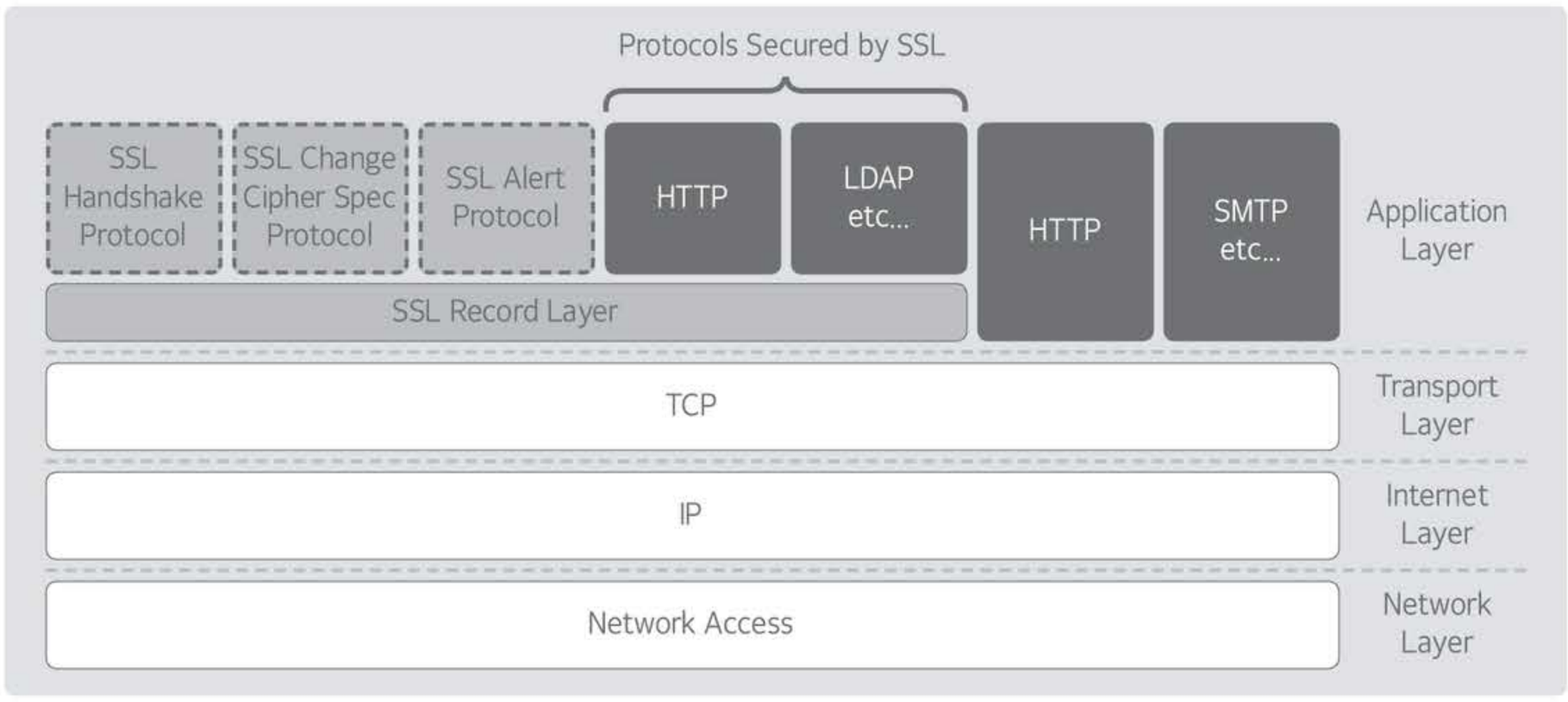
• SSL session: An SSL session refers to an association between a client and a server. To start a session, the

handshake protocol should be used, which will be described below. A session defines cryptographic security parameters that are shared by multiple connections, which is used to avoid negotiating required new security parameters for each connection.

② Structure and operation

• Structure of the SSL protocol

As shown in [Figure 64], SSL is composed of four protocols, including handshake, change cipher Spec, record, and alert.



[Figure 64] Composition of the SSL protocol

• Type of SSL protocols

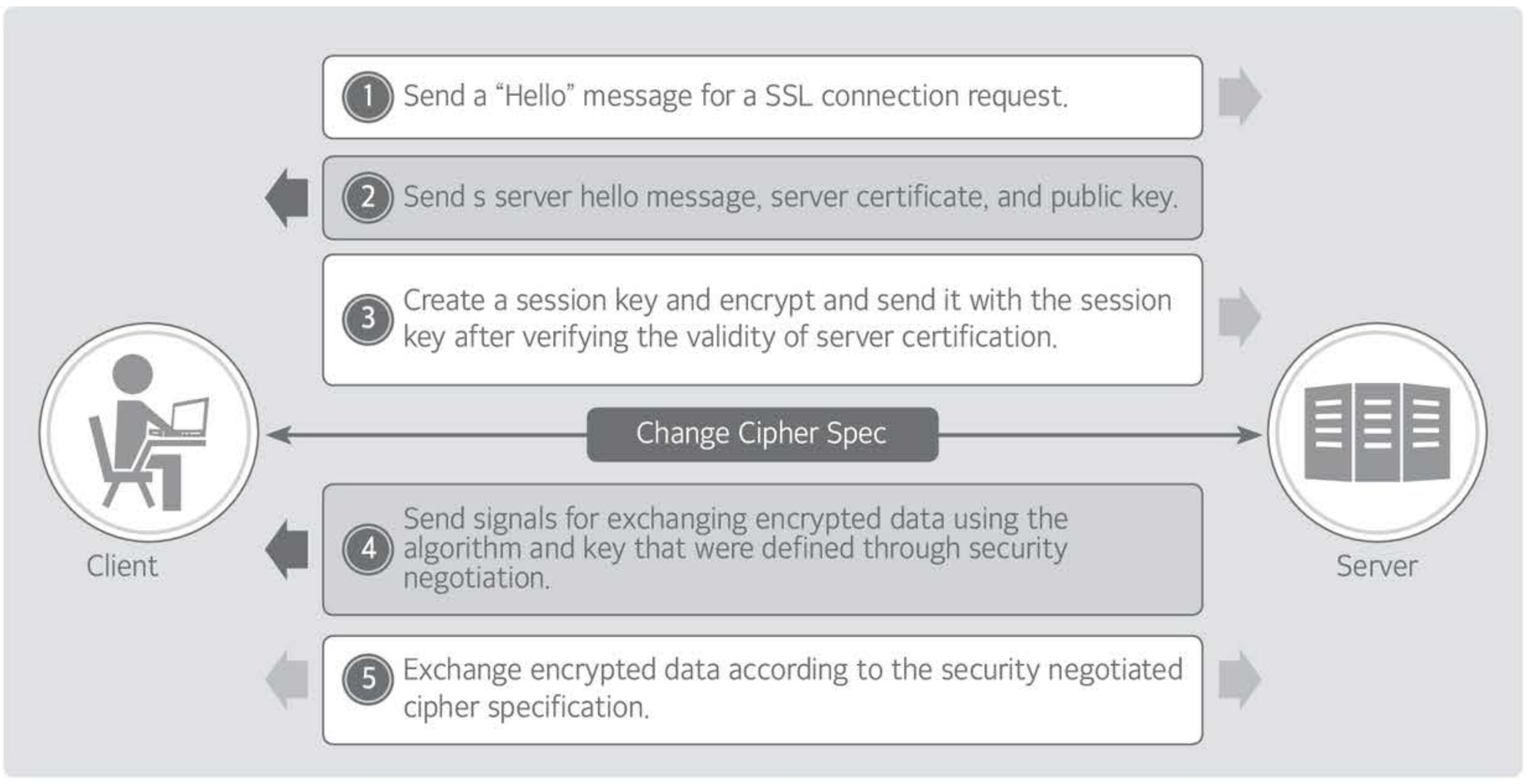
<Table 37> shows the functions by SSL protocol type.

<Table 37> Function of the SSL protocol

Type	Description
Handshake protocol	• Mutual authentication between the server and client • Negotiating the encryption algorithm, MAC algorithm, and cryptographic key to be used. • Performed before any application data transport
Record protocol	• Providing the confidentiality and integrity service for SSL connections • Encrypting messages, using the determined secret key cipher algorithm • Performing encryption, using the distributed symmetric key
Change cipher spec protocol	• Notifying the other party that the authentication and encryption system, defined in the cipher specification, will be applied from now on • One-byte long message with the value of 1
Warning protocol	• Used to deliver warnings, while performing SSL • A warning is composed of 2 bytes, and the first byte conveys the severity of the message: Warning(1), Fatal(2)

• Operating procedure of the SSL protocol

[Figure 65] shows the main operating procedure of the SSL protocol, and <Table 38> shows the operating details of each phase.



[Figure 65] Operating procedure of the SSL protocol

<Table 38> Operation by phase of the SSL protocol

Sequence	Description
Phase 1	The client sends a "Hello" message to the server.
Phase 2	The server sends a Server Hello message, server certificate, and public key to the client, together with a client certificate request if it is needed.
Phase 3	The client verifies the validity of the server's certificate, creates a session for encryption, and encrypts it with the server's public key. If the cipher specification and server request the client's certificate, the client's certificate is also sent.
Phase 4	The client sends signals to exchange encrypted data, using the algorithm, and the key is defined in cipher specification through security negotiation.
Phase 5	Encrypted data is exchanged according to the cipher specification for which security negotiation is performed.

③ Utilization

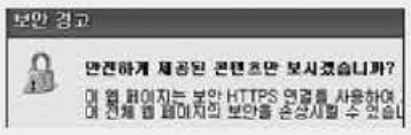
• Installing an SSL certificate in the server

An SSL certificate should be installed in the web server to apply SSL. A certificate signature request document, called CSR (Certificate Signing Request) should be created and requested to the certification authority after creating a private key in the running web server. Then, an SSL certificate should be received from the certification authority and installed in the web server in order to set the web server. If the SSL accelerator is used, the certificate can also be installed in the SSL accelerator.

• How to check SSL application

<Table 39> describes how to check the SSL installed in the web server.

<Table 39> Checking SSL application

Item	Contents
	Displays “https://” and a padlock icon in URL address bar of the web browser.
	Displays a security warning window when the page is changed.
	Displays a security certification seal.

• Consideration on the load after SSL application

Various computing tasks created during the SSL handshake process put a heavy workload on the CPU. The SSL accelerator is a solution released to solve such a heavy workload on the CPU. The SSL accelerator can be installed on the server as a separate PCI card or dedicated equipment. Recently, since the web accelerator and L4 switch provide an SSL accelerator as a separate function, only a separate SSL accelerator license needs to be purchased.

The connection URL and the URL included in the web application source should be changed to “https://” after applying SSL. In addition, the web application response speed can be improved when the SSL load of the static content, such as images, JavaScript, CSS (CascadingStyleSheets), etc. is increased, using an SSL web browser cache or a web accelerator.

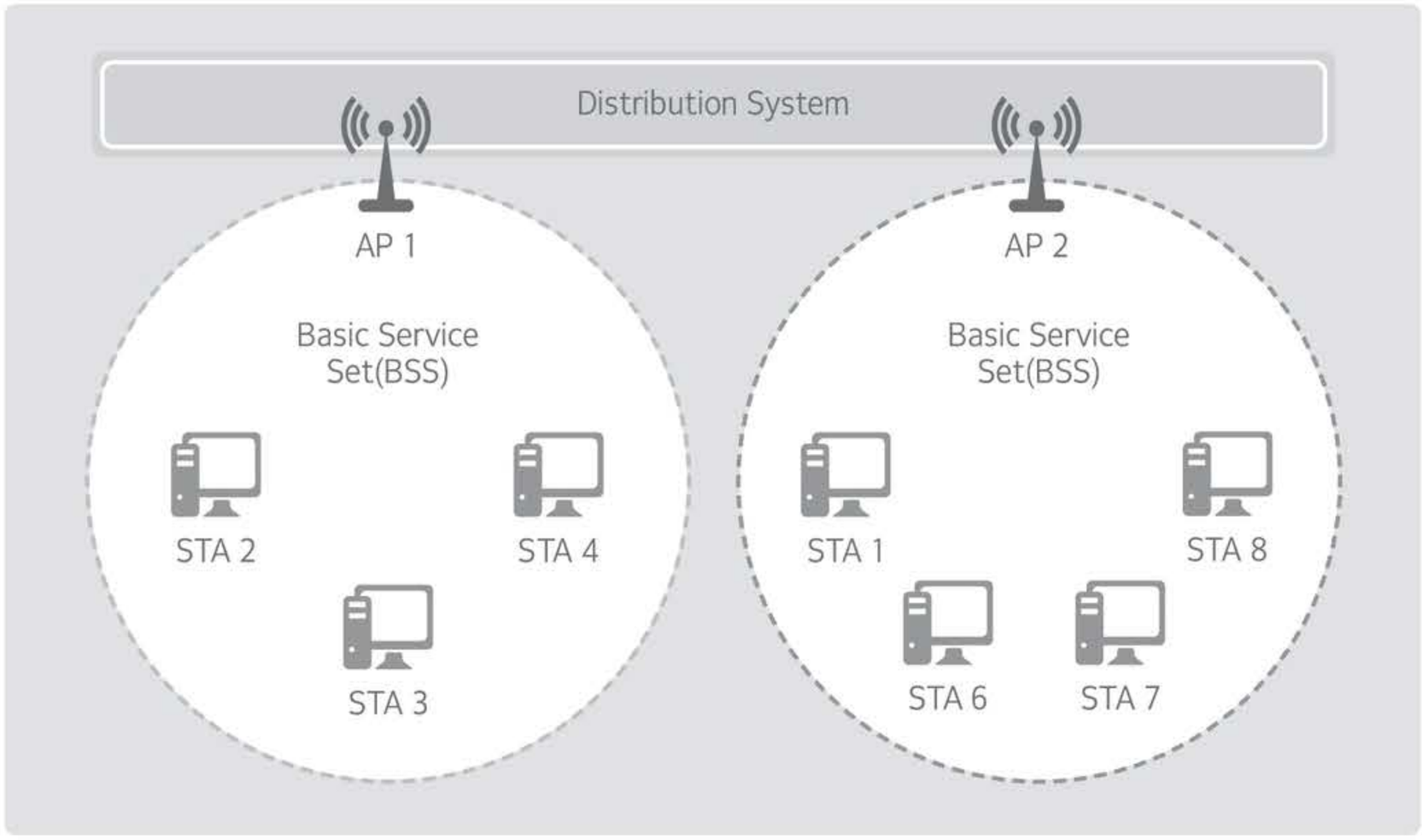
03 WLAN security

A) Characteristics of the WLAN

Since incoming and outgoing data is broadcast in the air in the wireless LAN, using radio waves, the data is exposed to all wireless LAN users while it is being transmitted.

The use of wireless LAN is increasing rapidly because it has various advantages and convenience. However, security is more vulnerable than wired LAN because of the characteristic of using radio waves as a communication medium. Therefore, security should be considered more seriously. In particular, there is a high possibility of various security incidents in the environment that is opened to the public, like a public wireless LAN. Therefore, security should be taken into account.

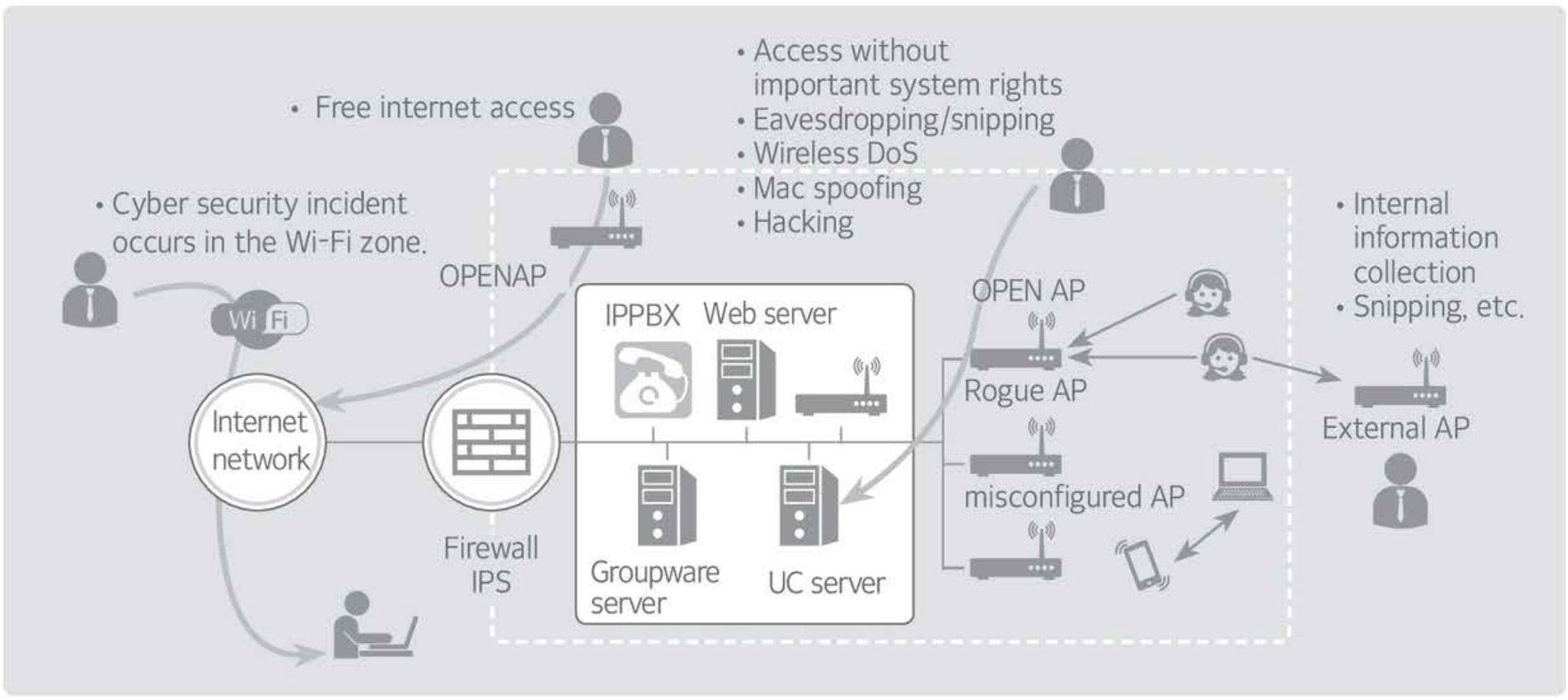
[Figure 66] shows the structure of the general WLAN, defined by the IEEE 802.11. In this figure, the Basic Service Set (BSS) is a unit composed of stations (STAs) that compete for access to the same wireless medium, while running with the same MAC protocol. And the extended service set refers to an environment in which multiple basic service sets can be connected to a distribution system in order to communicate with each other.



[Figure 66] Extended service set of IEEE 802.11
(Source: W. Stallings, Network Security Essentials, Pearson, p.180)

B) Security threats and responses

Since wireless LAN communication uses radio waves, physical access control on the communication medium is impossible. Therefore, anyone can use wireless LAN services and various security threats can be caused by radio wave collection and disturbance. [Figure 67] shows various security threats in the wireless LAN.



[Figure 67] Wireless LAN security threats
(Source: Baek Jonghyeon, Domestic Wi-Fi Security Status and Guide to Safe Wireless LAN Usage, TTA Journal)

① Technical security threats

- There are various types of attacks in the technical security threat of the wireless LAN, including the leakage of important user information through radio wave collection, illegal access, and man in the middle attack; jamming, denial of service attack using large packet transmission, and hacking weak security settings, such as WEP (Wired Equivalent Privacy) to illegally access and infiltrate into the internal network.
- Most technical security threats to wireless LAN can be blocked by setting security features provided by the wireless AP (Access Point), such as WPA2 (Wi-Fi Protected Access2). However, when using a wireless LAN in a place where important information is handled, such as in a corporate environment, a professional wireless security system, such as WIPS (Wireless Intrusion Prevention System) must be introduced.

② Administrative security threats

- A strong security technology can be easily bypassed if the threat is not properly managed, even though the technology is applied to the wireless LAN. Administrative security threats include insufficient management of wireless LAN equipment and devices, intrusion, due to a lack of user security awareness, and allowing outsiders to access internal APs and insiders to access external Aps, due to insufficient radio wave management.
- To respond to the administrative security threat of wireless LAN, management plans for access devices and terminals, such as Aps, should be established and implemented, user awareness should be raised periodically, training should be implemented, and illegal internal and external accesses should be checked.

③ Physical security threats

- Most network devices in the wired LAN environment are installed and managed in a place that is difficult to access by general users. On the contrary, most of the wireless AP are exposed and installed outside because radio waves should be transmitted. In this case, the wireless AP is exposed to risks, such as theft and damage, power shutdown, LAN cable separation, etc., so service failure may occur. Also, if the wireless device is lost and stored WLAN access information and security setting information is leaked, unauthorized persons can access the wireless LAN.
- To prepare for such a threat, it should be ensured that the wireless AP is not exposed to the outside, setting information should be changed periodically, and a method of managing devices that use the WLAN, along with a loss prevention plan, should be devised.

C) Wireless LAN security

① IEEE 802.11i services

WEP was developed to reinforce the security functions of IEEE 802.11 (wireless LAN standard).
However, it is exposed to various attack techniques, such as the brute force attack, due to insufficient security features. Accordingly, the 802.11i working group has developed various functions to solve the security problem of the wireless LAN.

To protect wireless LAN users, the IEEE 802.11i standard defines user authentication, key exchange, and advanced wireless section encryption algorithms. It also satisfies standardization goals by implementing IEEE

802.1X authentication, 4-way handshake key exchange, and CCMP (Counter Mode With CBC-MAC Protocol) encryption algorithm, as essential functions.

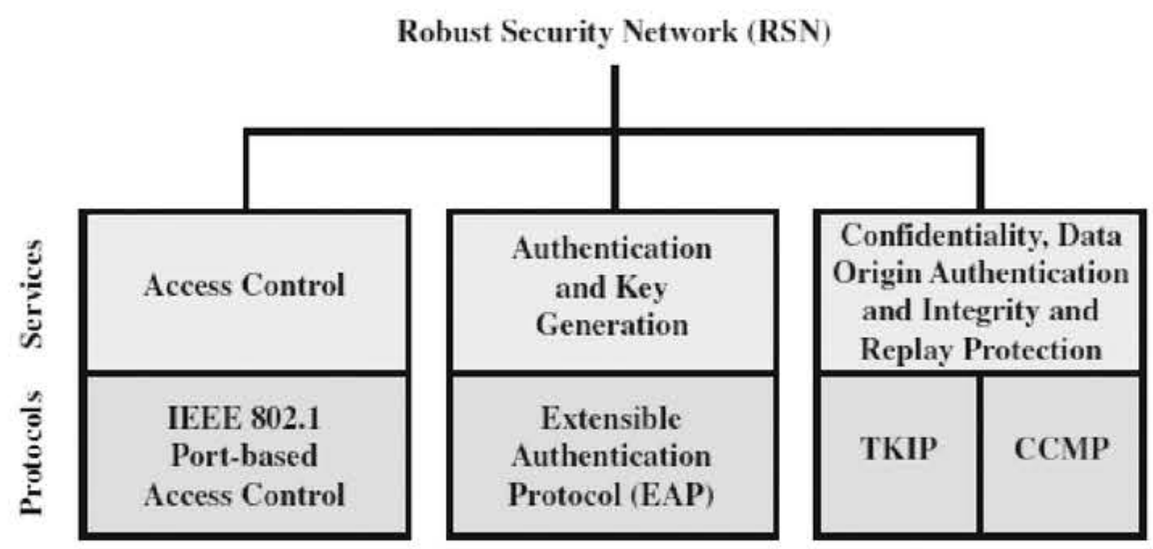
② IEEE 802.11i components

The security standard of IEEE 802.11i defines the following services. [Figure 68] shows the structure of the security protocol and encryption protocol used to provide these services.

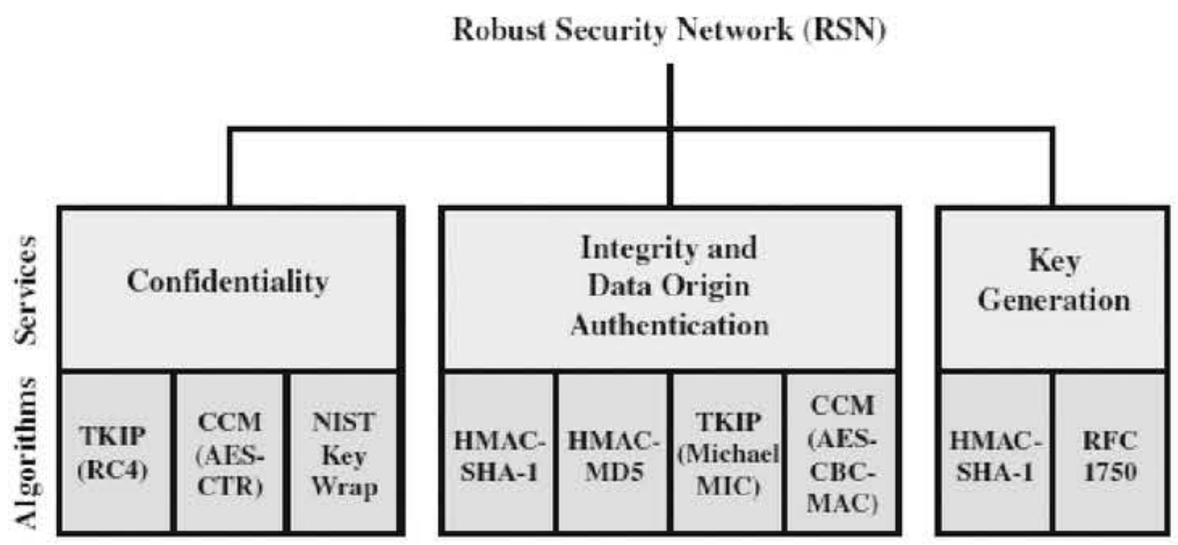
• Authentication: The user and the authentication server (AS) should authenticate with each other using the protocol, and a temporary key, to be used between the client and the AP on the wireless link, should be generated.

• Access control: Proper message routing and key exchange should be performed using the authentication function. This function can be performed together with various authentication protocols.

• Privacy through message integrity: MAC layer data is encrypted together with message integrity code, to guarantee that it is not been tampered with.



(a) Services and protocols



(b) Cryptographic algorithms

CBC-MAC = Cipher Block Block Chaining Message Authentication Code (MAC)
CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol

[Figure 68] IEEE 802.11i components

(Source: W. Stallings, Network Security Essentials, Pearson, p.184)

③ IEEE 802.11i operation

IEEE 802.11i operation may vary depending on the configuration and device of the WLAN and can be described by a five-step operation, as shown in [Figure 69].

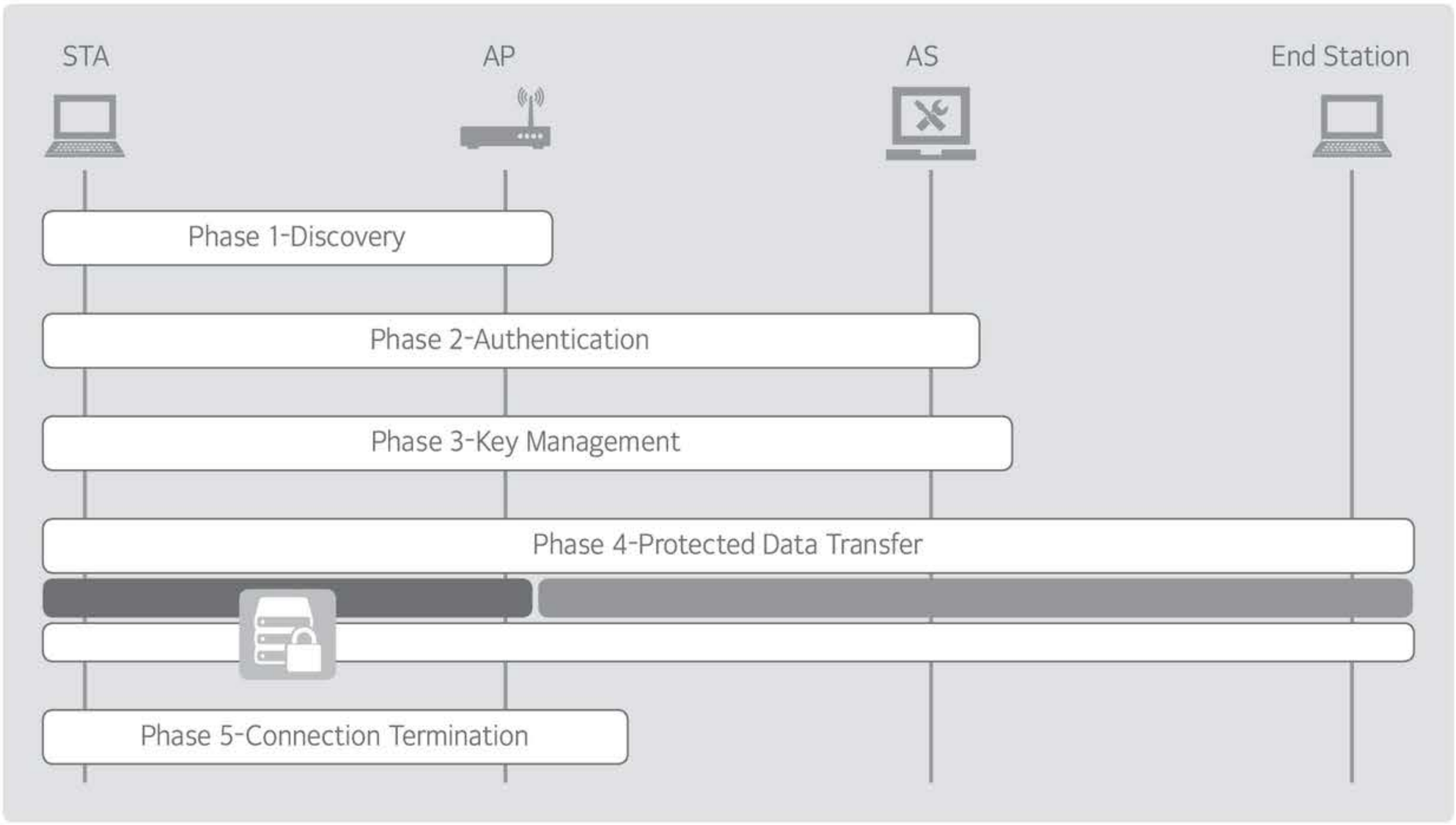
(1) Search: The STA that wants communication, searches for the desired WLAN AP to generate an SA with an AP, using the function that the AP broadcasts security policies.

(2) Authentication: The STA and AS (authentication server) authenticate with each other. At this time, the AP only transfers communication data between the STA and the AS.

(3) Key generation and distribution: In this phase, the AS transfers PMK (Pairwise Master Key) to the AP of the STA, using the key distribution protocol, based on RADIUS (Remote Authentication Dial-In User Services). After that, the AP and STA generate and share the cryptographic key, by exchanging messages using the 802.11x protocol.

(4) Secure data transmission: The STA and the other party's end station securely exchange frames using the AP. In this case, data is only transmitted between the STA and the AP.

(5) Disconnection: The secure connection of the AP and the STA is released by exchanging messages, and the original connection is restored.



[Figure 69] IEEE 802.11i operation steps
(Source: W. Stallings, Network Security Essentials, Pearson, p.185)