Chapter 6

Security

1 Overview of Information Security

Information systems and the Internet are becoming part of the infrastructure of modern society. As dependence upon IT increases, so does the importance of information security. Since measures implemented in information security are broadly divided into technological measures and management measures, this section discusses information security overall in terms of both technology and management.

1-1 Concept of Information Security

CIA

ISO/IEC 27000:2014 (JIS Q 27000:2014) describes information security as "preservation of confidentiality, integrity, and availability of information; in addition, other properties such as, authenticity, accountability, non-repudiation, and reliability can also be involved."

Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes
Integrity	The property of safeguarding the accuracy and completeness of assets
Availability	The property of being accessible and usable upon demand by an authorized entity
Authenticity	The property that an entity is what it claims to be
Accountability	The property that ensures that the actions of an entity may be traced uniquely to the entity
Non-repudiation	The property of proving that an action or event has taken place, so that this event or action cannot be repudiated later
Reliability	The property of consistent intended behavior and results

In information security, the following three objects to be managed and four management functions are given attention to maintain the confidentiality, integrity, and availability of information.

[Objects to be managed in information security]

Asset	Anything that has value to the organization
Threat	A potential cause of an unwanted incident, which may result in harm to a system or organization

Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more threats

[Management functions of information security]

Prevention functions	Functions to prevent the occurrence of threats
Detection functions	Functions to discover and detect threats that have occurred
Minimization functions	Functions to minimize the damage from a threat that has occurred and to prevent its expansion
Restoration functions	Functions for prompt restoration from damage caused by threats

In addition, the OECD (Organization for Economic Cooperation and Development) recommends the following nine principles for participants (information system owners, providers, and users) in its "Guidelines for the Security of Information Systems and Networks."

(1) Awareness

Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

(2) Responsibility

All participants are responsible for the security of information systems and networks.

(3) Response

Participants should act in a timely and co-operative manner to prevent, detect, and respond to security incidents.

(4) Ethics

Participants should respect the legitimate interests of others.

(5) Democracy

The security of information systems and networks should be compatible with essential values of a democratic society.

(6) Risk assessment

Participants should conduct risk assessments of information systems and networks.

(7) Security design and implementation

Participants should incorporate security as an essential element of information systems and networks.

(8) Security management

Participants should adopt a comprehensive approach to security management.

(9) Reassessment

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures, and procedures.

For understanding of the concept of information security, objects to be managed by information security are detailed in order.

1-1-1 Assets

Assets are defined as anything that has value to be protected by the organization. Among these, assets that involve important information in particular are known as information assets.

[Types of information assets]

- Tangible information assets

  These are information assets with tangible form, including hardware assets such as computers and communication equipment, and software assets such as business software, system software, and documents.
- Intangible information assets

  These are information assets without tangible form, including some types of information such as customer information, sales information, intellectual property-related information, and personnel information, and other types of information such as the reputation and image of an organization.

1-1-2 Threats (or Perils)

Threats (or perils) are things which may cause loss to information assets. Examples of threats that pertain to the Internet and other networks include the following.

- Tapping

  The interception of data by a third party with malicious intent
- Falsification

  The fraudulent rewriting of information in e-mail or web pages
- Spoofing

  The performance of fraudulent actions by impersonating another person (e.g., authorized user)
- Theft

The theft of files or data by a third party with malicious intent

- Destruction

  The fraudulent destruction or erasure of files or data

Threats are classified into three types as follows:

- Personal threat

  This is the type of threat that is caused by human behavior (with or without malicious intent).
- Technological threat

  This is the type of threat in which a third party with malicious intent uses computer technology to make attacks.
- Physical threat

  This is the type of threat against equipment itself or against the buildings in which equipment is located.

Specific examples of each type of threat are presented below. A case that corresponds to more than one type of threat is included among the type of threat that displays its characteristics most strongly.

(1) Personal threats

Typical examples of personal threats include the following. In particular, the acts that are recognized as fraudulent are sometimes termed fraudulent behavior.

- Information leakage

  This is the leakage of information to a third party. It includes intentional leakage with the aim of receiving payment for information provision, and unintentional leakage of important information accidentally overheard by a third party. In addition, information in discarded equipment may be restored and leaked if not physically deleted (i.e., destroyed).
- Loss / Theft / Damage

  This means that IT devices, such as PCs and USB memory, where information is stored are left behind, stolen, or destroyed during use.
- Error / Incorrect operation

  This is data erasure or such other error that is caused by wrong operation. It includes the leakage of important information through mistaken entry of recipient e-mail addresses.

- Social engineering

  This is the act of stealing information through everyday and common means.

  - Trashing (scavenging, dumpster diving)

    This is the act of stealing important information from memos thrown away in the garbage bin, data left in memory or cache, etc. It is also used as a method of foot printing for prior collection of information about the target of attacks.

  - Spoofing

    This is the impersonation of a person by a third party. The spoofer may pretend to be a customer or a supervisor in order to ask for PINs (PIN Numbers) or passwords.

  - Peeping

    This is the act of sneaking a peek at keyboard operation of a person who is entering a password, or classified information displayed on another person's screen. In particular, the act of sneaking a peek at information over a person's shoulder is called shoulder hacking.

- Cracking

  This is the act of intruding into another person's PC with malicious intent, to steal or destroy data. A person who engages in cracking is called a cracker. Note that the software package used by a cracker after unauthorized intrusion is called a rootkit, and the path installed to facilitate later intrusion is called a back door.

- Targeted attack

  This is the act of attacking a specific organization or person as a target. Since humans select the target of the attack, this is classified as a personal threat. However, the attack method itself is primarily classified as a technological threat.

(2) Technological threats

Typical examples of technological threats include unauthorized access or denial of service using computer technology, and computer crime. The compromise of safety due to advances in computer technology can also be called a technological threat.

Typical attack methods using computer technology, which are classified as technological threats, include the following.

- DoS attack (Denial of Service)

  This is an attack that sends a large amount of data continually to the target server to place an excessive load on the server's CPU and memory, and thereby obstructs service. In addition, there is also a DDoS (Distributed DoS) attack in which malicious programs used for targeted attacks are used to attack the single target all at once from multiple PCs.

- Key logger

  This is an attack that uses the mechanism (e.g., software) that records keyboard input, and fraudulently acquires information (e.g., password) entered by another person.

- Clickjacking

  This is an attack that sets up a web page with some sort of function that causes a user's click to execute operations not intended by the user.

- Phishing

  This is an attack that leads a user to a fake website through means such as e-mail pretending to be sent from a real company (e.g., financial institution), and defrauds the user of the credit card number, a bank account number, a PIN, and other personal information.

- Cache poisoning

  This is an attack that fraudulently overwrites cache information. In particular, DNS cache poisoning, which overwrites DNS cache, is used to lead users to fake websites for phishing.

- IP spoofing

  This is an attack that sends packets to another party with the source IP address disguised. This is used in actions including leading users to fake websites for phishing.

- XSS (Cross Site Scripting)

  This is an attack where a vulnerable target website is used as a stepping stone; a malicious script is sent to a user who is accessing the target website, and then executed on the user's browser to enable the theft of information.

- CSRF (Cross Site Request Forgery)

  This is an attack which, when a user is logged in to a website and then accesses another website that has a trap installed, causes a malicious request to be sent to and executed by the logged-in website in the guise of a request from the user (i.e., as a forgery).

- Session hijacking

  This is an attack that takes over a session (i.e., a series of communications between specified parties) during communication between correctly authorized users.

- Directory traversal

  This is an attack that accesses normally undisclosed directories (or files) by appending "../" to file names, to traverse upward through directories.

- Drive-by download

  This is an attack that causes a user to download a malicious program, without permission during website browsing.

- SQL injection

This is an attack that falsely modifies a database or fraudulently obtains information by providing part of an SQL statement as a parameter to a program (CGI program) in the website that is linked to the database.

- Side channel attack

  This is an attack that obtains confidential information by measuring and analyzing some additional information (i.e., side channel information), such as the electric power consumption or radiated electromagnetic waves of active IC chips.

- Zero-day attack

  This is an attack that takes advantage of a vulnerability in software before a fix for the vulnerability can be released by the software vendor.

- Password cracking

  This is an attack that fraudulently decodes or otherwise obtains the password of a true user.

  - Dictionary attack

    This is a method that uses a file (i.e., a dictionary file) that contains character strings likely to be used as passwords, to try such words in sequence.

  - Brute force attack

    This is a brute-force method that attempts every combination of characters. It is used as an attack method of performing the exhaustive search for a decryption key.

- Third-party relay

  This is an attack that abuses a freely usable server (e.g., mail server) as a “stepping stone” to transmit e-mail and other data.

- Gumblar

  This is an attack that falsifies the website of a famous company or public institution, and infects the computer of a user who is browsing the falsified website with a computer virus.

- Buffer overflow

  This is an attack that continually sends long character strings or such other data to flood the memory area (i.e., buffer) secured by a program, for the purpose of seizing access privileges to the program and creating malfunctions.

Fraudulent programs (i.e., malware) created with malicious intent are also classified as technological threats.

The following are typical examples of malware.

- Computer virus

In the Japanese Ministry of Economy, Trade and Industry's "Standards for Measures Against Computer Viruses," a computer virus is defined as "a program that is created to intentionally cause some form of damage to third parties' programs or databases, and that has one or more of the following functions."

Self-infecting function	Viruses make copies of themselves to infect other systems.
Concealment function	Viruses do not reveal symptoms until the onset of their action.
Onset function	Viruses perform actions not intended by designers, such as destruction of data.

However, in general at present, file-infecting viruses that infect specific files are called computer viruses (in a narrow sense).

  - Boot sector virus

    This virus infects the boot sector (i.e., the system area that contains the boot program) that is read before an OS starts up.

  - Program file virus

    This virus infects the executable program files such as applications.

  - Interpreter virus

    This virus infects non-executable files, such as data files, other than program files. It includes two types of viruses: a macro virus that infects through the macro functions of application software, and a script virus that infects through a scripting language like JavaScript or VBScript.

- Worm

A worm proliferates by duplicating itself on other computers through networks, without the need for a program to be infected. It often spreads a copy of itself automatically as an e-mail attachment file, or uses networks to continue spreading infection.

- Bot

This is a program that is created for the purpose of controlling infected computers from outside via networks (e.g., the Internet).

- Spyware

This is a program that illicitly obtains a user's information, such as personal information and access histories, and automatically sends such information to another party other than the user.

- Trojan horse

This is a malicious program that pretends to be useful software but causes damage to users. While a Trojan horse does not infect files nor self-propagate, the concealed virus is delivered to a PC to transmit private files on the PC over the Internet, destroy the contents of files or disks, or otherwise cause damage.

The following computer crimes are also said to be types of technological threats.

- Salami technique (Salami slicing)
  This is a method of repeatedly stealing assets little by little so that they are negligibly small when taken as a whole. An example is a technique that collects money from a bank account into another account, in fractions of less than one yen.
- One-click fraud
  This is a type of fraudulent act; for example, clicking an image or link on matchmaking or adult websites causes an unfair fee to be charged.
- Phishing fraud
  This is a general name for the act of phishing, or for fraudulent acts committed using information obtained illicitly through phishing.

(3) Physical threats

The following are typical examples of physical threats.

- Disaster
  This means that equipment or buildings are made unusable, or equipment itself is lost, due to a natural disaster (e.g., earthquake, flood) or a human disaster (e.g., fire).
- Destruction
  This means that equipment or buildings are made unusable, due to sabotage or destructive acts by a third party with malicious intent.
- Accident / failure
  This means that equipment or buildings are made unusable, due to unforeseen accidents or failures.
- Unauthorized intrusion
  This means that unauthorized persons intrude into buildings or rooms in which equipment is located.

1-1-3 Vulnerabilities (or Hazards)

Vulnerabilities (or hazards) are weaknesses or flaws that are exploited by threats, becoming the cause of even greater threats. A variety of vulnerabilities in equipment, technologies, management, and many other areas cause problems.

- Security hole
  This is a vulnerability of software or systems that is caused by software design flaws, bugs, etc.
- Man-made vulnerability
  This is a vulnerability that is caused by human behavior, due to a lack of enforcement or preparation of a code of conduct for companies, organizations, and people.

1 - 2 Information Security Technology

Information security technology is computer technology used within the technological measures that are implemented as information security measures.

1-2-1 Cryptography

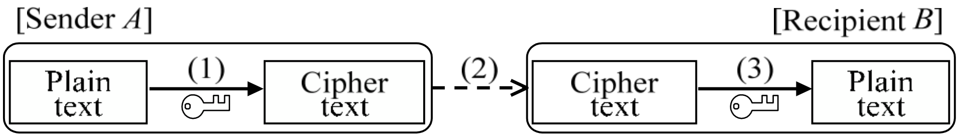
Cryptography is encryption technology implemented as measures against information leakage or measures against tapping of communications. Terminology that pertains to cryptography is defined as follows:

Term	Meaning
Plain text	Data in an unencrypted state
Cipher text	Data in an encrypted state
Encryption	The conversion of plain text to cipher text
Decryption	The conversion of cipher text to plain text
Encryption key / decryption key	Special data used in encryption/decryption
Key length	The length (usually in bits) of an encryption key or decryption key A longer key length is more difficult to decode.
Decoding	The obtaining of plain text from cipher text, by improper means
Encryption algorithm	An algorithm (i.e., program) that performs encryption / decryption
Encryption strength	The degree to which cipher text is difficult to decode

(1) Common key cryptography

Common key cryptography (also known as symmetric key cryptography or secret key cryptography) is a method for performing encryption/decryption between parties that exchange data, using a common key. This encryption method performs both encryption and decryption using the same key, and therefore, the parties must in advance have a common key that is kept secret from third parties.

[Common key cryptography procedure]



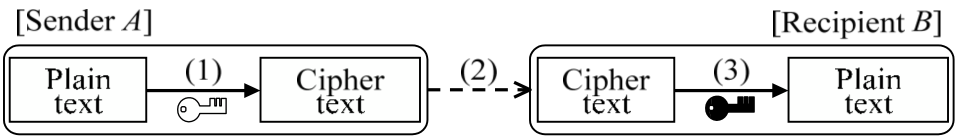
(1) Sender *A* encrypts plain text by using a common key.
(2) Sender *A* sends the cipher text (i.e., encrypted plain text) to Recipient *B*.
(3) Recipient *B* decrypts the cipher text by using the common key.

Typical methods of common key cryptography include AES (Advanced Encryption Standard) from the NIST (National Institute of Standards and Technology) which adopted the Rijndael method, TripleDES which repeats DES three times, and IDEA (International Data Encryption Algorithm) which repeats several rounds of the XOR (exclusive OR), addition, and multiplication operations.

(2) Public key cryptography

Public key cryptography is a method that uses a pair of private key and public key. The private key is concealed by its owner, while the public key is disclosed or distributed, and is made usable by anyone. This cryptography can encrypt plain text by using one key, and can decrypt the cipher text with the other key. However, this does not mean that the public key is always used for encryption and the private key for decryption; rather, they are used according to purpose (see details later). In order to prevent decryption of encrypted text by third parties when measures against information leakage or measures against tapping of communications are taken, encryption is performed with the recipient's public key, and decryption with the recipient's private key.

[Public key cryptography procedure]



(1) Sender *A* encrypts plain text by using Recipient *B*'s public key.

(2) Sender *A* sends the cipher text (i.e., encrypted plain text) to Recipient *B*.

(3) Recipient *B* decrypts the cipher text by using Recipient *B*'s private key.

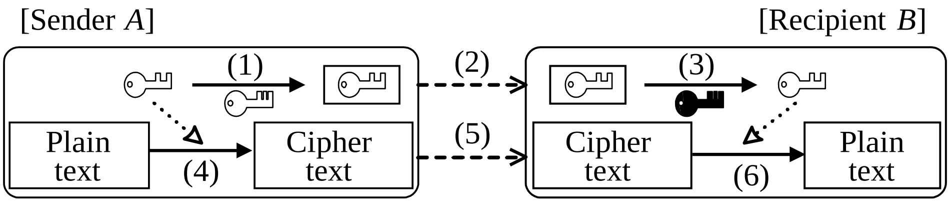
Typical methods of public key cryptography include RSA (from the initials of the three developers, Rivest, Shamir, and Adleman), ElGamal encryption which applies the discrete logarithm problem, and Elliptic Curve Cryptography which uses elliptic curve equations.

The strengths and weaknesses of common key cryptography and public key cryptography can be summarized as follows:

	Common key cryptography	Public key cryptography
Strengths	• For the same key length, common key cryptography has higher encryption strength than public key cryptography. • Common key cryptography requires less time for encryption/decryption than does public key cryptography.	• Management and transfer of keys is easy. (In encrypted communication among *n* persons, the number of keys is *n* pairs [the number of types of keys is 2*n*].)
Weaknesses	• Common keys may be leaked under long-term tapping. • Management and transfer of keys is difficult. (In encrypted communication among n persons, the number of types of keys is $n(n-1)/2$.)	• For the same key length, public key cryptography has lower encryption strength than common key cryptography. • Public key cryptography requires more time to process due to complex encryption/decryption algorithms. • Public key cryptography may allow spoofing.

Session key cryptography (hybrid cryptography) uses public key cryptography for the transfer of keys, which has a weakness of common key cryptography, and performs encrypted communication using common key cryptography.

[Session key cryptography procedure]



(1) Sender *A* encrypts a generated common key by using Recipient *B*'s public key.

(2) Sender *A* sends the encrypted common key to Recipient *B*.

(3) Recipient *B* decrypts the encrypted common key by using Recipient *B*'s private key.

(4) Sender *A* encrypts plain text by using the common key.

(5) Sender *A* sends the cipher text (i.e., encrypted plain text) to Recipient *B*.

(6) Recipient *B* decrypts the cipher text by using the common key.

In session key cryptography, common keys are generated using means such as a hash function (i.e., a function that obtains a unique, fixed-length output value from an input value) which is based on the communication session number or a random number. The generation of a common key is performed for each encrypted communication session, and the key is transferred using public key cryptography. For that reason, damage is limited even if the common key is leaked. In addition, since only one pair of public key and private key usually needs to be managed, management of keys is simple, and encrypted communication can be carried out at high speed by using common key cryptography. In other words, this approach can be said to combine the strengths of common key cryptography and public key cryptography. However, even session key cryptography is not able to eliminate the possibility of spoofing.

(3) Session key cryptography (hybrid cryptography)

(Block cipher mode of operation)

Block cipher mode of operation defines the use of a block cipher that performs encryption in units of fixed-length blocks. (The cipher used in the method of encrypting in units of bits or bytes is called a stream cipher.) For example, AES of common key cryptography adopts a 128-bit block cipher, while IDEA adopts a 64-bit block cipher.

In block cipher modes of operation, there are two major types of modes: one mode is used for concealing messages (encryption method), and the other mode for message authentication (message authentication code). For example, ECB mode is a mode of operation for concealing messages. When this mode is used to encrypt multiple blocks, there is the possibility that the same cipher text may be generated from the same plain text, and the contents may be guessed. For this reason, another mode such as CBC mode, which generates differing cipher text even when the same plain text is encrypted, is recommended.

1-2-2 Authentication Technique

(1) User authentication

User authentication is an authentication technique that includes the process of verifying a user’s identity. It is used as a measure against the impersonation of authorized users by malicious third parties.

In user authentication, there are a variety of methods according to purpose and application.

(1) User ID / Password

A user ID is an identifier that is assigned to an individual user, while a password is a character string (i.e., a keyword) that is registered in advance. During the login process, this technique searches for a registered password corresponding the user ID entered by the user. If the registered password matches the password entered by the user, the user is authenticated as a valid user who knows the password.

When this technique is used, it is necessary for users to thoroughly follow password management and password requirements to prevent any abuse of passwords.

[Points to note for password management]

- Use a meaningless character string that combines alphameric characters, symbols, etc.
- Make the password as long as necessary. (at least 6 or 8 characters)
- Do not use the same password for a long time. Change it regularly.
- Do not reuse passwords (i.e., do not use the same password for multiple authentications).

- Do not record passwords where they will be seen. (Jotting down passwords does not need to be prohibited, but this should be properly managed).
- Do not share passwords with others nor give passwords to others.
- If a password is forgotten, leaked, or no longer needed, promptly contact the administrator and take required actions (e.g., invalidation of password)
- To prevent theft (or leakage), encrypt a password (or convert it to a hash value) and record the password.

(2) IC card

This is a technique that authenticates users through plastic IC cards with embedded IC chips that are able to record information. It is used for commuter passes, employee ID cards, etc. When an IC card is used, the user may be asked to enter the PIN code (Personal Identification Number) recorded in the IC chip in order to confirm that the user is the rightful holder of the card.

IC cards have over 100 times more storage capacity than magnetic cards and enable data encryption to make the cards resistant to forgery. The cards also have an advantage in tamper resistance to prevent unauthorized access or falsification.

(3) OTP (One-Time Password)

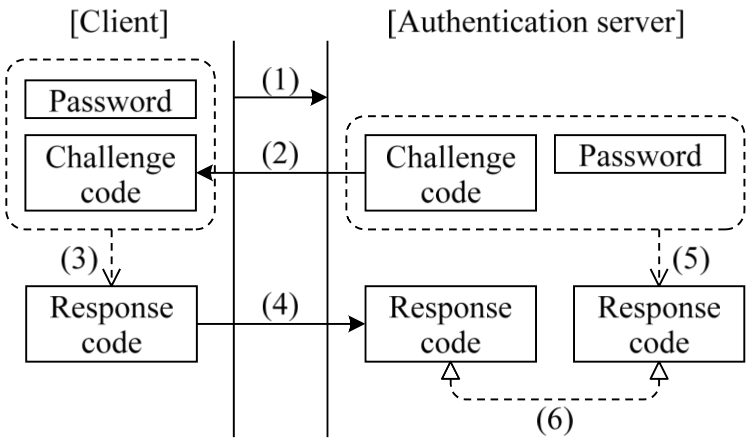
This is a password-based user authentication technique that is primarily used by computers connected to communication lines. By using a different password for each login, this technique avoids the risk of password leakage.

Typical one-time password methods are as follows:

- Challenge-response authentication

  This method does not transmit passwords directly over communication lines. Instead of a password, the method uses a response code that is generated from both the password and a challenge code (a random number) that differs for each access request, in order to authenticate a user.

  In some cases, a one-time password generation function is built into the IC card, which is used together with PIN code-based authentication.



(1) The client sends a user ID and requests access.
(2) The authentication server generates and sends a challenge code.
(3) The client generates a response code from its own password and the received challenge code.
(4) The client sends the response code to the authentication server.
(5) The authentication server generates another response code from both the password of the user indicated by the user ID and the challenge code that was sent.
(6) The authentication server compares the received response code with the response code generated in (5), and authenticates the client if those two response codes are the same.

- Time synchronous authentication

This method uses cash card-sized dedicated client hardware that displays a PIN code that changes at set time intervals. The code is attached after the time and user ID, and sent along with them. Since the dedicated client hardware and authentication server are synchronized, the login is approved if the PIN code sent by the client is the same as that of the server.

(4) Biometric authentication

This authentication technique identifies an individual (i.e., a user) by using physical information or behavioral information (e.g., speed or pen pressure used in a signature) that is unique to the individual, and such information is registered in advance on the authentication system. In addition to managing entry into secure areas, this authentication is also used by bank ATMs and individual PCs.

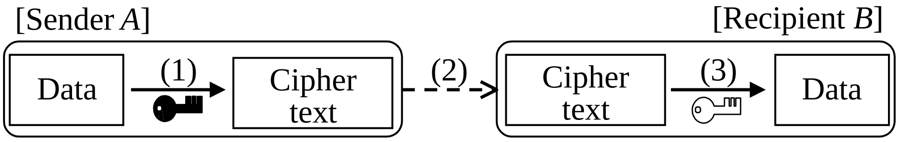
Although it is effective in preventing spoofing, it requires special authentication systems and continues to present issues in areas such as authentication precision (FRR (False Rejection Rate) and FAR (False Acceptance Rate)), difficulty of substitution, adaptation to physical changes over time, and personal information protection.

Name	Authentication information
Face authentication	Facial characteristics (e.g., positional relationships among eyes, nose, and mouth)
Iris authentication	Pattern shape, shading, etc. of the iris (the folds emanating from the pupil) of the eye
Voice authentication	Characteristics of the voice wave pattern
Palm authentication	Width of the palm, length of the fingers, etc.
Vein authentication	Branching angle, length, etc. of veins * This is sometimes included in palm authentication.
Fingerprint authentication	Characteristics (called “minutia points”) of fingerprints (i.e., the pattern formed by ridges on fingertips)

(5) Public key cryptography

This is an authentication technique that uses private keys that are kept secret by the holders.

[Authentication procedure in public key cryptography]



(1) Sender *A* encrypts data by using Sender *A*’s private key.

(2) Sender *A* sends the cipher text (i.e., encrypted data) to Recipient *B*.

(3) Recipient *B* decrypts the cipher text by using Sender *A*’s public key.

→ When decryption is successfully performed, it is confirmed that “*A*” is the sender.

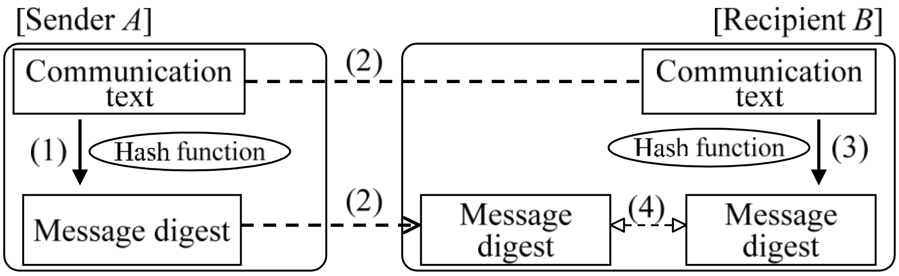
Step (3) is the key point in user authentication. The fact that Recipient *B* successfully performed decryption using Sender *A*’s public key means that the cipher text had been encrypted using *A*’s private key (because cipher text encrypted from plain text by using one of the key pairs can only be decrypted using the other key). Since only *A* has (i.e., conceals) *A*’s private key, this cipher text cannot be created by any party other than *A*. In other words, it is confirmed (i.e., authenticated) that the sender is unquestionably *A*.
However, it is necessary to note that this authentication works well on the assumption that *A*’s public key, which *B* has, must belong to *A* without doubt, and its paired private key must be owned by *A* alone.

(2) Message authentication

Message authentication is an authentication technique that confirms that data is not improperly overwritten. It is used as a measure to prevent falsification involving improper overwriting of data.

As a typical message authentication method used in data communication, there is a method of calculating a message digest from the communication text (i.e., the data) by using a hash function.

[Message authentication procedure]



(1) Sender *A* calculates a message digest from the communication text.
(2) Sender *A* sends the communication text and its message digest to Recipient *B*. (3)
Recipient *B* calculates a message digest from the received communication text. (4)
Recipient *B* compares the received message digest with the message digest generated in (3), and if the two message digests are the same, it is confirmed that the communication text is not falsified (nor tampered with) during communication.

- Hash function

This is a function that obtains an output value (i.e., a hash value) of fixed length from an input value of arbitrary length. It has the property (often referred to as the one-way property) that the same output value is obtained from the same input value, and the input value cannot be obtained from the output value.

Hash function name		Length of hash value	Standardization/normalization
SHA-1		160 bits	Standardized by NIST
SHA-2	SHA-256	256 bits	Standardized by NIST as the successor to SHA-1
	SHA-512	512 bits	
MD5		128 bits	Standardized as RFC 1321

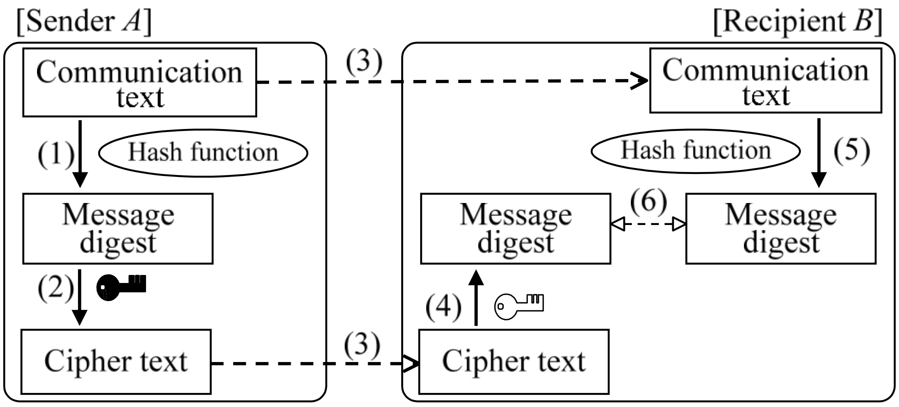
On the basis of the property of a hash function, if there is even a small difference in the communication text between the sender side and the recipient side, the message digests that are delivered to and generated by the recipient side will be different, and as a result, falsification can be detected.

However, when an already-known hash function is used, there is a possibility that both the communication text and the message digest can be falsified so as not to be detected. MAC (Message Authentication Code) is a technique that can resolve this issue. This method uses a key (i.e., a common key) owned by the sender and the recipient, and also uses a MAC value, which is calculated from the communication text plus the common key, as a message digest. (As a method for calculating the MAC value, a block cipher mode of operation or a hash function is used.) When this method is used, a third party who does not know the common key cannot calculate the correct MAC value, and therefore, the level of security is enhanced.

(3) Digital signature

Digital signature is an authentication technique that combines user authentication and message authentication using public key cryptography. (To distinguish digital or other electronic-based signatures from regular signatures, these are sometimes called electronic signatures.)

[Digital signature procedure]



(1) Sender *A* calculates a message digest from the communication text.

(2) Sender *A* encrypts the message digest by using Sender *A*’s private key.

(3) Sender *A* sends the communication text and its cipher text to Recipient *B*.

(4) Recipient *B* decrypts the cipher text by using Sender *A*’s public key.

(5) Recipient *B* calculates a message digest from the received communication text.

(6) Recipient *B* compares the message digest decrypted in (4) with the message digest calculated in (5). If these two are the same, it is confirmed that “*A*” is the sender, and in addition, the communication text is not falsified.

A typical digital signature method is DSA (Digital Signature Algorithm) developed by NIST

(National Institute of Standards and Technology) as a US government standard. DSA is an improved version of ElGamal signature, which uses the ElGamal encryption scheme known as one of the public key cryptography standards, and generates message digests using SHA-1 or SHA-2. It is noted that SHA-1 is being migrated to SHA-2 (e.g., a general term for SHA-256, SHA-512).

Another method is the W3C-recommended XML signature, which defines a digital signature syntax for XML documents. XML signatures can be attached to communication text like normal signatures, and can also be attached to specified elements or content.

In digital signatures, third parties (private companies) known as certification bodies guarantee the validity of public and private keys on which user authentication by public key cryptography is predicated. These certification bodies are also used for specified purposes (e.g., public key cryptography) other than digital signatures.

Certification bodies are composed of third-party organizations, such as CA (Certification Authority), RA (Registration Authority), and VA (Validation Authority), which issue digital certificates to users and lower-level certification authorities in order to guarantee the validity of public keys and digital signatures. In addition, in order to certify the validity of certification bodies themselves and distribute public keys, they issue root certificates signed with their own private keys.

- Digital certificate (public key certificate)

  This is an electronic certificate for an individual or organization, which is issued by a certification authority. It contains the signature algorithm (hash function), encryption method, expiration date, public key of the certified party, and other information. In addition, it is encrypted with the private key of the certification authority so that users can confirm that it was issued by the certification authority.

  The decryption key (i.e., the public key) for a digital certificate can be obtained from the root certificate released by the certification authority. The following is the standard specification for digital certificate released by ITU-T (International Telecommunication Union — Telecommunication Standardization Sector) X.509.

Item name	Content
Version information	v1–v3
Serial number	Certificate number
Signature algorithm	The type of algorithm used for signatures: SHA-1 or MD5 (hash function), RSA (public key), etc.

Issuer name	Issuing body (usually the name of a certification authority)
Period of validity	Starting date and time and ending data and time (from several seconds to hundreds of years)
Certifier	Subject name (holder of certificate)
Public key information	Certifier’s public key information

- CRL (Certificate Revocation List)

  This is a list of digital certificates that must be revoked due to leakage or loss of keys, even during the period of validity. It contains the serial numbers and expiration dates of digital certificates, and is made publicly available in the repository of a certification authority. Users can confirm the validity of a digital certificate by searching the CRL.

- OCSP (On-line Certificate Status Protocol)

  This is a protocol to confirm the validity of a digital certificate on an online real-time basis. OCSP is defined in RFC 2560 of the IETF (Internet Engineering Task Force). OCSP servers are operated by CAs (Certification Authorities) and by VAs (Validation Authorities) which centrally manage CRLs. By confirming digital certificates with OCSP servers, OCSP clients can reduce the burden of CRL acquisition and collation. However, OCSP only confirms the revocation status of a digital certificate, and therefore, the period of validity and other information must be confirmed on the client side.

CAs (Certification Authorities) include two types of CAs: public CA that issues certificates for external web services, and private CA that takes on a role within a closed environment, such as a specified organization.

(4) Other certification techniques

(1) Time authentication (timestamp authentication)

This is a certification technique by which a third-party time stamping authority (TS authority, which may be a certification authority) guarantees the existence and authenticity of electronic documents, in accordance with the Japanese Act on Utilization of Telecommunications Technology in Document Preservation, etc. Conducted by Private Business Operators, etc. of 2005. Normally, a creator’s digital signature and digital certificate are attached to an electronic document.

[Authentication procedure in time authentication]

1) The user generates a message digest from an electronic document.
2) The user sends the message digest to a time stamping authority.
3) The time stamping authority generates a TS token that stamps the received message digest with time information, and securely stores a duplicate.
4) The time stamping authority encrypts the TS token by using its own private key.
5) The time stamping authority sends the encrypted TS token and its own digital certificate to the user.

<The following are steps to confirm the electronic document's existence and authenticity.>

6) The checker obtains the public key from the digital certificate of the time stamping authority.
7) The checker decrypts the encrypted TS token by using the obtained public key.
8) The checker compares the TS token's message digest with the message digest obtained from the original electronic document, to confirm that there is no falsification. In addition, the checker looks up the time information and confirms the existence of the electronic document.

(2) IEEE 802.1X

This is a client authentication technique used for LANs. It is implemented using a RADIUS server or other authentication server, and authentication software (i.e., supplicant).

(3) CAPTCHA (image authentication)

This is an authentication technique that requires users to identify a distorted image of letters or numbers displayed on the screen and then enter the corresponding correct characters, in order to confirm that they are human beings. It is used to prevent automatic posting by programs and such other automated processes.

1-2-3 PKI (Public Key Infrastructure)

PKI (Public Key Infrastructure) is a security platform using public key cryptography, certification bodies, and digital signatures. It is used in EC (Electronic Commerce) and in the SSL (Secure Sockets Layer) security protocol. Another authentication infrastructure is GPKI (Government PKI), which uses PKI for performing applications and notifications to administrative bodies. Since mutual authentication between government agencies' certification authorities and private certification authorities is required in GPKI, a BCA (Bridge Certification Authority) must mediate between such certification authorities.

1-3 Information Security Management

Information security management refers to the actions of analyzing and evaluating diverse risks pertaining to information assets (e.g., physical assets, software assets, intangible information assets), and planning and implementing appropriate security measures. This subsection discusses information security management, information security evaluation and certification scheme, and risk management in companies and other organizations.

1-3-1 Information Security Management

Information security management refers to the actions of clearly defining an organization's perspective to consider information security, and actually implementing and managing it.

(1) Information security policy

Information security policy clearly defines an organization's perspective to consider information security. Information security policy is systematically organized and managed as follows:

Name		Role
Information security policy		Concepts concerning information security
	Fundamental information security policy	The organization's unified and fundamental concepts and principles
	Information security measures criteria	Compliance items and criteria for the practice of fundamental policy
Information security measures implementation procedures, etc.		Specific implementation procedures, etc.

Fundamental information security policy clarifies the information assets to be protected by the organization and the reasons for their protection, and describes approaches (ideas and principles) to information security in a document.

Information security measures criteria defines the organization's unified behavior and decision-making criteria that should be observed with regard to information security, on the basis of its fundamental information security policy.

Information security measures procedures is a set of the specific implementation procedures for information security measures. They define specific security measures (security controls) for each specific target (e.g., hardware products, software products), from the standpoint of information security management functions (prevention, detection, minimization, and restoration). In particular, it is important to define in advance any response measures for situations that would present difficulties for business continuity.

- Contingency plan (emergency response plan)

  A contingency plan defines a set of response measures (e.g., minimization, recovery) that is primarily used in the event of urgent or emergency situations. Recovery from emergency situations resulting from disaster, in particular, may be termed disaster recovery.

Within companies and other organizations, a variety of security rules and regulations must be created on the basis of their information security policies. The following list shows some typical rules and regulations. In general, approval for these rules and regulations comes from top management.

[Security rules and regulations of corporate activities]

- Rules and regulations concerning employment agreements
- Office rules and regulations
- Security control rules and regulations
- Documentation control rules and regulations
- Information management rules and regulations
- Privacy policies (personal information protection policies)
- Rules and regulations on measures to be taken against computer virus infection
- Security education rules and regulations
- Penal rules and regulations
- Outward explanation rules and regulations
- Rules and regulations for updating rules

Among these rules and regulations, privacy policies (personal information protection policies) have been regarded as important in recent years.

Privacy policies (personal information protection policies) are policies related to activities for the protection of information (i.e., personal information) identifying individuals, such as name and date of birth. Personal information protection is implemented on the basis of these policies, as a part of a systematically integrated compliance program (i.e., a plan for compliance with laws and regulations by the company).

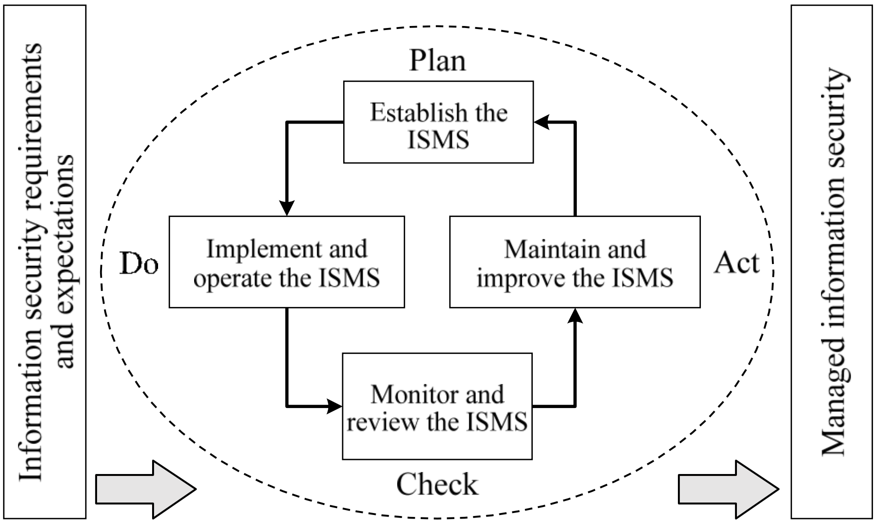
(2) ISMS (Information Security Management System)

ISMS (Information Security Management System) refers to a management system for the proper operational management of the organization's information assets overall, and for securing and maintaining the security of these. ISMS is built upon BS7799-1 and BS7799-2 of the British Standards Institution, and at present is standardized as the ISO 27000 family.

ISO/IEC standard	Overview
ISO/IEC 27000	Information security management systems - Overview and vocabulary
ISO/IEC 27001	Information security management systems – Requirements
ISO/IEC 27002	Code of practice for information security controls

ISMS provides a model for responsible persons (management team) and staff members in an organization so that they can build and operate an effective information security management system. Responsible persons must have commitment to (i.e., must have an official involvement in, and give approval to) the establishment, implementation, operation, monitoring, review, maintenance, and improvement of ISMS.
ISMS is operated according to the PDCA cycle (Plan, Do, Check, Act) indicated below.

[ISMS PDCA cycle (overview)]


Information security requirements and expectations
Plan
Establish the ISMS
Do
Implement and operate the ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Managed information security

(1) Plan: Establish the ISMS

1) Construct an information security promotion structure
2) Define and determine the scope and boundaries of the ISMS
3) Define an ISMS policy (including fundamental information security policy)
4) Conduct risk assessment (identification, analysis, and evaluation of risks)

5) Select control objectives and controls for the treatment of risks
6) Obtain management authorization to implement and operate the ISMS
7) Prepare a Statement of Applicability

(2) Do: Implement and operate the ISMS

1) Formulate and implement a risk treatment plan
2) Implement controls to meet the control objectives for risk treatment
3) Define how to measure the effectiveness of the controls
4) Implement training and awareness programs
5) Manage operation of the ISMS and resources for the ISMS

(3) Check: Monitor and review the ISMS

1) Undertake regular reviews of the effectiveness of the ISMS
2) Measure the effectiveness of controls
3) Conduct internal ISMS audits

(4) Act: Maintain and improve the ISMS

1) Implement the identified improvements
2) Take appropriate corrective and preventive actions

In Japan, the ISMS conformity assessment system of the JIPDEC (Japan Institute for Promotion of Digital Economy and Community) is available for evaluation and certification of ISMS by a third party. In order to acquire ISMS certification, the application documents must be prepared and submitted to an organization (i.e., an ISMS certification body or registration body) accredited by JIPDEC. The ISMS certification body evaluates the ISMS of certification applicants by using ISO/IEC 27001 (JIS Q 27001) control objectives and controls as criteria.

[Control objectives in ISO/IEC 27001 (JIS Q 27001)]

1. Security policy
   Fundamental information security policy
2. Organization of information security
   Internal organization, external parties
3. Asset management
   Responsibility for assets, classification of information
4. Human resource security
   Prior to employment; during employment; termination or change of employment
5. Physical and environmental security
   Secure areas, security of equipment
6. Communications and operations management

Operational procedures and responsibilities, third party service delivery management, system planning and acceptance, protection against malicious code and mobile code, back-up, network security management, media handling, exchange of information, electronic commerce services, monitoring

7. Access control

   Business requirements of access control, user access management, user responsibilities, network access control, operating system access control, Application and information access control, mobile computing and teleworking

8. Information systems acquisition, development and maintenance

   Security requirements of information systems, correct processing in applications, cryptographic controls, security of system files, security in development and support processes, technical vulnerability management

9. Information security incident management

   Reporting information security events and weaknesses, management of information security incidents and improvements

10. Business continuity management

    Information security aspects of business continuity management

11. Compliance

    Compliance with legal requirements; compliance with security policies and standards, and technical compliance; information system audit considerations

1-3-2 Risk Management

ISO 31000:2009 defines risk management as "coordinated activities to direct and control an organization with regard to risk."

Risk is defined as "the effect of uncertainties on objectives" in ISO 31000:2009. Here, an effect is a positive or negative deviation from what is expected. As an example, companies perform business activities to obtain targeted profits through a variety of capital investments, such as investment in land or stocks, or development of new products. A certain type of risk makes more profits than expected, or conversely, causes losses. (Such type of risk that occurs under the control of the managing entity is called a speculative risk). In contrast, there is also another type of risk such as natural disaster, man-made disaster, and theft that result only in negative effect. (The type of risk that occurs outside of the control of the managing entity is called a pure risk).

Risk management determines and manages organizational responses to these risks (especially speculative risks) in advance. Risk management is also implemented as part of ISMS.

[Risk management procedure]

(1) Confirmation of the organization’s status

Identify the information assets that are subject to risk analysis, and classify those assets in consideration of the importance of each asset from aspects of confidentiality, integrity, and availability. On the basis of the results, determine criteria (i.e., the required information security standards) for protection of information assets.

(2) Implementation of risk assessment

1) Risk identification

Identify risks on the basis of threats to information assets, vulnerabilities, etc.

2) Risk analysis

Analyze the frequency of occurrence of risks, the scale of impacts (damage, losses) made when the risks are exposed, or such other factor. Risk analysis focuses on perils (i.e., causes of loss) and hazards (i.e., dangerous conditions). Perils are factors that lead to risk, but no risk is likely to occur so readily without any hazards. As an example, even in the event of an earthquake (a peril), a building will not collapse readily if it is not in deteriorated condition (a hazard). (Threats can be thought of as perils, and vulnerabilities as hazards). It is also necessary to be cautious of moral hazards that are conditions where the sense of danger is decreased due to compensations, such as insurance against risks, and as a result, risks are increased.

3) Risk evaluation

On the basis of the results of risk analysis, evaluate whether each risk is acceptable or allowable.

(3) Treatment for risk

Taking into account both an evaluated risk and the required level of information security, determine and implement treatment measures for that risk.

(1) Types of risks

Risk identification distinguishes risks for each information asset. Each targeted information asset has the different types of risks, such as failure, breakage, or theft for hardware and other physical assets, and errors or malfunctions for software assets, so it is necessary to check for missing assets.

In addition, risk analysis may classify risks according to the types of losses caused by the risks. Losses caused by risks include the following types. Note that risk analysis targets not only pure risks that cause only losses but also speculative risks that can cause both profits and losses.

- Property loss
  Loss incurred due to loss of property or decline in the value of property
- Responsibility loss
  Loss incurred due to compensation, penalties, etc. paid for liabilities borne
- Net operating income loss
  Loss incurred due to reduced income caused by sales opportunity loss, etc.
- Human cost
  Loss incurred due to human resources or due to decline in human capacity

(2) Measures against risks

Measures to be considered for implementation as risk treatment include the following types.

Risk measure name		Content
Risk control		Prevents the occurrence of risk and reduces loss.
	Risk avoidance	Ceases activities or the use of assets, or makes substitutes.
	Risk prevention	Makes improvements to vulnerabilities, and decreases the frequency of occurrence of threats.
	Risk isolation	Isolates assets and reduces the effect of risks.
	Risk concentration	Concentrates the sources of risks, and performs centralized management.
	Risk transfer	Transfer risks through means such as agreements with rental businesses.
	Risk optimization	Makes risks acceptable through risk isolation or other means.
Risk finance		Conducts financing to cover damages borne by the exposure of risks.
	Risk retention	While retaining risks, prepares for losses through operating expenses or reserve funds.
	Risk transfer	Purchases insurance to share losses with other companies at the occurrence of risks.

Measures against risks are to be selected with consideration of cost-effectiveness (i.e., the balance between the values (or incurred losses)) of information assets and the costs of the measures. For that reason, since residual risk may be exposed after risk treatment, it is necessary to fully investigate the status of damages from the risk and confirm that there is no problem.

Moreover, it is also necessary to determine the priority of risk treatment in preparation for the simultaneous occurrence of multiple risks.

1-4 Information Security Agencies and Evaluation Criteria

Before ending the Overview of Information Security, this subsection discusses agencies related to information security and typical information security evaluation criteria.

1-4-1 Information Security Agencies

- CSIRT (Computer Security Incident Response Team)
  This is a general name for organizations that collect and monitor information pertaining to security incidents, and investigate causes and the scope of effects in the event of problems.
- NISC (National Information Security Center)
  This is an information security center established in the Japanese Cabinet Secretariat to perform integrated and efficient execution of Japan's information security policies.
- IPA Security Center
  This is an organization within IPA (Information-technology Promotion Agency, Japan) that cooperates with related institutions to perform information collection and analysis not easily performed by private parties, and generalizes the knowledge.
- CRYPTREC (CRYPTography Research and Evaluation Committees)
  This is a project and an institution that evaluate and monitor the security characteristics of ciphers recommended for digital government, and investigate and consider appropriate implementation methods and operational methods for cryptography.
- JPCERT/CC (JaPan Computer Emergency Response Team / Coordination Center)
  This is an incorporated association that collects and communicates information concerning security. It also plays a role as a coordinating body for the Information Security Early Warning Partnership.

1-4-2 Information Security Evaluation Criteria

- Common Criteria (ISO/IEC 15408)
  This is a standard for evaluation criteria disclosed by certification bodies, in the JISEC (Japan Information technology Security Evaluation and Certification scheme) operated by IPA (Information-technology Promotion Agency, Japan). It regulates security functional requirements and security assurance requirements, and serves as criteria for EAL (Evaluation Assurance Level).
- JCMVP (Japan Cryptographic Module Validation Program)
  This is a set of evaluation criteria and an operational procedure to certify that cryptographic modules, implementing cryptography, digital signatures, and such other functions, appropriately protect sensitive information contained within.
- PCIDSS (Payment Card Industry Data Security Standard)
  This is security criteria (i.e., certification evaluation criteria) for the protection of credit card information and transaction information. PCIDSS also defines the implementation of penetration testing, the tamper resistance of cards, etc.

2 Information Security Measures

Information security measures must be implemented comprehensively, so as to include not only information systems but also the environments surrounding people. An ISMS addresses three aspects: human security, technical security, and physical security from the perspective of information security measures.

2-1 Human Security Measures

Human security is security concerning human procedures, management, and operational rules and has an objective to prevent accidents and incidents such as security breaches by concerned parties.

With respect to the organization, management and monitoring are performed by appointing a CISO (Chief Information Security Officer), an information officer of each division or section, and an information system administrator, all of whom own authority and responsibility for information security. On the other hand, with respect to the organization's personnel, management and monitoring are performed by formulating a company regulation that includes the following items, in the form of information security policy.

- Screening at the time of employment, dispatch, or outsourcing contract of a staff member
- Non-disclosure (or confidentiality) agreement
- Information security education/training
- Handling/contact in the event of a security accident or an incident
- Disciplinary process for security breach
- Handling of information systems
- Account management / password management

In the PDCA cycle of human security, information security policy is established at the ISMS planning (Plan) stage, and security education and training are implemented at the execution (Do) stage. Furthermore, the security compliance status of personnel is checked through log management and monitoring at the inspection (Check) stage. Any deficiencies or improprieties are handled and corrected at the Act stage.

In human security measures, the greatest importance should be placed on information leakage by concerned parties. Information leakage due to inattention of concerned parties is difficult to completely prevent through agreements, rules, or information security education. As a measure against information leakage, unnecessary information disclosure should be avoided under the “need-to-know” principle. For example, appropriate access permissions should be set or important documents should be kept in a locked location.

Such activities regarding information leakage measures are also important in acquiring the Privacy Mark (P Mark). The Privacy Mark system confers the mark on private or other businesses that have prepared an appropriate protection system for the handling of personal information.

2-2 Technical Security Measures

Technical security is security that utilizes hardware, software, networks, and other technologies. The following are types of technical security measures and related techniques (Details of implementation technology are discussed in “2-4 Security Implementation Technology”).

- Anti-cracking measure

  It is difficult to prevent cracking only through a human security measure (e.g., a punitive regulation) that is aimed at a cracker. For that reason, a measure against unauthorized access is implemented to prevent unauthorized intrusion into another person’s PC, and a measure against information leakage such as cryptographic processing is implemented to prevent peeping of data by others.

- Measure against malware / measure against computer virus

  This is a technical measure for the prevention and detection of infection, prevention of the spread of damage, and restoration from damage caused by malware (i.e., computer viruses). This measure often uses security software that combines multiple security measure functions, such as antivirus measures or anti-spyware measures. Since an infection is often passed via networks by means of e-mail, an attachment file. etc., this measure is effective when used in conjunction with software that achieves network security.

  - Antivirus software (vaccine software)

    This is software that performs detection or elimination of computer viruses. The following are two typical methods of computer virus detection.

    - Pattern matching method

      This is a method that creates a database (a pattern file or a definition file) of the characteristic portions of viruses in the form of “signature code” (i.e., patterns), and performs a matching check between the database and a target program code. Since this method is unable to detect viruses that have not been registered, it is necessary to always update the pattern files to the latest versions.

    - Rule-based method

      This is a method that detects viruses by analyzing program behavior on the basis of established rules. This method includes the heuristic method that statically analyzes source code obtained by means such as disassembly of binary code, and the behavior method that runs programs to detect (i.e., dynamically analyze) dangerous behavior that indicates a virus.

Initial measures (e.g., disconnection from networks, contact with administrators) taken in response to a virus infection are defined within information security policy and are implemented as human security measures. The person initially detecting a virus should, in principle, not perform operations such as elimination of the virus or initialization of memory. This is because doing so disallows investigation and analysis of the type of virus, the infection path, the status of damage, and other information.

- Updating

This is a measure that is provided by a manufacturer or a software vendor to remove vulnerability from an operating system or an application, through an update program (patch program) which is aimed at defects in software security. This can also be effective in preventing the newly discovered malware or infection by computer viruses. It should be noted that while it is recommended to use the latest updates, OS updating may have impacts on the operation of other programs. This should be confirmed in advance.

- Measure against spam

Spam (i.e., spam e-mail, also called junk e-mail) is an advertisement message, a chain message, or other e-mail that is sent to an unspecified number of recipients. Measures against spam include denial of receiving spam, and avoidance of being used as a stepping stone for unauthorized relaying of spam. When spam is received, the optimal measure is to delete the spam without taking any other action, such as opening or replying to the spam.

  - Blacklist / whitelist

  This is a method that uses a blacklist of e-mail addresses from which receipt is rejected, and a whitelist of e-mail addresses from which receipt is accepted.

  - SPF (Sender Policy Framework)

  This is a method for sender domain authentication that manages an IP address list of proper mail servers authorized to send e-mail from a given domain. It enables automated rejection of e-mail sent from unrelated mail servers. It is an extended specification of SMTP, and is defined as RFC 4408.

  - OP25B (Outbound Port 25 Blocking)

  This is a method that is used by an ISP in order to prevent outbound communication from its internal networks via TCP port 25 (SMTP), through routers or such other devices at the boundary with external networks. When OP25B is active, SMTP communications attempting to connect through the ISP’s network to mail servers outside the ISP are all blocked, and it is possible to prevent unauthorized relaying of spam.

- Measure against mail header injection

  This is a measure that prevents mail header injection attacks which improperly rewrite e-mail recipient addresses found on websites, and use them as a stepping stone for unauthorized relay.

- DKIM (Domain Keys Identified Mail)

  This is a digital signature-based technique for source domain authentication, which checks whether received e-mail is from authorized senders and is not falsified. At the time of sending an e-mail message, it writes signature information, generated from a private key, into the header of outbound mail message, and at the time of receiving the e-mail message, verifies signatures by using a public key on the DNS server of the signing domain. This allows verification of the legitimacy of the source domain and body text of an e-mail message (i.e., verification that the message was not falsified during sending).

- Content filtering

This is a technique that restricts the viewing of content published on websites, through filtering to check for inappropriate keywords, etc. This is sometimes used to prohibit minors from viewing content containing harmful information, and is sometimes used for security purposes to prohibit access when the safety of content cannot be confirmed.

  - URL filtering

    This is a technique that prohibits the viewing of content at specified URLs. Many products have a prohibited-viewing URL list (i.e., filter) prepared from the start.

- Honey pot

This is a "decoy" server or device that is set up on the Internet for the purpose of investigating and analyzing methods and pathways of unauthorized intrusion, or the behavior of viruses. A honey pot is set up to disable external attacks from the honey pot (i.e., to prevent damage from spreading).

- Digital watermarking

This is a technique to embed data, which is imperceptible in normal viewing and playback, into documents, still images, videos, and other content. Since the information is displayed when special detection software is used to read the data, unauthorized copying or data falsification can be detected.

- Personal Digital Assistance (PDA) security

PDA contains personal data, like a telephone directory, and confidential data, so security measures for such a device are also necessary. PDA is portable, so it is important to make special preparations against loss and theft.

- Cell phone / smartphone

  A cell phone and a smartphone commonly have a feature to lock the device after a set period of non-use, and such a feature should be used. Although a password method is commonly used to unlock the devices, some models use fingerprint authentication or face authentication. When the device is lost or stolen, the features can also be used by which a key operation on the device can be remotely disabled, or the device itself is initialized. Furthermore, smartphones lent by companies are sometimes centrally managed according to a security policy by using MDM (Mobile Device Management).

- Tablet device

  A tablet device requires the same sort of security measures as a notebook PC. A computer viruses that targets a tablet device begins to appear, which means that antivirus software must be installed. In addition, data should be encrypted or otherwise protected as a measure against loss or theft.

- Digital forensics

  Forensics has meanings of medical jurisprudence, criminal identification, and scientific investigation, and here refers to digital criminal identification. It is a general name for the technique that collects and analyzes devices, data, and electronic records required for investigation of cause in legal disputes and computer crimes such as unauthorized access and leakage of information, to clarify legal grounds for action.

2-3 Physical Security Measures

Physical security is security that pertains to environmental management including facilities and equipment, and document management including recording media. While physical security measures enhance the S (Security) of RASIS, the adoption of RAS technology (e.g., technology to control the occurrence of failure) to enhance RAS (Reliability, Availability, Serviceability) can also be thought of as part of physical security.

Typical types of physical security measures and related technologies include the following.

- Zoning (i.e., the setting of security zones for facilities and equipment)

  Zoning sets areas that are to be managed as security zones, such as locations of installed hardware, storage locations for software, and storage locations for confidential documents and recording media. Earthquake- and fire-resistant equipment is adopted for security zones, and preparations are made for disasters and other physical threats.

- Entrance and exit control

  This is the management of security zone entrance and exit, and management of visitors from outside. Entry is controlled through means such as ID cards, with the names of entrants, dates of entry, purpose of entry, and other information recorded.

- Locking management

  Security zones are locked so as not to allow someone to enter and exit such zones without permission.

- Monitoring camera

  Persons entering and exiting zones can be recorded by installed cameras.

- Remote backup

  This is a method of storing backups in a remote location, in preparation for disasters and such others.

- Security cable

  This is a device for connecting equipment to a desk leg or secure point on fixture, to prevent theft.

- Disk encryption

  This is a method for encrypting information on recording media to prevent information leakage.

- Authentication device

  This is a device for user authentication used in entrance and exit control. Depending on the usage environment, the following points of caution should be noted.

  - When large amounts of electric power are required, it is advised to use a contact-type IC card to which electric power is directly supplied and is not advised to use a non-contact type that generates electric power from electromagnetic waves.
  - Since an optical type of device for biometric authentication may be affected by lighting, it is advised to compare an optical type with a capacitive type prior to installation.

- USB key

  This is a user authentication device on which unique authentication information is recorded, to enable user authentication by inserting the device into equipment. This is used in client authentication that is based on IEEE 802.1X used with LANs, or such other authentication and there is no standard for the capacity of built-in memory or such other specification.

- Disposition

  Physical destruction of media or overwriting of specified bit sequences prevents information leakage.

2-4 Security Implementation Technology

Security implementation technology refers to the technological measures implemented for

each target of attacks (threats), such as networks and databases.
It is important to use the security technology that is optimal against each of these attacks.

2-4-1 Secure Protocols

Secure protocols are protocols to prevent eavesdropping of communication data or unauthorized connections. A variety of secure protocols are used in TCP/IP networks.

- IPsec (Security Architecture for Internet Protocol)
  This is a secure protocol that is a standard specification for IPv6. Since IPsec performs packet cryptography and authentication in the Internet layer, it enhances the confidentiality and validity of data.
- SSL (Secure Sockets Layer)
  This is a secure protocol that is used between the application layer and the TCP layer, and performs authentication (digital signature) and encryption of communication content (session key cryptography) between client and server. TLS (Transport Layer Security) 1.0 was drafted by the IETF as RFC 2246 that was standardized on the basis of SSL.

Original protocol	Secure protocols combined with SSL
MIME	S/MIME (Secure MIME)
HTTP	HTTPS (HTTP over SSL/TLS)
FTP	FTPS (FTP over SSL/TLS)
SMTP	SMTP over SSL/TLS
POP3	POP3 over SSL/TLS

  - SSL accelerator
    This is hardware that reduces the cryptographic processing load on servers to increase speed.
- SSH (Secure SHell)
  This is a protocol that performs encryption of passwords and data at the TCP layer and application layer, and enhances the security of a UNIX-like command (e.g., rsh).
- PGP (Pretty Good Privacy)
  This is an individual-oriented secure protocol that encrypts the body text of e-mail by using a hybrid method (common key: IDEA; public key: RSA).
- APOP (Authenticated POP)
  This is a protocol that uses the POP with added security functions and encrypts passwords during login to mail servers. However, it does not encrypt the body text of e-mail.
- SET (Secure Electronic Transactions)

This is a credit card settlement protocol that uses cryptography and digital signatures. It restricts information that can be looked up at the retail store and credit card company, offering high confidentiality.

The protocols used for SPF and DKIM, described in “2-2 Technical Security Measures,” are called authentication protocols. Authentication protocols can be called a type of secure protocol used to prevent unauthorized use of services or unauthorized connections caused by or resulting from spoofing.

- SMTP-AUTH

  This is a protocol by which authentication of users is performed by the mail server during transmission of e-mail. SMTP does not have a user authentication mechanism, which creates a problem in the increasing unauthorized use of mail servers for sending spam e-mail. SMTP-AUTH authenticates users by specifying user IDs and passwords in advance.
- OAuth

  This is an authentication protocol that performs handover of user privileges, with user consent, between services (i.e., applications) that have an already-established relationship of trust. Specifically, it accesses resources on Web servers on behalf of users, and enables a service to perform acquisition, addition, updating, and deletion of information that is managed by another service. With OAuth, a user can transfer access privileges to a service without handing over a password, and can set the scope of applicability and the period of validity.
- DNSSEC (DNS SECurity Extensions)

  This is an extended specification that improves the security of DNS. While a normal DNS server is unable to authenticate communicating parties, DNSSEC is able to confirm the creator and integrity of data by using digital signatures. The responding DNS server signs with a private key, and the recipient validates with a public key.
- EAP (PPP Extensible Authentication Protocol)

  This is a protocol that is used to authenticate remote access users. Authentication methods using EAP, which adds authentication functions to PPP, include the following.

  - EAP-TLS (EAP Transport Layer Security)

    This uses digital certificates on both server and client. It is defined by the IETF as RFC 2716.
  - PEAP (Protected EAP)

    This issues digital certificates on the server side, and authenticates on the client side by user ID and password. It was developed by three companies: Microsoft, Cisco Systems, and RSA Security.

In contrast to authentication protocols aimed at user authentication, the anonymous FTP protocol enables provision of service to unspecified users. This protocol enables anyone to use an FTP service by entering “anonymous” as a user ID. While it is convenient as a means of reducing workload such as registering and administering user IDs, it is easily targeted by crackers and requires that sufficient security measures be taken.

2-4-2 Network Security

Network security is a general name for security against attacks using networks. Network access control to prevent intrusion (i.e., unauthorized access) into internal networks is important in network security.

(1) Firewall

Firewalls are mechanisms that are installed at the boundary between internal networks (e.g., LANs) and other networks in order to protect internal networks from unauthorized access.
Two typical firewall techniques are as follows:

- Packet filtering

  This is a technique that permits or denies the passing of packets according to configuration rules of delivery information, such as the source IP address/port number and destination IP address/port number in the packets. Control is primarily based on information included in headers of IP, TCP, UDP, ICMP, and such other protocol, to restrict unnecessary communication from outside.
- Application gateway

  This is a gateway that is deployed at the boundary of networks, and controls (i.e., permits or denies) communications between internal and external networks by means of a program (i.e., proxy program) that relays an application. Although a separate relay program must be prepared for each type of application, it can control application commands and data at a detailed level, and thereby can help achieve a high level of security.

A network segment isolated by a firewall from other internal LAN segments is called a DMZ (DeMilitarized Zone). If a server to be made publicly available is installed in a DMZ, unauthorized access from the outside can be blocked by a firewall. Moreover, even if the server is attacked, damage to internal segments can be prevented. However, if sufficient measures are not taken on mail servers and other servers, the servers may be used as stepping stones for spam e-mail.

A reverse proxy also performs the same type of role as a firewall. A reverse proxy receives requests from a client in place of a specified server and relays the request to the specified server. Since this flow is reversed from that of a regular proxy server, which acts as a proxy to relay access from the inside to the outside, the server is called a reverse proxy. By embedding the functions to scan the content of packets and URLs during relay, access to a specified server can be blocked. (This function corresponds to an application gateway). However, a reverse proxy is often used for the purpose of reducing the load on servers by acting as a proxy to respond to requests coming from large numbers of clients, or for the purpose of speeding response by storing content in cache.

(2) IDS (Intrusion Detection System)

IDS (Intrusion Detection System) refers to a system that detects intrusion into network-connected equipment and such others, and performs collection and analysis of logs. It detects patterns corresponding to registered intrusion patterns, or those differing from access patterns in normal operation.

- Host-based IDS
  This is a host-based IDS that monitors the access status of specified servers or clients, and detects intrusion.
- Network-based IDS
  This is a network-based IDS that monitors packets passing through a network, and detects intrusion.

An IPS (Intrusion Protection System) sometimes have an extended function of IDS that can prevent any unauthorized intrusion by blocking the connection of an unauthorized intrusion when detected

(3) Quarantine network

A quarantine network is a mechanism to confirm the security of PCs connected to an internal network. The PCs is temporarily connected to an independent network (the quarantine network) for check, and if they present a problem with the network, measures are taken. Quarantine networks are generally used together with authentication servers, to confirm security through the flow “authentication → quarantine → connection.” The mechanism is also used to ensure security under BYOD (Bring Your Own Device) whereby employees are allowed to use personally-owned information devices for work.

- Authentication server

  This is a server that is dedicated to performing authentication processing. There are various types such as RADIUS (Remote Authentication Dial-In User Service) servers that unify the management of system-wide authentication. The use of the authentication server enables single sign-on that allows users to access multiple systems (i.e., services) by logging on just once (i.e., one-time authentication).

(4) Call back

Call back is a user verification technique used for connections to internal networks via public lines such as regular telephone lines. Under this method of user verification, during dial-up access to a RAS (Remote Access Service) server via a public line, the RAS server cuts the outgoing call, identifies the user from a caller telephone number (or caller ID) registered with the RAS server, and calls back. However, as only the telephone or other communication device of the caller can be identified, unauthorized use of such a device by a third party cannot be detected. For that reason, the method is often used in combination with another user verification method, such as verification by user ID and password.

(5) Wireless LAN security

Since a wireless LAN allows easy connection to the LAN as long as the user is within an area where electromagnetic waves used for the wireless LAN reach, security measures to prevent unauthorized connection are important.

- ANY connection refusal function

  This is a function that refuses connection requests when the ESSID set for the access point and the ESSID of the device do not match (i.e., when the ESSID is set to “ANY” or is left blank).
- MAC address filtering function

  This is a function by which the MAC addresses of devices that are allowed to connect are registered with an access point, and connections from devices with unregistered MAC addresses are refused.
- Stealth function

  This is a function that conceals ESSIDs by stopping the beacon signals emitted regularly from access points.
- WEP (Wired Equivalent Privacy) / WPA (Wi-Fi Protected Access)

  This is an encryption method for wireless LANs. WEP is a method that performs encryption using a WEP password and SSID. WPA is an improved WEP that uses the encryption protocol TKIP which generates and renews keys at regular intervals. WPA2 is also available, which uses the new encryption protocol CCMP (sometimes labeled AES).

(6) Other forms of network security

- NAT / NAPT (IP masquerade)
  This is a function that converts private IP addresses to global IP addresses. Since private IP addresses are concealed, NAT and NAPT have some effect on security.
- VPN (Virtual Private Network)
  This is a service that can be used by multiple users as if each had a unique dedicated line. A VPN can aid in preventing eavesdropping, etc.
- Access log analysis
  This is a method of analyzing access logs to uncover traces of address scanning (an attack that repeats the ping command to find connectable IP addresses) and port scanning (an attack that attempts access while changing the port number to find services allowing intrusion). While it does not provide immediate results, it is relatively effective.
- UTM (Unified Threat Management)
  This is a method that integrates multiple differing security functions into a single hardware device and performs centralized network management.
- Penetration test
  This is a test that attempts actual intrusion to verify the efficacy of security measures.

2-4-3 Database Security

Database security is a general name for security against attacks on databases.
In general, it uses the security protection functions offered by DBMS. Security is further enhanced by concurrently implementing usage control of external media, detection of unauthorized access, or such other function.

Security protection functions	Protected content
Encryption	Encrypt the content that is stored in a database.
Setting of access privilege	Set up access privileges to a database.
Setting of password	Authenticate users with their user IDs and passwords.
Recording to log files	Record the status of use to detect unauthorized use.

2-4-4 Application Security

Application security is a general name for security against attacks that exploit vulnerabilities (i.e., security holes) in application software. Application security includes secure programming that implements security functions in the process of programming. As an example of such functions, there is a function that places restrictions on data written out to the buffer area of a program, in order to increase protection against "buffer overflow attacks" that improperly write data in excess of its buffer size.

- WAF (Web Application Firewall)
  This is a device or software that blocks attacks against vulnerabilities created by Web application security holes, etc.
- Security measures for Web systems
  Measures against attacks using Web systems include the following.
  - Measures against SQL injection: Character string conversion through escape processing
  - Measures against XSS: Sanitizing to make dangerous scripts harmless
  - Measures against CSRF: Re-authentication that requests a repeat of password entry before execution

2-4-5 Secure OS

Secure OS refers to an OS developed under the concept of least privileges and the access mechanism called mandatory access control, in order to implement sufficient security functions.

- MAC (Mandatory Access Control)
  This is a mechanism where a system administrator set an access right and the access right is enforced.
- Least privilege
  This is a mechanism where a finely-set privilege is given as needed.

Chapter 6 Exercises

Q1

According to ISO/IEC 27001 (JIS Q 27001), which of the following is the definition of availability in information security?

a) Ensuring that information and a processing method are accurate and complete
b) Ensuring that a user of an information system is the correctly authorized user
c) Ensuring that information is not disclosed to third parties
d) Ensuring that a user can access information assets at the required time

Q2

Which of the following is the action that corresponds to social engineering?

a) Performing an attack that exploits the security hole in an OS
b) Externally controlling a virus-infected computer
c) Intruding into a computer room by using a PIN that is analyzed by a program
d) Impersonating an authorized person to request the password via telephone

Q3

When there exists a vulnerability that enables scripts to be embedded in a Web application, which of the following is an attack that exploits this vulnerability to execute the unauthorized script on a user's browser of the Web application?

a) DoS attack
b) SQL injection
c) Cross Site Scripting
d) Phishing

Q4

Which of the following is an effect of e-mail encryption?

a) The loss of an encryption key can be prevented.
b) The leakage of e-mail content can be prevented.
c) The sending log of the mail server can be protected from falsification.
d) The attack that obstructs mail service can be prevented.

Q5

When a retail store receives an order (i.e., a message) from a customer via a network, the retail store uses public key cryptography to keep the content of the order from being seen by third parties. Which of the following is the key that the customer of this retail store uses for encryption?

a) Public key of the customer
b) Private key of the customer
c) Public key of the retail store
d) Private key of the retail store

Q6

Which of the following is an appropriate description of cryptography?

a) Common key cryptography is safe for communication with multiple parties, even when the same encryption key is used.
b) Public key cryptography requires that the encryption key be privately distributed to the communicating party.
c) Public key cryptography offers simpler and faster decryption than common key cryptography does.
d) A method is made practical by which at the start of communication a common key is encrypted by public key cryptography and sent to the other party, and encryption of data is performed by common key cryptography.

Q7

When an internal user of a company forgets the password, which of the following is an appropriate action a security administrator should take after the identity of the user is verified?

a) Decrypting the encrypted password that is managed by the security administrator, and informing the user by e-mail
b) Decrypting the encrypted password that is managed by the security administrator, and informing the user by telephone
c) Converting the password that is managed on the security administrator’s own PC into a hash value, and informing the user by using a classified internal document
d) Resetting the password, and having the user set a new password

Q8

Which of the following is biometric authentication that uses information which can be obtained from the human eye?

a) Iris authentication
b) Fingerprint authentication
c) Voice authentication
d) Palm authentication

Q9

Which of the following is a purpose of use of a message digest in message authentication?

a) To confirm that the message is not falsified
b) To confirm the encryption method of the message
c) To confirm an overview of the message
d) To ensure the confidentiality of the message

Q10

Which of the following is an objective of a software developer in attaching a digital signature to software when software is released on the Internet?

a) To assure that the software developer bears responsibility for maintenance
b) To restrict use of the software to specified users
c) To show that the software copyright lies with the developer
d) To assure that the content of the software is not changed illegally

Q11

Which of the following is an appropriate description of information security policy?

a) A company's security policy is for the purpose of defining the content that should be set within each security system, and therefore, its content differs according to the security-related product to be installed.
b) A company's security policy consists of behavior and judgment criteria to be followed, and does not include stance and direction concerning the security activities.
c) A company's top management should externally disclose information system vulnerabilities that are factors behind the development of a security policy.
d) In order to achieve the targeted security level, it is necessary to clearly indicate the organization's thinking concerning behavior and judgment to be followed.

Q12

Which of the following is performed in the Plan phase of a PDCA model that is applied to any ISMS process?

a) Management of operational status
b) Implementation of improvement measures
c) Review of implementation status
d) Risk assessment of information assets

Which of the following is an appropriate description of risk assessment?

a) Since it requires too much time and expense to address all conceivable risks, an organization should forecast the loss values and frequency of occurrence, and rank risks in order of size.

b) Until all measures to risks that are evaluated through risk analyses are completed, an organization should avoid implementing repeated risk analyses.

c) Since risk analysis is for the purpose of preventing future losses, an organization should avoid referencing data that is collected from a similar past project.

d) Since the purpose of risk analysis is to determine the value of losses resulting from the materialization of risk, an organization should consider measures on *prioritized* risks with the highest loss value.

Q14

Which of the following is an appropriate description of JPCERT/CC?

a) It is a project to investigate appropriate implementation methods and operational methods for cryptography.

b) It is a coordinating body for the Information Security Early Warning Partnership.

c) It is a security center under the jurisdiction of the Information-technology Promotion Agency, Japan.

d) It is an information security center that is established in the Cabinet Secretariat of Japan.

Q15

Which of the following is an appropriate description concerning antivirus software?

a) A signature file for antivirus software is a database that contains the first 16 bytes or 32 bytes of the code of each virus.

b) Virus detection using the signature files of antivirus software is an effective method for detecting known viruses and identifying virus names.

c) If the size of a file that is infected by a virus is the same as the size before the infection, the file can be restored to its pre-infection state by removing the virus.

d) In the method of detecting a virus by identifying unauthorized behavior, the name of the virus can be identified from the behavior characteristics.

Q16

Which of the following is an appropriate explanation of OP25B?

a) Setting up a server on the Internet which appears to have vulnerabilities, and collecting information about a method and pathway of unauthorized intrusion

b) Authenticating the source domain of the e-mail by recording signature information in e-mail headers

c) Restricting access to websites from the internal network by filtering content

d) Performing port number-based filtering of e-mail which is sent from the internal network to an external mail server

Q17

Which of the following is a secure protocol that combines an authentication function between a client and a server with an encryption function for communication data?

a) APOP   b) EAP   c) OAuth   d) SSL

Q18

Which of the following is an appropriate description of the role of a reverse proxy?

a) It sends an access request, in place of a client, to a server.

b) It receives an access request, in place of a server, from a client.

c) It ensures the security of a PC that connects to a network.

d) It detects intrusion into a network.

Q19

Which of the following is an appropriate description of WPA?

a) It is software that blocks an attack against vulnerabilities in the Web application.

b) It is a method for one-to-one conversion of an internal address to an external address.

c) It is a method that integrates and centrally manages multiple different security functions.

d) It is an encryption method for a wireless LAN