Guideline on Protection of Personal Information in Telecommunications Business
- Efforts with Security Control Measures to Prevent Personal Information Leakage -

1. Main Points of Revised Guideline

The Ministry of Internal Affairs and Communications (MIC) revised the "Guideline on Protection of Personal Information in Telecommunications Business" (hereunder called the "Guideline") in July 2010 including the following two points:

① Specify appropriate security control measures when storing personal information on mobile PCs, etc. and matters that require attention when doing so in the explanations of the Guideline.

② Procedures for incidents of information leakage can be simplified if appropriate technical protection measures, etc. have been taken to prevent secondary damage being caused to the person concerned.

2. Simplification of Procedures for Incidents of Information Leakage

When personal information has been leaked, the Guideline requires business operators to : [1] promptly notify the relevant persons of the facts involved from the point of view of preventing secondary damage, unless their contact information is unavailable, [2] release as much as possible of the facts, etc. involved from the point of view of preventing secondary damage and similar incidents from taking place, and [3] promptly report the facts involved in any such case to MIC.

Regarding these rules, the revised Guideline provides for the notification to the person of concern and announcement being no longer necessary and with the report to MIC only necessary within a given period of time rather than as promptly as previously, if (i) the personal information is jeopardized as a result of a notebook-type personal computer, etc. being lost or stolen and (ii) appropriate technical protection measures, etc. are taken to prevent any secondary damage being caused. In addition to notebook-type computers any device for which "appropriate technical protection measures" are also applicable, including mobile phones, telecommunications devices such as PDAs, and external storage devices such as USB memory, etc. that are generally used outside facilities.

For the content of the concrete measures that are accepted as being appropriate technical protection measures refer to the respective items described in 3 (3.Appropriate Security Control Measures).

<Reference 1>

At present simplification of the procedures for incidents of information leakage is provided for in some of the telecommunication business guidelines. The government policy of "Information Security 2010", however, provides for that by from the point of view of preventing personal information leakages by business operators ideal incentives for business operators that

implement encryption of information, etc. being discussed by around June 2010 with consideration given to characteristics of respective business areas, including simplification of the procedures for incidents of information leakage if the appropriate technical protection measure was taken with in regard to the leaked information, etc., by facilitating the appropriate encryption of information, etc.

<Reference 2>

Section 1. Overview of the “Act on the Protection of Personal Information” in Japan

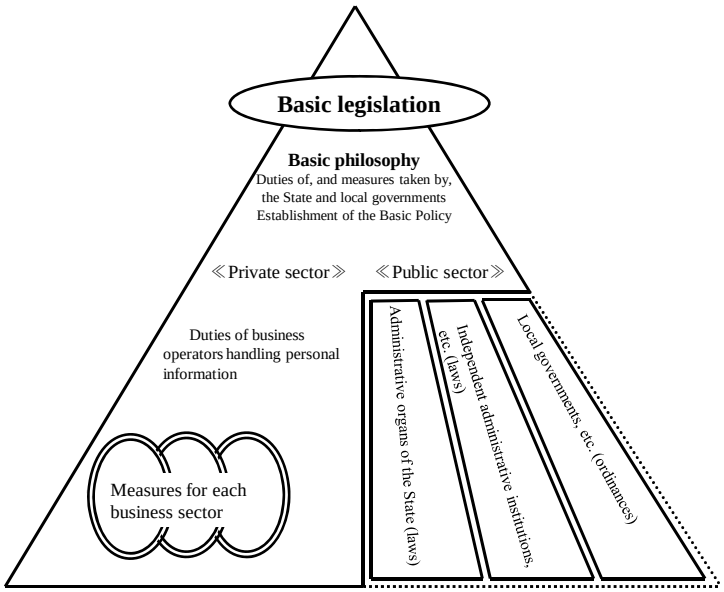
In response to the increased risk of infringement of the rights and interests of individuals due to rapid advances made in information technology and international trend of enactments being made through legislation, the “Act on the Protection of Personal Information” was enacted in May 2003, and fully enforced in April 2005.

The “Act on the Protection of Personal Information” consists of six chapters.

Chapters 1 through 3 provide for “basic laws” common to both the government and the private sector. For example, the basic principle provides for “in view of the fact that personal information should be handled cautiously under the philosophy of respecting the personalities of individuals, proper handling of personal information shall be promoted” (Article 3 of the Act).

Chapters 4 through 6 provide for the “private sector”, or lower left part of the triangular diagram below, and impose obligations on certain business operators (entities handling personal information). In addition, guidelines are also individually formulated by the ministries and agencies responsible for providing guidance/supervision in respective business areas (competent ministers) according to their actual situation.

The lower right part of the triangular diagram, or the “public sector”, reveals that the “Act on the Protection of Personal Information Held by Administrative Organs”, which involves regulation of administrative organs of the State, the “Act on the Protection of Personal Information Held by Independent Administrative Agencies, etc.”, which involves regulation of independent administrative institutions, etc., and the “Personal Information Protection Ordinance”, which is formulated by respective local governments in regulating prefectural and municipal governments, etc., have all been enacted.



Section 2. Guideline on Protection of Personal Information in Telecommunications Business

The “Act on the Protection of Personal Information” that was enacted in 2003 provides for a competent minister system being adopted and for ministries and agencies taking any necessary measure, including the formulation of guidelines, etc., according to the actual situation in the respective business area. MIC responded to this by formulating the “Guideline on Protection of Personal Information in Telecommunications Business” in August 2004.

The Guideline aims to improve the accessibility of telecommunications services but at the same time protecting the rights and interests of users by providing for the basic matters that telecommunications carriers should observe in ensuring the appropriate handling of matters concerning the secrecy of communications and other personal information.

Chapter 1, the general provisions, clarifies the purpose, definitions, and provisions of the Telecommunications Business Act concerning the secrecy of communications, along with the relationship between the provisions of the Act on the Protection of Personal Information and the Guideline, etc. Chapter 2 provides common principles with the handling of personal information while chapter 3 outlines the provisions for the handling of the variety of information (communication history records and information on defaulting persons, etc.) that telecommunications carriers handle.

3. Appropriate Security Control Measures

(1) Overview

The accepted appropriate technical protection measures which can simplify the procedures for incident of information leakage are as follows.

I. Taking advanced encryption measures

Using an encryption algorithm included in the e-government recommended ciphers list or ISO/IEC 18033, automatically encrypt all areas that are available for storing personal information of storage media.

II. Managing encrypted information and encryption keys properly

The encrypted information and the decryption keys that can decrypt the encrypted information shall be properly managed by using method (a) or (b) below. The encryption measures, in addition, shall be implemented such that (in method (a)) the decryption keys are isolated from the encrypted information and (in method (b)) unauthorized person cannot illegally duplicate or re-create a deleted decryption key remotely.

(a) Encrypted information and their decryption keys shall be separated, using the following method A or B.

A. All decryption keys shall be separated from encrypted information and are configured such that, even for lost encrypted information, the decryption keys are placed under the management of authorized personnel.

B. Each decryption key shall be split into components that are saved at distributed locations, using a secret sharing scheme included in the public domain. In the scheme, it has been proven impossible to restore whole information from only part of distributed components, so if encrypted information is lost, the encrypted information cannot be decrypted using the decryption key components that are not separate from the lost encrypted information. The components are placed under the management of authorized personnel.

(b) Authorized personnel shall be able to remotely delete decryption keys and/or the encrypted information from storage media. They also shall be able to confirm that until the time that a decryption key or encrypted information is deleted, the key was not duplicated and none of the information was read or copied.

III. Technical protection measures (a) and (b) shall be implemented effectively against personal information leakage and other such problems (the evidence of implementing measuses (a) and (b) shall be able to proof by authorized personnel.)

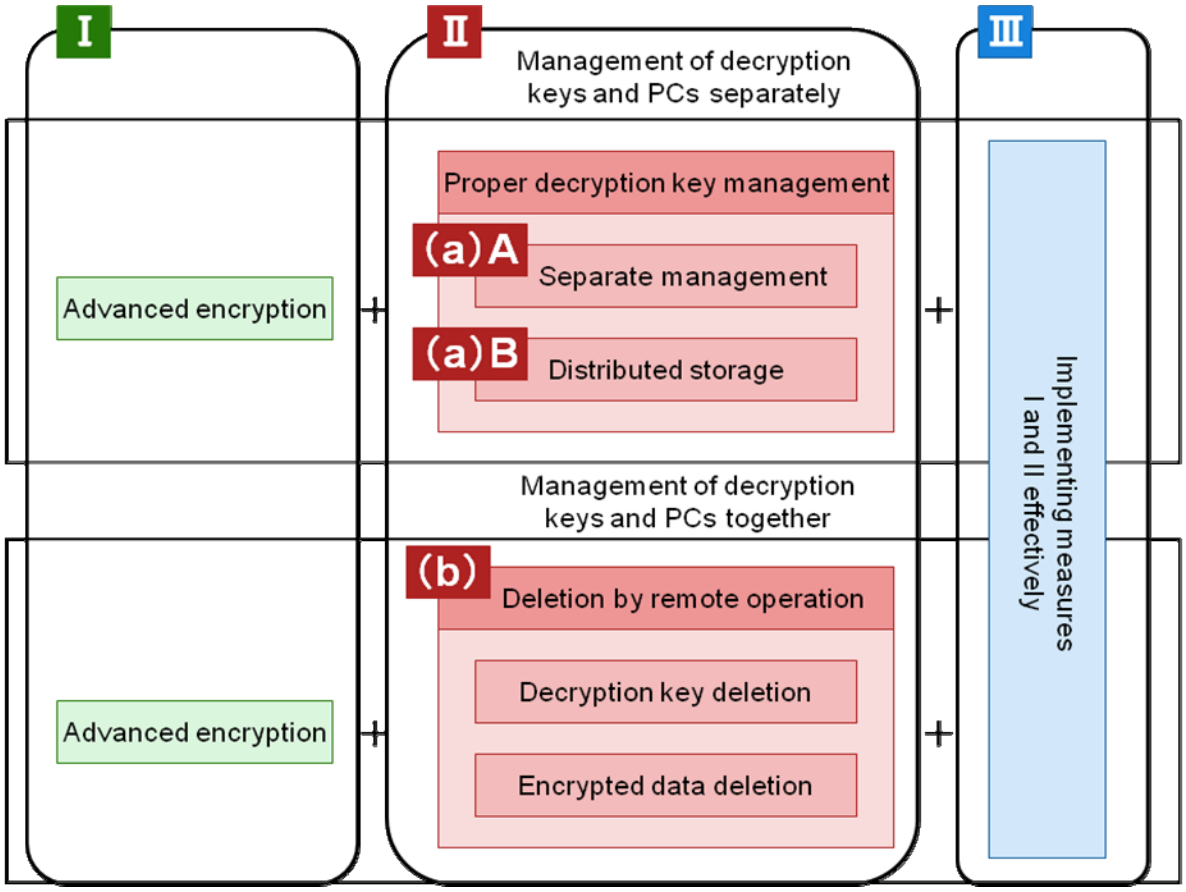


Figure 1　Outline of appropriate security control measures

Generally, any third party who acquires personal information encrypted with an advanced algorithm (encryption procedure) will have difficulty decrypting the information or taking similar action (I). However, even advanced encryption measures will fail to work effectively if passwords, keys, and other personal authentication information are inadequately managed. Therefore, proper key management is important (II). Since the measures in I and II need to actually work against personal information leakage, provision III is included. (For details of the measures in I through III, see “(2) Explanation of each provision.”)

Various technologies for personal authentication exist, including authentication with a password or other something else remembered, authentication with a physical device like an IC card, and authentication with fingerprints or other biometric information. However, no criteria have yet been established to assess the strength of security and there seem to be no existing effective means of confirming that personal authentication works properly in cases where personal information is lost. For these reasons, this review does not include these technologies in the provisions for appropriate technical protection measures. They will be reviewed again in future examinations of these guidelines.

Considering that the security of technology varies with time and that more secure technologies may emerge in the future, the appropriate technical protection measures will be

examined as necessary.

(2) Explanation of each provision

I. Taking advanced encryption measures (1) Using an encryption algorithm included in the e-government recommended ciphers list or ISO/IEC 18033, (3) automatically encrypt (2) all areas that are available for storing personal information on storage media.

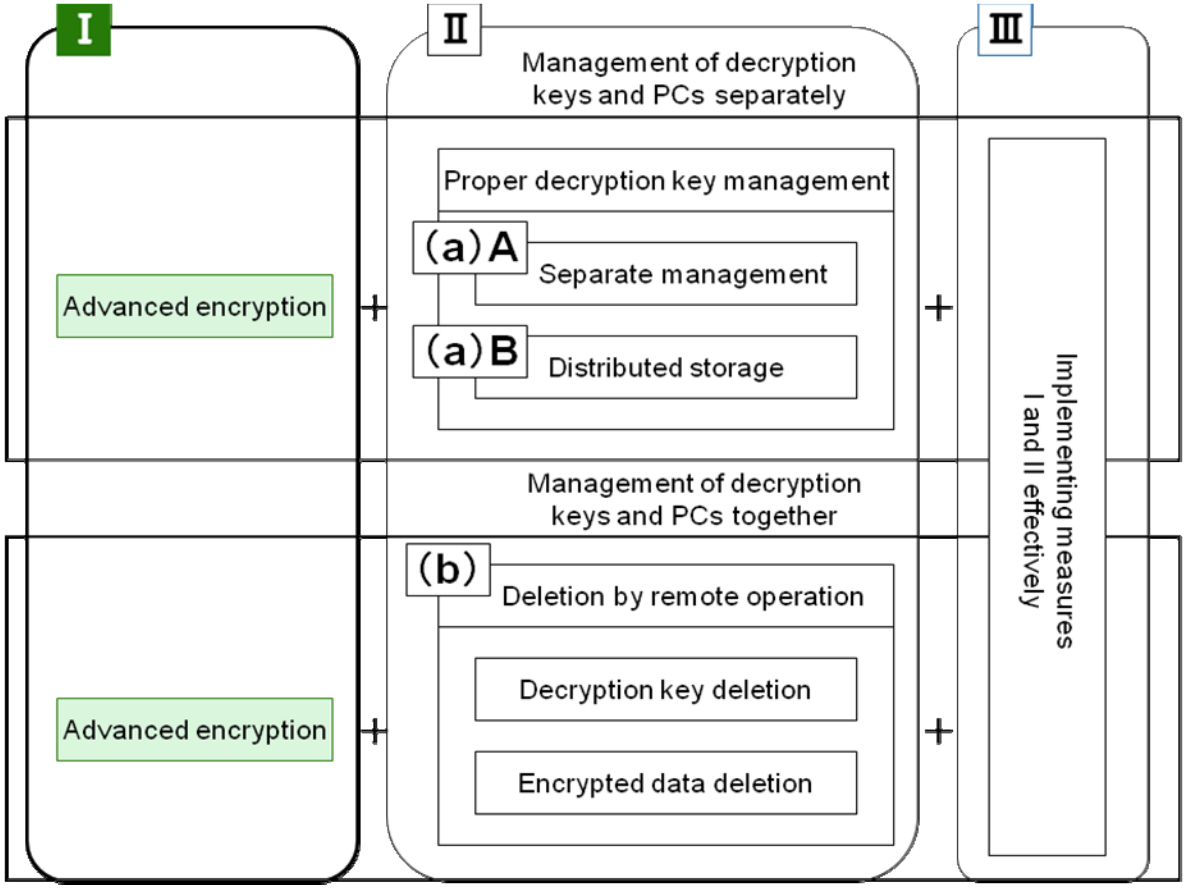


Figure 2 Outline of appropriate security control measures (I. Advanced encryption measures)

(Explanation)

Generally, any third party who acquires personal information encrypted with an advanced encryption algorithm will have difficulty decrypting the encrypted information or taking similar action.

(1) "An encryption algorithm included in the e-government recommended ciphers list or ISO/IEC 18033" means the following. Encryption algorithms include public-key ciphers used mainly for identity verification, symmetric key ciphers used mainly for data encryption, and hash functions used mainly for falsification detection. Since the concern here is to encrypt large volumes of information stored on hard drives, symmetric key ciphers will be the encryption algorithms substantially used (although public-key ciphers and hash

functions will also be used where applicable).
The following table lists expiration dates and other conditions specified for the respective algorithms. Therefore, those who will actually utilize the listed algorithms need to read the source documents carefully.

Table 1 Encryption algorithms included in the e-government recommended ciphers list or ISO/IEC 18033

	e-Government recommended ciphers list (2003 version) (*1, *2)	ISO/IEC 18033 series (*4)
	Published by: Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry Originally developed by: CRYPTREC (*3)	International standard regulations Established by: ISO/IEC JTC 1/SC27 (*5)
Public-key ciphers		
Signature	RSA-PSS (1024-bit), RSASSA-PKCS1-V1_5 (1024-bit), DSA (1024-bit), ECDSA (160-bit)	None (stipulated in ISO/IEC 9796-2, etc.)
Confidentiality	RSA-OAEP (1024-bit), RSAES-PKCS1-V1_5 (1024-bit)	RSA-KEM, RSA-OAEP, PSEC-KEM, ACE-KEM, HIME(R), ECIES-KEM
Key sharing	PSEC–KEM (160-bit), DH (1024-bit), ECDH (160-bit)	None (stipulated in ISO/IEC11770-3)
Symmetric key ciphers		
64-bit block ciphers	3-key TDES, MISTY1, Hierocrypt-L1, CIPHERUNICORN-E	TDES (3-key recommended), MISTY1, CAST-128
128-bit block ciphers	AES, Camellia, SC2000, CIPHERUNICRON-A, Hierocrypt-3	AES, Camellia. SEED
Stream ciphers	MUGI, MULTI-S01, RC4 (128-bit)	MUGI, MULTI-S01, SNOW 2.0
Hash functions		
	SHA-256, SHA-384, SHA-512, SHA-1, RIPEMD-160	None (stipulated in ISO/IEC 10118)

*1 The encryption technology conferences and other meetings jointly sponsored by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry publicly invited proposals on ciphers and rated them objectively. On February 20, 2003, the ministries determined and published a list of recommended

ciphers for e-government procurements (e-government recommended ciphers list).

*2 A review is underway to examine the list in preparation for the start of a new recommended encryption system in 2013. Instead of SHA-1, which is a 160-bit hash function, hash functions of 256 bits or longer should be selected if available when the new system for e-government is constructed. However, this does not apply to any hash functions specified for use under public-key encryption specifications. Also, once any encryption algorithm is found to be compromised, it should not be used and it should be immediately replaced with another algorithm that has not been compromised.

*3 CRYPTREC: Cryptography Research and Evaluation Committees, which is a secretariat (Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry, NICT, IPA)

*4 International encryption standards established and issued by ISO/IEC JTC 1SC 27 (IT Security Techniques), which is an organization for international standardization of information security rules. ISO/IEC 18033 is a four-part standard—Part 1: General; Part 2: Asymmetric ciphers; Part 3: Block ciphers; Part 4: Stream ciphers.

*5 ISO/IEC Joint Technical Committee 1/Subcommittee 27, “IT Security techniques”
ISO: International Organization for Standardization
IEC: International Electrotechnical Commission

(2) “All areas that may be available for storing personal information on storage media” means hard drive areas managed by the OS or user. (Generally, storage media refers to hard drives, CD-ROM, USB memory, etc. in PCs; here, it refers to hard drives in PCs.)
A full volume of a hard drive can be used as an area that may be available for storing personal information on storage media. (A hard drive consists of manageable units called volumes, and a full volume means an entire volume or all the areas of hard drive partitions). Depending on the PC specifications, however, a full volume contains some areas where personal information will never be recorded, such as an area used only by the hard drive manufacturer. These areas where no personal information is ever recorded are excluded from the encryption targets.
Since these guidelines focus on personal information, the areas concerned are described here as “area that available for storing personal information.” Generally, these areas store all kinds of information used by users.

[Examples of meeting requirements defined independently in provision I (encrypting all personal information storage locations)]

i. Storage media with a cipher function

All areas that are available for storing personal information are encrypted since a dedicated

encryption chip automatically encrypts all the data written to the media. (Such products on sale include hard drive drives and SSDs (Solid-State Drives: Flash-memory storage media).)

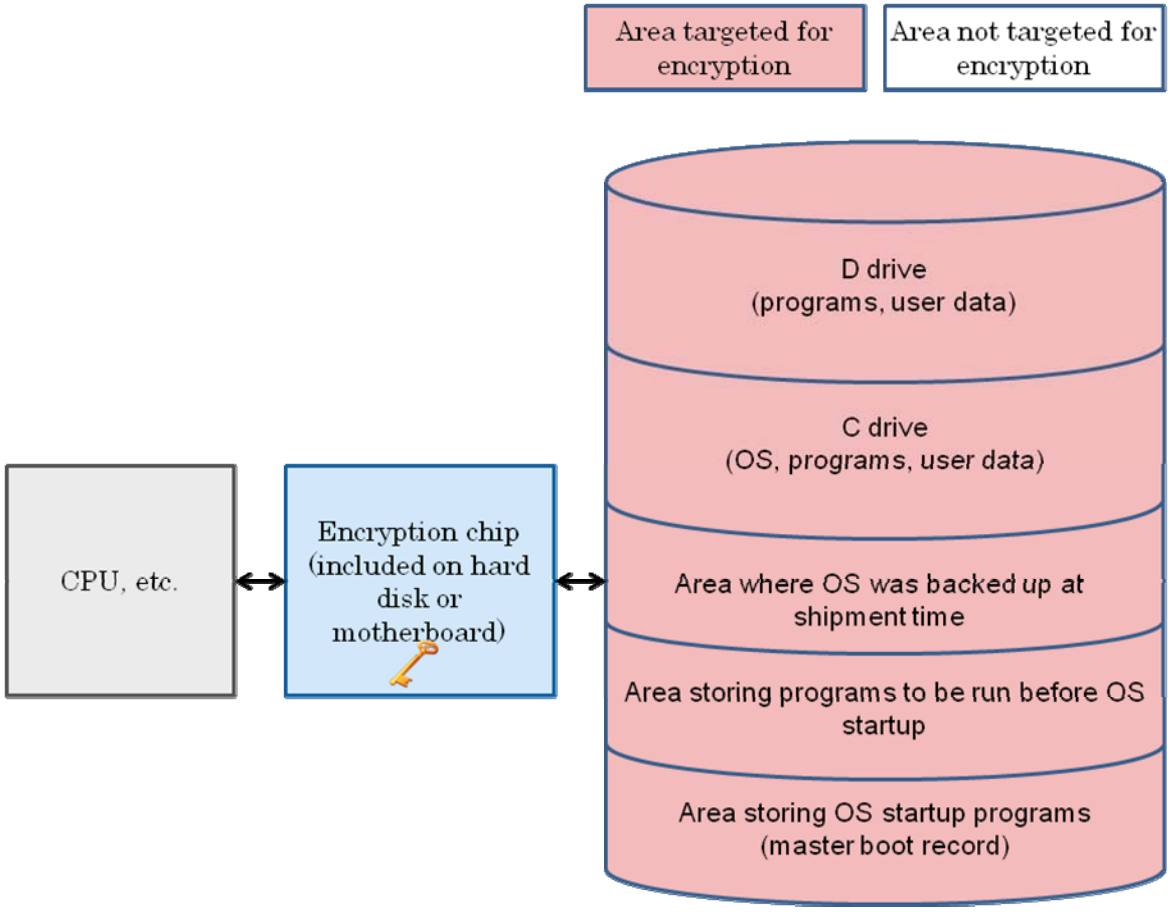


Figure 3 Example of encryption of all hard drive areas

ii. Disk encryption software

Encryption software (FDE software: Full Disk Encryption software) automatically encrypts or decrypts all of the OS, programs, and data. Some areas, including the area containing the encryption software, are not encrypted. However, this causes no problem because these areas cannot be used as personal information storage locations.

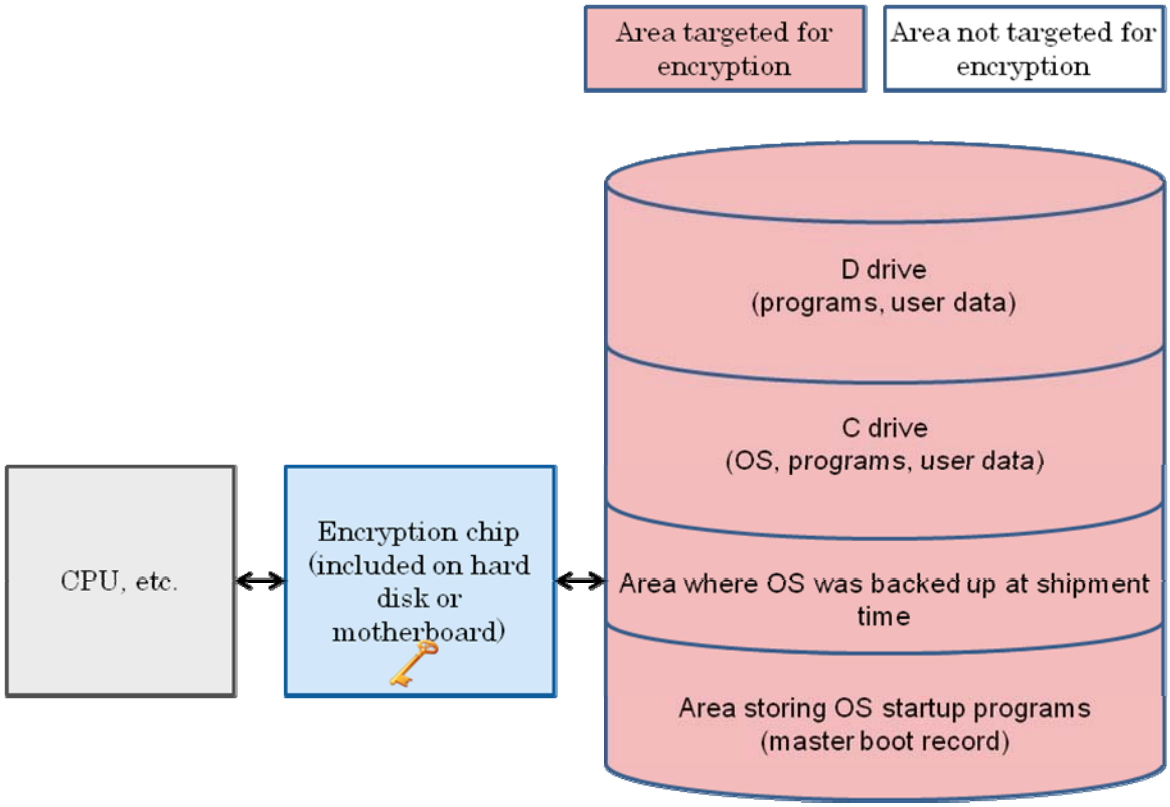


Figure 4　Example of using disk encryption software

[Example of not meeting requirements defined independently in provision I]

i. Encryption targeted only at specified files

After OS startup, encryption software is started as an application running under the OS, and it encrypts only the files and folders specified as encryption targets. This does not meet the requirements defined independently in provision I because ordinary OS areas, data areas, and other areas that do not contain encrypted files or folders are not encrypted and temporary data may be left unencrypted.

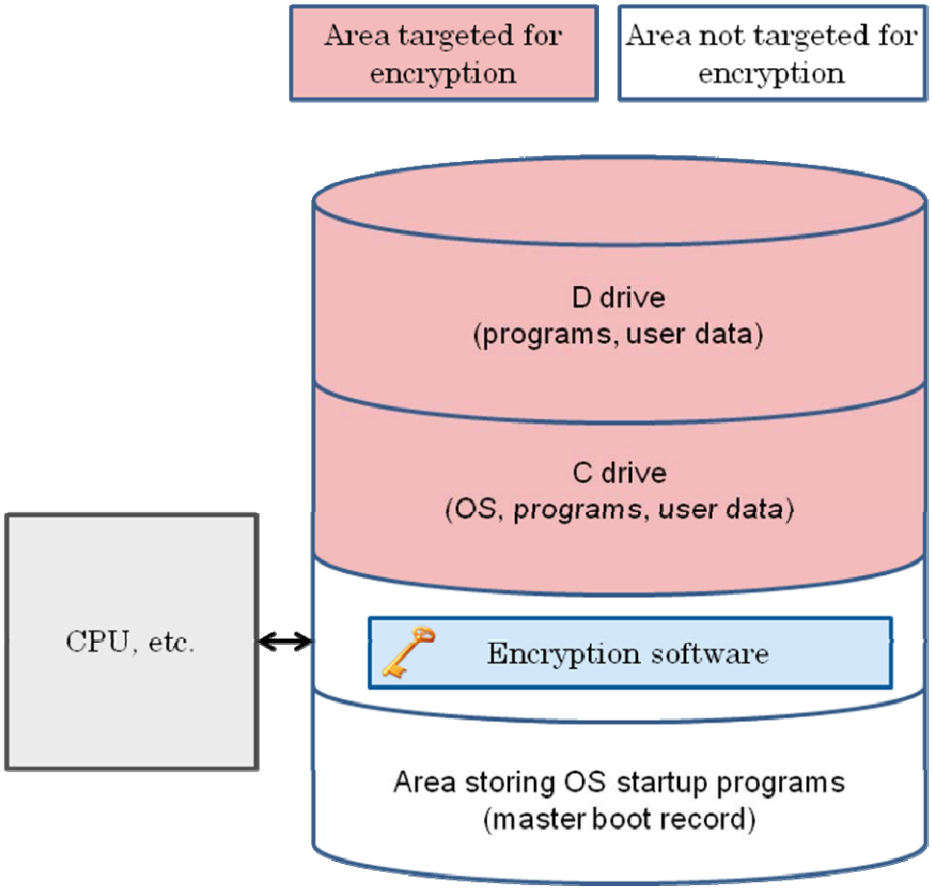


Figure 5　Example of encryption of only the specified files and folders

(3) “Automatically encrypt” means the automatic encryption performed by the system each time data is written to a hard drive. In cases where the user needs to perform a specific operation for encryption, the requirements defined independently in provision I are not met because there is a risk that the user will forget to encrypt data.

“All areas that are available for storing personal information on storage media” requires that “automatically encrypt” cover all these areas, though it may be possible to prevent personal information leakage through appropriate operational procedures without relying on automatic encryption. That being said, this provision considers security aspects, because of risks such as users unintentionally saving personal information on their PCs or forgetting to encrypt data.

II. Managing encrypted information and keys properly

(1) Properly manage encrypted information and the decryption keys that can decrypt the encrypted information by using method (a) or (b) below. The encryption measures used, however, shall be designed such that (2) (in method (a)) the decryption keys are isolated from the encrypted information and (in method (b)) no unauthorized person can illegally duplicate or re-create a deleted decryption key remotely.

(a) Encrypted information and their decryption keys are separate, using the following method A or B.

A. All decryption keys are separate from encrypted information and are configured such that, even for lost encrypted information, the decryption keys are placed under the management of authorized personnel.

B. Each decryption key is split into components that are saved at distributed locations, using (3) a secret sharing scheme included in the public domain. In the scheme, it has been proven impossible to restore whole information from only part of distributed components, so (4) if encrypted information is lost, the encrypted information cannot be decrypted using the decryption key components that are not separate from the lost encrypted information. The components are placed under the management of authorized personnel.

(b) Authorized personnel (5) can remotely delete decryption keys and/or the encrypted information from storage media. They also (6) can confirm that until the time that a decryption key or encrypted information is deleted, the key was not duplicated and none of the information was read or copied.

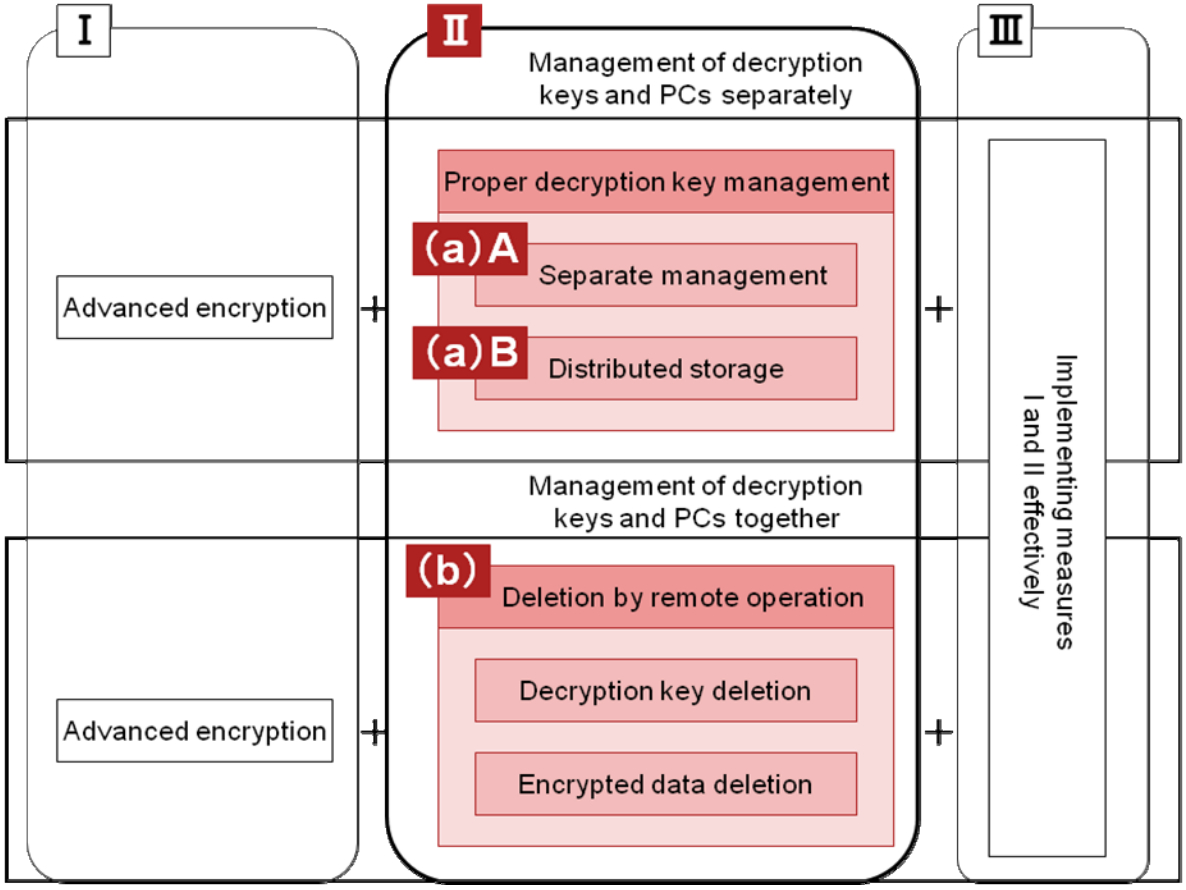


Figure 6　Outline of appropriate security control measures (II. Managing encrypted information and decryption keys properly)

(Explanation)

(1) As described above, generally, any third party who acquires personal information encrypted with an advanced algorithm (encryption procedure) will have difficulty decrypting the information or taking similar action. However, unless keys are adequately managed, personal information would be decrypted by a third party even if advanced encryption measures are implemented. Therefore, proper management of encrypted information and encryption keys is important.

The measures for properly managing encrypted information and their decryption keys include (a) managing encrypted information and decryption keys separately and (b) deleting encrypted information and/or their decryption keys remotely before the encrypted information is decrypted by a third party.

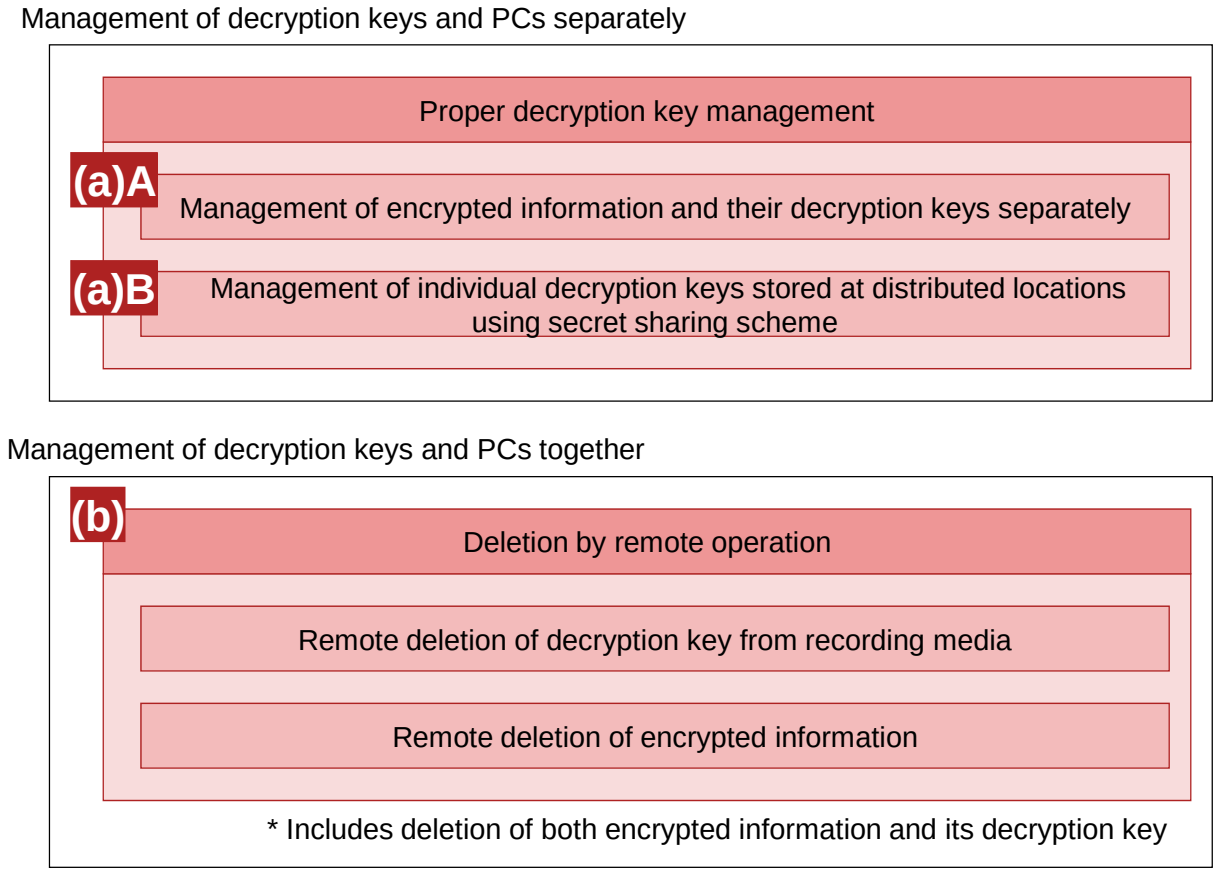


Figure 7　Proper management of encrypted information and their decryption keys

(2) The statements “(in method (a)) the decryption keys are isolated from the encrypted information” and “no unauthorized person can illegally duplicate or re-create a deleted decryption key remotely” mean the following. For method A, examples i, ii, and iii refer to satisfying the following conditions.

i. The keys are saved in storage areas in USB memory or IC cards, isolating them from hard drives or other media containing personal information.

ii. Appropriate measures are taken to prevent the keys saved in storage areas in USB memory or IC cards from being read or duplicated by a third party (a party other than the rightful owners or users of the personal information). (For example, restrict access to the USB memory or IC cards by using password or fingerprint authentication. Alternatively, register IDs or electronic certificates for USB memory and IC cards as unique identifiers on PCs, and do likewise for the PCs on the USB memory and IC cards. This enables mutual authentication between a PC and USB memory or an IC card, so they can mutually confirm a one-to-one relationship between the two when used.)

iii. Appropriate measures are taken to prevent alternate key creation, such as with a restore keyword, so that encrypted information cannot be decrypted using an alternate key.

For method B, examples i and ii refer to satisfying the following conditions.

i. Encrypted personal information and the keys used to encrypt it are saved at distributed locations (e.g., one part is stored on a PC and another part is stored in USB memory), using a secret sharing scheme. The scheme can distribute information and prevent the original information from being restored from individual parts of the distributed information.

ii. Even if part of distributed information is lost, the remaining information is properly managed (which includes preventing duplication by a third party).

The statement "(in method (b)) no unauthorized person can illegally duplicate or re-create a deleted decryption key remotely" means keeping the keys such that no unauthorized person is allowed to duplicate them. It also means that all duplicate keys created by authorized personnel are managed using an appropriate management scheme or stored on specific storage media (e.g., hard drive with a cipher function) that can prevent any unauthorized outside party from accessing the hard drive areas that contain the keys and tampering with the keys.

[Example of meeting the requirement of A in (a)]

i. A PC was lost, but the USB memory storing the key that can decrypt data on the hard drive in the PC has been kept in hand. If the key is stored in spare USB memory, it is also necessary to be able to confirm its location.

[Examples of not meeting the requirement of A in (a)]

i. Both a PC and the USB memory storing the key that can decrypt data on the hard drive in the PC were lost at the same time. If the USB memory were kept in hand but the spare USB memory cannot be located, the requirement is not met.
ii. A PC was lost and the USB memory storing the key that can decrypt the data recorded on the PC has been kept in hand. However, the key in the USB memory can easily be duplicated (such as by simple file copying or duplication of a whole storage area), and it cannot be confirmed that the key remains unduplicated.
iii. A PC was lost and the USB memory storing the key that can decrypt the data recorded on the PC has been kept in hand. However, the encrypted data on the PC can be decrypted by means other than the key (such as by entering an authentication bypass password), or the key can be re-created by entering a certain keyword.

[Reference: Secret sharing]

Secret sharing is a scheme that realizes confidentiality by splitting secret information into components that are saved at distributed locations. One of its features is that the original information cannot be restored from the individual parts of distributed information. Generally, secret sharing is used to save keys for encrypted information at distributed locations rather than

to distribute the information (data) itself. The figure below shows an example where key data is split into five components. The original key can be restored with three of the components.

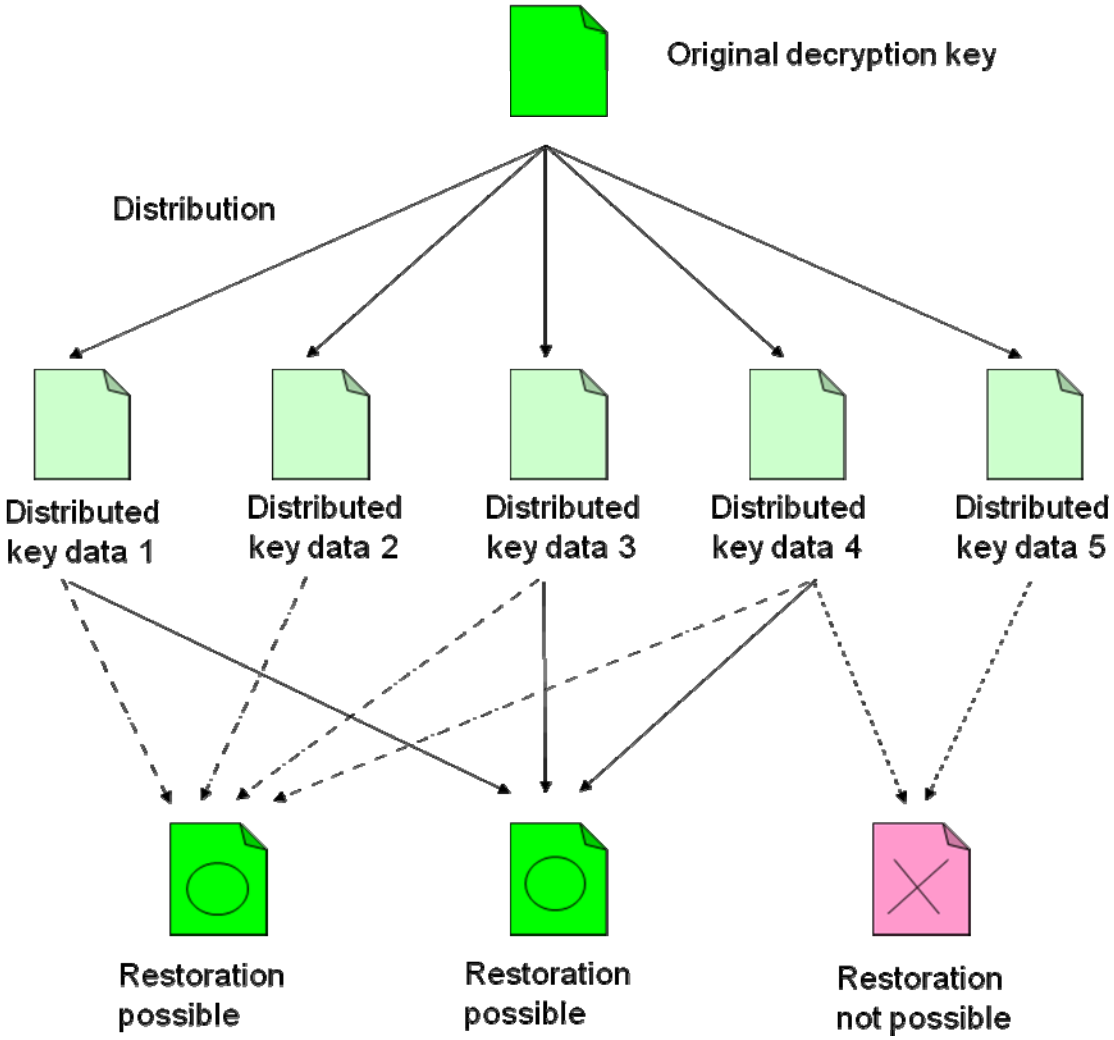


Figure 8 Distributed key management based on secret sharing

(3) "Scheme included in the public domain" in B in (a) means a scheme whose mechanism of secret sharing is disclosed and can be verified by a third party. It also means that documentation such as reports on evaluations by third parties can be obtained.
"In the scheme, it has been proven impossible to restore whole information from only part of distributed components" means a scheme whose mechanism is disclosed and has been verified by third parties with multiple documentations such as reports. Specifically, one scheme is a threshold secret sharing scheme, which uses polynomials that are insoluble unless a prescribed amount of information (threshold value) is available.

(4) In the statement "if encrypted information is lost, the encrypted information cannot be decrypted using the decryption key components that are not separate from the lost encrypted information" about method B, "decryption key components" means a combination of the components of distributed key data stored on a PC and the components of distributed key

data stored on storage media or a server. “Decryption key components that are not separate from the lost encrypted information” refers to the components of distributed key data stored on the PC. That is to say, the above statement means that the encrypted information stored on the lost PC cannot be decrypted using only the components of distributed key data stored on the PC.

Figure 9 shows an example of using a method that can restore the original key by using three of five distributed components of the original key data. Suppose that four of the five components are saved in external storage or on a server and that the remaining component is saved on a PC. If the PC is lost, the original key cannot be restored using only the key data stored on the PC because the PC contains only one distributed component of key data.

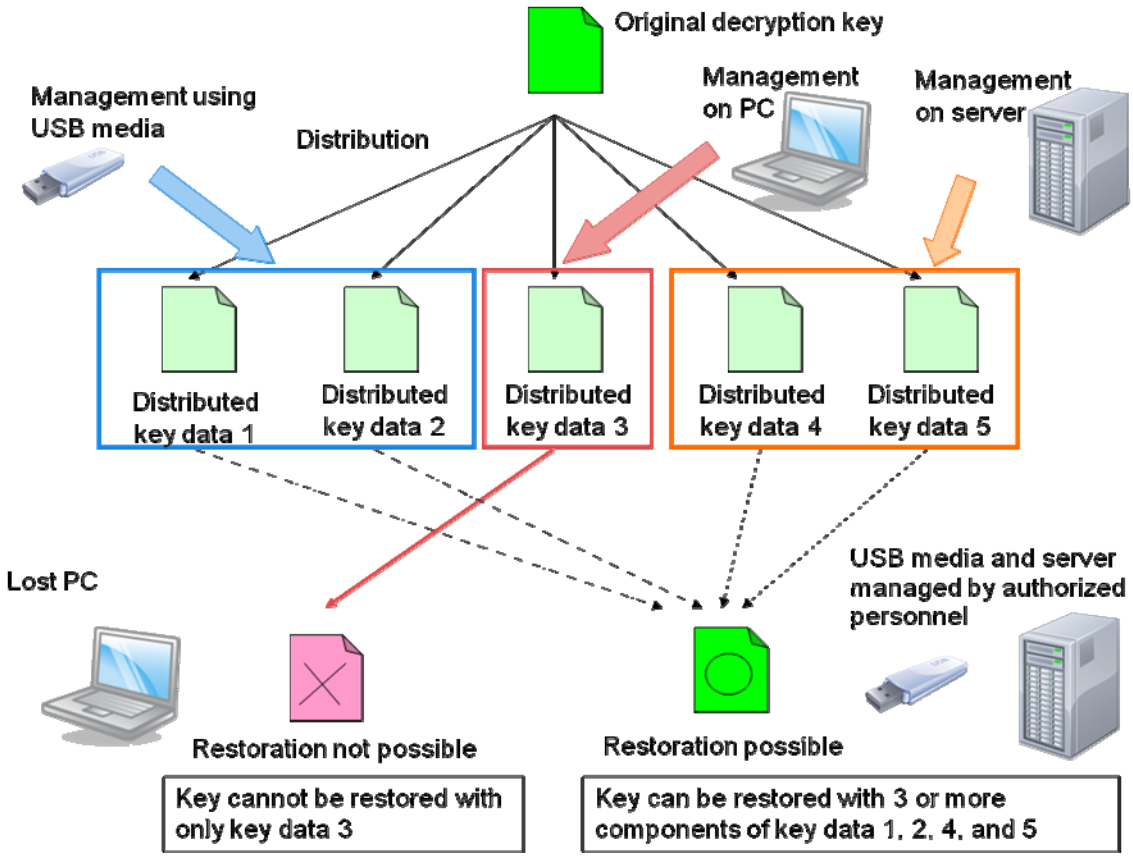


Figure 9 Example of distributed key management based on secret sharing

[Examples of meeting the requirement of B in (a)]

i. Distributed key management is implemented based on a scheme included in the public domain. Theoretically, the scheme can prevent partial decryption. Suppose a PC is lost. The encrypted personal information on the PC cannot be decrypted using only the component(s) of distributed key data stored on the PC. The components of distributed key data are stored in USB memory or other media, which is kept in hand.

ii. Distributed key management is implemented based on a scheme included in the public

domain. Theoretically, the scheme can prevent partial decryption. Suppose a PC is lost. The components of distributed key data other than that on the lost PC are under the management of authorized personnel. For example, they are stored on a server or other such device under the management of authorized personnel.

[Examples of not meeting the requirement of B in (a)]

i. A secret sharing scheme that theoretically may allow partial decryption is used. For example, suppose a PC is lost and the PC uses a distributed key management method that is likely to allow one to correctly guess the key in whole or in part from part of the components of distributed key data.
ii. The components of distributed key data managed by authorized personnel are too few to restore the key. Alternatively, as many components of distributed key data as required to restore the key were lost.

(5) “Authorized personnel can remotely delete decryption keys and/or the encrypted information from storage media” means authorized personnel can remotely delete a key and/or encrypted information from storage media, even without a PC on hand. (i) They can use the method categorized in NIST 800-88 (*1) as "purging" (defined as a sanitization process that protects the confidentiality of information against a laboratory attack). (ii) They can use the method categorized in NIST 800-88 as "clearing" or a method that complies with ii in JEITA's(*2) “Notes on erasing data from a hard drive when discarding or transferring a PC.”

Specifically, one possible method ((i) in the above paragraph) is to erase the data by using the Firmware Secure Erase Command (*3). (For example, executing the ATA Security Erase Unit command with normal erase mode on an ATA(*4)-compatible hard drive will delete all the data on the entire hard drive. Alternatively, if the hard drive is equipped with a cipher function, it will delete and replace the key from the hard drive by executing the ATA Security Erase Unit command with enhanced erase mode.) Another possible method ((ii) in the above paragraph) is to erase the data by overwriting the entire hard drive more than once in a fixed pattern using dedicated software.

Encrypted information is considered deleted from storage media when all the information and/or its decryption key has been erased or overwritten.

*1 NIST 800-88: National Institute of Standards and Technology Special Publication 800-88 Guidelines for Media Sanitization
*2 Japan Electonics and Information Technology Industries Association
*3 Firmware Secure Erase Command: Firmware purge commands that can be executed to securely erase data by using firmware in the ATA hard drive
*4 ATA: AT Attachment interface, which is a hard drive standard

(6) “They also can confirm that until the time that a decryption key or encrypted information is deleted, the key was not duplicated and none of the information was read or copied” means that authorized personnel can look at a completion report indicating the completion of key or data deletion and can confirm that the PC was not used before the deletion.

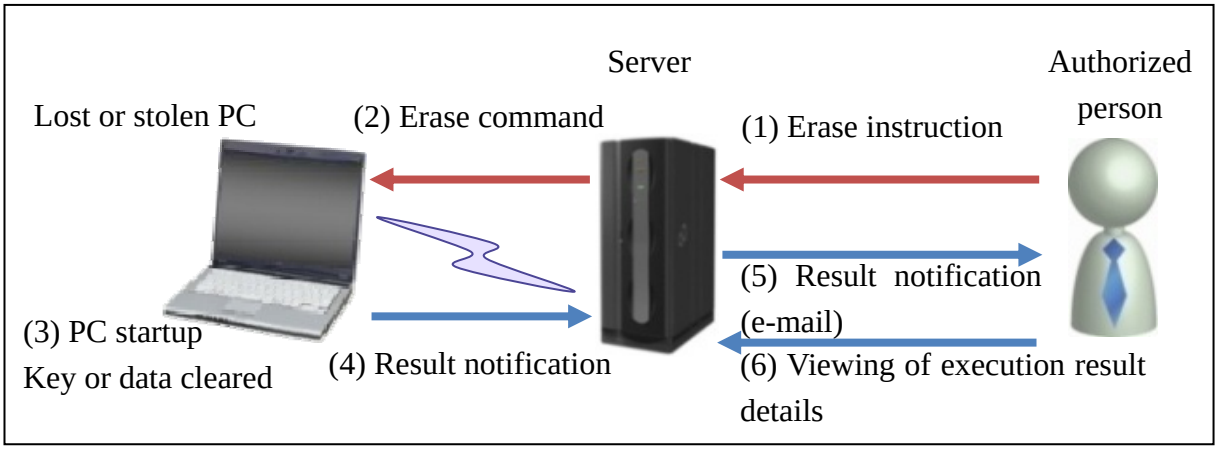


Figure 10　Example of a case where authorized personnel can confirm that a key was not duplicated and information was neither read nor copied

III. Implementing technical protection measures (a) and (b) effectively against personal information leakage and other such problems

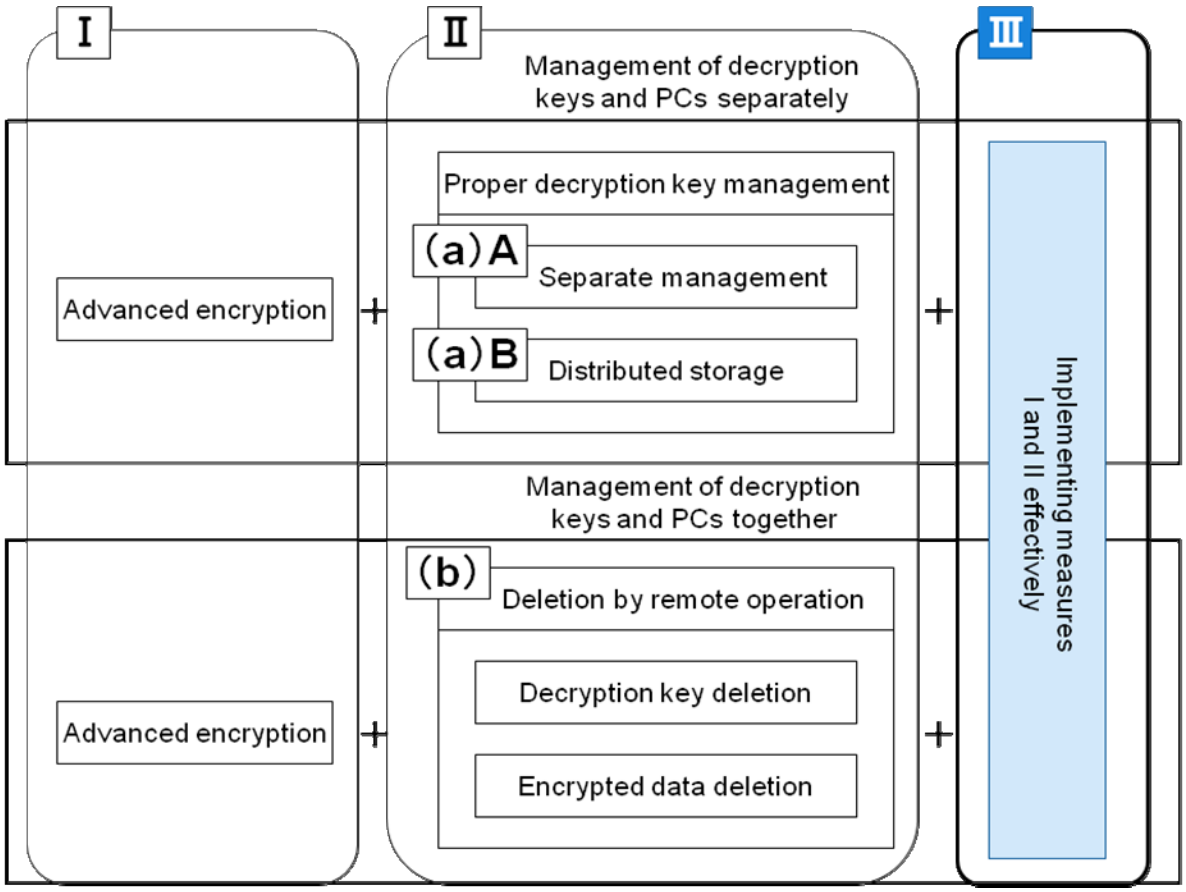


Figure 11　Outline of appropriate security control measures (III. Implementing technical protection measures effectively)

(Explanation)

Cases considered not meeting the requirement in this provision include the following. A business operator implemented technical protection measures I and II, but one or more employees has disabled the associated functions by changing settings at their own discretion. A PC is stolen while powered on, so personal information in the PC is easily accessible.

Other cases considered not meeting the requirements in this provision include the following. Though authorized personnel could remotely delete keys and/or encrypted information from the hard drive of a lost PC (that is, the requirements in provisions I and II (b) are met), the authorized personnel found from a deletion completion report that the PC was used before the deletion of the keys or information was completed. Alternatively, the authorized personnel failed to receive a deletion completion report, such as because the PC was brought outside the communication area.

Supplementary information:

1. Symmetric key ciphers listed in the e-government recommended ciphers list (2003)

1) Symmetric key ciphers (64-bit block ciphers)

(1) 3-key Triple DES

A 64-bit block cipher with a key length of 168 bits, which is a DES hybrid cipher approved under the U.S. Federal Information Processing Standard (FIPS) in 1979. 3-key Triple DES was standardized by NIST in 1998 as FIPS 46-3 and also defined in ANSI X9.52. It is used in SSL 3.0 and TLS 1.0.

(2) MISTY1

A 64-bit block cipher with a key length of 128 bits, announced by Mitsubishi Electric Corporation in 1996. MISTY1 is one of the algorithms recommended by the New European Schemes for Signature, Integrity, and Encryption (NESSIE) project, which is a European project to evaluate ciphers.

(3) Hierocrypt-L1

A 64-bit block cipher with a key length of 128 bits, announced by Toshiba Corporation in 2000

(4) CIPHERUNICORN-E

A 64-bit block cipher with a key length of 128 bits, announced by NEC Corporation in 1998

2) Symmetric key ciphers (128-bit block ciphers)

(1) AES (Advanced Encryption Standard)

A 128-bit block cipher with a key length of 128, 192, or 256 bits, which was standardized based on Rijndael by NIST as Federal Information Processing Standard 197 (FIPS 197) in 2001. AES is one of the algorithms recommended by NESSIE, a European project to evaluate ciphers. Rijndael is a block cipher that was proposed by J. Daemen and V. Rijmen (Belgium) for the AES project in 1998 and selected as the AES winner in 2000.

(2) Camellia

A 128-bit block cipher with a key length of 128, 192, or 256 bits. Announced in 2000, it was jointly developed by NTT Corporation and Mitsubishi Electric Corporation. Camellia is one of the algorithms recommended by NESSIE, a European project to evaluate ciphers.

(3) SC2000

A 128-bit block cipher with a key length of 128, 192, or 256 bits. Announced in 2000, it was

jointly developed by Fujitsu Limited and the Tokyo University of Science.

(4) CIPHERUNICRON-A

A 128-bit block cipher with a key length of 128, 192, or 256 bits, announced by NEC Corporation in 2000

(5) Hierocrypt-3

A 128-bit block cipher with a key length of 128, 192, or 256 bits, announced by Toshiba Corporation in 2000

3) Symmetric key ciphers (stream ciphers)

(1) MUGI

A stream cipher with a key length of 128 bits, announced by Hitachi, Ltd. in 2001

(2) MULTI-S01

A stream cipher with a key length of 256 bits, announced by Hitachi, Ltd. in 2000

(3) RC4 (128 bits)

A stream cipher with a key length of 128 bits, announced by the Security Division of EMC Corporation (formerly called RSA Data Security Inc.) in 1987. RC4 is used in SSL 3.0 and TLS 1.0. CRYPTREC assumes that 128-bit RC4 should be used only with SSL 3.0 or TLS 1.0. Another cipher included in the list should be used whenever possible. RC4 allows for the selection of a key length of either 40 or 128 bits in SSL 3.0 and TLS 1.0. For security reasons, however, CRYPTREC warns against using RC4 with a key length of 40 bits and advises using RC4 with a key length of 128 bits.

2. Ciphers listed in the ISO/IEC 18033 series

1) Symmetric key ciphers (64-bit block ciphers)

(1) 3-key Triple DES

A 64-bit block cipher with a key length of 168 bits, which is a DES hybrid cipher approved under the U.S. Federal Information Processing Standard (FIPS) in 1979. 3-key Triple DES was standardized by NIST in 1998 as FIPS 46-3 and also defined in ANSI X9.52. It is used in SSL 3.0 and TLS 1.0.

(2) MISTY1

A 64-bit block cipher with a key length of 128 bits, announced by Mitsubishi Electric Corporation in 1996. MISTY1 is one of the algorithms recommended by the New European Schemes for Signature, Integrity, and Encryption (NESSIE) project, which is a European project

to evaluate ciphers.

(3) CAST-128

A 64-bit block cipher developed by Carlisle Adams, Stafford Tavares, et al. Its key length is a multiple of 8 bits between 40 and 128 bits. CAST-128 was approved by the Canadian government as an algorithm for confidential communication. It is also called CAST5. CAST-256, which is an extended 128-bit block version of the CAST cipher, was one of the AES candidates.

2) Symmetric key ciphers (128-bit block ciphers)

(1) AES (Advanced Encryption Standard)

A 128-bit block cipher with a key length of 128, 192, or 256 bits, which was standardized based on Rijndael by NIST as Federal Information Processing Standard 197 (FIPS 197) in 2001. AES is one of the algorithms recommended by NESSIE, a European project to evaluate ciphers. Rijndael is a block cipher that was proposed by J. Daemen and V. Rijmen (Belgium) for the AES project in 1998 and selected as the AES winner in 2000.

(2) Camellia

A 128-bit block cipher with a key length of 128, 192, or 256 bits. Announced in 2000, it was jointly developed by NTT Corporation and Mitsubishi Electric Corporation. Camellia is one of the algorithms recommended by NESSIE, a European project to evaluate ciphers.

(3) SEED

A block cipher developed by the Korea Information Security Agency (KISA) in 1998. It has been adopted as a standard cipher in the Korea Information and Communications Society (KICS) standard, S/MIME (RFC 4010), SSL/TLS (RFC 4162), and IPsec (RFC 4196).

3) Symmetric key ciphers (stream ciphers)

(1) MUGI

A stream cipher with a key length of 128 bits, announced by Hitachi, Ltd. in 2001

(2) MULTI-S01

A stream cipher with a key length of 256 bits, announced by Hitachi, Ltd. in 2000

(3) SNOW 2.0

A stream cipher proposed in Sweden

[Reference: Mechanism of PC storing]

The devices that perform the storing process for PC user data include memory and hard drives. The contents of memory are cleared when the power is turned off, and the contents of hard drives remain there when the power is turned off. Memory can read and write data more quickly than hard drives, but hard drives have larger storage capacities than memory. PC operation in general begins with PC startup, proceeds to the loading of data from a hard drive to memory, saves data from memory to a hard drive after the end of an intended operation, and ends with the power-off of the PC. The data in memory is cleared at PC power-off after operation.

PCs record data from memory to hard drives in steps that users may not be aware of. For example, to prevent memory data loss due to a power failure or other such problem, software may automatically save data in the editing process to a hard drive. Also, in the process of reading a large amount of data to memory, part of the data is saved on a hard drive.

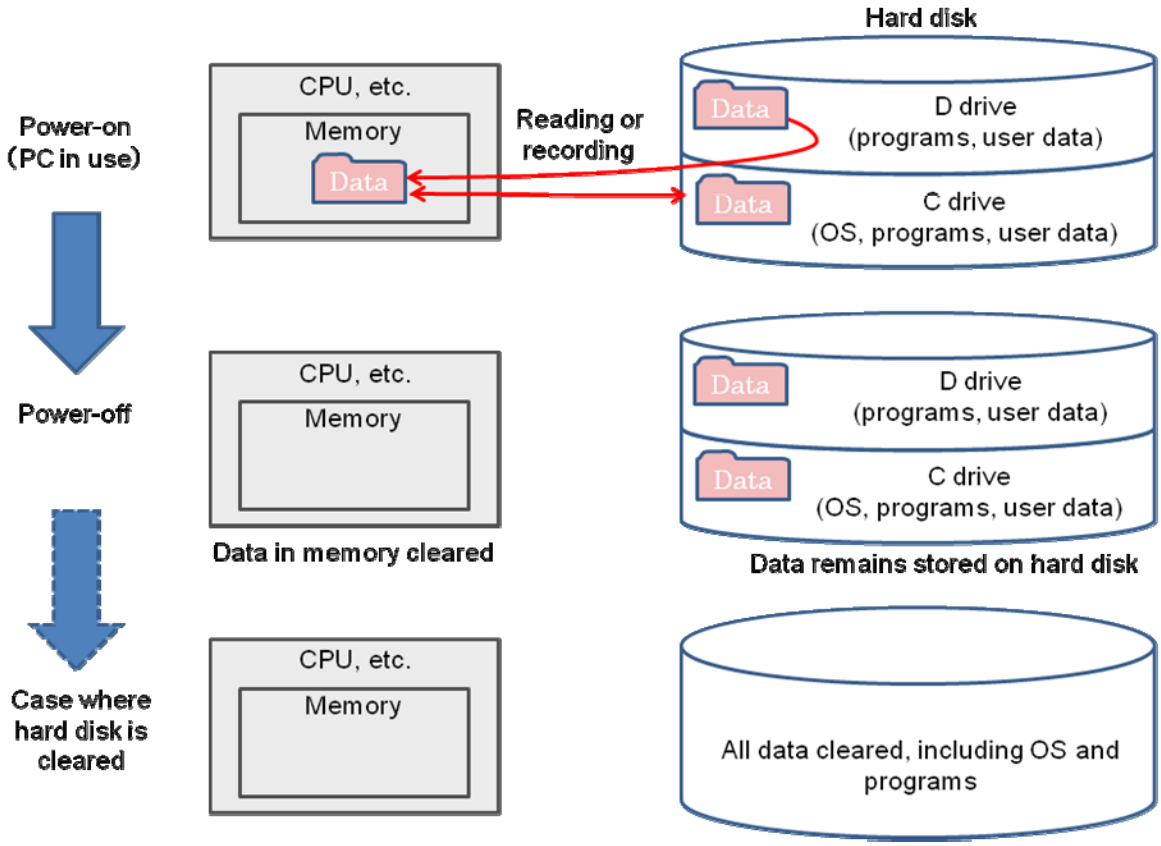


Figure 12　Mechanism of data recording on memory and hard drives

(* The hard drive partitions in the above figure are an example (the same as below).)

[Reference: Mechanism of hard drives]

Users can save information in some areas on hard drives but not in other areas. (See Figure 13, “Hard drive areas.”) The former is OS areas and data areas, and the latter is areas configured as hidden to users. The hidden areas include the area with the master boot record (MBR), which

contains the OS startup programs, and the area storing the data used to restore the OS installed at the shipment time by the PC vendor. Before OS startup by the user to run application software, certain encryption software will start its encryption programs on another OS, load it into memory, and then start the OS for the user to run application software. Users cannot save information to the areas containing these programs that run before OS startup. All these areas never used by users to save information are not included in “all areas that are available for storing personal information on storage media.”

As explained above, “all areas that are available for storing personal information on storage media” means all hard drive areas except those used exclusively by the hard drive manufacturer or PC manufacturer.

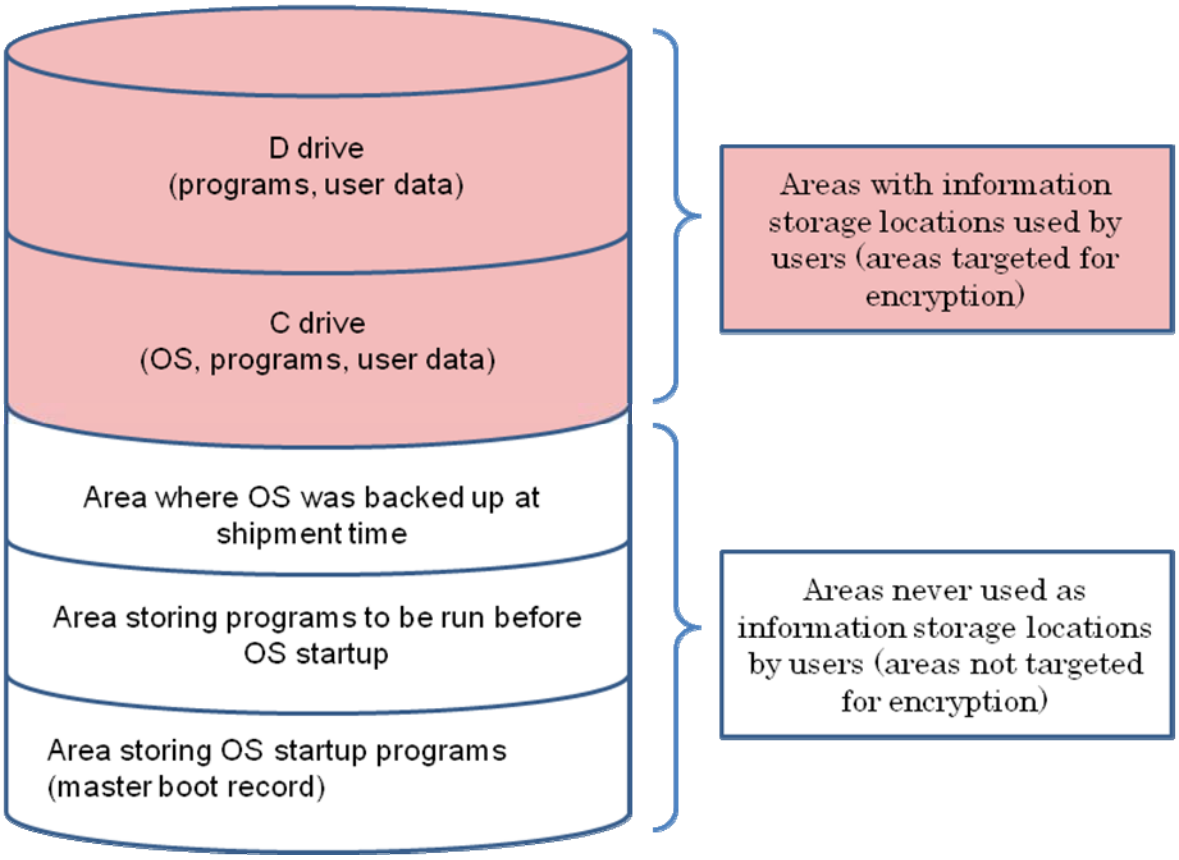


Figure 13 Hard drive areas