Guidance for Evaluating the Impact of Operations and Information in ISMAP-LIU

November 1, 2022
NISC; Digital Agency; Ministry of Internal Affairs and Communications;
Ministry of Economy, Trade and Industry

The original texts of the Standards are prepared in the Japanese language, and these translations are to be used solely as reference material to aid in the understanding of the Standards.
For all purposes of interpreting and applying the Standards in practice, users should consult the original Japanese texts available on the following website:
https://www.ismap.go.jp/csm

Revision History

Date	Revision Contents
November 1, 2022	Creation of first edition

Table of Contents

1. Introduction

1.1. Purpose of This Guidance

ISMAP is a program that evaluates cloud services through a process of external auditing by a third party based on the Control Criteria of ISMAP, which are unified security criteria formulated based on international standards, etc. Among cloud services, services categorized as SaaS include highly important services used for core business. However, the usage and functions of SaaS services are limited, and there are some services that handle information with a relatively low degree of importance even among Confidentiality class-2 information. If these services are handled uniformly with ISMAP, it was assumed that there will be excessive security requirements. Therefore, it was necessary to formulate a new evaluation system according to the risks of the operations and information being handled.

To that end, we established ISMAP for Low-Impact Use (hereinafter, "ISMAP-LIU") as a mechanism for SaaS that handles Confidentiality class-2 information and is used for operations and information processing with low security risks.

On the other hand, the concept of "operations and information with a low security risk among Confidentiality class-2 information" is judged by the contents of the operations and information, and it is difficult to establish a uniform definition. Therefore, in order to contribute to the judgment of low-risk operations and information in ISMAP-LIU, we defined the "Criteria for Evaluating the Impact of Operations and Information" as an appendix to the ISMAP-LIU Registration Rules. This Guidance aims to assist persons in procurement at government agencies, etc., and person in charge of information security departments in determining based on the Criteria for Evaluating the Impact of Operations and Information whether or not the risk of the operations and information handled by the cloud services they use is "low." Please note that the final judgment on Evaluation of the Impact of Operations and Information is the responsibility of the applicable government agencies, etc.

1.2. Structure of This Guidance

Chapter 2 explains an overview of Evaluation of the Impact of Operations and Information. After stating the need for Evaluation of the Impact of Operations and Information in the use of ISMAP-LIU, the concepts and risks of impact evaluation of operations and information are presented. Finally, the timing of the assumed Evaluation of the Impact of Operations and Information is presented.

Based on the concepts in Chapter 2, Chapter 3 explains the specific process for Evaluation of the Impact of Operations and Information.

Appendix 1 provides a List of Target Operations for ISMAP-LIU.

1.3. Definitions

1.3.1. SaaS (Software as a Service)

Specific business applications, communication functions, etc., that are provided to users as services. Specifically, outside the government, they include business services such as safety confirmation and stress checks, and communication services such as email services and file storage. Within the government, functions provided by the inter-ministry common system, and communication-related services and business-related services provided on the government common platform fall under this category.

1.3.2. Confidentiality

Confidentiality means restricting access and disclosure of information to only persons with proper authority. Breach of confidentiality means unauthorized disclosure of information.

1.3.3. Integrity

Integrity means protecting information from inappropriate modification or destruction. It also means ensuring the authenticity of the information. Breach of integrity means unauthorized modification or destruction of information.

1.3.4. Availability

Availability means ensuring that information is accessible and usable to those with proper authority whenever needed. Breach of availability means interference with accessing or using information or information systems.

1.3.5. Impact of Operations and Information

The extent of impact when Confidentiality, Integrity, and/or Availability are compromised against specific risks assumed in the use of SaaS.

1.3.6. Evaluation of the Impact of Operations and Information

The act of evaluating and determining the impact of operations and information.

1.3.7. List of Target Operations

Examples of representative operations that are highly likely of being handled by SaaS subject to ISMAP-LIU. These examples are used as reference at the time of Evaluation of the Impact of Operations and Information by government agencies, etc.

2. Overview of Evaluation of the Impact of Operations and Information

2.1. Need for Evaluating the Impact of Operations and Information

ISMAP-LIU stipulates that its targets are SaaS used for low-risk operations and information processing. However, as discussed above, it is difficult for government agencies, etc., to establish a uniform definition. Therefore, based on the Criteria for Evaluating the Impact of Operations and Information, which are used to judge whether or not the risk of operations and information is low, this Guidance establishes the concept for appropriate Evaluation of the Impact of Operations and Information. By doing so, we seek to suppress excessive dispersion of the Impact Evaluation Results of operations and information, and to support the determination of whether the SaaS used by each government agency, etc., can be eligible for ISMAP-LIU.

Furthermore, assuming changes in the environment surrounding operations and the evolution of cloud services, it is important to continuously perform Evaluation of the Impact of Operations and Information according to those changes.

2.2. Concept for Evaluation of the Impact of Operations and Information

Based on the Criteria for Evaluating the Impact of Operations and Information, in regards to operations and information handled by the user on SaaS, evaluation is performed for impact in the event of a breach in Confidentiality, Integrity, or Availability, which are the three elements of information security. For each instance of information handled in operations, impact is evaluated in the four categories of “N/A,” “low,” “moderate,” or “high.” Ultimately, the Impact of Operations and Information evaluated for each instance of information is comprehensively judged, and the comprehensive Impact Evaluation Results of operations and information are calculated.

2.3. Concept of Risk in Evaluation of the Impact of Operations and Information

In particular, risks in this Guidance are “Risks Envisioned for SaaS Usage,” and were set based on the fact that the service is mainly used in operations of government agencies, etc., due to the characteristics of SaaS. The Risks Envisioned for SaaS Usage were identified in reference to the “Risks Envisioned for Online Procedures” listed in compliance rule 6.1.1(1)(b) in Chapter 6 of Guidelines for Formulating Countermeasure Criteria for Government Agencies, Etc. (2002 version).

Risks Envisioned for SaaS Usage

(1) Inconvenience, distress, or damage to standing or reputation
(2) Financial loss (for example, monetary damage or liability to the user)
(3) Harm to agency programs or public interests
(4) Unauthorized release of sensitive information (personal information, etc.)
(5) Impact to personal safety
(6) Civil or criminal violations

For each of these six risks, we established the four impact categories of "N/A," "low," "moderate," and "high" based on the properties of SaaS, in reference to Appendix A "7. Calculating Impact for Each Type of Risk" in the Guidelines for Online Identity Verification Methods in Administrative Procedures.

Potential impact of "1. Inconvenience, distress, or damage to standing or reputation"

Level	Contents
N/A	No risk (not envisioned).
Low	At worst, limited, short-term inconvenience, distress, or embarrassment to any party.
Moderate	At worst, serious short-term or limited long-term inconvenience, distress, or damage to the standing or reputation of any party.
High	Severe or serious long-term inconvenience, distress, or damage to the standing or reputation of any party. This is ordinarily reserved for situations with particularly severe effects or which potentially affect many individuals.

Potential impact of "2. Financial loss (for example, causes monetary damage or liability to the user)"

Level	Contents
N/A	No risk (not envisioned).
Low	At worst, an insignificant or inconsequential financial loss to any party, or at worst, an insignificant or inconsequential agency liability.
Moderate	At worst, a serious financial loss to any party, or a serious agency liability.
High	Severe or catastrophic financial loss to any party, or severe or catastrophic agency liability.

Potential impact of "3. Harm to agency programs or public interests"

Level	Contents
N/A	No risk (not envisioned).
Low	At worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) Mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness. (ii) Minor damage to organizational assets or public interests.
Moderate	At worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) Significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness. (ii) Significant damage to organizational assets or public interests.
High	A severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) Severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions (ii) Major damage to organizational assets or public interests.

Potential impact of “4. Unauthorized release of sensitive information (personal information, etc.)”

Level	Contents
N/A	No risk (not envisioned).
Low	At worst, a limited release of personal, government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a limited adverse impact on the activities or assets of agencies, etc., or on the user.
Moderate	At worst, a release of personal, government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a significant adverse impact on the activities or assets of agencies, etc., or on the user.
High	A release of personal, government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a catastrophic or devastating impact on the activities or assets of agencies, etc., or on the user.

Potential impact to “5. Personal safety”

Level	Contents
N/A	No risk (not envisioned).
Low	At worst, minor injury not requiring medical treatment.
Moderate	At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.
High	A risk of serious injury or death.

Potential impact of “6. Civil or criminal violations”

Level	Contents
N/A	No risk (not envisioned).
Low	At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.
Moderate	At worst, a risk of civil or criminal violations that may be subject to enforcement efforts.
High	A risk of civil or criminal violations that are of special importance to enforcement programs.

2.4. Position of List of Target Operations

The List of Target Operations provides examples of operations that are highly likely to have a “low” degree of Impact of Operations and Information in ISMAP-LIU. In principle, ISMAP-LIU should be used by government agencies, etc., for operations with a “low” grading at the Evaluation of Impact of Operations and Information. The List of Target Operations is provided to support decisions in ISMAP-LIU usage by each government agency, etc., by showing what kinds of operations generally have a “low” impact.

Since the List of Target Operations shows examples of operations which are highly likely to have a “low” degree of impact, it is necessary for each government agency, etc., to identify specific operations to be actually handled on SaaS and then to refer to the List of Target Operations to

appropriately evaluate the impact for each instance of information processed in operations.

2.5. Timing for Evaluation of the Impact of Operations and Information

Evaluation of the Impact of Operations and Information assumes that the person in charge of procuring information systems cooperates with their operations implementation department and the information security department when planning services and operations.

The Digital Government Promotion Standard Guidelines state the necessity of assessing and analyzing current conditions when planning services and operations. In particular, implementation of "1) Assessing and analyzing users, "2) Assessing and analyzing operations," and "3) Assessing and analyzing data," enables listing of the subject of operations, the scope of operations, and the information handled in operations, which are items necessary to perform the Evaluation of the Impact of Operations and Information. "6) Related research" stipulates the needs to research similar services. After conducting the aforementioned analysis, when the overall results of the Evaluation of the Impact of Operations and Information are judged to be "low," the person in charge of procurement may, by cooperating with the CSP (cloud service provider) related to the bid and having the SaaS provided by the CSP to be registered in ISMAP-LIU, enable procurement using the ISMAP-LIU cloud service list during the procurement process.

Table 1 Implementation Items for Assessing and Analyzing Current Conditions as Defined in the Standard Guidelines

1) Assessing and analyzing users Investigate the scale, locations, characteristics, behavior, degree of satisfaction, requirements, etc., of each person or organization that can obtain value or effect from using the service or operation
2) Assessing and analyzing operations Investigate the scope, work flow, work volume, implementation system, timing/hours of implementation, place of implementation, etc., of service/operation
3) Assessing and analyzing data Identify and analyze information assets handled the operation, and investigate the listing, definitions, input/output, flow, transaction volume, number of processed items, quality, usage status of standards, status of ownership format, management rules, management processes, status of disclosure as open data of information system data
4) Assessing and analyzing existing information systems Investigate the materials, remaining issues, etc., of existing information systems
5) Assessing and analyzing information system operation Investigate the operation record, status of various indices, remaining issues, etc., of

information systems

6) Related research

Investigate the existence of similar services/operations, status of standardization for data being handled, best practices, failures, related factors, etc.

Source: Created based on the Digital Government Promotion Standard Guidelines (September 10, 2022)

3. Process of Evaluation of the Impact of Operations and Information

3.1. Identification of Operations

The first step in the Evaluation of the Impact of Operations and Information is to identify specific operations to be processed by cloud services. Some examples are “using e-learning to educate staff,” “disseminating administrative information to the public via the internet,” and “confirming the safety of staff in the event of a disaster.”

The operations to be identified differ depending on the kinds of operations and scope of operations assumed in the procurement department. For example, in the case of staff education held throughout the organization, it is conceivable to set “using e-learning to educate staff” as a specific task, however, If it is a specialized training for staff in specific departments, it is also possible to identify the task in greater detail; for example, “using e-learning to educate staff on DX literacy.”

3.2. Confirming the Eligibility of Identified Operations for the List of Target Operations

Refer to “Appendix 1. List of Target Operations” to determine if the operations identified in “3.1 Identification of Operations” are eligible for the List of Target Operations. For example, the task of “using e-learning to educate staff” mentioned above corresponds to “(7) Operations to educate organization members on organizational rules, business skills, etc.” in “Appendix 1. List of Target Operations.” The task of “confirming the safety of staff in the event of a disaster” corresponds to “(6) Operations to confirm organizational members in the event of a disaster.”

Even if the identified work does not correspond to the List of Target Operations, the procedures defined in the next and subsequent steps will be performed in the same way.

3.3. Listing of Operations and Information

List the entities (persons, organizations, information systems, etc.) related to the operations identified in “3.1. Specification of Operations.” Also, subdividing the operations content makes it easier to proceed with subsequent work, and easier to notice omissions in the list of related items.

During subdivision, listing specific operation events (operations that occur at a specific time or due to specific factors, etc.) in the target operation area is an effective way to create awareness of important operations.

Recently, there are many SaaS with a wide variety of functions. Therefore, it is preferable to subdivide the operation content while confirming with the CSP that provides the SaaS regarding the functions of the SaaS which is attempting to process the applicable operations. In particular, message functions and file sharing functions can lead to the spread of information in an unintended way, so it is preferable to check for the existence of such functions.

Next, for each entity related to the listed operations, clarify the outline of operations content and list the information handled in the operation. At this time, omitted information will be easily noticed by conducting a review that focuses on what kind of (which entity's) information flows from what location (which entity) to what location (which entity) during operations.

As a result of the process of review and market research on SaaS conducted thus far, the need to subdivide or add operation contents or entities may be recognized. In such cases, repeat the process specified in this section from the beginning.

Important Notes

- It is conceivable that specific information identified in the process of listing operations and information may not be handled on SaaS even if it is necessary for the task. In that case, it is not necessary to evaluation the impact for that information.
- For the authentication information used to log in to the SaaS, the impact is assumed to follow the impact of other information handled on the SaaS. For example, if there are no operations or information handled on SaaS, there will be no impact if the SaaS login information is breached.[1] On the other hand, when information that requires strict confidentiality and has a "high" impact is handled on SaaS, the impact of the login information is also considered to be "high." For this reason, generally speaking, it is sufficient to evaluate the impact on the information listed based on the operations content. It is not necessary to evaluate the impact of authentication information used to log in to the SaaS, unless it is necessary to conduct individual evaluation due to special circumstances.

[1] In general, there is a threat of list-based attacks in the breach of login information for web services such as SaaS. The security impact of this threat is greatly influenced by the password management method of individual users, and it is difficult to conduct uniform evaluation as an organization.

Table 2 Example of Listing of Operations and Information

Operations (listing operations identified in "3.1 Specification of Operations")				
Using e-learning to educate staff				
Entity	**Operation Type**	**Operation Content**	**Overview of Operation Content**	**Information Handled in Operation**
Person in charge of education	Provision of educational contents	Approval of user registration	Confirmation and approval of user registration information	Name and email address of staff
		Registration/deletion of contents	Register and delete educational contents	General educational contents for administrative officials
		Response to opinions/comments	Response to opinions/comments from participants	Opinions/comments (title, main text, name of poster, posting date)
Student	Attendance in educational content	Approval of user registration	Registration of name and email address to be eligible to use the service	Name and email address of staff
		Viewing of content	Viewing and enrollment in registered educational content	General educational contents for administrative officials
		Posting of opinions/comments	Posting of opinions/comments on educational contents	Opinions/comments (title, main text, name of poster, posting date)

3.4. Confirmation of Requirements for SaaS Security

ISMAP-LIU requires the CSP to provide security-related information as reference information for the person in charge of procurement to perform Evaluation of the Impact of Operations and Information. Specifically, the required information is "(1) SLA/SLO," "(2) Server location and data storage location," "(3) Use of external services and status of ISMAP registration of such external services," and "(4) Provided security functions."

Based on this information, the person in charge of procurement carries out the "Implementation of Evaluation of the Impact of Operations and Information" defined in the next section. For example, these security information can used in the following types of judgment.

(1) SLA/SLO

Determine whether or not the service utilization rate is within a permissible range for operation. For example, for an information system in which Availability is extremely important, if the Availability of the service is unacceptable for operation, the evaluation result of Availability in the evaluation of impact is considered to be "moderate" or "high." However, please note that SLA/SLO may not be the same for each contract plan or function, even for the same SaaS.

(2) Server location and data storage location

When personal information is handled and a domestic data center cannot be selected, it is

conceivable to set the impact of Confidentiality and Integrity to “moderate” or “high.”

(3) Use of other cloud services and status of ISMAP registration of such cloud services

If the SaaS to be used utilizes IaaS/PaaS provided by other CSPs as its infrastructure, it is possible to determine if ISMAP can be used to check the security measures of the applicable IaaS/PaaS.

(4) Provided security functions

Among the Control Criteria of ISMAP, the Controls related to security functions that are selected from among the Controls for which the Controls themselves are basic statement requirements. Normally, in the case of SaaS registered in ISMAP-LIU, auditing has been performed to confirm that the SaaS meets the security requirements. Since it cannot be stated with certainty that SaaS satisfies the applicable security requirements before the SaaS is registered in ISMAP-LIU, it is required to confirm that the SaaS is equipped with basic security functions.

3.5. Implementation of Evaluation of the Impact of Operations and Information

Evaluate the impact of each instance of information identified in “3.3. Listing of Operations and Information.” Specifically, for each instance of information, the impact is derived in accordance with “Criteria for Evaluating the Impact of Operations and Information” for each risk from (1) to (6) envisioned for SaaS usage. In calculating the impact, conduct evaluation that considers not only situations in which Confidentiality is breached, but also for when Integrity and Availability is breached.

For example, in e-learning for the purpose of educating administrative staff, if the impact of breaching the Confidentiality, Integrity, or Availability pertaining to the names and email addresses in regards to the risk “(1) Inconvenience, distress, or damage to standing or reputation” is “limited, short-term inconvenience, distress, or embarrassment to any party,” the impact of the risk “(1) Inconvenience, distress, or damage to standing or reputation” can be said to be “low.”

If it is necessary to consider the volume of information to be handled for the listed information, conduct an evaluation of impact that considers volume.

For each instance of information identified during the identification of operations and information, when calculating the results of evaluating the impact for risks defined in “Criteria for Evaluating the Impact of Operations and Information,” adopt the highest level among the impact judged for each risk.

For example, assume that the results shown in Table 3 are obtained by evaluating the impact of specific information. In this case, the evaluation of impact for risks (1), (2), (4), (5), and (6) is “low.” However, since the evaluation of impact for risk (3) is "moderate", the result of evaluating the impact of specific information is judged as “moderate.”

Table 3 Example of Evaluating the Impact on Specific Information

(the table shows an example of the judgment of impact)

Example of information) Name and email address of staff	**Impact**
① Inconvenience, distress, or damage to standing or reputation	Low
② Financial loss (for example, causes monetary damage or liability to the user)	Low
③ Harm to agency programs or public interests	Moderate (due to large volume of information)
④ Unauthorized release of sensitive information (personal information, etc.)	Low
⑤ Impact to personal safety	Low
⑥ Civil or criminal violations	Low

→ The overall judgment is "moderate."

Next, for the results of evaluating the impact of each instance of information, describe the "evaluation concept" so that the judgment can be objectively understood as appropriate.

In this way, by evaluating the impact of each risk for each instance of information, it is possible to obtain results like those shown in Table 4 for Table 2 that was prepared in "Listing of Operations and Information."

Table **4** Example of Evaluating the Impact on Listed Information

(the table shows an example of the judgment of impact)

Operations (listing operations identified in "3.1 Identification of Operations")			
Using e-learning to educate staff			
Entity	**Information Handled in Operation**	**Impact**	**Concept in Evaluation**
Person in charge of education	Name and email address of staff	Low	Due to the assumption that extremely limited information is handled as staff information and the sensitivity of that information is low

	General educational contents for administrative officials	Low	The training is intended for general staff and no sensitive information is handled
	Opinions/comments (title, main text, name of poster, posting date)	Low	Due to low sensitivity of educational contents and assumption of low sensitivity of opinions and comments in conjunction with those contents
Participants	Name and email address of staff	Low	Same as above
	General educational contents for administrative officials	Low	Same as above
	Opinions/comments (title, main text, name of poster, posting date)	Low	Same as above

Important Notes

- It is important to note that, depending on the type of information, impact is “low” for individual instance of information, but there may be “high” impact when aggregating multiple instances of information of the same type. For example, due to aggregating specific information, there are cases in which trends, patterns, plans, etc., can be clarified, and cases in which it becomes possible to access other important information. Therefore, you must also consider the volume of information being handled when judging the impact of listed information.

3.6. Implementation of the Comprehensive Evaluation of Impact of Operations and Information

In principle, the highest impact among the impact on each instance of information listed in “3.5 Implementation of Evaluation of the Impact of Operations and Information” shall be the comprehensive impact of the operations specified in “3.1 Specification of Operations.”

Even if the impact of specific information is “moderate” or “high”, if the results of the comprehensive Evaluation of the Impact of Operations and Information is judged as “low” for special reasons (for example, the information is anonymized and handled on a cloud service), clearly write the reason so that the appropriateness of the judgment can be objectively understood.

3.7. Confirmation of Results of Evaluation of the Impact of Operations and Information

Since the Evaluation of the Impact of Operations and Information is closely related to operation requirements, it is generally assumed that the procurement department will take the lead. The final

evaluation results are, however, to be confirmed under the names of both the procurement department and the information security department, and the appropriateness of the contents will be judged.

If the confirmation results in a judgment of no problems, managers from both the procurement department and information security department sign the confirmation section of "Form 1-2 Sheet for Evaluating the Impact of Operations and Information Related to the Use of SaaS." If it is judged that a problem exists, it is necessary to take measures such as reviewing the operations and information handled on SaaS.

3.8. Continual Monitoring of Evaluation of the Impact of Operations and Information

As the environment surrounding operations and cloud services changes, the operations and information processed on cloud services are also expected to change over time. Therefore, when using ISMAP-LIU, it is not sufficiently to conduct a single evaluation; instead, it is important to continuously evaluate the impact of operations and information.

To this end, for SaaS procured using ISMAP-LIU, it is necessary to periodically confirm whether only the operations and information targeted for evaluation of impact are being handled. Specifically, every year from the start of using SaaS, confirm that the use of SaaS at the information security department of each government agency, etc., is within the scope listed at the time that Evaluation of the Impact of Operations and Information was implemented.

If the status of SaaS usage differs from the operations and information stated for the Evaluation of the Impact of Operations and Information that was conducted and confirmed in the previous year, the information security department will cooperate with the procurement department to conduct a new Evaluation of the Impact of Operations and Information. The purpose of the new evaluation is to confirm that the overall result of the Evaluation of the Impact of Operations and Information is "low." If the result of the newly implemented Evaluation of the Impact of Operations and Information is not "low," the procurement department and the operations execution department will be asked to correct to conform with the appropriate usage method. If such correction is difficult, it is necessary to request the CSP to obtain ISMAP instead of ISMAP-LIU.

Appendix 1. List of Target Operations

The List of Target Operations consists of types (1) to (8) listed below. For each type of operation, the list provides examples of assumed services, examples of specific operations, and examples of information to be handled. It also explains the concept for each type of operation.

We plan to review the List of Target Operations during operation of the system, and to expand the list as necessary.

① Operations performed in collaboration with the private sector in the process of planning and coordinating policies and systems on the premise of public disclosure

(Examples of envisioned services)

Web conference service

File sharing service

(Examples of specific operations)

Hosting and holding of web conferences associated with the operation of conferences which invite experts from private companies and organizations

Administrative operations for conference materials, etc., associated with the operation of conferences which invite experts from private companies and organizations

(Example of handled information)

Video/audio of meetings to be disclosed externally, meeting materials, names of meeting participants, minutes, etc.[2]

(Concept)

Operations performed in collaboration with the private sector in the process of planning and coordinating policies and systems on the premise of public disclosure is envisioned to involve handling of information such as conference materials related to policies and systems under planning; opinions, questions, etc., on policies and systems associated with conferences; and information on the conference participants such as their names and names of their organizations. Normally, if the information handled in operations is breached, the impact will be limited or insignificant, and it is highly likely that the impact will be “low.”

[2]Special attention should be paid to evaluating the impact if information considered as private is contained, if information on conference participants, etc., is contained and there is no disclosure agreement with participants, or if a breach of the above information when using the cloud service would have a limited or insignificant impact.

Even when not collaborating with the private sector in the process of planning and coordinating policies and systems on the premise of disclosure, there may be cases where information with a "low" level of impact is handled. Normally, differing uses of SaaS services according the impact of information is not assumed. For example, when using web conferencing services in the process of planning and coordinating policies and systems within government agencies, etc., it is normal to use standard services procured by each government agency, etc., and it is difficult to envision cases where different services are used in accordance with the instances of the information handled. Therefore, in processing SaaS that is used by government agencies, etc., in the process of planning and coordinating policies and systems within the organization, it is appropriate to use a cloud service to which ISMAP (not ISMAP-LIU) is registered. On the other hand, in collaborative work with the private sector, it is not always possible for the private sector to use SaaS to which ISMAP has been registered. Therefore, this type (1) is limited to collaboration with the private sector.

② Operations that handle information of staff at government agencies, etc. such as job titles and names

(Examples of envisioned services)

Personnel administration service

Talent management service

Hiring administration services

(Examples of specific operations)

Administrative operations for staff at government agencies, etc.

Staff assignment and skill identification operations at government agencies, etc.

Operations related to recruiting and hiring government staff

(Example of handled information)

Staff labor information, staff personnel transfer history, current affiliation, information on qualifications, etc., job seeker history information, job description, selection information[3]

(Concept)

Operations that handle information such as job titles and names of staff at government agencies,

[3] Special attention should be paid to evaluating the impact if the handled information contains private information or sensitive information of the general public or employees, if it contains personnel information that has not yet been disclosed, if it contains information that should be kept confidential from the viewpoint of fairness such as selection criteria, or if it includes staff information requiring strict confidentiality due to the nature of work.

etc., may include those related to personnel administration and recruiting/hiring of staff at organizations.

It is conceivable that operations related to personnel administration in an organization may handle information related to staff labor, job titles, career history, staff assignment, skills, etc. Normally, if the information handled in operations is breached, the impact will be limited or insignificant, and it is highly likely that the impact will be "low."

Furthermore, it is conceivable that operations related to the recruitment and hiring of staff will handle information such as the career history of job seekers, job descriptions, and selection information. Normally, if the information handled in operations is breached, the impact will be limited or insignificant, and it is highly likely that the impact will be "low."

Additionally, it is conceivable that other types of target operations will handle information such as job titles and names in the operations of staff at government agencies, etc., at the time of user registration or administration, etc. For example, when using e-learning to educate staff in "(7) Operations to educate organization members on organizational rules, business skills, etc.," it is conceivable to handle the job title and name of the staff enrolled in the educating during registration administration. Therefore, even in such usage cases, it is highly likely that the impact will be "low."

③ Operations handling information generally provided in a broad scope (business card information, etc.) and administrative information such as destinations for distribution of public information

(Examples of envisioned services)

Cloud business card management service

Cloud video and content distribution services

(Examples of specific operations)

Operations to register and manage business card information such as company name, title, name, etc.

Registration and administration of information for the purpose of specifying destinations for the distribution of video content, etc., to customers such as government agencies

(Example of handled information)

Information on business cards (name, work location, telephone number, email address, etc.), information necessary for distributing public information (identifiers, etc., for specifying distribution destinations)

(Concept)

Due to the nature of business cards, the information listed on business cards is within a scope that is widely provided to the general public (name of affiliated organization, name, position, contact information). Therefore, if the information listed on a business card is breached, the impact will be limited or insignificant, and it is highly likely that the impact will be “low.”

Furthermore, it is assumed that some of the operations related to the distribution of information such as video content to customers such as government agencies will handle information for specifying users at distribution destinations. Normally, if this information is breached, the impact will be limited or insignificant, and it is highly likely that the impact will be “low.”

④ Operations which process information that is provided by the private sector and that is considered to be low risk by the information provider

(Examples of envisioned services)

Web conference service

File sharing service

(Examples of specific operations)

Operations for the receipt and management of information from private corporations and groups

Operations to participate in conferences, etc., hosted by private companies and organizations

(Example of handled information)

Video/audio of meetings to be disclosed externally by private corporations, meeting materials, names of meeting participants, minutes, etc.

(Concept)

Operations which process information that is provided by the private sector and that is considered to be low risk by such information provider assumes handling of information related to specific services and technologies held by the private sector, as well as mid- to long-term plans of the private sector such as business strategy, and recommendations and requests for improvement, etc., in regards to political measures. Regarding this information, if there is a breach of information judged to be low risk in the private sector (for example, information on the premise of external disclosure), the impact will be limited or insignificant, and it is highly likely that the impact will be “low.”

Also, in operations for exchanging information between government agencies, etc., there may be cases where information with a “low” level of impact is handled. Normally, using different

SaaS services in accordance with the impact of information is not assumed. For example, when using web conferencing services for exchanging information among government agencies, etc., it is normal to use standard services procured by each government agency, etc., and it is difficult to envision cases where different services are used in accordance with the instances of the information handled. Therefore, in operations for exchanging information among government agencies, etc., it is appropriate to use a cloud service to which ISMAP (not ISMAP-LIU) is registered. On the other hand, when receiving information provided from the private sector, it is not always possible for the private sector to use SaaS to which ISMAP has been registered. Therefore, this type (4) is limited to receipt of information provided from the private sector.

⑤ When the operations handle open source, common knowledge, or public information, but there are exceptions requiring confidential handling

(Examples of specific operations)

Operations for developing open-source software
Operations for contents administration on websites
Operations for translation of published policy information and technical information
Operations for collecting and responding to public comments
Operations for creating, administering, and responding to questionnaires

(Examples of envisioned services)

Source code administration service
CMS (Contents Management System) service
Automatic translation service
Web questionnaire service

(Example of handled information)

Special attention should be paid to evaluating the impact if handling information that requires strict control over the timing of disclosure such as the source code of open source software, information scheduled to be disclosed on each ministry's website[4], information that was entered by each ministry on documents to be translated (for example, information to be disclosed

[4] or information that requires strict control over the timing of disclosure, such as information affecting the stock market.

overseas)[5], information on the contents and results of questionnaires conducted by each ministry[6],

(Concept)

In general, open source, common knowledge, and public information are classified as Confidentiality class-1 information; however, there are exceptions in which some information is judged as being confidential. For example, in the development of open source software, the source code of each open source software, the related design documents, etc., are widely disclosed. Information. On the other hand, information such as the agency's contribution strategy, financial support plan, and project plan for the open source software project are assumed to be confidential. If the impact of breach of such confidential information handled in operations is limited or insignificant, it is highly likely that the impact will be "low."

Contents management operations on websites can be considered as operations that handle common knowledge and public information. Normally, the contents on a website such as official government information are intended for public disclosure. Strictly speaking, such information is not considered to be public information before the moment the information is disclosed on the website. However, information before disclosure on the website can be considered as information for which the decision to disclose has already been made. If this information is breached, the impact will be limited or insignificant, and it is highly likely that the impact will be "low."

Additionally, translation of information that is normally disclosed can be considered as operations that handle common knowledge and public information. In this case, common knowledge and public information are not confidential information. Still, it is possible that the very fact that the information was translated is confidential. However, when such information is accessed through the internet, such fact is normally obvious from access logs, etc. Therefore, even if such fact is confidential and becomes breached, the impact will be limited or insignificant, and it is highly likely that the impact will be "low."

This type (5) may be applicable to operations other than the examples listed above. In that case, for the element which needs to be handled confidentially as an exception, it is necessary to judge whether or not such element corresponds to the applicable type based on the properties of that element.

---

[5] Special attention should be paid to evaluating the impact if assuming that impact would be significant in the event that the content of the document to be translated or the fact that the document was input were leaked.

[6] Special attention should be paid to evaluating the impact if the questionnaire contains personal information (name, address, age, etc.) or if it is assumed that impact would be significant in the event that the content of the questionnaire were leaked.

⑥ Operations to confirm the status of damage, etc., to organizational members in the event of a disaster, etc.

(Examples of envisioned services)

Safety confirmation service

(Examples of specific operations)

Operations to manage contact information of government staff in the event of a disaster, etc.

Operations to manage the status of damage to government staff in the event of a disaster, etc.

(Example of handled information)

Information for confirming the safety of employees in the event of a disaster (names email addresses, etc.)[7]

(Concept)

"Operations that handle information such as job titles and names of staff at government agencies, etc." are already shown in the List of Target Operations. If information such as the status of damage to government staff in the event of a disaster is breached, the impact will be limited or insignificant, and it is highly likely that the impact will be "low."

(Special Points)

Generally speaking, the ISMAP Operation Criteria focus on security measures related to Confidentiality. However, Integrity and Availability are also important in tasks such as confirming the status of damage in the event of a disaster. Therefore, when using SaaS for this operation, it is important to separately confirm whether the level of Integrity and Availability of the service meets the operation requirements. For example, when using a safety confirmation service, etc., in a department with extremely high urgency and comprehensiveness, the impact may be judged as "high" or "moderate" based on the SLA or the service.

[7] Special attention should be paid to evaluating the impact when handling staff information that requires strict confidentiality due to the nature of operations (for example, operations related to national security and public order), when staff privacy information or sensitive information is included, or when the impact of leaking safety confirmation itself is significant.

⑦ Operations to educate organization members on organizational rules and business skills

(Examples of envisioned services)
E-learning service

(Examples of specific operations)
Operations to provide educational materials to government staff regarding organizational regulations, rules, and public notices
Operations to provide general business skills, etc., for human resource development and career advancement

(Example of handled information)
Information on learning contents for staff that can be disclosed externally, names of staff who take the course, and information on learning results[8]

(Concept)
Operations to educate organization members on organizational rules and business skills are assumed to handle general learning content related to organizational rules, business skills, etc., information such as the names of staff who attend the course, and information related to learning results. Normally, if this information is breached, the impact will be limited or insignificant, and it is highly likely that the impact will be “low.”

[8] Special attention should be paid to evaluating the impact when handling highly confidential information as educational materials.

⑧ Operations handling standardized and routine business correspondence, etc., from among documents whose storage period is less than one year according to the “Guidelines for Managing Official Document”

(Examples of specific operations)

Operations for responding to inquiries on facts related to administrative affairs of government agencies, etc.

(Example of handled information)

Information regarding to facts related to administrative affairs of government agencies, etc., and inquiries on those facts

(Examples of envisioned services)

Chatbot service

(Concept)

Documents with storage period less than one year according to the “Guidelines for Managing Official Document” are likely to be the official documents with low degree of importance. Therefore, for documents whose storage period is less than one year in the “Guidelines for Managing Official Document,” if the information is breached, the impact will be limited or insignificant, and it is highly likely that the impact will be “low.”

For example, regarding the “responses to inquiries on facts of administrative affairs under the control of a particular Ministry” specified in the guidelines, it is considered in principle that the content will be widely disclosed to the public. Therefore, it is highly likely that the impact will be “low.”

(Important Notes)

There may be cases of target operations other than those listed from among documents whose storage period is less than one year in the “Guidelines for Managing of Official Document.” However, it is assumed that some documents with low importance may be sensitive documents depending on the content of operations. Therefore, special attention should be paid to evaluating the impact.