ISMAP-LIU における
業務・情報の影響度評価ガイダンス

2022 年（令和 4 年）11 月　1 日

NISC・デジタル庁・総務省・経済産業省

改定履歴

日付	改定内容
2022 年 11 月 1 日	初版作成

目次

1. はじめに

1.1. 本書の目的

ISMAP は、国際標準等を踏まえて策定した統一的なセキュリティ基準である ISMAP 管理基準に基づき、第三者が外部監査するプロセスを経てクラウドサービスを評価する制度である。クラウドサービスのうち SaaS に類型されるサービスは、基幹業務に使用する重要度の高いサービスがある一方、用途や機能が限定的であり、機密性 2 情報の中でも比較的重要度が低い情報を取り扱うサービスも存在し、これらサービスについて ISMAP と一律の取扱いとした場合、過剰なセキュリティ要求となる場合が想定される。そのため、取り扱う業務・情報のリスクに応じた、新たな評価の仕組みの策定が必要とされたところである。

そこで、機密性 2 情報を扱う SaaS のうち、セキュリティ上のリスクの小さな業務・情報の処理に用いるものに対する仕組みとして ISMAP for Low-Impact Use（以下、ISMAP-LIU という）を創設した。

一方で、「機密性 2 情報のうちセキュリティ上のリスクの小さな業務・情報」という考え方は、実施する業務や情報の内容によって判断されるものであり画一的な定義をするのは困難である。そのため、ISMAP-LIU においてリスクの小さな業務・情報の判断に資するため、ISMAP-LIU の登録規則の別紙として、「業務・情報の影響度評価基準」を規定している。本ガイダンスは、各政府機関等の調達担当者、情報セキュリティ部門の担当者が、利用するクラウドサービスが扱う業務・情報のリスクが低位であるかどうかを、「業務・情報の影響度評価基準」に基づいて判断できるように支援することを目的としたガイダンスである。なお、最終的な業務・情報の影響度評価の判断は、各政府機関等の責任で行われることに留意されたい。

1.2. 本書の構成

2 章では業務・情報の影響度評価の概要について説明する。ISMAP-LIU の利用において業務・情報の影響度評価を行う必要性を述べた後、業務・情報の影響度評価の考え方及びリスクについて示した上で、想定される業務・情報の影響度評価を実施する時期について示す。

3 章では 2 章の考え方を踏まえ、業務・情報の影響度評価の具体的なプロセスについて解説を行う。

また、別紙 1 として ISMAP-LIU における対象業務一覧を示す。

1.3. 用語の定義

1.3.1. SaaS (Software as a Service)

利用者に、特定の業務系のアプリケーション、コミュニケーション等の機能がサービスとして提供されるもの。具体的には、政府外においては、安否確認、ストレスチェック等の業

務系のサービス、メールサービスやファイル保管等のコミュニケーション系のサービス等がある。政府内においては、府省共通システムによって提供される諸機能や、政府共通プラットフォーム上で提供されるコミュニケーション系のサービス・業務系のサービスが該当する。

1.3.2. 機密性

機密性とは、情報へのアクセス・開示を適正な権限を持つ者のみに限定するよう制限すること。機密性の侵害とは、情報の不当な開示を意味する。

1.3.3. 完全性

完全性とは、情報を不適切な変更や破壊から保護すること。また、情報の真正性を保証すること。完全性の侵害とは、情報の不当な改変・破壊を意味する。

1.3.4. 可用性

可用性とは、適正な権限を持つ者が必要なときにいつでも情報にアクセスし利用できることを保証すること。可用性の侵害とは、情報又は情報システムへのアクセス・利用が妨げられることを意味する。

1.3.5. 業務・情報の影響度

SaaS の利用において想定される特定のリスクに対し、機密性、完全性、可用性が侵害された際の影響を及ぼす大きさの度合い。

1.3.6. 業務・情報の影響度評価

業務・情報の影響度を評価し決定すること、その行為。

1.3.7. 対象業務一覧

利用省庁等が業務・情報の影響度評価を行う際の参考として、ISMAP-LIU の対象となる SaaS が扱う蓋然性の高い代表的な業務を例示したもの。

2. 業務・情報の影響度評価の概要

2.1. 業務・情報の影響度評価の必要性

ISMAP-LIU においてはその対象を、リスクの小さな業務・情報の処理に用いる SaaS と規定しているが、前述したとおり、リスクの小さな業務・情報について、政府機関等において画一的な定義をするのは困難である。そこで、本ガイダンスにおいて、リスクの小さな業務・情報であるかどうかを判定するための「業務・情報の影響度評価基準」に基づき、業務・情報の影響度評価を適切に行うための考え方を示すことで、業務・情報の影響度評価結果の過度な分散を抑制するとともに、各政府機関等が利用する SaaS が ISMAP-LIU に該当しうるかどうかの判断を支援する。

また、業務をとりまく環境の変化や、クラウドサービスの進化を想定すると、業務・情報の影響度評価はそれらの変化に応じて継続的に行うことが重要となる。

2.2. 業務・情報の影響度評価の考え方

利用者が SaaS 上で取り扱う業務・情報に関して情報セキュリティの 3 要素である機密性、完全性、可用性が侵害された場合の影響度を「業務・情報の影響度評価基準」に照らして評価する。影響度は、「N/A」「低位」「中位」「高位」の 4 段階とし、業務で取り扱う情報ごとに影響度を評価する。最終的には情報ごとに評価した業務・情報の影響度を総合的に判断し、総合的な業務・情報の影響度評価結果を導出する。

2.3. 業務・情報の影響度評価におけるリスクの考え方

本ガイダンスにおけるリスクとは、特に「SaaS の利用において想定されるリスク」であり、SaaS の特性により政府機関等の業務におけるサービス利用が主となることを踏まえ設定した。なお、「SaaS の利用において想定されるリスク」は「政府機関等の対策基準策定のためのガイドライン（令和 3 年度版）」　第 6 部 情報システムのセキュリティ要件の遵守事項 6.1.1(1)(b)に記載の、「オンライン手続において想定されるリスク」を参考とした。

SaaS の利用において想定されるリスク
①国民に不便、苦痛を与える、又は機関等が信頼を失う
②利用者に金銭的被害や賠償責任が生じるなど、財務上の影響を与える
③機関等の活動計画や公共の利益に対して影響を与える
④個人情報等の機微な情報が漏えいする
⑤利用者の身の安全に影響を与える
⑥法律に違反する

また、これら六つのリスクについて、「行政手続きにおけるオンラインによる本人確認の手法に関するガイドライン」付録A「7．各リスクの種類による影響度の導出」をもとに、SaaSの特性を踏まえ、「N/A」「低位」「中位」「高位」の4段階の影響度についての考え方を下記の通り整理した。

「1．国民に不便、苦痛を与える、又は機関等が信頼を失う」リスクの影響度

レベル	内容
N/A	リスクがない（想定されない)。
低位	限定的かつ短期間の不便や苦痛又は、機関等の地位や評判に対し軽微な影響がある。
中位	深刻かつ短期間又は限定的かつ長期間の不便や苦痛又は、機関等の地位や評判に対する影響がある。
高位	深刻又は長期間の不便や苦痛又は、機関等の地位や評判に対する影響がある。この影響は、特に深刻な影響や多くの機関等の利用者に影響する状況をいう。

「2．　利用者に金銭的被害や賠償責任が生じるなど、財務上の影響を与える」リスクの影響度

レベル	内容
N/A	リスクがない（想定されない)。
低位	機関等の軽微又は若干の財務上の損失、若しくは機関等の軽微又は若干の賠償責任が生じる。
中位	機関等の深刻な財務上の損失、若しくは機関等の深刻な賠償責任が生じる。
高位	機関等の壊滅的な財務上の損失、若しくは機関の深刻又は壊滅的な賠償責任が生じる。

「3．機関等の活動計画や公共の利益に対して影響を与える 」リスクの影響度

レベル	内容
N/A	リスクがない（想定されない)。
低位	機関等の運営又は資産、若しくは公共の利益に対する限定的な悪影響がある。限定的な悪影響の例としては以下が考えられる。(i) 機関等の主要な機能が「著しく」低下した状態が継続し、業務能力の劣化が生じている。(ii) 機関等の資産や公共の利益の軽微な損害が生じる。
中位	機関等の運営又は資産、若しくは公共の利益に対する深刻な悪影響があ

	る。深刻な悪影響の例としては以下が考えられる。(i) 機関等の主要な機能が「大幅に」低下した状態が継続し、業務能力の大幅な劣化が生じている。(ii) 機関等の資産や公共の利益の重大な損害が生じる。
高位	機関等の運営又は資産、若しくは公共の利益に対する重大又は壊滅的な悪影響がある。重大又は壊滅的な悪影響の例としては以下が考えられる。(i) 機関等の主要な機能の 1 つ以上が実施できない状態が継続し、業務能力の激しい劣化又は喪失が生じている。(ii) 機関等の資産又は公共の利益の際立った損害が生じている。

「4． 個人情報等の機微な情報が漏えいする」リスクの影響度

レベル	内容
N/A	リスクがない（想定されない)。
低位	公開許可のない個人情報、政府の機密情報又は企業秘密の限定的な公開により、機関等の活動や資産、又は利用者に機密性喪失の限定的な悪影響をもたらすことが予測される。
中位	公開許可のない個人情報、政府の機密情報又は企業秘密の公開により、機関等の活動や資産、又は利用者に機密性損失の重大な悪影響をもたらすことが予測される。
高位	公開許可のない個人情報、政府の機密情報又は企業秘密の公開により、機関等の活動や資産、又は利用者に致命的又は壊滅的な機密性損失の悪影響をもたらすことが予測される。

「5． 利用者の身の安全に影響を与える 」リスクの影響度

レベル	内容
N/A	リスクがない（想定されない)。
低位	医療措置を必要としない軽症の影響を与える。
中位	軽症が生じる中程度のリスク又は医療措置を必要とする負傷が生じる限定的な影響を与える。
高位	深刻な負傷又は死亡の影響を与える。

「6． 法律に違反する」リスクの影響度

レベル	内容
N/A	リスクがない（想定されない)。
低位	法執行の対象とならないような性質の民事上又は刑事上の法律違反のリスクがある。
中位	法執行の対象となる可能性のある民事上又は刑事上の法律違反のリスクがある。
高位	法執行の計画で､特に重要とされている民事上又は刑事上の法律違反のリスクがある。

2.4. 対象業務一覧の位置づけ

対象業務一覧は、ISMAP-LIU における業務・情報の影響度が低位である蓋然性が高い業務を例示したものである。政府機関等の ISMAP-LIU の利用においては、業務・情報の影響度評価を実施した結果が「低位」である業務に用いることが原則であるが､「対象業務一覧」を例示することでどのような業務が一般的に「低位」であるかを示し、各政府機関等の ISMAP-LIU の利用における判断を支援することを目的としている。

なお､「対象業務一覧」は影響度が低位である蓋然性が高い業務を例示するものであるため、各政府機関等は、SaaS 上で実際に取り扱う具体的な業務を設定し、業務上処理する各種情報に対し、「対象業務一覧」を参考の上、適切な影響度評価を行う必要がある。

2.5. 業務・情報の影響度評価を実施するタイミング

業務･情報の影響度評価は情報システムの調達担当者が、サービス・業務企画を行う際に、業務実施部門及び情報セキュリティ部門と協力して実施することを想定している。

デジタル・ガバメント推進標準ガイドラインではサービス・業務企画を行う際､「現状の把握と分析」を行うこととしており､具体的な実施内容として表 1 のように定めている。特に「1）利用者の把握と分析」､「2）業務の把握と分析」､「3）データの把握と分析」を実施することで､業務･情報の影響度評価を実施する上で必要となる業務における主体や業務の範囲、業務で扱う情報の列挙が可能となる。また､「6）関連調査」においては類似サービスの調査を行うことが定められており、当該分析を実施した上で、総合的な業務・情報の影響度評価の結果が「低位」だと判断した時点で、調達担当者が入札に関連する CSP（クラウドサービスプロバイダ）と連携し、当該 CSP が提供する SaaS が ISMAP-LIU に登録されることで、調達プロセスにおいて、ISMAP-LIU のクラウドサービスリストを活用した調達が可能となる。

表 1　標準ガイドラインが定める「現状の把握と分析」における実施事項

1）利用者の把握と分析 　サービス・業務を利用することで価値や効果を得られる者・組織のそれぞれの規模、拠点、特徴、行動、満足度、要求事項等 2）業務の把握と分析 　サービス・業務の範囲、業務フロー、業務量、実施体制、実施時期・時間、実施場所等 3）データの把握と分析 　業務において取り扱う情報資産の特定及び分析並びに情報システムのデータの一覧、定義、入出力、流れ、取扱量、処理件数、品質、標準の活用状況、保有形態の状況、管理ルール、管理プロセス、オープンデータとしての公開状況 4）既存の情報システムの把握と分析 　既存の情報システムの資料、残存課題等 5）情報システム運用の把握と分析 　情報システムの運用実績、各種指標の状況、残存課題等 6）関連調査 　類似するサービス・業務の存否、取り扱うデータに関する標準化状況、優良事例、失敗事例、その要因等

出典：「デジタル・ガバメント推進標準ガイドライン（令和 3 年 9 月 10 日）」に基づき作成

3.　業務・情報の影響度評価のプロセス

3.1.　業務の特定

業務・情報の影響度評価を行う上でまず始めに行うことは、クラウドサービスで処理する具体的な業務を特定することである。例えば、「E ラーニングを用いた職員教育」や「インターネットを介した国民向けの行政情報発信」、「災害時の職員安否確認」等が考えられる。

なお、特定する業務は調達部門においてどのような業務、及び業務の範囲を想定するかによって異なる。例えば、組織全体に実施する職員教育であれば、「E ラーニングを用いた職員教育」を特定した業務として設定することが考えられるが、個別の課室職員に向けた特定分野の職員教育であれば「E ラーニングを用いた DX リテラシーに係る職員教育」のように、より具体化することも可能である。

3.2.　特定した業務の対象業務一覧への該当性確認

「3.1．業務の特定」において特定した業務が対象業務一覧に該当するかを、「別紙１．対象業務一覧」に照らし合わせて確認する。例えば、前述した「E ラーニングを用いた職員教

育」であれば、「別紙１．対象業務一覧」における「⑦組織構成員に対する組織ルールやビジネススキル等の教育を行う業務」に該当し、「災害時の職員安否確認」であれば、「⑥災害時等に組織構成員の確認等を行う業務」に該当する。

特定した業務が対象業務一覧に該当しない場合も、同様に次ステップ以降に定める手順を実施する。

3.3. 業務・情報の列挙

「3.1. 業務の特定」において特定した業務に関する主体（人物、組織、情報システム等）を列挙する。また、業務内容を細分化しておくと後の作業が進めやすくなる上、主体の列挙漏れにも気づきやすい。

細分化に当たっては、対象とする業務領域における特有の業務イベント（特定の時期や要因により発生する業務等）を列挙すると、重要な業務の気づきにつながるため有効である。

また、昨今の SaaS には多種多様な機能を持つものも少なくないため、当該業務を処理しようとする SaaS の機能について、SaaS を提供する CSP にも確認しながら、業務内容の細分化を進めることが望ましい。特に、メッセージ機能やファイル共有機能は、意図しない形での情報の拡散につながることもあるため、それらの機能の有無は確認した方が良い。

次に、列挙した業務に関する主体ごとに、「業務内容の概要」を明文化し、「業務で取り扱う情報」を列挙する。この際、業務において「どのような（誰の）情報が、どこ（誰）から、どこ（誰）に流れるのか」を意識して検討すると、情報の漏れに気がつきやすい。

ここまでの検討の過程や、SaaS に関する市場調査を進めた結果、業務内容や主体の細分化や追加の必要性に気がつく場合があるため、そのような場合は本節に定めるプロセスを一から繰り返し実施する。

留意事項

- 業務・情報の列挙を行う中で洗い出した特定の情報について、業務の中で必要であったとしても、SaaS 上で取り扱わない場合が考えられる。その場合、当該情報については影響度評価の対象とする必要は無い。
- 当該 SaaS にログインするための認証情報について、その影響度は当該 SaaS 上で取り扱う他の情報の影響度に従うものと考えられる。例えば SaaS 上取り扱う業務・情報が無い場合においては、SaaS のログイン情報が侵害された場合の影響は無く[1]、一方、厳格な秘匿が求められ、影響度が高位である情報を SaaS 上で取り扱う場合においてはそのログイン情報の影響度も高位となることと考えられる。このため、基本的には業務内

[1] 一般に、SaaS 等 WEB サービスのログイン情報の侵害に関して、リスト型攻撃による脅威が考えられるが、本脅威に対するセキュリティ上の影響度は個々の利用者のパスワード管理方法に大きく左右されるものであり、組織としての一律的な評価は困難である。

容に基づき列挙した情報について影響度評価を実施すればよく、当該 SaaS にログインするための認証情報については、特段の事情により個別に評価する必要がある場合を除き、影響度評価の対象とする必要は無い。

表 2　業務・情報の列挙の例

業務（「3.1 業務の特定」にて特定した業務を記載）				
E ラーニングを用いた職員教育				
主体	**業務種別**	**業務内容**	**業務内容の概要**	**業務で取り扱う情報**
教育担当者	教育コンテンツの提供	利用登録の承認	利用登録情報の確認を行い、承認する	職員の氏名・メールアドレス
		コンテンツ登録・削除	教育コンテンツの登録、削除を行う	行政官に対する一般的な教育コンテンツ
		意見・コメントに対する回答	受講生からの意見・コメントに対して回答する	「意見」「コメント」（タイトル、本文、投稿者、投稿日時）
受講生	教育コンテンツの受講	利用登録の承認	氏名・メールアドレスを登録して、サービスの利用資格を得る	職員の氏名・メールアドレス
		コンテンツの閲覧	登録されている教育コンテンツを閲覧し、履修する	行政官に対する一般的な教育コンテンツ
		意見・コメントの投稿	教育コンテンツに対する意見・コメントを投稿する	「意見」「コメント」（タイトル、本文、投稿者、投稿日時）

3.4. SaaS に関するセキュリティに係る要件の確認

ISMAP-LIU では、調達担当者が業務・情報の影響度評価を行う上での参考情報として、CSP に対してセキュリティに係る情報の提供を求めている。具体的には「①SLA/SLO」、「②サーバの所在地並びにデータの保存場所」、「③外部サービスの利用とその ISMAP 登録有無」、「④提供されているセキュリティの機能」である。

調達担当者はこれらの情報を踏まえつつ、次節に定める「業務・情報の影響度評価の実施」を行うこととなる。これらのセキュリティに係る情報は、例えば次のような判断に利用できる。

「①SLA/SLO」

サービスの稼働率が業務上許容して差し支えない範囲に収まっているのかどうかを判断する。例えば、可用性が極めて重要な情報システムにおいてサービスの稼働率が業務上許容できない場合、影響度評価において可用性の評価結果が「中位」「高位」となると考えられる。ただし、SLA/SLO は同一の SaaS であっても、契約プランや機能ごとに一様でない場合があるため留意する。

「②サーバの所在地並びにデータの保存場所」

個人情報を扱う場合であって、かつ国内のデータセンターが選択できない場合に、機密性・完全性の影響度を「中位」「高位」とする等も考えられる。

「③利用している他のクラウドサービスとその ISMAP 登録有無」

利用する SaaS が基盤部分として他の CSP が提供する IaaS/PaaS を利用している場合、当該 IaaS/PaaS のセキュリティ対策について ISMAP を利用して確認できるのかどうかの判断が可能である。

「④提供されているセキュリティ機能」

ISMAP 管理基準のうち、管理策自体が基本言明要件である管理策の中から、セキュリティの機能に係る管理策を選定したものである。本来、ISMAP-LIU に登録済みの SaaS であれば、監査を通じて当該セキュリティ要件を満たしていることが確認されているが、ISMAP-LIU に未登録の段階においては必ずしも SaaS が当該セキュリティ要件を満たしているとはいえないため、基本的なセキュリティ機能を SaaS が具備していることを確認するために定めている。

3.5. 業務・情報の影響度評価の実施

「3.3. 業務・情報の列挙」で洗い出した各情報について影響度を評価する。具体的には、情報毎に、SaaS の利用において想定されるリスク①～⑥のそれぞれに対し、影響度を「業務・情報の影響度評価基準」に従って導出する。影響度の導出にあたっては、機密性が侵害された場合のみでなく、完全性、可用性が侵害された際の影響についても考慮して評価を行う。

例えば、行政職員の教育を目的とした E ラーニングにおいて、職員の氏名・メールアド

レスについて「①国民に不便、苦痛を与える、又は機関等が信頼を失う」リスクに関し機密性・完全性・可用性が侵害された場合の影響度が「限定的かつ短期間の不便や苦痛又は、機関等の地位や評判に対し軽微な影響がある。」場合、「①国民に不便、苦痛を与える、又は機関等が信頼を失う」リスクの影響度は「低位」だといえる。

また、列挙した情報について扱う情報の数量について考慮が必要な場合においては、数量を踏まえた影響度評価を実施する。

「業務・情報の洗い出し」で洗い出した各情報について、「業務・情報の影響度評価基準」で定める各リスクに対する影響度評価の結果を導出する際は、各リスクに対して判断した影響度の中で最も高位のレベルを採用する。

例えば、特定の情報に対して影響度評価を実施した結果として、表３を得たとする。この場合、①、②、④、⑤、⑥のリスクに対する影響評価は「低位」であるが、③のリスクに対する影響度評価は「中位」であることから、特定の情報に対する影響度評価の結果は「中位」だと判断される。

表 3　特定の情報に対する影響度評価の例

（記載は、影響度判定を含めて例示）

情報の例）　職員の氏名・メールアドレス	影響度
①　国民に不便、苦痛を与える、又は機関等が信頼を失う	低位
②　利用者に金銭的被害や賠償責任が生じるなど、財務上の影響を与える	低位
③　機関等の活動計画や公共の利益に対して影響を与える	中位 （情報の量が多いため）
④　個人情報等の機微な情報が漏洩する	低位
⑤　利用者のみの安全に影響を与える	低位
⑥　法律に違反する	低位

→ 全体として、「中位」と判断されることになる。

次に、各情報に対して判断した影響度評価の結果について、客観的にその判断が適切であることが分かるよう、「評価における考え方」を記載する。

このようにして、情報ごとに各リスクに対する影響度評価を実施することで、「業務・情報の列挙」において作成した表２に対して表４で示すような結果を得ることが可能となる。

表 4　列挙した情報に対する影響度評価の例

（記載は、影響度判定を含めて例示）

業務（「3.1 業務の特定」にて特定した業務を記載）			
E ラーニングを用いた職員教育			
主体	**業務で取り扱う情報**	**影響度**	**評価における考え方**
教育担当者	職員の氏名・メールアドレス	低位	職員情報として極めて限定的な情報を扱い、かつ当該情報については機微性が低いと考えられるため
	行政官に対する一般的な教育コンテンツ	低位	一般職員に対する教育を実施するものであり、機微な情報の取り扱わないため
	「意見」「コメント」（タイトル、本文、投稿者、投稿日時）	低位	教育コンテンツは機微性が低く、それに伴う意見やコメントについても機微性が低いと想定されるため
受講生	職員の氏名・メールアドレス	低位	同上
	行政官に対する一般的な教育コンテンツ	低位	同上
	「意見」「コメント」（タイトル、本文、投稿者、投稿日時）	低位	同上

留意事項

- 情報の種類によっては、単体では影響度が低位であるが、同種の情報が多数集約することで高位の影響度となるものが存在することに留意すること。例えば、特定の情報が集約することで傾向やパターン、計画などが明らかになる場合や、他の重要な情報へのアクセスが可能になる場合があり、列挙した情報の影響度の判定においては、取り扱う情報の量についても考慮すること。

3.6.　総合的な業務・情報の影響度評価の実施

「3.5 業務・情報の影響度評価の実施」において列挙した各情報に対する影響度のうち、原則、最も高位の影響度を「3.1 業務の特定」において特定した業務に対する総合的な影響度とする。

特定の情報において影響度が「中位」「高位」であった場合でも、当該情報を匿名化の上、クラウドサービス上で取り扱うなど、特段の理由により総合的な業務・情報の影響度評価の結果を「低位」だと判断する場合は、その理由を客観的にその判断が適切だと分かるように記載する。

3.7.　業務・情報の影響度評価結果に対する確認

業務・情報の影響度評価は業務要件と密接に関連していることから、基本的には調達部門が主導で行うものだと想定されるが、最終的に得た評価結果については調達部門と情報セキュリティ部門の両名で確認を行い、内容の妥当性を判断する。

確認の結果、問題ないと判断された場合は、「様式 1-2　SaaS の利用に係る業務・情報の影響度評価シート」の確認欄に、調達部門、情報セキュリティ部門の責任者両名が署名する。問題があると判断された場合は、SaaS 上で扱う業務・情報を見直す等の対応が必要となる。

3.8.　業務・情報の影響度評価の継続的モニタリング

業務やクラウドサービスを取り巻く環境の変化に伴い、クラウドサービス上で処理する業務・情報についても時間とともに変化していくと想定される。そのため ISMAP-LIU の利用に当たり、業務・情報の影響度評価は単発的に行えば良いものではなく、継続的に行うことが重要となる。

そのため、ISMAP-LIU を利用して調達した SaaS については、影響度評価の対象とした業務・情報のみが扱われているかどうか等を定期的に確認する必要がある。具体的には、当該 SaaS の利用開始から 1 年ごとに、各政府機関等の情報セキュリティ部門において、SaaS の利用が業務・情報の影響度評価を実施した際に記載した範囲を超えて利用されていないかどうかを確認する。

SaaS の利用実態が前年に実施、確認した業務・情報の影響度評価において記載した業務・情報と異なる場合は、情報セキュリティ部門は調達部門と協力しながら新たに業務・情報の影響度評価を実施し総合的な業務・情報の影響度評価結果が「低位」であることを確認する。新たに実施した業務・情報の影響度評価の結果が「低位」でない場合は、適切な利用方法について調達部門・業務実施部門に対し是正を求める。是正が困難な場合は、CSP に対して ISMAP-LIU ではなく、ISMAP の取得を求めることなどが必要となる。

別紙１．対象業務一覧

対象業務一覧として類型①～⑧を下記のとおり示す。また、各類型において、想定されるサービス例、具体的な業務の例及び取り扱う情報の例を示すとともに、各類型の考え方を説明する。

なお、対象業務一覧は制度運用の中で見直しを行い、必要に応じて拡充していくことを予定している。

① 公表を前提とした政策・制度の立案・調整過程等で民間と連携して作業する業務

（想定されるサービス例）

Web 会議サービス

ファイル共有サービス

（具体的な業務例）

民間企業・団体の有識者を招いた会議体の運営に伴う Web 会議の開催・運用業務

民間企業・団体の有識者を招いた会議体の運営に伴う会議資料等の管理業務

（取り扱う情報の例）

外部に公開する会議の動画・音声、会議資料、会議参加者の氏名、議事録など[2]

（考え方）

公表を前提とした政策・制度の立案・調整過程等で民間と連携して作業する業務は、立案中の政策・制度に係る会議資料等の情報や会議に伴う政策・制度に対する意見や質問等のほか、会議参加者の所属組織名や氏名等の情報を扱うことが想定される。通常、当該業務で扱う情報が侵害された場合の影響は限定的あるいは軽微であり、影響度が「低位」である蓋然性が高いものと考えることができる。

なお、公表を前提とした政策・制度の立案・調整過程等において民間と連携をしない場合においても、影響度が「低位」である情報を扱うケースは考えられるが、情報の影響度に応じた SaaS サービスの使い分けは通常想定されない。例えば、政府機関等内での政策・制度の立案・調整過程等で Web 会議サービスを用いる場合、各政府機関等で

[2]非公開とされる情報が含まれる場合、会議参加者などの情報が含まれる場合は参加者に公開される旨の合意がとれていない場合、クラウドサービス利用時点で上記の情報が侵害された場合に影響が限定的あるいは軽微であるといえない場合については、影響度評価の際に留意が必要。

調達した標準のサービスを用いるのが通常であり、扱われる情報に応じてサービスを使い分けるケースは想定することが難しい。そのため政府機関等が組織内で政策・制度の立案・調整過程で用いる SaaS は ISMAP-LIU ではなく ISMAP を登録したクラウドサービスで処理することが妥当である。他方、民間との連携作業においては必ずしも民間が ISMAP 登録済みの SaaS を利用可能とは限らないため、本対象業務においては、その対象を民間との連携に限定している。

② 政府機関等職員の業務上の役職・氏名等情報を扱う業務

（想定されるサービス例）
人事管理サービス
タレントマネジメントサービス
採用管理サービス

（具体的な業務例）
政府機関等における人員の管理業務
政府機関等における人員の配置や能力の識別業務
政府職員の職員募集・採用に係る業務

（取り扱う情報の例）
職員の労務情報、職員の人事異動履歴、現所属、保有する資格等に関する情報、求職者の履歴情報、職務記述書、選考情報[3]

（考え方）
政府機関等の職員の業務上の役職・氏名等の情報を扱う業務として、組織の人員管理や職員募集・採用に関連する業務が考えられる。

組織の人員管理に関連する業務は、職員の労務、職位、経歴、配員や能力等に係る情報を扱うことが考えられる。通常、当該業務で扱う情報が侵害された場合の影響は限定的あるいは軽微であり、影響度が「低位」である蓋然性が高いものと考えることができる。

また、職員募集・採用に係る業務は、求職者の経歴、職務記述書、選考情報等の情報を扱うことが考えられる。通常、当該業務で扱う情報が侵害された場合の影響は限定的あるいは軽微であり、影響度が「低位」である蓋然性が高いものと考えることができる。

その他、他の対象業務の類型において、ユーザ登録や管理等を行う上で政府機関等の職員の業務上の役職・氏名等の情報を扱う事が考えられる。例えば、「⑦組織構成員に対する組織ルールやビジネススキル等の教育を行う業務」においてＥラーニングを用いた職員教育を行う場合、受講職員の登録管理に当該職員の役職や氏名等を扱うことが考えられ、このようなユースケースにおいても、影響度が「低位」である蓋然性は高い。

[3] 国民一般や職員のプライベートな情報や機微な情報が含まれている場合、公示前の人事情報が含まれている場合、選考基準など公正さの観点から秘匿すべき情報が含まれている場合、業務の性質上厳格な秘匿が求められる職員の情報が含まれている場合については、影響度評価の際に留意が必要。

③ 名刺情報等の一般に広く提供する範囲の情報、公開情報の配信に伴う配信先等管理情報を扱う業務

（想定されるサービス例）
クラウド型名刺管理サービス
クラウド型映像・コンテンツ等配信サービス

（具体的な業務例）
企業名、役職、氏名等の名刺情報を登録・管理する業務
政府機関等の顧客に対する映像・コンテンツ等の配信に伴う配信先の特定を目的とした情報の登録・管理業務

（取り扱う情報の例）
名刺に記載されている情報（氏名、勤務地所在地、電話番号、メールアドレス等）、公開情報の配信のために必要となる情報（配信先を特定するための識別子等）

（考え方）
名刺に記載される情報は名刺の性質上、一般に広く提供する範囲の情報（所属組織名、氏名、役職、連絡先）である。そのため、名刺に記載される情報が侵害された場合の影響は限定的あるいは軽微であり、影響度が「低位」である蓋然性が高いものと考えることができる。
また、政府機関等の顧客に対する映像・コンテンツ等の情報の配信に係る業務の一部において、配信先利用者を特定するための情報を取り扱うことが想定される。通常、これらの情報が侵害された場合の影響は限定的あるいは軽微であり、影響度が「低位」である蓋然性が高いものと考えることができる。

④ 民間から提供される情報であり、当該情報提供者が低リスクだと判断している情報を処理する業務

（想定されるサービス例）
Web 会議サービス
ファイル共有サービス

（具体的な業務例）
民間企業・団体からの情報を受信・管理する業務
民間企業・団体が主催する会議等に参画する業務

（取り扱う情報の例）
民間企業が外部に公開する会議の動画・音声、会議資料、会議参加者の氏名、議事録など

（考え方）
民間から提供される情報であり、当該情報提供者が低リスクだと判断している情報を処理する業務は、民間が保有する特定のサービスや技術に係る情報や、民間における経営戦略等の中長期計画、政策に対する提言や改善要望等が想定される。当該情報について、外部に公開することを前提にしているなど、民間において低リスクだと判断している情報については、侵害された場合の影響は限定的あるいは軽微であり、影響度が「低位」である蓋然性が高いものと考えることができる。

なお、政府機関等間における情報の授受を行う業務においても、影響度が「低位」である情報を扱うケースは考えられるが、情報の影響度に応じた SaaS サービスの使い分けは通常想定されない。例えば、政府機関等間の情報の授受において Web 会議サービスを用いる場合、通常は各政府機関等で調達した標準のサービスを用いるのが通常であり、扱われる情報に応じてサービスを使い分けるケースは想定することが難しい。そのため政府機関等間における情報の授受を行う業務は ISMAP-LIU ではなく ISMAP を登録したクラウドサービスで処理することが妥当である。他方、民間から情報提供を受ける際は必ずしも民間が ISMAP 登録済みの SaaS を利用可能とは限らないため、本対象業務においては、その対象を民間から情報提供を受ける場合に限定している。

⑤ オープンソース・公知の事実・一般公開情報を扱う業務だが例外的に要機密扱いとする必要がある場合

（具体的な業務例）

オープンソース化したソフトウェアの開発業務
Web サイト上のコンテンツ管理業務
公開されている政策情報や技術情報等の翻訳業務
パブリックコメントの募集・及び回答業務
アンケートの作成・管理・回答業務

（想定されるサービス例）

ソースコード管理サービス
CMS（Contents Management System）サービス
自動翻訳サービス
Web アンケートサービス

（取り扱う情報の例）

オープンソースソフトウェアのソースコード、各省のホームページに公開する予定の情報[4]、海外の公開情報などの各省が入力した翻訳したい文書の情報[5]、各省が実施するアンケートの内容や結果に関する情報[6]、

（考え方）

一般に、オープンソース・公知の事実・一般公開情報は機密性 1 情報と整理されているところ、例外的に一部の情報が要機密扱いと判断される場合がある。例えば、オープンソースソフトウェアの開発業務においては、個々のオープンソースソフトウェアのソースコードやそれに付随する設計書などは広く公開される情報である一方、機関のオープンソースソフトウェアプロジェクトに対する貢献戦略や金銭的支援計画、プロジェクト計画等の情報は要機密扱いとなることが想定される。当該要機密情報が侵害された場

[4] 株式市場に影響を与える情報など、公開のタイミングを厳格に管理する必要がある情報を扱う場合については、影響度評価の際に留意が必要。
[5] 翻訳したい文書の内容や、その文書を入力したという事実そのものが漏洩した場合に影響が軽微でないと考えられる場合については、影響度評価の際に留意が必要。
[6] 個人情報（氏名、住所、年齢等）が含まれる場合や、アンケートの内容が漏洩した場合の影響が軽微でないと考えられる場合については、影響度評価の際に留意が必要。

合の影響は限定的あるいは軽微である場合、影響度が「低位」である蓋然性が高いものと考えることができる。

また、公知の事実・一般公開情報を扱う業務として、Web サイト上でのコンテンツ管理業務が考えられる。通常、Web サイト上のコンテンツは政府公式情報等、公開を意図する情報である。だが、厳密には Web サイトにおいて当該情報が公開される瞬間より前の段階では公開情報ではないと考えられる。しかし、Web サイトにおける公開前の情報は、既に公開されることが意思決定されている情報であると考えられ、侵害された場合の影響は限定的あるいは軽微であり、影響度が「低位」である蓋然性が高いものと考えることができる。

その他にも、公知の事実・一般公開情報を扱う業務として、一般に公開されている情報の翻訳業務が考えられる。この場合、公知の事実・一般公開情報は要機密ではない情報であるが、当該情報を翻訳したという事実そのものが要機密となる場合は考えられる。しかし、通常、インターネットを通じて当該情報にアクセスした時点で当該事実はアクセスログ等から明らかである。そのため、当該の事実が要機密であっても侵害された場合の影響は限定的あるいは軽微であり、影響度が「低位」である蓋然性が高いものと考えることができる。

当該類型においては上記に挙げた業務例の他にも適用されうると考えられる。その場合、例外的に要機密扱いとする必要がある要素に対して、その特性を踏まえた上で当該類型に該当するか判断を行う必要がある。

⑥ 災害時等に組織構成員の被災状況確認等を行う業務

（想定されるサービス例）
安否確認サービス

（具体的な業務例）
災害時等の政府職員の連絡先等を管理する業務
災害時に政府職員の被災状況の管理を行う業務

（取り扱う情報の例）
職員の氏名・メールアドレス等、災害時の職員の安否情報[7]

（考え方）
「政府職員の業務上の役職・氏名等情報を扱う業務」については既に対象業務一覧として例示している。また災害発生時における政府職員の被災状況等の情報が侵害された場合の影響は限定的あるいは軽微であり、影響度が「低位」である蓋然性が高いものと考えることができる。

（留意点）
ISMAP の管理策基準は基本的に機密性に関するセキュリティ対策に重点を置いているが、災害時の被災状況確認等を行う業務においては、完全性や可用性が重要となる。そのため、当該業務に用いる SaaS を利用する際、完全性や可用性に係るサービス側の水準が業務要件に適合しているかは、別途確認することが重要である。例えば、極めて緊急性、網羅性の高い部署において安否確認サービス等を利用する場合においては、サービスの SLA も踏まえ影響度を「高位」、「中位」と判断するケースが考えられる。

[7] 国家安全保障、治安維持に係る業務等、業務の性質上厳格な秘匿が求められる職員の情報を取り扱う場合、職員のプライバシー情報や機微情報が含まれる場合、安否確認そのものが漏洩した場合に影響が軽微でないと考えられる場合については、影響度評価の際に留意が必要。

⑦ 組織構成員に対する組織ルールやビジネススキル等の教育を行う業務

（想定されるサービス例）
e-ラーニングサービス

（具体的な業務例）
組織の規定やルール、周知事項に関して政府職員に対して教育教材を提供する業務
人材育成やキャリアアップを行うための一般的なビジネススキル等を提供する業務

（取り扱う情報の例）
外部に公開可能な職員への学習コンテンツ、受講する職員の氏名等、学習結果に関する情報[8]

（考え方）
組織構成員に対する組織ルールやビジネススキル等の教育を行う業務は、組織ルールやビジネススキル等に係る一般的な学習コンテンツや受講する職員の氏名等情報、学習結果に関する情報を扱う事が想定される。通常、これらの情報が侵害された場合の影響は限定的あるいは軽微であり、影響度が「低位」である蓋然性が高いものと考えることができる。

[8] 機密性の高い情報を教材として扱う場合については、影響度評価の際に留意が必要。

⑧ 「行政文書の管理に関するガイドライン」において保存期間１年未満に該当するもののうち、定型的・日常的な業務連絡等を扱う業務

（具体的な業務例）
政府機関等の掌握事務に対する事実関係の問合せへの応答業務

（取り扱う情報の例）
政府機関等の掌握事務に対する事実、当該事実に対する問合せに係る情報

（想定されるサービス例）
チャットボットサービス

（考え方）
「行政文書の管理に関するガイドライン」において保存期間１年未満に該当するものは重要度の低い行政文書であると考えられる。そのため、「行政文書の管理に関するガイドライン」において保存期間１年未満に該当するものには、情報が侵害された場合の影響が限定的あるいは軽微であり、影響度が「低位」である蓋然性が高いものが含まれていると考えられる。
例えば、当該ガイドラインに定められている「○○省の掌握事務の事実関係の問い合わせへの応答」については、その内容が広く国民に開示されることが原則であると考えられるため、影響度が「低位」である蓋然性が高いと考えられる。

（留意事項）
「行政文書の管理に関するガイドライン」において保存期間１年未満に該当するもののうち、上記に挙げた以外にも対象業務であると考えられるケースは存在すると考えられるが、重要度の低い文書であっても扱う業務の内容に応じては機微な文書である場合が想定されるため、影響度評価の際に留意が必要となる。