■「ISMAP-LIUクラウドサービス登録規則（案）」等に対する意見募集について　御意見に対する回答

| 項番 | 御意見 | 御意見に対する回答 |
|---|---|---|
| 1 | 平素おせわになります。<br>今般の意見募集について、下記申し上げます。<br><br>1.まず、本件のみならずこういった重要な案件につき、「毎回”こっそり”やりましたという、アリバイ作り」としか思えないやり方を止めるべきです。一体誰がこのサイトを普段から見ますか？当方がこれを見たのは本当に偶々です。異常な短期間に加えて資料はたくさんあり、そういった状況から見てもアリバイ作りとしか映りません。<br><br>2.当案件の適用省庁はいずれも省庁の中でも重要な組織であり、１つもセキュリティを甘くしてよい所はありません。それ処が現時点においても度々情報漏洩するなど、教育含めて極めてセキュリティが甘い状況です。不適切かつ安易な考えは捨てるべきです。<br><br>3.2.のような状況に加えて、外部監査を甘くし、３年かけて内部監査をするなど最早何もしないと言っているのと同然です。誰が責任を負うのかも言及なし、即刻案件ごと撤回すべきであり、自らの職分が何であるか自戒する所からやり直してください。<br><br>最後に、これを了承した人物は職に不適当であり、即刻辞職ないしは解雇すべきです。国たる責任も理解できない者が座してよい場所ではありません。<br><br>以上です。 | ISMAP-LIUにおける各種規定等の案への御意見ではないと理解致しますが、御意見は拝聴いたしました。 |
| 2 | ガバメントクラウドを見据えたISMAP-LIUかと思いますが、クラウド技術仕様、機能面だけでなく下記の観点も重要かと思います。<br>「想定外を想定する」という教訓を東日本大震災で学びましたよね？<br>1. 地政学的な安定性、安全性<br>　クラウドといっても物理的にどこかに構築せねばならず、国政の基幹システムを海外に置くのはあり得ない。ネットワークの破壊や妨害などにより機能不全に陥ることは十分にある。<br><br>2. 法的な安定性、安全性<br>　いわゆる米国のクラウド法などのリスク・影響範囲から及ばないクラウドであることもまた重要。<br>3. 将来的に政治的に守られており、安全で安定していること<br>　同盟国といえども、トランプのような人がトップになることもある。他国の政治力の干渉範囲外に置くこともまた重要。<br>以上の３つは確保は必須条件で、確保したうえで次の技術的な仕様を検討できると考えます。技術的にいかに優れていようとも、上記の３つの一つでも崩れることはシステムの根幹以上に国として危うくなります。<br>ということで、クラウドは国産であることは必須で、国外からの技術支援は許容する方針になると考えます。 | 1. に関して、クラウドサービスの利用の在り方に関する政府決定文「政府情報システムにおけるクラウドサービスの利用に係る基本方針（令和３年３月30日各府省情報化統括責任者（CIO）連絡会議決定）」において、我が国の法律及び締結された条約が適用される国内データセンタと我が国に裁判管轄権があるクラウドサービスを採用候補とするものとする旨記載しているところであり、政府機関等においては本方針に基づいた調達・選定が行われているものと理解しております。<br><br>2.,3.に関して、ISMAPにおいては、ISMAPクラウドサービス登録規則3.4（2）において、「クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用され、 調達府省庁等が意図しないまま当該調達府省庁等 の管理する情報にアクセスされ又は処理されるリスクについて、ISMAP運営委員会及び当該省庁等がリスク評価を行うために必要な情報」の提供を求めており、国外の法令等のリスク判断が可能な枠組みとなっております。 |
| 3 | ・ISMAP-LIUのコンセプトには賛成。適切に運用されれば日本のガバメントクラウドのマーケットや競争力向上に大きく貢献するポテンシャルを秘めていると思う。<br><br>・見る限りかなりチェックリストが多くそれなりに参入障壁が高い印象。<br>・既にISMAP自体がその参入コストの大きさから大手SI企業がメインとなり既得権益化してしまっているので、AWS/GCP以外は日系の新規事業者が参入できないという本末転倒な状況になっているので、ISMAP-LIUの敷居はどんどん下げた方が良い。<br>・今回の案件でも、ISMAP-LIUの適用範囲が限定されてしまい、結局は大手SI（またはそのグループ会社）の牙城になり、ベンダーロックインの懸念が全く解消されないのでないかという点が非常に心配。<br><br>・「Low Impact」の定義が重要になると思う。領域といっても、どうしてもSaaSの中に部分的に個人情報や機密情報が含まれることはある。それらをいちいちしらみつぶしにしていたら、コストが跳ね上がってしまい、この運用自体に意味がなくなってしまう。<br>・こういったグレーゾに対して政府側の個別判断の要素が大きすぎるので、もっと判定基準を明示的にしてもらわないと、申請する側としてはリスクが大きい。<br>・初期に厳格に審査して承認率を下げる運用も、最初は門戸を広げてSaaSの承認率を上げつつ、問題が発生すれば早めに承認を取り消す、といった帰納法的な運用の方が良いのでは。ちょっと入り口はとにかく広げた方が良い。<br><br>・Low Impactかどうかもあるが、本質的には、Low-Impactかどうかよりも、安全保障上の懸念のある国の企業が出資する法人や外資などがSaaSを運用することのリスクを懸念すべきと思う。<br>・通常の民間企業であれば外資の参入はWelcomeでも、やはり日本政府に関わるSaaSなのであれば、日本のスタートアップに門戸を開いてほしい。 | 参入障壁について、ISMAP-LIUの設計においては、ガバナンス・マネジメント基準は全量を対象としつつも、管理策基準の外部監査対象はサービス基盤・構成に直接的な影響を及ぼし得る管理策（一部の重要な管理策）を主な対象に数年に平準化しつつ実施することで、全体として外部監査対象範囲を縮小しており、また、内部監査の実施状況報告を3年で一巡することによって、監査全体としては現行ISMAPよりも緩やかな制度設計となっております。<br>「Low Impact」の定義について、ISMAP-LIUは「SaaSの中でも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」を対象としており、この該当性の判断基準として、参考資料「ISMAP-LIUクラウドサービス登録規則（案）の別紙１」にございますように利用省庁における影響度評価結果が低位となる条件の基準を明示しております。<br>また、利用省庁等の影響度評価によって当該定義に該当することが確認されたサービスについては、ISMAP-LIUへの申請が可能な枠組みとしており、ベンダーロックイン等の可能性も十分低減されているものと考えております。<br>加えて、取消・公表制度を用いることで、帰納的な制度運用も考慮に入れ、制度設計に努めております。 |
| 4 | ・ISMAP-LIUにおける監査業務を行う監査機関は決められているか。決められていればその対象機関はどこになるか。<br><br>・ISMAP-LIUは従来のISMAPと比較して監査範囲はどこまで縮小されるのか。ISMAPでかかるコストと比較して、監査費用など何割くらい削減できるか知りたい。<br><br>・ISMAP-LIUの適用範囲は「利用省庁等」などの記載があるが、具体的な対象となる利用機関はどこか。今後、自治体や独法が対象となるか。なるとすればいつ頃から対象となるか。<br><br>・対象業務一覧に8個の対象業務が定義されているが、これが拡大される予定はあるか。<br><br>・ISMAP-LIUの適用が「該当性なし」とされる業務は具体的にどういった業務が該当するか。具体的な例などはあるか。 | ・ISMAP-LIUにおける監査機関について、ISMAPと同様であり、現時点において、ISMAPポータルサイトに掲載されている監査機関リストに登録されている機関によって監査業務を実施いただく想定をしております。<br><br>・ISMAP-LIUにおける監査範囲、監査費用について、ISMAPの外部監査は、ISMAP監査機関とCSPによる民民の契約によって実施されるため、費用負担がどの程度軽減されるか一概には言えないものの、外部監査において対応すべき管理策数は現行ISMAPの概ね1/5程度になると想定しております。したがって、外部監査に係る業務量及びコストについても、相応の削減が見込まれるものと考えております。<br><br>・制度の適用範囲について、ISMAP、ISMAP-LIUともに、サイバーセキュリティ基本法に定める国の行政機関、独立行政法人及び指定法人を対象としております。<br>また、自治体等を対象にする想定は現在ございません。<br><br>・対象業務一覧について、今後、ISMAP-LIUの事前申請を通して蓄積される「業務・情報の影響度評価」の内容・傾向をふまえ、拡充していくことを検討しております。<br><br>・ISMAP-LIUの適用に当たり「該当性なし」とされる業務について、典型的には、用途を限定しない形でのWeb会議の開催やファイルの保管・管理を行う業務については、SaaSの利用に係わる影響度評価の結果が低位と評価される可能性は低いと想定され、ISMAP-LIUに該当しないものと考えております。 |

| | | |
|---|---|---|
| 5 | ISMAP-LIUの策定および意見募集感謝します。意見が2点ございます。<br>1)「ISMAP-LIU クラウドサービス登録規則(案)」及び既存の各種規程等について英語（および必要に応じて他の言語）を併記するべき<br>2)意見の内容について、今後検討していくものがあると予想されるが、その後の実施状況についてISMAPサイトなどで随時確認できるようにして欲しい<br><br>1)ですが、ISMAP/ISMAP-LIUの基となる「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組み」を読むに、正しいクラウドサービスを選択することによって、コスト削減や情報システムの迅速な整備などの利点が期待できる一方で、不十分な情報セキュリティ管理基準を持つサービスが選定された場合のリスクを低減するためにISMAP/ISMAP-LIUは規定されるべきものと理解します。<br>つまり、あくまでクラウドサービスを導入する政府機関のために策定されるべき規則であると解釈されます。<br>一方で、ソフトウェア、特に今回の対象となるようなSaaSサービスにおいては、日本企業のみならずグローバル企業から有用性の高いサービスが多く提供されており、一般的な機能やシェアにおいて日本企業のサービスを上回るケースが多く見受けられます。<br>ここで、グローバル企業においてもFedRAMPやIRAPなど各国規定に準拠できる高い運用セキュリティを確保していたとしても、運用担当者や運用責任者、ならびに経営層が日本語を解するメンバーで構成されているケースは多くないと考えられます。これは、日本にも法人を持ち日本語を用いて事業を行っているグローバル企業においても同様です。<br>しかしながら、ISMAP-LIUおよびISMAPの規定やISMAPポータルサイトのコンテンツが日本語でのみ提供されていることで、運用責任者や経営層が日本語を解さない企業にとっては非関税障壁となってしまい、経営判断や準拠作業に遅れが生じたり、結果として見送りになるリスクがあると考えられます。<br>ISMAP/ISMAP-LIUが上述したように（日本のベンダーを守るために規定されたものではなく）導入する政府機関のために作られていることを考えると、有用性が高く適切なセキュリティレベルで運用されるサービスの準拠が促進されることが好ましく、ISMAPの制度所管省庁においても英語を解する担当者を増やし、英語（および必要に応じて他の言語）での規定等の対訳など情報提供を積極的に行うべきだと考えます。<br><br>2)ですが、おととしのISMAPに対する意見についての考え方を拝見しますと、規定の誤りなどすぐに修正したものや、意見として承ったが追加の対応はしない旨返答されているもののほかに、今後検討する、と回答されているものが複数見られます。<br>https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000202723<br>1)で意見させていただいた英語の情報提供についても、#61や#184で類似のコメントがなされており、今後検討する旨の回答がついています。今回の意見募集においても、そのようなケースはあると考えます。<br>これらにつきまして、ISMAPポータルサイトなどにて、項目ごとに、検討の進捗状況や、対応しない旨決定した、などを確認できるようにてはいかがでしょうか。意見をしても対応されるものと対応されないものがあるのは理解できますが、検討する、といってその後どういう状況なのかわからないまま、またLIUの意見募集がなされている、という状況を見ると、これらの意見を寄せた方はどう思われるでしょうか。<br>ISMAP/ISMAP-LIUの制度所轄官庁や対応の事業者は基本的なITツールを使う知識があると考えられますので、いわゆるイシュートラッカーのようなシステムを導入して随時状況を閲覧できるようになっているとよろしいかと思いますがいかがでしょうか。<br><br>以上、ご検討いただければ幸いです。 | 主要な制度規程については、参考英訳を作成し、ISMAPポータルサイト上で提供しております。<br>https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010301<br>ISMAP-LIUクラウドサービス登録規則についても、参考英訳を追って提供する予定です。<br><br>パブリックコメントでいただいた御意見につきましては、最終的な決定における参考とさせていただくものです。いただいた御意見についての個別の回答はいたしかねます。なお、制度規程の改訂や運用の改善・見直し等の最新の情報は、引き続きISMAPポータルサイト上で公開します。 |
| 6 | 1.ISMAP基本規程の「5.4 登録の一時停止又は削除」<br>情報セキュリティインシデントが発生した場合に行われる「登録の一時停止」は、ISMAP-LIUクラウドサービスと、ISMAPクラウドサービスの両方にて行われるとの理解でよいか。<br><br>2.ISMAP-LIUクラウドサービス登録規則（案）の5.3及び5.4<br>登録規則（案）5.3の「ただし、5.1（1）の対象業務一覧に該当しない場合は、各年度の上半期、下半期の期間中になされた事前申請について、原則として各半期末日の3 か月後までに一括してISMAP-LIU の該当性有無を判断する。」とは、以下のいずれの意味か？　いずれか判断しかねる表現であった。<br>A）対象業務一覧に該当しない業務の事前申請に対する判断結果は、半期に一度判断する。その3ヶ月後までの「対象業務一覧」が更新されたタイミングで、申請者に、5.4にある様式1-4「事前申請結果通知書」を通知する。<br>B）対象業務一覧に該当しない業務の事前申請に対する判断結果は、半期に一度判断する。この時点で、申請者に5.4にある様式1-4「事前申請結果通知書」を通知する。「対象業務一覧」の更新は、その3ヶ月後までい行う。<br>C）ISMAP-LIU の該当性有無の判断結果を、個別の申請ごとに申請者へ判断結果を5.4にある様式1-4により通知した上で、半期に一度、その3ヶ月後までに「対象業務一覧」を登録する。<br><br>3.ISMAP-LIUクラウドサービス登録規則（案）　別紙2の(4)<br>内部監査の発見事項「軽微であることの要件の１つとして、発見事項に係る統制が申請日から2 か月以内に改善することが示された改善計画書が存在すること。」とある。<br>が、内部監査においては、各組織は、発見事項の種類として、改善を必須としない推奨、助言レベルの事項も規定していることも多い。<br>このような事項は、ISMAPにおける「発見事項」には該当しない事項として扱うのか。<br>あるいは、軽微な発見事項かつ改善計画を必須としない事項として扱うのか。<br><br>4.ISMAP標準監査手続　別紙3<br>別紙3の「クラウドサービスの基盤・構成に深刻な影響を与え重大な事故につながるリスクに関連する詳細管理策」として、1-4の管理策が列記されているが、1-4に関連する詳細管理策は、毎年必ず外部監査・内部監査の対象になるという意味か。<br><br>5.ISMAP-LIUクラウドサービス登録規則（案）　様式1-2の「「対象業務一覧」への該当有無」ついて<br><br>(1)「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」とあるが、「公表を前提としない業務」、例えば、以下などは、「対象業務一覧」には該当しないと判断するのか。<br>A）省庁内の職員、一部有識者限りの会議等に使うWeb会議サービスやファイル共有・送受信サービス等は、本一覧には該当しないと判断するのか。<br>B）「公表を前提としない業務」で「機密性の高い情報」を取り扱うが、当該情報を暗号化して共有・送受信するサービス等、SaaS事業者が情報の内容に一切アクセスしない場合は、アクセスし得ない状態でも業務・情報にはリスクがあるということで、本一覧には該当しないと判断するのか。<br><br>(2)「2.政府職員の業務上の役職・氏名情報を扱う業務」とあるが、「業務上の」とはどこまでが範囲となるのか。例えば、職員の人事考課結果や特殊なスキル、経歴情報などを取り扱う人事管理システムなどは、本一覧には該当しないと判断するのか。また、採用活動（候補者の個人情報を含む）などは該当しないと判断するのか。 | １．について、情報セキュリティインシデントが発生した場合の登録の一時停止は、ISMAP、ISMAP-LIUの両方にて行われますが、その判断基準が異なります。<br>ISMAPにおいては、ISMAPクラウドサービス登録規則9.3に記載の通り、利用者に重大な影響を及ぼしうる情報セキュリティインシデントが発生した際に、クラウドサービス登録者がISMAP運営委員会に報告を行っていないにもかかわらず、ISMAP運用支援機関がそのインシデントの発生を認知した場合に、当該クラウドサービスの登録の一時停止を行います。<br>ISMAP-LIUにおいては、上記に加え、ISMAP-LIUクラウドサービス登録規則13.5に記載の通り、発生したインシデントが利用者に特に重大な影響を及ぼしうるとISMAP運営委員会が判断した場合、当該クラウドサービスの登録の一時停止を行います。<br><br>２．について、(A)(B)(C)すべてにおいて「対象業務一覧」の更新や登録が言及されており、いずれにも該当いたしません。<br>御指摘の登録規則（案）5.3の「ただし」以降の文章については、各年度の上半期、下半期の期間中になされたISMAP-LIUの事前申請について、各半期末日の3か月後までに一括してISMAP-LIU の該当性有無を判断する、としているものです。<br><br>３．について、標準監査手続3.5の注釈に示した外部監査における発見事項の定義を考慮すると、内部監査において見出された「改善を必須としない推奨・助言レベルの事項」は発見事項には該当しないといえるため、「様式2-3 内部監査に係る報告書」によりISMAP運営委員会に報告する必要はないと考えられます。<br>内部監査における発見事項の定義を明確にするため、ISMAP-LIU登録規則の別紙2「内部監査に求める要件」を修正いたします。<br><br>４．について、ISMAP標準監査手続 別紙３の1-4に関連する詳細管理策すべてについて毎年外部監査を実施するのではございません。パブリックコメントの関連ファイルとして公開している概要資料のP.7に記載しているように、1-4に関連する詳細管理策を主な対象に、数年に平準化して外部監査を実施する予定です。また、内部監査については、標準監査手続の1-4ではなく、ISMAP-LIUクラウドサービス登録規則の別紙２「内部監査の要件」に記載されているように、すべての統制目標に対して、３年で一巡するように内部監査対象とすることを想定しております。<br><br>５．（１）について A）、B)いずれもご認識の通りです。<br><br>５．（２）について、「業務上」につきましては、一般的な政府における業務を想定しておりますが、治安維持や安全保障に係る業務等、業務の性質上極めて厳格な管理を行う必要がある場合は、その対象としないことを「業務・情報の影響度評価ガイダンス」において定めております。また、同ガイダンスにおいて採用管理サービスについてもISMAP-LIUの対象として想定しております。 |

| | | |
|---|---|---|
| | (3)「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」において、「低リスクだと判断している情報」は具体的にどのようなものがあるのか。<br>例1：情報提供者(民間企業)が政府機関等に情報提供するサービス（ファイル共有サービス等）において、A)一般的な会社情報や製品情報などの共有は、情報提供者である民間企業が低リスクと判断すると想定されるが、B)調達関連の具体的な提案情報や、民間企業が政府機関等から受注した業務を実施する際に提供する技術情報などは、低リスクではないと判断することが想定される。このような場合、A)とB）の両方を扱う業務ならば、「対象業務一覧」には該当せず、A）のみを扱う業務ならば、「対象業務一覧」に該当するのか。<br>例2：民間（国民）からの意見募集、問合せなどで寄せられる意見・質問・コメント等は、本事例に該当するのか。（質問等の内容よっては、情報提供者＝国民本人が、低リスクではないと判断するケースもあるのでは） | ５．（３）について、具体的な想定例としては、例示いただたいた2例が該当すると考えております。例１におきましては、基本的にはご認識のとおりですが、B)につきましては、低リスクと判断可能なケースもあると考えております。<br>例２におきましては、意見募集等の結果として当該意見とその回答が公表されるような類であれば、ISMAP-LIUに該当するものと考えております。 |
| | (4)「5.オープンソース・公知の事実・一般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」は、基本的に公開情報だが、何らかの理由があって、やや機密性が高くなる情報という認識でよいか。<br>ソース管理サービス（構成管理サービス）、CMSサービス、Webアンサーサービスなども該当するのか。 | ５．（４）について、ご認識のとおりです。 |
| | (5)「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」で、教育内容に、機密性の高いルール内容などが含まれていた場合、本一覧には該当しないと判断するのか。 | ５．（５）について、ご認識のとおりです。 |
| | (6)「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」は、該当するサービス例としては、チャットボットサービスなどか。 | ５．（６）について、具体的には、「行政文書の管理に関するガイドライン」における○○省の掌握事務に対する事実関係の問合せへの応答業務が想定され、当該業務を遂行する上で利用する具体的なSaaSサービスとしてチャットボットサービスが考えられます。 |
| | 6.ISMAP-LIUクラウドサービス登録規則（案）　様式1-2の「「対象業務一覧」への該当有無」<br>政府機関等にセキュリティ機能等を提供するSaaSではあるが、政府機関等が持つ、機密性の高い行政情報等は一切取り使わない場合、「対象業務一覧」には入っていなくとも、「リスクの小さな業務・情報の処理」にあたるのか。<br>例えば、クラウド型のWAFや、VNP・無線LAN、シンクライアントなどは「リスクの小さな業務・情報の処理」に該当するのか。<br>また、クラウド型のネットワークインフラサービスなどは、IaaSとして、「対象業務一覧」には該当しないと思われるが、ネットワーク管理サービスは該当するのか。（後者の場合、行政情報は取り扱わなくとも、政府機関等の機器情報や設定情報など取り扱うので機密性が高い情報を取り扱うとして、対象業務一覧には該当しないと判断するのか。） | ６．について、特定の情報を扱う業務が「リスクの小さな業務・処理」に該当するかどうかは、各政府機関等で実施する「業務・情報の影響度評価」の結果によるものでありますので、現時点において「対象業務一覧」に例示をしていない業務につきましては、各政府機関等の影響度評価次第であると考えております。 |
| | 7.ISMAP-LIUクラウドサービス登録規則（案）　様式1-2の「サーバの所在地並びにデータの保存場所」<br>「リスクの小さな業務・情報の処理」を行うSaaSサービスなので、「サーバの所在地並びにデータの保存場所」の他に、取り扱うデータの種類や概要を述べ、左記のリスクが小さいことを示す記入欄を様式1-2に設けた方がよいと考えます。 | ７．について、取り扱うデータの種類やその概要に対するリスクの考え方につきましては、当該サービスの利用者がどのような情報をサービス上で取り扱うか、また、それぞれの情報においてどのような影響度評価がなされるか、に依拠するとの考えのもと、様式1-2の[影響度評価]シートの「影響度（詳細）」の表のうち「業務内容の概要」および「業務で取り扱う情報」にて記入いただくことを想定しております。 |
| | 8.ISMAP-LIUクラウドサービス登録規則（案）　様式1-2の「提供されているセキュリティ機能」<br>「リスクの小さな業務・情報の処理」であるので、様式1-2の「提供されているセキュリティ機能」の機能を必要としない、実装しないケースもあると考えます。<br>本様式は、実装しないという回答が記入される前提での様式なのか。<br>実装しない回答が記入される前提ならば、実装しない理由を記載する欄があった方がよいと考えます。 | ８．について、様式1-2の「提供されているセキュリティ機能」については、本制度より実装を要求するものでは無く、対象サービスの具備するセキュリティ機能の内容について事業者に記入いただき、政府機関等による影響度評価の参考とすることを意図しております。 |
| 7 | （1）ISMAP for Low-Impact Use における業務・情報の影響度評価ガイダンス<br>別紙1対象業務一覧について<br>例えば、「公表を前提とした～業務」で、Web会議システムの例が挙がってるが、Webシステムの機能では、公表を前提とした業務以外でも利用できる。例えば、省庁内の機密情報について取り扱う会議も実施できる。製品の運用を指定してLIUの申請をするという理解であっているか？だとすると、同じ製品群（Web会議システム）でも、ISMAP、LIUの両方が登録されることになるのか？同じ製品でも異なる業務や運用を想定して、ISMAP、LIUの両方を登録することもあるのか？同じ製品で両方登録するのは、コストもかかるので、ISMAPのみ登録するなど、その判断は事業者側の経営判断になるという理解でよいか？ | （１）政府機関における具体的な業務・情報の処理の影響度に基づき、当該業務・情報の処理に使用するSaaSがLIUの対象となるかどうかを判断する想定です。制度としては、あるSaaSがISMAPとISMAP-LIU双方のサービスリストに登録することを妨げておりませんが、通常は事業者の判断のもと、ISMAP、ISMAP-LIUどちらかに申請がなされ登録されるものと考えます。 |
| | （2）ISMAP for Low-Impact Use における業務・情報の影響度評価ガイダンス<br>別紙1対象業務一覧について<br>VPNサービスやファイル共有サービス、Web会議システム、メールシステムなど、会計や人事などの特定の業務向けではなく、情報共有や基盤のネットワークサービスなどの場合でも、運用を想定してLIUの申請を行うのか？それとも、機能としては制限がないため、運用の想定はあっても、想定運用以外の利用もできるため、ISMAPの適用になるのか？あるいは、そこも事業者の判断になるのか？ | （２）当該SaaSで処理される情報の性質と、政府機関等の具体的なニーズに応じて定まるものと考えております。 |
| 8 | ・ISMAP-LIUの特性上政府や行政機関で利用する前提であるという点は理解できるが、国内で利用されているSaaSは3000種類は超える中、入札に参加をするようなサービスは極一部であることから、本来的には民間企業も含めて信頼できる公的認証となることが好ましい。<br>しかし既存の公的認証との互換性がなく、監査機関のチェック対象が減るとはいえ、全体の評価プロセスがヘビーなことはISMAPとあまり変わらないことから、広く国内で利用される公的認証になる道筋が見えない点がもったいない。 | ・御意見いただきありがとうございます。いただいた点も含め、今後の制度改善に向け検討をさせていただきます。 |
| | ・国産SaaS事業者の海外進出を容易にするためにも、グローバル基準の採用が望ましいが、互換性がないように見えることから、なぜそういった基準にしているのかの背景が気になった。 | ・ISMAP及びISMAP-LIUにおいては、ISO/IEC 27001や27017といった国際基準を中心に策定していることに加え、NIST SP8000-53や統一基準など、幅広い基準についても取り込む形で管理基準を策定しております。 |
| | ・内部監査組織と工数を大きく取れない組織（主にスタートアップなどを想定）が取得できるイメージが沸かない。<br>結果として、どういったサービスが取得ターゲットとして想定されているのか不明瞭。 | ・IMSAP-LIUにおいては、機密性２情報を扱うサービスのうち、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SaaSをターゲットとしております。 |
| | ・インシデントによる認証取消プロセスが設定されているのは良い。運用の徹底に期待する。 | ・頂いた御意見を踏まえて当該プロセスの運用を図ります。 |
| | ・監査コストと期間がどの程度削減される見込みなのかを明記してほしい。<br>ISMAP取得事業者が口をそろえて「思っていたよりコストがかかった」と言っているので、どの程度のコストと期間が見込まれるのかのモデルケースを記載してほしい。 | ・外部監査は、ISMAP監査機関とCSPによる民民の契約によって実施されるため、費用負担がどの程度軽減されるか一概には言えないものの、外部監査において対応すべき管理策数は現行ISMAPの概ね1/5程度になると想定しております。<br>したがって、外部監査に係る業務量及びコストについても、相応の削減が見込まれるものと考えております。 |

| | | |
|---|---|---|
| 9 | 4点コメントさせていただきます。<br>※便宜上、現在のISMAP制度を「通常版ISMAP」と記載します<br><br>１．ISMAP-LIU 対象業務一覧「3. 名刺情報等の一般に広く提供する範囲の情報、及びユーザ名・パスワード・メールアドレス等の情報を扱う業務」について、<br>パスワードを扱う業務は、ISMAP―LIUではなくISMAP通常版の対象とするのが望ましいと考えます。<br><br>２．ISMAP 通常版のリストに掲載されている場合、ISMAP- LIU のリストにも自動的に掲載されるのかどうかの表記をお願いします。<br><br>３．SaaS ファーストでシステムを調達することが前提であることから、ISMAP―LIUを含めたクラウドサービスの選定方法を以下のように明確に整理するのが妥当ではないでしょうか。<br>・Step1：まずは、ISMAP-LIUリストに載っている特定目的のためのSaaSで実現可能か？<br>・Step2：次に、用途を特定しないSaaSで実現可能か？<br>・Step3：Step1/Step2で要件が満たされない場合、ISMAP通常版リストに掲載されている、PaaS / IaaS の検討<br><br>上記のようにStep2を含めたフローを定義しないと、SaaS を積極活用するという制度の目的を阻害するのではないでしょうか。<br><br>４．新制度が施行されても、監査を行う監査機関が少なく（現時点5法人）制度普及が進まないことを懸念します。<br>FedRAMPのように、セキュリティベンダーも対象とするなど監査機関の拡充のための仕組みを早急に検討いただきたいです。 | １．「対象業務一覧の３番目の例示中にあるユーザ名、パスワードの取り扱いに関して、例示の趣旨としては、SaaSの利用に当たって必須となるログイン情報に関して、その影響度は、SaaS上で取り扱われ処理される業務・情報に依存するとの考え方のもと、ログイン情報のみで過度な影響度評価がなされ、ISMAP-LIUの対象外とならないよう記載したものです。このため、御指摘いただいたような一律ISMAPの対象となるものでは無いものと考えますが、例示については誤解を与えないよう、より適切なガイダンスの記載を検討いたします。<br><br>２．通常版ISMAPのリストであるISMAPクラウドサービスリストについては、ISMAPクラウドサービス登録規則に基づき登録がなされたサービスを掲載し、ISMAP-LIUクラウドサービスリストには、ISMAP-LIUクラウドサービス登録規則に基づき登録がなされたサービスを掲載する旨をISMAP基本規程に定めているところです。これらの定めから、両クラウドサービスリストは独立したリストであり、一方に掲載されたサービスが他方にも掲載される旨を読み取る余地は無いものと考えられますので、原案の通りとさせていただきます。<br><br>なお、ISMAPクラウドサービスリストに登録されたサービスについては、ISMAP-LIUのような利用業務の制限はございませんので、今後も、ISMAPクラウドサービスリストに登録されたサービスを、ISMAP-LIUの対象となるセキュリティ上のリスクの低い業務に利用することは可能です。<br><br>３．ISMAP-LIUの登録要件として、SaaSの用途を限定しておりませんので、Step1、Step2の区別は想定しておりませんが、クラウドサービス選定におけるISMAP、ISMAP-LIUの利用方法については、引き続き政府機関等に周知することを検討致します。<br><br>４．現時点においては、監査実務の安定性等の観点から、監査法人からの申請を受け付けているものです。御意見いただいた点については、必要性含め、引き続き検討をさせていただきます。 |
| 10 | ISMAP-LIUの妥当性判断に「利用する各省庁における業務・情報の影響度評価の提出が必須」とありますが反対です。理由としては以下となります。<br>・利用することが前提となっており、検討段階や検討もされていないSaaSサービスの参入に大きな制限となる条件と考えます。各省庁と太いパイプがないサービスはISMAP-LIUの妥当性判断にすら参加できないことが懸念されます。<br>・そもそもISMAPは「 政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度です。」と言う意図で準備されたという認識です。リストにあるサービスを選択することで円滑な導入に寄与するため。「利用する各省庁の影響度評価の提出」は利用を前提にISMAP-LIUのリストに載せるための作業となり、本来の趣旨からも離れていると考えます。<br>・より多くのセキュアで便利なSaaSサービスが各省庁の選定時に参加できるような条件に変更すべきと考えます。 | ISMAP-LIUは、セキュリティ上のリスクの小さな業務・情報の処理を対象としており、各政府機関において、具体的にどのような業務・情報の処理がISMAP-LIUの対象となり、また対象外となるかを評価する必要があるため、原案の通りとさせていただきます。 |
| 11 | 概要<br><br>セキュリティ上のリスクへの影響に応じてセキュリティ要求の水準を変化させるという考え方を具体的な制度に取り込むことは、たいへん意義深いことであると考えます。<br>一方でセキュリティ上のリスクを事前に予測することは困難でもあります。したがいまして一定のセキュリティ対策や補償のポリシーが明記されていることも、制度の普及にとって重要になると考えます。<br><br>コメント<br><br>・情報の機密性について<br>SaaSであっても、クラウド上の情報を一時的にPC内にキャッシュとして保持することは一般的に広く行われております。ここで、たとえば複数のSaaSを活用しているユーザーのパソコンが攻撃を受けたとき、複数のLow Impactな情報が組み合わさって結果的に深刻な情報漏洩事件に発展する可能性は考慮に入れておくべきであると考えます。<br>ISMAP-LIU認定のSaaSにあたっては、他のセキュリティ要求を下げる代わりに、キャッシュの暗号化等によって複数の情報が組み合わさらないような対策を要求に盛り込む必要があると考えます。<br><br>・障害対策について<br>機密性の低い情報が他者から覗き見られた場合、情報の悪用がされた場合、あるいは情報が消滅した場合に採られうる（あるいは望まれる）事業者や行政での対応について、何か基本的なポリシーは存在しますでしょうか。将来的にLIUの段階を増やすケース等を想定しながら、セキュリティ面での対策を視野に入れておくことが望ましいと考えます。<br>一ザの理解も深まると思います。<br><br>・対象業務ごとの疑問点、提言<br>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<br>クラウドに不慣れなユーザがシステムを利用することが想定されます。クラウドのアカウントをなくした場合、ユーザは情報にアクセスすることができますか？オンラインで作業が可能になると、ユーザの孤立も想定されます。不慣れなユーザに対するサポート、人為ミスに対するフォローなども考慮に入れてください。<br><br>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<br>クラウドシステムへのニーズは、一般の市民にもあると思います。セキュリティ面での対策や補償をしながら、個人情報を扱うクラウドシステムの登録も増やしていただけたらと思います。<br><br>5. オープンソース・公知の事実・一般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<br>知的財産にあたる情報を取り扱う場合、情報の流出による不正利用も想定されます。クラウドに対する侵入や、不正アクセス、情報流出などのセキュリティ対策をとっているかどうかの評価も望まれます。<br><br>・その他<br>国際情勢の変化に対応するためにも、国産で信頼できるクラウドの普及が必要になっていると理解しています。また、個人PCやUSBなどの外部記憶は情報流出の危険性があるため、より安全性の高いクラウドへの業務転換が求められています。国産クラウドの普及を勧めるにあたり、ユーザへのトレーニングを政府が推奨するのはどうでしょうか。オンライントレーニング、スキル認定、セキュリティ講習などでユーザの理解も深まると思います。 | ・ISMAP-LIUで求めるセキュリティ要求は現行のISMAPと同等のものとなっております。その上で、御指摘の暗号化に係わる管理策については、ISMAP管理基準の8.1.2において定めております。<br><br>・制度としての対応については、クラウドサービス登録規則に記載しております。<br>また、調達側の対応として統一基準を踏まえた基本的な情報セキュリティポリシーについては各政府機関において整備・運用されております。<br><br>・以降の「対象業務ごとの疑問点、低減」および「その他」でいただきましたご意見について、制度における規定類の案への御意見ではないと認識しておりますが、御意見は拝聴いたしました。 |

| | | |
|---|---|---|
| 12 | 現行のISMAPクラウドサービスリストに登録されたサービスは、ISMAP-LIUの対象業務一覧に該当する業務で使用する場合、あるいは当該業務に係わる業務・情報の影響度評価の結果が低位であることの妥当性を複数の省庁から認められた場合、速やかにISMAP-LIUに移行できるようにしていただきたい。<br>ISMAP-LIUが策定されるという想定が当初なく、ISMAPクラウドサービスリストへの登録をしたサービス事業者が存在すると思われる。ISMAP-LIUは外部監査対象範囲が現行ISMAPより縮小されることから、事業者にとっては維持負担を考慮するとISMAP-LIUに移行したいというニーズが発生するものと思われる。<br>ISMAP登録済のサービスであれば任意の時点で基準の全量が達成されていることを確認されているため、影響度評価が低位であることを確認するための事前審査は必要であろうが、事前審査で低位の該当性があると確認されれば、その後の「外部監査、内部監査の実施状況確認によるコントロールの評価」は不要と思われる。その点を明記していただきたい。 | ご意見いただいた、現行ISMAP登録サービスのISMAP-LIUへの移行について、基本的には各事業者の判断になろうかと存じますが、制度としてもそのようなニーズがあることは想定しております。<br>なお、ISMAPからISMAP-LIUへの移行に関して、特別なプロセス等は用意しておらず、サービスの新規登録時と同様に、ISMAP-LIUクラウドサービス登録規則に基づき登録申請のプロセスによる対応を実施いただくことになりますが、本制度運用の状況を踏まえ、必要に応じて手続等に係わる支援情報の整備等進めて参ります。 |
| 13 | 今年はISO27001の改定（ISO/IEC 27001:2022）が予定されております。<br>※既に管理策規格であるISO27002は2022年版が公開されているようです。<br><br>ISMAPの管理基準について、現規格[例：JIS Q 27001:2014（ISO/IEC 27001:2013)]等の、現規格がベースとなっておりますが、既に改定されることが確定ISO規格との対応付、管理基準、管理策の内容の整合性がどう取られ、改定がされていくのか、見通しについてご教示頂きたいです。<br><br>企業としては、直近の数年で新規格でのISO認証（マネジメントシステム）の取得・更新対応が求められる状況です。<br><br>このような状況において、ISMAP-LIUの取得・運用にも並行で取り組まなければならなくなった場合、新旧ISO規格の入り混じった状態でマネジメントシステムの運用が求められる状態は、あまり好ましくはないと考えております。 | 国内規格(JIS)の改定時期が確定していないため、具体的な時期についてはご回答できかねますが、ISO/IEC 27001:2022及びISO/IEC 27002:2022に対応するJISの発効後にISMAP管理基準の改訂を行う方向で検討を進めております。 |
| | ・該当箇所<br>「ISMAP-LIU クラウドサービス登録規則 （案）」　第3章～6章、 附則<br><br>・意見内容<br>対象となる業務や情報を透明性を持って示すことを求めます。<br><br>・理由<br>ISMAP-LIUでは、クラウドサービスプロバイダー（CSP）の事前申請プロセスを新たに導入しています。ISMAPとは異なり、サービス登録申請に先立ち、制度所管省庁によるISMAP-LIUの該当性についての審査が行われます。この事前申請では、申請者が提供するSaaSが取り扱う業務や情報に関して、利用省庁等が実施した影響評価の結果を添付する必要があります。<br><br>この新たな仕組みにおいて意図されているのは、ISMAP-LIUへの登録に該当する業務の代表例一覧を拡大していくことですが、このようなアプローチでは、対象となるサービスが過度に狭まるでのはないかと我々は懸念しています。<br><br>「ISMAP-LIUにおける業務・情報の影響度評価ガイダンス 」は、ISMAP-LIUの該当性のある、影響度の低い業務であるか否かを省庁等が判断するために策定されていますが、提示された基準の曖昧さにより、申請者や省庁等が事前にISMAP-LIUへの該当性を見極めるのが難しくなっています。<br><br>「対象業務一覧」を提示するのではなく、ISMAPにおける評価を要する、より機微な業務一覧を設け、その一覧に含まれない業務はISMAP-LIUの対象とすることを推奨します。<br><br>上記を実施することにより、どのようなサービスがISMAP-LIUに該当するかの予見性が向上し、政府に対して、最も費用対効果が高く、安全で高品質なサービスをCSPから提供することが可能となります。<br><br>結論<br>ISMAP-LIUの登録規則（案）等に対して意見する機会に感謝します。意見募集にかけられた多数の文書を関係者が検討し、提案されているアプローチについて議論するための十分な時間を確保するためにも、今後は少なくとも30日間の意見募集期間を設けることを関係省庁に強く要望します。また、我々の今回の提言が、文書の確定に役立つことを期待しています。推奨事項を実施するため、また、政府調達における選択肢を増やし、民間が提供するクラウド・サービスへの政府投資から、さらなる価値を生み出すために、CSPがどのように関係省庁と連携していけるかについて話し合いの機会を頂ければ幸いです。 | ・「「ISMAP-LIU クラウドサービス登録規則 （案）」　第3章～6章、 附則」に対する意見について、ISMAP-LIUにおいては「対象業務一覧」で例示する代表的な業務以外の業務についても、利用する政府機関等において影響度が低位であると評価され、かつ、低位であることの蓋然性があることが確認できたものについてはISMAP-LIUの対象となりますので、対象となるサービスが過度に狭まることは無いと考えております。<br>他方、対象となるかどうかの判断に、利用者である政府機関等の評価が必要であることから、申請者において事前に該当性を見極めることが困難である点につきまして、本制度の運用状況を見つつ、事業者への情報提供や、説明会などを通して制度普及に努めて参ります。 |

| | | |
|---|---|---|
| 14 | ・該当箇所<br>「ISMAP-LIU クラウドサービス登録規則（案）」第5章 事前申請の審査、第7章 申請者に対する要求事項<br><br>・意見内容<br>審査プロセスの改善を求めます。（以下、意見内容の詳細と理由を記載）<br><br>・理由<br>外部監査の対象となる管理策基準の数を減らすことは、現行のISMAPの要件に比べ有効な改善ではありますが、ISMAP-LIUと現行のISMAPの両方に関し、以下を実施することにより、評価プロセスをさらに改善し、政府側の限りある人的資源の負担を軽減することが可能となります。<br><br>·事前申請の手続きを迅速化すること。事前申請の審査について、ISMAP-LIUクラウドサービス登録規則（案）の5.3には、対象業務一覧に該当しない場合、「各年度の上半期、下半期の期間中になされた事前申請について、原則として各半期末日の3ヶ月後までに一括してISMAP-LIUの該当性有無を判断する」と記されています。事前申請の審査を年2回の特定期間に限定することは、調達省庁のクラウドサービス導入の大幅な遅れにつながります。対象業務一覧への掲載の有無にかかわらず、同じ審査期間を設定することで、このプロセスを迅速化することを要望します。<br><br>·反復的な監査手続を削減すること。既に取得済みの国際規格と重複する管理策基準の適用を免除することで、監査手続を簡素化することが可能となります。多くのCSPは、国際的に認定された認証機関から国際規格（ISMS-JISQ/ISO 27000シリーズ）の認証を既に取得しています。それらを認め、過去の認証手続きで提供された証跡の再利用による日本国内における重複的監査や、その他の反復的な手順と要件を排除することで、政府関係者を含む、全てのステークホルダーの不要な負担を軽減することできます。また、これにより、日本でISMS/ISO認証を取得する企業が増え、そのような企業に国際的なビジネス・チャンスが広がり、政府に対して、より費用対効果の高いソリューションを提供するための競争が激化することにもなります。<br><br>·第三者機関による国際的に認定された認証および監査結果を認めること。ISMAP及びISMAP-LIUに関連する管理策基準および要件に準拠している証跡の重複を削除することによって、非実用的で反復的な現地監査の必要性も減らすことができます。現地監査は、本目的以外では権限を持たない者による現場へのアクセスを要するため、データセンターを不必要な物理的セキュリティリスクにさらすことになります。<br><br>·より具体的な監査ガイドラインを策定し、それらを国際的に認定された標準に合わせて位置付けること。ISMAPの制度運営者、監査人、およびCSP間の管理策基準の解釈の不一致は、CSPに非効率な手間、追加費用、および手続きの遅延を課すことになります。ISMAP制度運営者と監査人による管理策基準の解釈の違いにより、場合によっては、監査終了後に、CSPへISMAP制度運営者から再監査依頼が繰り返されることがあります。関係者間での解釈に一貫性をもたせることを推奨します。<br><br>·柔軟な監査期間を可能にすること。現行のISMAP及びISMAP-LIUにおいては、初回登録時に固定された監査期間を選択することが定められています。その後に監査サイクルが確立し、柔軟に調整することができない制度となっています。このような厳格な監査サイクルでは、CSPがグローバルに実施している監査サイクルに変更が生じた際に、それに合わせた期間調整をすることができず、ISMAP評価プロセスとのギャップが生じることとなり、ISMAPおよびISMAP-LIUクラウドサービスリストへのサービス登録が一時失効することにもなりかねません。このような状況を解決するために、直近の監査報告書の終了日から次の監査報告書の開始日までの空白期間をカバーするために、System and Organization Controls（SOC）のブリッジレター** のような制度を採用することを関係省庁に推奨します。ブリッジレターは、空白期間中に統制に重要な変更がないことを表明し、そのような状況下でも認証を維持することを可能にするものです。<br>** https://jicpa.or.jp/specialized_field/files/2-8-33-2-20200914.pdf、 Q15: 19-20ページ<br><br>また、現行制度では、監査報告書の提出は監査終了後4カ月以内とされていますが、これでは、CSP が必要な証跡をすべて収集するのに十分な時間がとれません。より実行可能な制度とするためにも、6 カ月に延長することを推奨します。<br><br>·頻度を減らした 監査スケジュールを設定すること。毎年監査を実施するというISMAPの現行の要件とは対照的に、国際的なクラウド・セキュリティのベスト・プラクティスでは、一般的に三年に一度の監査を求めています。監査の頻度を減らすことで、CSPと政府の双方にとって不要なコストを削減することができます。毎年の監査では、CSPは事実上、連続した監査手続を実施することになり、常時、監査対応に追われることとなり、セキュリティ担当者の注意を不必要にそらし、他の重要な人材も流用することとなります。調達省庁側にとっても、毎年度の契約更新が求められることから、負荷が増すこととなります。<br><br>·ISMAPへの登録が年間を通じて実施されるようにすること。現在、ISMAP制度運営者は、ISMAP登録を四半期ごとに実施しているため、ISMAP登録を目指すCSPにとっては、三ヶ月以上の遅れが生じる場合があります。このような遅延は、企業が貴重な調達機会に入札することを妨げ、企業には事業機会を、調達機関には対象となるクラウドサービスの恩恵を与えないことになります。年間を通して継続的に登録を行うことで、ISMAPは急速に進化するクラウドの技術をより迅速に取り入れることができます。<br><br>·ISMAPに登録する監査法人の数を増やすこと。関係省庁が認識しているように、登録監査法人の数が限定的であることから、ISMAPにおいて要求される監査手続を満たすための、人的資源が現在、また、将来的にも不足しています。登録監査法人の数を現行の５法人から増やすことで、人材不足が解消され、監査法人間の公正な競争が促進され、CSPに多様な選択肢を提供し、監査市場の効率化を図ることができます。<br><br>また、並行して、ISMAPを持続可能な制度にするためには、クラウドサービスのIT監査・認証要員を育成するための手続きを開発し、適切な人材を確保することが重要です。<br>上記のISMAPの改善を実施し、ISMAP-LIUへ反映することは、セキュリティが確保されたクラウドサービスが日本で普及することにつながり、公的部門、また民間部門の幅広いステークホルダーに恩恵をもたらすことになります。<br><br>結論<br>ISMAP-LIUの登録規則（案）等に対して意見する機会に感謝します。意見募集にかけられた多数の文書を関係者が検討し、提案されているアプローチについて議論するための十分な時間を確保するためにも、今後は少なくとも30日間の意見募集期間を設けることを関係省庁に強く要望します。また、我々の今回の提言が、文書の確定に役立つことを期待しています。推奨事項を実施するため、また、政府調達における選択肢を増やし、民間が提供するクラウド・サービスへの政府投資から、さらなる価値を生み出すために、CSPがどのように関係省庁と連携していけるかについて話し合いの機会を頂ければ幸いです。 | ・「「ISMAP-LIU クラウドサービス登録規則（案）」第5章 事前申請の審査、第7章 申請者に対する要求事項」に対するご意見について、現行のISMAP含め、審査プロセスについては、いただいた御意見も踏まえ継続して検討させていただきます。 |

| | | |
|---|---|---|
| 15 | 今後、従来のオンプレミス機器導入からクラウド製品導入を進められていく中で感じましたサイバーセキュリティ製品におけるISMAP登録に際した課題を以下4点の視点で意見を述べさせて頂ければと存じます。<br>１．ISMAP登録費用<br>日本官公庁様ビジネスに向けた認証基準であり、登録する際のコスト負担が高い<br>上記に対して、FedRAMPやSOC２を取得しているクラウド製品はISMAP認証基準を満たしている等の代替<br>もしくは、ISMAPでの認証を日本国有項目に関する簡易的なチェック項目にて対応出来るようにしていただきたい<br>２．認証取得期間<br>申請から承認、取得まで長期間に渡り対応する必要があり、最新技術を官公庁様にてご活用頂くのに時間を要してしまっている<br>取得までの期間短縮にあたって、ISOやFedRAMPの代替を含め、認証取得期間短縮をご検討いただきたい<br>３．認証項目内容<br>クラウド製品によってサービス面に差異があり、以下観点にて同基準とみなした際の認証取得が難しいと考える<br>・機密情報、様々なデータを保管するサービス<br>・機密情報や様々なデータ保管を目的としないサービス（ネットワーク系の製品など）<br>上記に対して機密情報をサービス利用上保持要否の観点にて認証項目を変更いただきたい<br>４．ルール適用<br>各省庁様保有システム更改移行期間にて、現状ISMAPを取得していないサービスを要件上、採用されるケースがあり<br>ISMAP認証取得の要否を各ベンダー様側が判断しかねているケースが散見されている<br>上記に対して半年ー1年間程度の猶予期間等を設けた上で、適用基準の明確化と厳密化を実施いただきたい | １．他の認証制度の活用やISMAPとの互換性については、認証を実施している認証機関に対する要求事項がISMAPと異なる点、監査の深度や手法が異なる点等を踏まえ、現時点においては活用を検討しておりません。こちらについても、今後の制度運用の状況を鑑みつつ、活用可否については継続して検討をさせていただきます。<br>なお、コスト負担について、ISMAPで要求している外部監査はISMAP監査機関とCSPによる民民の契約によって実施されるため、ISMAP-LIUの仕組みにおいて費用負担がどの程度軽減されるか、一概にお答えすることは困難ですが外部監査において対応すべき管理策数は現行ISMAPの概ね1/5程度になるものと想定しております。<br>したがって、外部監査に係る業務量及びコストについても、相応の削減が見込まれるものと考えております。<br>２．～４．について、ISMAP-LIUにおける各種規定等の案への御意見ではないと理解致しますが、御意見は拝聴いたしました。 |
| 16 | a) 国際認証を有するクラウドサービスを優先して認証する仕組みについて ： ISMAP-LIUの認証プロセスを合理化し、利用省庁等がより広くより迅速にクラウドサービスを、資格を有するクラウドプロバイダーから採用できるようにするために、SOC2 やISO27001 など国際的に認められた規格に基づく有効な認証を然るべき認証機関から受けている事業者を、政府が認定CSP として認めることを提案いたします。なお、米国政府の制度であるFedRAMP も対象であり、こうした認証はいずれも事業者による内部監査よりも厳格であるといえます。つまり、このように認定されたCSP は、日本で再度監査プロセスを経ることなくISMAP-LIU に承認されるという考え方になります。ISMAP-LIU は機密性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重点を置いているため、重大な発見事項やセキュリティリスクが特定されていない限り、国際的な規格に基づいた認証資格または報告書は政府に対して十分な保証を提供するに足りると考えられます。<br>また、すでにISMAP 認証を受けているCSP にとっては、ISMAP-LIU の申請に係る追加の内部監査や外部監査の要件により、常に外部監査に加えて二重の検証を行うことになり、すでに認証機関による検証が行われている場合でも政府の限られたリソースに不必要な負担をかけることになります。このような企業の監査の要件を削除することで、自発的な統制整備・運用が促進されるだけでなく、CSPは、その経営資源を日本のデジタル トランスフォーメーションに貢献すべく自らのクラウドサービスの改善と革新のために投資をすることができるようになります。<br>政府が引き続き外部監査が必要であると判断をするのであれば、監査を通じて確認できる項目の中でもSOC2/ISO27001/FedRAMP でまだカバーされていない分野に焦点を当てることを推奨いたします。このような監査であれば、インシデントが発生した場合に利用省庁等が被る損害のリスクに対処し、そのリスクを軽減することに焦点を当てることができます。また、CSP がいくつかの重要な管理策に焦点を当てた、将来のインシデントを回避するための取り組みを示す内部監査リポートの提出を求めることで、自発的な統制整備・運用を促すこともできます。こうしたアプローチにより、関係するあらゆるステークホルダーの必要以上の負担を軽減することができると考えられます。<br>b) 登録のあり方について: 現在、ISMAPに認証されたCSPおよびサービス名がサービスリストに掲載されています。ISMAP-LIU においても同じことが当てはまるかと想定しておりますので、今後は審査中や審査に向けた作業が進行中のものも公表することを提案いたします。これにより、利用省庁等はCSP の申請の進捗状況を的確に理解できるので、より多くの選択肢の中から相応しいクラウドサービスを計画的に選定できるようになるかと思います。<br>c) 英語での文書作成について ： ISMAPの審査は現在日本語で実施されており、企業は監査をサポートするために日本を拠点とする要員を雇う必要があります。英語での文書作成をお認めいただくことで、シスコのような日本国外に本社を有する企業は、現在日本語でのみ受け入れられている文書や監査成果物の作成ではなく、ISMAP 要件を満たすための迅速な対応が可能になります。<br>・どのCSP も常に自らのクラウドサービスの開発と改善を行うことで、日本におけるデジタルトランスフォーメーションの促進に貢献していると確信しております。ISMAP-LIU に込められたCSP による自発性を促すアプローチは、CSP が効率性と省力化を実現しながらセキュリティの問題に対処するための措置を講じるのに有効であり、結果として、さらなる開発と品質向上のために経営資源を活用できるようになると考えています。<br>・この度の政府による意見募集に際し、上述のコメントをお送りすることができる機会をいただいたことを心より感謝申し上げます。今後、内容に関するご質問や、追加のご要望などございましたら速やかに対応いたしますのでお知らせいただけますと幸いです。 | a) について、他の認証制度については、認証を実施している認証機関に対する要求事項がISMAPと異なる点、監査の深度や手法が異なる点等を踏まえ、現時点においては活用を検討しておりません。こちらについても、今後の制度運用の状況を鑑みつつ、活用可否については継続して検討をさせていただきます。<br>b) について、今回の協議対処案に対するご意見では無くISMAP全体に係わるものと認識しておりますが、ご意見は拝聴致しました。<br>c) について、申請者が提出書類、申請手続及びISMAP運用支援機関との連絡に使用する言語は、日本語のみとしております。なお、提出書類のうち、言明書の別添に限っては日本語又は英語のいずれかを用いることができますが、英語を使用する場合には、参考和訳をつけることを求める場合があります（ISMAP-LIUクラウドサービス登録規則7.10）。<br>今後、使用する言語について制度規程の改訂があった場合、ISMAPポータルサイト上で公開いたします。 |
| 17 | 「内部監査の要件について」<br>別紙２ 内部監査に求める要件のなかで、監査体制、責任者や実施者の要件や運用評価実施の有無について記載がないと認識しており、これらの要件についてはCSP側で適切と考える要件によって実施するとう理解で正しいでしょうか。<br>様式2-3の報告書のひな型に、監査体制の記載事項があり、また内部統制の実施方法にはサンプルテストという記載もあります。監査体制や実施する手続やサンプル数の認識の齟齬により要件を満たないという可能性があるのであれば、最低限の要件はお示し頂ければ考えます。別紙２の要件が最低限の要件ということかもしれませんが、確認させてください。<br>「影響度評価の入手方法について」<br>「ISMAP for Low-Impact Use における業務・情報の影響度評価ガイダンス」2.5 業務・情報の影響度評価を実施するタイミングでは、「～調達担当者がCSPと連携して～」とあり、調達担当者が導入するSaaSサービスの候補を検討して、そのCSPと連携して評価を実施することを想定しており、LIU制度は具体的な調達がある場合に適用可能な制度という理解で正しいでしょうか。<br>「既存ISMAPとの関係について」<br>既にISMAPリストに登録のあるサービスについては、LIUを要件としてた調達にも参加できるという理解で正しいでしょうか。<br>「政府機関の利用数」<br>これは、CSPが申請時に申請時点の状況について記載するものでしょうか。その場合どの様式に記載するものになるでしょうか。 | 「内部監査の要件に係わるご意見」について、「別紙２ 内部監査に求める要件」を最低限の要件として定めており、監査体制、責任者や実施者の要件や運用評価実施の有無などは、CSP側の方で適切と考える要件によって実施するという理解で相違ございません。<br>CSP側の自発的な統制整備・運用を促すことを目的に、CSPが自ら実施する内部監査の内容について報告を求めているものとなります。<br>「影響度評価の入手方法に係わるご意見」について、ご理解のとおり、ISMAP-LIUは具体的な調達ニーズのある場合に適用される制度です。<br>「既存ISMAPとの関係に係わるご意見」について、ご理解のとおりです。<br>「政府機関の利用数に係わるご意見」について、政府機関における利用数の把握方法については、事業者より利用数を聴取するのでは無く、政府機関内における利用事態調査等の活用を想定し検討を進めております。 |

| | | |
|---|---|---|
| 18 | ISMAP 管理基準の「2.2.5 監査の対象となる期間」において、 監査の対象期間は最大１年とし、登録申請を行う際の監査対象期間は、前回の監査対象期間の末日の翌日とすることで、期間の隙間なく監査 が行われなければならないと記されております。また、これらはISMAP 標準監査手続「3.1 手続の実施 3.1.1 前提」「（別紙３）ISMAP-LIU における監査業務」を通じて具体化されますが、今般のISMAP-LIUの制度が、SaaSはサービスの幅が広く、用途や機能が極めて限定的なサービスや、機密性２情報の中でも比較的重要度が低い情報のみを取り扱うサービス等リスクが低いサービスもあり、それらのサービスについて現行の 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り、それにより当該サービスの活用が進まない場合も考えられるとの観点を踏まえると、少なくとも更新後については、複数年監査が許容されることや、年次で実施あっても監査項目自体をサンプリングで点検することが許容されるなど、更新後の監査工数の低減措置について検討のうえで明記していただきたいです。 | ISMAP-LIUにおいては、ガバナンス・マネジメント基準の全量に加え、管理策基準のうち、サービス基盤・構成に直接的な影響を及ぼし得る管理策（一部の重要な管理策）を主な対象として、数年に平準化しつつ監査を実施する予定です。ご指摘いただいた点については、今後も継続的に検討をさせていただきます。 |
| 19 | ISMAP-LIU クラウドサービス登録規則 案 P1に記載されている「対象業務一覧」については、この影響評価ガイダンスでの公開にあたって、「誰が使うサービスを対象にするか」も明確化していただきたく存じます。たとえば、システム開発等を請け負った事業者が、その開発の際に開発プロジェクト内で情報共有を行うサービスのように、調達元が直接使うのではないが関係するサービスも存在しており、その扱いについてもご検討をいただきたく存じます。なお、SaaSを対象にするにあたって、サービス提供者側はISMAP-LIU導入はコストアップにつながるため、適用範囲のご検討や、調達の際の予算取りにおいてはご配慮を賜りたくお願い申し上げます。 | ISMAP、ISMAP-LIUともに、政府機関が調達を行うクラウドサービスを対象としたものであり、ISMAP-LIUの影響度評価を行う主体も政府機関等を想定しております。 |
| 20 | 「ISMAP-LIUクラウドサービス登録規則(案)P1及びISMAP for Low-Impact Use における業務・情報の影響度評価ガイダンス（参考資料） 全体」<br>ISMAPクラウドサービス登録規則の総則では、「リスクの小さな業務・情報の処理に用いる SaaS サービスを対象とした仕組み（以下「ISMAP-LIU」という。）による登録（以下「サービス登録」という。）に関する事項を定める」とあり、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べく「業務・情報の影響度評価ガイダンス」が参考として示されているが、個別の案件のリスクや影響度を官庁の方々が都度、判断されていくのは煩雑さも含めて困難を伴うのではないか。ISMAP-LIUを官庁の方々が選択しやすくなるよう判断基準をより明確化すべきと考えます。<br>併せて、入札側が「ISMAP-LIU」を選択できる判断基準も明確化していただくと、より利用者が増加すると考えます。 | 「ISMAP-LIUクラウドサービス登録規則(案)P1及びISMAP for Low-Impact Use における業務・情報の影響度評価ガイダンス（参考資料） 全体に係わるご意見」について、情報システムにおけるリスク評価とリスク評価結果に応じたセキュリティ管理策の選択は、本来どのような調達においても実施すべきものであり、ISMAP-LIUにおける業務・情報の影響度評価ガイダンスは当該判断を支援する位置づけとして整理しています。 |
| | 「ISMAP-LIUクラウドサービス登録規則(案) P.2」<br>「第3章 サービス登録に関する事前申請」<br>調達省庁において、ISMAP-LIUであるかISMAPであるかに関わらず、検討するクラウドサービス全てに対して影響度分析を行い、ISMAP-LIU/ISMAPのどちらを適用するか判断するプロセスにしていただきたい。<br>上記プロセスがなく、ISMAP-LIUを適用したい場合のみ影響度評価等の負荷がかかると、調達側がISMAP-LIUをそもそも利用するインセンティブがないため、ISMAP-LIU利用のケースは少なくなることが想定されます。 | 「ISMAP-LIUクラウドサービス登録規則(案) P.2に係わるご意見」の１点目について、政府情報システムの整備及び管理に関する政府共通ルールである「デジタル・ガバメント推進標準ガイドライン」を踏まえると、本来的には、ISMAP であれ ISMAP-LIUであれ、クラウドサービス上で取り扱う業務・情報の分析は必須で行うプロセスとして位置づけられております。その上で、ISMAP-LIUは業務情報の影響度が低いSaaSについて外部監査を緩和する仕組みであり、影響度が低いことの証跡として、利用省庁等による業務・情報の影響度評価結果を提出いただく枠組みとしております。 |
| | 「ISMAP-LIUクラウドサービス登録規則(案) P.2」<br>「第3章 サービス登録に関する事前申請」<br>複数の省庁が同じクラウドサービスを導入する場合、取り扱う業務や情報がほぼ同じ場合は、省庁によって影響度評価の結果が異なることがないように、省庁間またはISMAP運営委員会が間に入り必要な情報連携を行っていただきたい。 | 「ISMAP-LIUクラウドサービス登録規則(案) P.2に係わるご意見」の２点目について、影響度評価の結果については制度ISMAP運営支援機関で審査の上、必要に応じて制度所管省庁で内容の妥当性を判断することとしています。 |
| | 「ISMAP-LIUクラウドサービス登録規則(案) P.2」<br>「第3章 サービス登録に関する事前申請」<br>クラウドサービスプロバイダーがISMAP-LIUを適用するための事前申請時に提供する情報のいずれかを会社の方針上等の理由で提供できない場合であっても、当該クラウドサービスがISMAPを取得できる強固なセキュリティを有している場合もあります。単に事前申請時に提供する情報が共有されないだけで、影響度評価の結果が高リスクと判断されることがないよう、影響度評価の結果の共有範囲、ルール等を整理していただきたい。 | 「ISMAP-LIUクラウドサービス登録規則(案) P.2に係わるご意見」の３点目について、ISMAP-LIUクラウドサービス登録規則への直接的なご意見では無く、影響度評価の評価方法に係わるご意見であると認識いたしました。政府機関等が影響度評価を行う際の考え方については、政府機関等を対象に影響度評価ガイダンスを作成しており、適切な影響度評価が行われるよう努めて参ります。 |
| | 「政府情報システムのためのセキュリティ評価制度(ISMAP)基本規程　P5」<br>「2.3 制度の基本的枠組み」<br>本段落の11行目「調達府省庁等はISMAPクラウドサービスリストに掲載されているクラウドサービスの中から調達を行うことを原則とする。」の記載については、この前行にて新たに「ISMAP等クラウドサービスリスト」と定義しているため、「調達府省庁等はISMAP等クラウドサービスリストに掲載されている～」と記載すべきと考えます。<br>また、「ISMAP等クラウドサービスリスト～」という記載であることを前提に、「リスクの小さな業務・情報の処理に用いる 」場合、ISMAP-LIUクラウドサービスリストからのみの選択となるのか、あるいはISMAP及びISMAP-LIUクラウドサービス両方を含んだ「ISMAP等クラウドサービスリスト」から選択されるのか明確にして頂きたいです。 | 「政府情報システムのためのセキュリティ評価制度(ISMAP)基本規程　P5、2.3 制度の基本的枠組み」に対するご意見」について、御指摘を踏まえ、政府情報システムのためのセキュリティ評価制度(ISMAP)基本規程について、「ISMAP等クラウドサービスリスト」という用語に統一した記載に修正いたします。<br>なお、ISMAP基本規程はクラウドサービス事業者、 調達府省庁等 、監査機関、制度所管省庁、 ISMAP 運営委員会が<br>遵守しなければならない基本的事項を定めた文書であり、調達時における条件等は個別の案件に応じて異なることが想定されることから、調達府省庁による調達時のリストの利用に係わる記載ついては原案の通りとさせていただきます。 |
| | 「政府情報システムのためのセキュリティ評価制度（ISMAP）基本規程 p9」<br>「第7章 制度を構成する者の責任範囲」<br>調達者に対し、仕様書内の業務を適切に分類し、業務分類毎に必要となる機能を一覧化した上で何がISMAP/ISMAP-LIUの範囲であるか明確化することを責任とすべきと考えます。<br>大規模システムの場合、調達単位が大きいため各アプリケーションが複数になり、各アプリが持つデータを分けて管理するケースが多いです。特定アプリAの機密性が高い場合でも、他アプリがそれを共有することがない場合、A以外のアプリについては柔軟に（ISMAP-LIUの適用を）検討することができるようになれば、各事業者が登録するインセンティブに繋がり、よりISMAP-LIUに登録するサービスが増えてくると考えます。 | 「政府情報システムのためのセキュリティ評価制度（ISMAP）基本規程 p9、第7章 制度を構成する者の責任範囲に対するご意見」について、ISMAP基本規程は、ISMAPの基本的な枠組みにおいてクラウドサービス事業者、 調達府省庁等 、監査機関、制度所管省庁、 ISMAP 運営委員会が遵守しなければならない基本的事項を定めた文書であり、調達仕様書の記載に係わる事項については本規程の範疇を逸脱するものであるため、原案の通りとさせていただきます。 |
| | 「ISMAP 標準監査手続　P15」<br>「（別紙３）ISMAP-LIU における監査業務」<br>「ISMAP-LIUに関しては、ガバナンス基準・マネジメント基準の全ての詳細管理策に加えて、以下に掲げるような、クラウドサービスの基盤・構成に深刻な影響を与え重大な事故につながるリスクに関連する詳細管理策を中心として監査を実施する。」とフォーカスすべきコントロール基準の詳細管理策が例示されているが、LIU＝セキュリティレベルが低いという誤解を与えないようにすべきと考えます。また他の認証などの利用によって管理策への対応を効率化するなどの仕組みを検討して頂きたいです。 | 「ISMAP 標準監査手続　P15、（別紙３）ISMAP-LIU における監査業務に対するご意見」について、ご指摘いただいた「LIU＝セキュリティレベルが低いという誤解を与えないようにすべき」という点については、ご意見も踏まえ今後検討をさせていただきます。<br>また、他の認証制度については、認証を実施している認証機関に対する要求事項がISMAPと異なる点、監査の深度や手法が異なる点等を踏まえ、現時点においては活用を検討しておりません。こちらについても、今後の制度運用の状況を鑑みつつ、活用可否については継続して検討をさせていただきます。 |
| | 「ISMAP制度全般について」<br>ISMAP取得には負担の大きいプロセスを経る必要があり、かつ製品ロードマップへの影響も大きく、取得までに多大な時間を要します。ISMAPの暫定措置期間の延長をご検討いただきたいです。 | 「ISMAP制度全般に対するご意見」について、ISMAP-LIUにおける各種規定等の案への御意見ではないと理解致しますが、御意見は拝聴いたしました。 |
| | 「ISMAP-LIU制度全般について」<br>ISMAP-LIUを適用できる8つの業務例がありますが、ISMAP-LIUを取得する対象のクラウドサービスを、その業務のみで利用するという責任はどう担保するのでしょうか。<br>例えば、ある省庁が特定の業務（8つの例の1つ）で利用するということでISMAP-LIUを取得したサービスがあったとして、そのクラウドサービスでは8つの業務以上のことも機能上できる場合、当初に特定されていた業務以外の利用目的でサービスが利用され、万が一、ISMAP-LIUで確認していないセキュリティ項目になんらかの問題があった場合、省庁、事業者のどちらが、どのような責任を持つことになるのでしょうか。<br>こうした責任の所在がはっきりしないと、8つの業務のうちの1つで利用する、という省庁の申し出があったとしても、事業者としてはなかなかISMAP-LIUを適用するという判断がし辛いのではないかと考えます。 | 「ISMAP-LIU制度全般に対するご意見」について、ご指摘いただいた対象業務の範囲内でのみ活用する責任は、調達した政府機関等に帰属するものであり、そのために業務・情報の影響度評価を政府機関等によって実施を求めております。 |

| | | |
|---|---|---|
| 21 | １．「ISMAP-LIUクラウドサービス登録規則（案）」第5章<br>ISMAP-LIU クラウドサービスリストは、ISMAPクラウドサービスリストと異なり、特定した業務（対象業務一覧に該当する業務およびリスク影響度評価結果低位であることが確認された業務）とクラウドサービス（SaaS）が紐づいた形で登録されるものと認識しました。<br>このようなサービスリストの場合、想定している特定業務以外へSaaSを利用する場合がどのように対処するのか明確にする必要があると考えます。<br>1-1.ISMAP-LIUは業務内容とSaaSが一体化しているため、業務内容が異なる場合は業務・情報の影響度評価をやり直し、妥当性を判断するのかどうかの明確にする必要があると考えます。<br>1-2.業務内容が異なり影響度評価をやり直しとなる場合、「低位でない」と判断された場合にISMAP-LIUではなくISMAPの再取得が必要となるかどうかの明確にする必要があると考えます。<br>1-3.ISMAP-LIU取得後にISMAPへの登録を行う場合の手続きについて明確にする必要があると考えます。（外部監査を含めすべてやり直しか管理策基準項目差分のみの監査のみか等）・ 1-4.ISMAP-LIU クラウドサービスリストに登録されていれば登録時に想定している業務以外でも利用可能である場合はその旨明記する必要があると考えます。 | １．1-1, 1-2, 1-4にて御指摘いただいた通り、政府機関等においては、ISMAP-LIUサービスリストに掲載されているサービスを調達する際、業務・情報の影響度評価を実施する必要があり、影響度評価の結果として「低位」ではない結論が出た場合、LIUではなく現行のISMAPに登録されているサービスから調達を行う必要がございます。こちらについては、ISMAP制度の利用の在り方に関するものとなりますので、CISO・デジタル社会推進会議幹事会決定にて定める予定です。<br>また、1-3にて御指摘をいただいた、ISMAP-LIU取得後から現行ISMAPを取得する場合については、更新申請のタイミングにおいて、ISMAPの更新プロセスに基づいて、外部監査・更新申請を実施いただくことを想定しております。 |
| | ２．「ISMAP-LIUクラウドサービス登録規則（案）」第3章　および　「【参考】ISMAP-LIUについて（案）」 P6について<br>事前申請には利用省庁（１省庁以上）等による業務・情報の影響度評価を行うと記載がありました。<br>・対象業務一覧の場合は1省庁<br>・要検討業務は２省庁<br>のリスク影響度評価結果を基に、該当性有無を判断と記載がありますが、要検討業務の場合の2省庁はどのような基準で選定するか明確にする必要があると考えます。<br>（1省庁は利用する省庁の業務が明確になっているかと考えますが、もう1省庁はどのように選定しリスク影響度評価を行っていただくか不明です。） | ２．要検討業務の場合の2省庁の選定については基本的には政府機関とクラウドサービス事業者とのコミュニケーションの過程で影響度評価結果を入手いただくことを想定しております。 |
| | ３．「ISMAP-LIUクラウドサービス登録規則（案）」制度全般について<br>今回の案では、「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」となっています。<br>SaaSでISMAPサービスリスト掲載のための管理策基準が多岐にわたるため、ISMAP取得のハードルが高いと考えます。<br>IaaS／PaaSはISMAP、SaaSはISMAP-LIUといった仕組みにならないか検討をお願いします。 | ３．SaaSにおいても、取り扱う業務・情報によってはセキュリティ上のリスクが大きくなるケースは想定されると考えます。管理策基準については、マネジメント基準で定めるリスク評価に応じて、CSPが自身に必要な管理策を選択し、言明することを求めておりますので、SaaSだから一概に管理策基準が多岐にわたる、ということはないと考えます。 |
| 22 | コメント(1)<br>【ISMAP-LIU クラウドサービス登録規則(案) 7.8 (7)】の例示である内部監査報告書及び内部監査調書を削除または一般的に外部公開可能な例示に変更して頂きたい。理由は、例示されている書類のように一般的に内部向けに作成した資料を外部者に閲覧して頂くためには、情報管理/文書管理を考慮すると相当な手続きが当事者に発生すると考えているためです。 | コメント(1)について、ISMAP-LIUクラウドサービス登録規則(案) 7.6 (7)に対するご意見と理解いたしました。<br>「様式2-3 内部監査に係る報告書」及び「様式2-3 内部監査に係る報告書_別紙」による報告内容に疑義が生じた場合に、報告内容の正確性等について確認する必要があるため、当該規定を設けております。<br>なお、マネジメント基準（ISMAP管理基準4.6.2等）において、内部監査の結果を内部監査報告書として管理すること、及び、監査結果の証拠として文書化した情報を保持することを求めていることから、マネジメント基準を遵守するクラウドサービス事業者にとって、内部監査報告書及び内部監査調書の情報管理・文書管理が過度の負担になるとは想定しておりません。 |
| | コメント(2)<br>対象業務一覧を明確化して頂きたい。例えば、【ISMAP for Low-Impact Use における 業務・情報の影響度評価ガイダンス（別紙1）】のP16脚注3とP17脚注4は同種の情報を別情報として扱っており定義が明確でないためです。 | コメント(2)について、対象業務一覧については、ISMAP-LIUの対象となる業務の幅が過剰に狭くならないよう抽象化しております。具体的な業務を列挙するとISMAP-LIUの対象となる業務が限定的となり、制度を広く利用頂けない懸念があるため、原案のとおりと致します。 |
| | コメント(3)<br>【ISMAP-LIU クラウドサービス登録規則(案) 5章 5.3】を対象業務一覧に記載されている業務と同じ審査期間にして頂きたい。理由は、対象業務一覧に記載されていないことで判断時期が異なることは、迅速なデジタル化の阻害要因になると考えているからです。 | コメント(3)について、対象業務一覧にない業務に使用するクラウドサービスに関しては、調達省庁等の影響度評価結果を含む事前申請について、制度所管省庁において慎重な検討を行う必要があり、現時点では、各半期末日の3ヶ月後にISMAP-LIU該当性を判断することとしています。 |
| | コメント(4)<br>【ISMAP-LIU クラウドサービス登録規則(案) 附則】は、調達を行う組織が単一の場合、実質的に実施が不可能と考えています。つきましては、2以上の政府機関等から影響評価結果を入手するではなく、1政府機関等から影響評価結果を入手するに変更して頂きたい。 | コメント(4)について、要検討業務の評価においては、対象業務の影響が低位であることの蓋然性を確認する必要があり、２省庁が低位であると評価したことをもって、この蓋然性の確認を行う想定であり、原案の通りとさせていただきます。 |
| | コメント(5)<br>ISMAP-LIU制度、特に影響度評価及び対象業務一覧の考え方について、調達府省間等で差異が生じないように十分な周知を実施して頂きたい。特に制度施行時は対象業務一覧が幅広に規定されているため徹底した周知をお願いしたい。 | コメント(5)について、制度における規定類の案への御意見ではないと認識しておりますが、御意見は拝聴いたしました。 |
| 23 | ＜対象箇所＞<br>（「ISMAP クラウドサービス登録規則」のうち改定箇所（第１章） p1中「ただし、リスクの小さな業務・情報の処理に用いる SaaS サービスを対象とした仕組みによる登録に関しては ISMAP-LIU クラウドサービス登録規則にて別途定める。」との記載部分）<br>・意見内容<br>当該部分について「ただし、リスクの小さな業務・情報の処理に用いる SaaS サービス、セキュリティ対策に関するSaaSサービス及び、遠隔地にあるパソコン環境を手元の端末から操作する仮想デスクトップ環境を提供するSaaSサービスを対象とした仕組みによる登録に関しては ISMAP-LIU クラウドサービス登録規則にて別途定める。」との変更を提案します。<br><br>（理由）<br>SaaSサービスは、今回のパブリックコメントの対象外であるISMAP-LIU クラウドサービス登録規則（案）「第２章用語の定義」にて「2.1 SaaS（Software as a Service）<br>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」と定義されていますが、明らかに業務系のサービスであるところのセキュリティ対策に関するSaaSサービス及び仮想デスクトップ環境を提供するSaaSサービスが例示されおらず、これらのサービスが扱う情報はコミュニケーション系のサービス等が扱う業務・情報とは大きく異なることから、現在の業務系のサービス及びコミュニケーション系のサービスを対象とした登録規則のみをISMAP-LIU クラウドサービス登録規則で定めると、セキュリティ対策に関するSaaSサービス及び仮想デスクトップ環境を提供するSaaSサービスに関する規則の検討が不十分となるため「ISMAP-LIU クラウドサービス登録規則にて別途定める」ものとして明示することが必要です。<br>（補足）具体的なセキュリティ対策に関するSaaSサービスとしては、EDR、MDM、CASB、DLP、WAFなどがあります。また、当該「ISMAP-LIU クラウドサービス登録規則にて別途定める」場合の検討事項として、セキュリティ系のSaaSでユーザーのPC内のファイルパス名としてユーザー名や個人名などが含まれるものを収集しているケース、未知の脅威かを確認するためファイルを一時的にクラウド上にアップロードしサンドボックス環境でテストするサービスがあることを踏まえる必要があります。 | ・「ISMAP-LIUクラウドサービス登録規則」「第2章　用語の定義」において、「SaaS」は「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。」として定めており、「具体的には」以降は代表的なSaaSの例を記載しているものです。このため、特定のSaaSを排除する意図は無く、セキュリティ対策に関するSaaSサービス、仮想デスクトップ環境を提供するSaaSサービス、他のクラウドサービスと連携するSaaSサービス等についても、定義に従いSaaSに含まれうるものと理解しております。<br>このため、御指摘の点につきまして、原案の通りとさせていただきます。 |

| | | |
|---|---|---|
| | ・意見内容<br>　当該部分について「ただし、リスクの小さな業務・情報の処理に用いる SaaS サービス、他のクラウドサービスと連携するSaaSサービスを対象とした仕組みによる登録に関しては ISMAP-LIU クラウドサービス登録規則にて別途定める。」との変更を提案します。<br><br>（理由）<br>SaaSサービスは、今回のパブリックコメントの対象外であるISMAP-LIU クラウドサービス登録規則（案）「第２章用語の定義」にて「2.1 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」と定義されていますが、二次的に影響が出るような情報を保存するSaaSサービスが例示されおらず、これらのサービスが扱う情報はコミュニケーション系のサービス等が扱う業務・情報とは大きく異なることから、現在の業務系のサービス及びコミュニケーション系のサービスを対象とした登録規則のみをISMAP-LIU クラウドサービス登録規則で定めると、他のクラウドサービスと連携するSaaSサービスに関する規則の検討が不十分となるため「ISMAP-LIU クラウドサービス登録規則にて別途定める」ものとして明示することが必要です。<br>（補足）他のクラウドサービスと連携するタイプのSaaSは、別のクラウドサービスのアカウントなどの認証情報が保存され、このアカウントなどの認証情報が漏えいした場合の影響が対象業務一覧にとどまらず、二次被害を誘発するケースがあります。当該「ISMAP-LIU クラウドサービス登録規則にて別途定める」場合の検討事項とする必要があります。 | ＜同上＞ |
| 24 | １　ISMAP-LIUについて<br>ISMAP-LIUの背景に、「過剰なセキュリティ要求より、当該サービスの活用が進まない」とあるが、そうではなく、監査費用＆内部工数/負荷が高い本制度をサービス提供者が利用したくないというのが本音なのでは。つまり、クラウドサービスリストに登録したいと思うサービス提供者が増えないということ。<br>政府系のクラウド調達だから仕方なく、政府に付き合ってあげているという所ではないのか？考え方はわかるが、実際の実務を考えると日本におけるIT関連の成長の足かせにしかならない制度では？<br><br>2　監査費用<br>これまで各省庁が選定する際の工数を、サービス提供者に転嫁しているだけではないのか？<br>ISMAPに登録しようとするサービス企業に対し、政府が監査費用を出すべきではないのか？<br><br>3 ISMAP-LIUについて<br>制度が煩雑かつ不明確である。<br>1 詳細管理策の内容が何を求めているのか？が分かりにくい。分かりやすいガイダンスを提供すべき。コンサルをつけないと、わからないような制度自体がナンセンスでは？<br>2 どこまでがクラウドサービスなのか？どういうサービスの範囲を登録するものなのか？が不明確である。<br>3 どこまで個別管理策に記載する必要があるのか？など、不明な部分が多い。個別管理策の記載という負荷が大きいのでは？<br>4 監査手続きも分かりにくい為、サービス提供者の監査負荷が増大するのでは？<br>5 対象となる業務に絞ることとによる煩雑さと対象なのかどうか？という曖昧さが増えることになるのではないか？LIUは、単純に管理策を限定した方がシンプルでよいのでは？<br><br>4　ISMAP管理基準<br>ISMAPおよびISMAPLIUのどちらも管理策の数は変わらないようだ。どうでもよい管理策もあるように見受けられる。現在にマッチしない管理策も多いように思われる。<br>3桁管理策が目標で、4桁管理策が手段であるので基本選択式と言われているが、果たしてそのような形になっているのだろうか？<br>詳細管理策の数は多いが、本当に有効な管理策に限定してはどうか？<br><br>5　ISMAP-LIUについて<br>ISO27001,ISO27017をベースとしたISMAP管理策であるが、ISMSおよびISO27017の認証取得をしている企業＆サービスでは、該当する管理策以外を監査等でみるなど効率的かつ意味のある制度であるべき。<br><br>6　ISMAP-LIUについて<br>限定的な管理策を外部監査対象とし、外部監査費用の低減となる。一方、内部監査による負荷は変わらないのではないか？<br><br>7.ISMAP-LIU クラウドサービス登録規則（案）<br>第7章 申請者に対する要求事項<br>7.1監査業務の業務契約を締結し監査を受ける<br>監査機関の監査に対する費用に対する補助金もしくは、負担無しで対応可能にするべきである。また、監査費用の負担を強いられるのであれば、27017等のISO（JIS）として規格化し、ISMSや27017のようなスキームにすべきである。<br><br>8.ISMAP-LIU クラウドサービス登録規則（案）<br>第5章 事前申請の審査5.3<br>対象業務一覧に該当しない場合のISMAP-LIUに該当判断に時間がかかりすぎる。<br><br>9.ISMAP-LIU クラウドサービス登録規則（案）<br>第5章 事前申請の審査5.1<br>対象業務一覧が特定のSaaSサービスの利用を前提とした内容に見える。<br><br>10.ISMAP-LIU クラウドサービス登録規則（案）<br>第2章 用語の定義1.1<br>SaaSサービスの具体例が書いてあるが、具体例以外のサービスが対象なのかの判断がつかないため、対象外の例示もしてほしい。セキュリティサービス（通信設備として）は対象なのかを明確にしてほしい（人によって解釈が変わる定義は望ましくない）<br><br>プロセスだけのパブコメではなく、意味のあるパブコメになることを期待する。 | １．ISMAP-LIUにおいては、従来のISMAPと比較して外部監査の監査項目が削減されており、クラウドサービス事業者にとっては監査コスト軽減が期待されています。また、ISMAP同様、クラウドサービスリストに登録し、原則利用を促すことで、調達省庁等において個別の審査項目が省略できることにより、調達省庁等にとっても効率化が期待できる制度と考えております。<br><br>２．ISMAPは、政府が調達するクラウドサービスに求められるセキュリティ水準が確保されていることを監査を通じて確認し、登録する仕組みです。監査費用はクラウドサービス事業者の負担となりますが、事業者にとっても、調達省庁等が登録サービスリストから原則利用すること、個別のセキュリティに係る審査項目が省略できることなどのメリットがあると考えられます。<br><br>３．いただいた御意見も踏まえ、継続して検討させていただきます。<br><br>４．ISMAP及びISMAP-LIUの管理策基準については、マネジメント基準で定めるリスク評価に応じて、CSPが自身に必要な管理策を選択し、言明することを求めております。ご指摘いただいた点については、今後継続的に検討をさせていただきます。<br><br>５．他の認証（監査）制度については、認証（監査）を実施している認証（監査）機関に対する要求事項がISMAPと異なる点、監査の深度や手法が異なる点等を踏まえ、現時点においては活用を検討しておりません。ご指摘の他認証制度との相互運用性については、制度運用の状況を鑑みつつ、今後の検討課題であると認識しています<br><br>６．ISMAP-LIUでは内部監査の結果の報告を求めておりますが、現行のISMAP制度においても、マネジメント基準として内部監査の実施を求めているため、内部監査の負担は大きく変わらないと考えております。なお、ISMAP-LIUは、外部監査対象範囲を縮小し、内部監査の実施状況報告については全統制目標を3年で一巡とすることによって、監査全体としては現行ISMAPよりも緩やかな制度設計としております。<br><br>７．現行ISMAP含めいただいた御意見については、継続して検討させていただきます。<br>また、LIUの対象業務一覧について、ISMAP-LIUは、セキュリティ上のリスクの小さな業務・情報の処理を対象としており、各政府機関において、具体的にどのような業務・情報の処理がISMAP-LIUの対象となり、また対象外となるかを評価する必要があるため、このような制度設計としております。制度の運用として、要検討業務に該当する事前申請を受け、当該申請がLIUの対象業務として整理される場合は、対象業務一覧を拡充する予定です。<br><br>８．対象業務一覧にない業務に使用するクラウドサービスに関しては、調達省庁等の影響度評価結果を含む事前申請について、制度所管省庁において慎重な検討を行う必要があり、現時点では、各半期末日の3ヶ月後にISMAP-LIU該当性を判断することとしています。<br><br>９．対象業務一覧においては、現時点で想定される対象業務を列挙したものであり、特定のSaaSサービスの利用を前提とするものではございません。要検討業務についても、事前申請をいただいた後、LIUの対象業務として整理される場合は、対象業務一覧を拡充する予定です。<br><br>10．一般に機密性2情報のうち、リスクが低いと整理される情報を扱う業務は限定的でありますが、リスクが中高位の業務は多岐にわたるため、例示を行う事は適切では無いと考えておりますので、原案のとおりと致します。 |
| | [意見１]<br>・該当箇所<br>・政府情報システムのためのセキュリティ評価制度(ISMAP)基本規程<br>・第3章 クラウドサービスの登録<br>・3.5 登録の更新<br>・3.4で認められた登録の有効期限は、登録の対象となった監査の対象期間の末日の翌日から1年4ヶ月後までとする。<br>・意見内容<br>・登録の有効期限を延長していただきたい（例：「3年4ヶ月後」）。<br>・理由<br>・プライバシーマークやISMSなど、ISO認証等の審査は3年毎等の実施であり、ISMAP-LIUに関しても、CSPの人員的・金銭的負担なども考慮に入れ、複数年毎の審査にしていただきたい。 | [意見１]について、監査対象期間が一年となるため、それに申請等にかかる期間4ヶ月合わせた1年4ヶ月としております。 |

| | | |
|---|---|---|
| 25 | [意見２]<br>・該当箇所<br>・ISMAP-LIUクラウドサービス登録規則（案）<br>・第3章 サービス登録に関する事前申請<br>・3.1 申請者は「様式1-1 事前申請書」を使用し、以下の文書を添えて、別表1 に示す提出方法によりISMAP 運用支援機関に提出する。<br>・意見内容<br>・「様式1-1 事前申請書」がパブリックコメント募集ページに掲載されていない。<br>・理由<br>・CSPとしてはできるだけ早いうちに書式を確認しておきたいので、ISMAP-LIUの正式施行前に書式を公開していただきたい。<br><br>[意見３]<br>・該当箇所<br>・ISMAP-LIU クラウドサービス登録規則（案）<br>・第3章 サービス登録に関する事前申請<br>・3.3 申請者は、「様式1-2 SaaS の利用に係る業務・情報の影響度評価シート」を準備するに当たり、自身が提供するサービスの機能等を記載の上、1 以上の政府機関等から業務・情報の影響度評価結果（以下「影響度評価結果」という。ただし、事前申請を行う日から1年以内に評価されたものに限る。）を入手しなければならない。<br>・意見内容<br>・影響度評価を行う「政府機関等」として、独立行政法人を含めた文章にしていただきたい。<br>・理由<br>・ISMAPにおけるクラウドサービス利用者には独立行政法人も含まれるので。<br><br>[意見４]<br>・該当箇所<br>・ISMAP-LIU クラウドサービス登録規則（案）<br>・第3章 サービス登録に関する事前申請<br>・3.3 申請者は、「様式1-2 SaaS の利用に係る業務・情報の影響度評価シート」を準備するに当たり、自身が提供するサービスの機能等を記載の上、1 以上の政府機関等から業務・情報の影響度評価結果（以下「影響度評価結果」という。ただし、事前申請を行う日から1年以内に評価されたものに限る。）を入手しなければならない。<br>・意見内容<br>・CSPから「政府機関等」へ評価依頼をすれば、多忙等を理由に拒否されたり、評価完了までに何か月も待たされたりしては申請が滞ってしまうので、「政府機関等は評価を速やかに実施する」といった記述を追加していただきたい。<br>・ISMAP-LIUが正式に施行されるにあたり、ISMAP運営委員会から「政府機関等」に対して、「CSPから影響度評価の依頼があった場合は速やかに評価を実施すること」というような通達を出していただきたい。<br><br>[意見５]<br>・該当箇所<br>・ISMAP-LIU クラウドサービス登録規則（案）<br>・第3章 サービス登録に関する事前申請<br>・3.3 申請者は、「様式1-2 SaaS の利用に係る業務・情報の影響度評価シート」を準備するに当たり、自身が提供するサービスの機能等を記載の上、1 以上の政府機関等から業務・情報の影響度評価結果（以下「影響度評価結果」という。ただし、事前申請を行う日から1年以内に評価されたものに限る。）を入手しなければならない。<br>・意見内容<br>・申請対象のクラウドサービスがISMAP-LIUに該当するか否かは、CSPによる自己申告としていただきたい。<br>・理由<br>・クラウドサービスがISMAP-LIUの対象であるか否かを確認するためだけに、決して作業量が少ないとは言えない影響度評価シート（様式1-2）への記入は、政府機関とCSPへ余計な負荷を与え、ISMAP-LIU新設の目的にそぐわないと考える。<br>・ISMAP（およびISMAP-LIU）は機密性2情報を取り扱うクラウドサービスが対象であるが、実際に各サービスがどのレベルの機密性情報を扱うかはCSPやクラウドサービス利用者の判断に委ねられるのであれば、申請対象となるクラウドサービスがISMAP-LIU対象か否かは、CSPによる自己申告でも問題ないと考える。<br><br>[意見６]<br>・該当箇所<br>・ISMAP-LIUクラウドサービス登録規則（案）<br>・第7章 申請者に対する要求事項<br>・7.2 申請者は、別紙2 に規定する要件を満たす内部監査を実施し、「様式2-3 内部監査に係る報告書」により、その結果をISMAP 運営委員会に報告しなければならない。<br>・意見内容<br>・ISMAP-LIUの対象となるような、リスクの小さな業務・情報を対象とするクラウドサービスについては、「様式2-3別紙 内部監査を実施した統制目標と内部監査結果の概要」における「17.2 冗長性」の項目を内部監査項目から外したい。<br>・理由<br>・手順を明確に定めた障害復旧案をまとめておくことで、冗長化を行わなくても運用に耐えられると考えられるため、ISMAP-LIUの対象となるようなクラウドサービスにおいては、冗長化は必須の要件ではないと考える。 | [意見２]について、制度規程が確定した段階に合わせて公開いたします。<br><br>[意見３]について、独法・指定法人を対象にするに当たっては、本制度の審査状況に支障がないことや、国の行政機関以外の政府機関等（独立行政法人又は指定法人）における影響度評価の体制についても留意する必要があると考えており、本制度開始当初においては、原案のとおりとすることが適当と考えます。<br><br>[意見４]について、ISMAP-LIUは政府機関等における具体的なニーズが存在するSaaSを対象とする仕組みとして想定しております。従いまして、業務・情報の影響度評価の実施はCSP及び政府機関等の双方向的なコミュニケーションにより実施されることが妥当であると考えております。政府機関等の具体的なニーズを考慮することなくISMAP-LIUの申請が実施されることは、制度の狙いではないため、原案のとおりとさせていただきます。<br><br>[意見５]について、クラウドサービスによっては、取り扱う利用者情報が比較的限定的であるものも存在する一方、取り扱う情報は利用者の使い方に大きく依存するサービスもあると考えており、クラウドサービス事業者において該当性を判断できないケースもあると考えております。このため、ISMAP-LIUにおいては利用者である政府機関の影響度評価を必須と位置づけ制度設計をしたものです。また、デジタル庁が策定し公表している「デジタルガバメント推進標準ガイドライン」においては、政府機関は調達プロセスに先だって「業務の把握と分析」および「データの把握と分析」を行うこととされており、この中でISMAP-LIUに係わる影響度評価を行うことを想定されるため、政府機関に対する追加的な負担はないものと考えております。<br>以上から、ご意見については原案の通りとさせていただきます。<br><br>[意見６]について、ISMAP-LIUは「リスクの小さな業務・情報を対象とするクラウドサービス」を対象としておりますが、管理策自体は現行ISMAPから削減しておりません。そのため、ISMAP-LIUクラウドサービスリストへの登録申請を行うクラウドサービスについては、全ての統制目標としての管理策を原則として実施する必要があり（ISMAP管理基準2.2.4）、また、実施している全ての統制目標を内部監査の対象とする必要があります。<br>なお、クラウドサービス事業者は、自身の提供するサービスと照らして統制目標の合理的な適用が不可能な理由を示すことにより、当該統制目標を対象外とすることができます。この場合、対象外とした統制目標を内部監査の対象とする必要はありません。ただし、「合理的な適用が不可能な理由」はISMAP運用支援機関による技術的審査（ISMAP-LIUクラウドサービス登録規則10.1）において確認され、当該理由が妥当でない場合には、ISMAP-LIUクラウドサービスリストへの登録が認められないことにご留意ください。 |