**政府情報システムのためのセキュリティ評価制度(ISMAP)に関する BSA からの提言**

| | |
|---|---|
| **①ISMAP の登録に向けてネックとなっている点** | **[ISMAP 登録に要する費用、管理項目数]**<br>・ISMAP 認証の取得と維持にかかる費用（外部監査機関に支払う費用、内部費用等）が高額であることがクラウドサービス事業者（以下、CSP）にとってネックとなっています。CSP の経営層は ISMAP に登録する重要性は理解しているものの、認証取得費用を考慮し、優先度を上げることに躊躇してしまう傾向があります。毎年度の監査が求められることと、監査対象となる管理項目数の多さから、CSP の中には専任職員の採用を含めて、1 億円近い費用が毎年かかる場合もあります。<br><br>・他国の政府認証プログラムと比較し、ISMAP は桁違いに高額であり、取得と維持にかかる費用の点では、米国の同等の Federal Risk and Authorization Management Program（FedRAMP）に匹敵するケースもあります（外部監査の費用だけではなく、年間のモニタリング等、各々の認証の取得と維持にかかる費用を含む）。また、外部監査費用が ISMAP の約 1/2 で更新期間が 2 年であるオーストラリアの The Infosec Registered Assessors Program (IRAP)と比較しても、ISMAP に約 4 倍の費用が必要となる場合もあります。管理項目数では、FedRAMP の約 3 倍の項目を指定するチェックリストベースのアプローチを採用していますが、リスク・ベースのアプローチをとることにより、制度を改善できると考えます。 |

| | |
|---|---|
| | ・CSP の社内分析では、ISMAP の監査項目の 50%以上が SOC2 ならびに ISO27000 シリーズの認証制度と互換性があることが判明しており、CSP が ISMAP の要件を満たすため大量の重複監査を実施することが要されていることを意味しており、厳密に開発された国際標準との不一致は、セキュリティの成果を改善することなくセキュリティのコンプライアンスのコストを増加させてしまうこととなり、重要な機会損失となっています。<br><br>・また、単価の高い IaaS 事業者も単価の安い SaaS 事業者も同程度の金額がかかっており、単価の低い SaaS 事業者は売上高も低くなりがちで事業として成立させにくくなります。このような事情から、ISMAP クラウドサービスリストに登録できない SaaS 製品を抱える CSP もおり、初期費用がかかるため、多くの中小規模の SaaS 企業は申請を控えることとなります。利用する政府にとっても、導入コスト削減や迅速な開発という点で、SaaS 活用が重要となることから、制度の見直しが必要と考えます。<br><br>・ISMAP の参入障壁を下げるためにも、他国制度や国が置かれている状況を考慮し（添付表を参照）、管理項目数の見直し等を通し、認証取得コスト（外部監査機関に支払う費用、内部費用等）を下げることを求めます。 |

| | |
|---|---|
| **②ISMAP 制度の一連のプロセスにおいて、特に負担と感じる点や課題と考える点** | **[管理基準数・構成]**<br>①でも触れているように、現在の ISMAP における管理基準の構成は複雑であり、CSP に管理項目をマッピングするよう求める方法は CSP 側にとっての負担を大きくしています。ISMAP は、機能や情報が顧客にどのように提供されるかについて詳細な記述を要求し、必須と非必須の管理策が混在し、最大で 4 桁の管理策が存在します。要求される詳細度や管理項目の分類の複雑さは、非常に大きな負担となります。既に CSP 側が設けている管理策が ISMAP の管理基準を満たすものがある場合、それを紐づける作業を要します。ISMAP が ISO をベースに構成されていてもこの作業は発生し、CSP にとっては選択制であること自体が大きな追加の負担になってしまっています。選択制であることは異例であり、他の認証制度は普段全ての管理基準が必須となっています。選択制であると、どの管理基準を言明する必要があるのかの確認、及び、言明しない場合にはその理由を提供する追加作業が発生します。選択した場合でも、数百の管理基準を言明する必要があり、主要国家の政府調達のためのクラウド認証制度の中でも管理基準の数が極めて多く、認証の取得を難しくしています。管理基準の数を大幅に削減し、CSP 側で非必須の管理基準を選択する負荷を軽減する制度に改定することを提案します。<br><br>**[監査サイクル]**<br>・上記にあるように、単年での監査サイクルにより、CSP にとって毎年の認証取得コストの負担が大きくなっています。監査 |

| | |
|---|---|
| | サイクルを、3 年に一回の頻度での更新に変更すること、また、監査内容の提出期限は監査完了後 6 か月に延長し、CSP がグローバルな監査サイクルを柔軟に管理できるシステムを導入することを推奨します。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。<br><br>・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2 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><br>**[登録サイクル]** |

| | |
|---|---|
| | 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>**[他認証の証跡再利用]**<br>また、運用状況監査のサンプリング手法に制限があり、母集団から監査機関が任意に証跡を指定（サンプリング）しています。他制度で提出した証跡と異なる指定により、他認証の証跡を再利用できない場合が多発しており、監査計画時の想定（制度設計上、他認証の証跡再利用が可能である）が崩れて証跡準備に多大な工数がかかる事態となっています。他認証の証跡再利用（特に運用状況監査のサンプリング手法）を可能および監査機関との認識を合わせて頂くことを奨めます。<br><br>**[制度側のリソース不足]**<br>また、一連のプロセスを長引かせている一因として、申請時に窓口担当となる制度運用担当者のクラウド監査に関する経験不足が挙げられます。共通理解に至るまで多くのやりとりが発生することから、申請から承認までに半年ほどの期間がかかる場合も発生しています。更新においても、初回申請と同様の問い |

| | |
|---|---|
| | 合わせを受けることがあり、容易に更新手続きが進まないまま、次の監査期間が開始するという、CSP にとって運用しづらい状況を生んでいます。<br><br>**[提出書類]**<br>ISMAP では、多くの提出書類を CSP が作成し提出することを要求していますが、申請プロセスに精通した認定審査員が申請者に代わって記入し、プロセスを簡素化することを求めます。例えば、様式１に求められている情報は、監査法人が監査報告にいずれ含む情報であるため、CSP が自ら提供する必要がないと考えられます。他にも監査報告にいずれ含まれる情報が CSP からも求められている場合は、CSP の提出物から省略して頂くことを推奨します。<br><br>**[ISMAP プロセスに無い追加要件]**<br>一方、文書にある要件に含まれない追加要件事項を満たすよう要請される場合もあり、正式な ISMAP のプロセスにはない、審査手続きが発生しています。CSP と監査法人は事前審査などの準備作業を進めないように ISMAP 運営委員会から要請される場合もあり、結果的に、CSP 側の ISMAP 登録スケジュールに数カ月の遅れが生じています。 |
| **③外部監査機関の逼迫状況に関する認識、CSP と監査機関とのコミュニケーション 上ネックとなる点** | **[登録監査機関]**<br>監査機関が少数の監査法人に限定されていることが、ISMAP 取得にかかる期間を長引かせています。外部監査機関に監査を依頼しても、監査機関のリソース不足を理由に半年以上待つこと |

| | |
|---|---|
| | となったり、また、CSP が提供するソリューションの特性や作業の複雑さから監査機関が監査を受託できない場合もあります。登録監査法人 5 社の能力の中で、ISMAP 認証取得を希望する CSP の需要に応えるには不十分な状況となっています。また、監査法人が CSP 提供のサービスのパートナーになっている場合においては、利益相反を理由に受託しない場合もあります。上記のように ISMAP に関連した監査を CSP が希望するタイミング及びコストで依頼することが難しくなっているため、監査機関のリソースの拡大、また、監査機関を監査法人以外にも広げる検討を求めます。また、監査人の要件が日本国籍を持つ者に限定されており、会計監査法人のグローバルネットワーク形態及び監査人の英語対応能力を考慮すると、海外の統制を監査する負荷が高くなります。 監査機関に海外監査が円滑にできる機関を追加することを奨めます。 |
| **④クラウドサービス登録後の運用（変更手続き、インシデント対応、ISMAP 運営 委 員会の運営等）において、改善すべき点** | **[新規サービスの追加]**<br>既に ISMAP 登録済みのプラットフォーム上に同 CSP による新規サービスが追加された場合に、その特定のサービスが登録されていない（ISMAP の言明書に記載がない）というだけで、サービスの導入を断念せざるを得ない場合があります。同一プラットフォーム上にあるサービスであれば、リスクも低く、言明書に記載のないサービス（機能）であっても、リスク判断を調達省庁でした上で導入できるように、同じプラットフォームでの新サービスの場合は、調達省庁の判断で導入できることを明示頂くことを奨励します。将来的に ISMAP への登録に進む予定のサービスであっても、文書で言明されていないことをリス |

| | |
|---|---|
| | クと受け止め、登録がないと使えないと調達省庁側で認識する傾向があることから、この点を通達、もしくは、明確にガイド頂くことを求めます。<br><br>**[国内の連絡窓口]**<br>日本国内にいる 連絡先窓口として指定する必要がありますが、グローバル事業者の多くは、日本国内にセキュリティフレームワークに精通した担当者がいないため、日本人以外でも海外にいる担当者を窓口とできるようにし、英語でのやり取りを可能にするなど、連絡窓口の指定に柔軟性を持たせることを求めます。<br><br>**[登録後の運用フィードバック先]**<br>運用期間中の問い合わせ先は IPA となっていますが、制度設計に関するフィードバック先がないため、制度改善に対する要望を受け付ける窓口を設置して頂くことを推奨します。 |
| **⑤その他、制度改善の方向性、制度全般に対するご意見・要望** | **[経済安全保障推進法と ISMAP との整合性]**<br>現在、政府で検討が進められている経済安全保障推進法案と ISMAP の位置付けを明確にして頂くことを求めます。ISMAP が経済安全保障推進法により導入されてくる諸要件と関連してくる場合は、製品や営業戦略に影響が出てくるため、可能な限り方向性等を早めに公表して頂くことを求めます。<br><br>**[ISMAP-LIU]** |

| | |
|---|---|
| | ・ISMAP LIU が今年の秋に開始しましたが、登録された CSP とし制度運営側との情報共有する場の設置を推奨します。このような機会を設けることで、制度運用者(IPA)、ISMAP 運営委員会と CSP 間の意思疎通が円滑となり、制度改善につながると考えます。<br><br>・ISMAP-LIU に関しては、対象業務を透明性を持った形で明確化することや、 対象業務一覧に掲載されていないクラウドサービスの事前審査の迅速化、 政府機関等から入手する影響度評価結果数の削減、 各省庁への啓蒙活動（勉強会など）の実施状況の共有、 現在の ISMAP LIU 採用省庁の共有等について協議することが有益と考えます。 |

| 認証制度名称 | 運営組織国籍 | 再監査頻度 | 管理基準数 | 報告書対応言語 | ISO相互認証 | 評価方法 | 参照 |
|---|---|---|---|---|---|---|---|
| ISMAP | 日本 | １年毎 | 1,157 | 日本語 | しない | 監査法人 | https://www.ismap.go.jp/csm |
| FedRAMP | 米国 | １年毎３分の１監査 | 325 (中), 421 (高) | 英語 | しない | 監査法人 | https://www.fedramp.gov/ |
| BSI C5 | ドイツ | １年毎 | 121 | 英語、ドイツ語 | する | 監査法人 | https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html |
| ENS | スペイン | ２年毎 | 73 | スペイン語 | する | 監査法人 | https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/esquema-nacional-de-seguridad |
| CSPN | フランス | ３年毎 | 該当なし | 英語、フランス語 | しない | 第三者評価 ＋ANS | https://www.ssi.gouv.fr/administration/produits-certifies/cspn/ |
| AgID | イタリア | ２年毎 | 20 | イタリア語 | しない | 自己評価 | https://cloud.italia.it/ |
| Cyber Essentials | 英国 | １年毎 | 89 | 英語 | しない | 自己評価 | https://www.ncsc.gov.uk/cyberessentials/overview |
| Cyber Essentials + | 英国 | １年毎 | 89 | 英語 | しない | 監査法人 | https://www.ncsc.gov.uk/cyberessentials/overview |
| IRAP | オーストラリア | ２年毎 | 837 | 英語 | 他の承認に使った | 監査法人 | https://www.cyber.gov.au/acsc/view-all-content/programs/irap |
| ISO 27001 | 国際 | １年毎の維持審査 | 93 (Annex A 規格) | 英語 | する | 監査法人 | https://www.iso.org/standard/82875.html |
| Common Criteria | 国際 | ５年間有効 | トによって異なる | 英語 | しない | 監査法人（認定テ | https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/IT-Sicherheiskriterien/CommonCriteria/commoncriteria_node.html |

| Certification Nam | Country | Frequency of Aud | Number of Contro | Submission langu | Recognition of ISO | Verification meth | Reference |
|---|---|---|---|---|---|---|---|
| ISMAP | Japan | Annual | 1,157 | Japanese | No | External audit | https://www.ismap.go.jp/csm |
| FedRAMP | US | 1/3 assessed annu | edium), 421 (High) | English | No | External audit | https://www.fedramp.gov/ |
| BSI C5 | Germany | Annual | 121 | English, German | Yes | External audit | https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html |
| ENS | Spain | Biennial | 73 | Spanish | Yes | External audit | https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/esquema-nacional-de-seguridad |
| CSPN | France | Triennial | N/A | English, French (re | No | Third party evaluat | https://www.ssi.gouv.fr/administration/produits-certifies/cspn/ |
| AgID | Italy | Biennial | 20 | Italian | No | Self-assessment | https://cloud.italia.it/ |
| Cyber Essentials | UK | Annual | 89 | English | No | Self-assessment | https://www.ncsc.gov.uk/cyberessentials/overview |
| Cyber Essentials + | UK | Annual | 89 | English | No | External audit | https://www.ncsc.gov.uk/cyberessentials/overview |
| IRAP | Australia | Biennial | 837 | English | Can re-use evidence u | External audit | https://www.cyber.gov.au/acsc/view-all-content/programs/irap |
| ISO 27001 | International | Annual verification | 93 Annex A Control | English | Yes | External audit | https://www.iso.org/standard/82875.html |
| Common Criteria | International | Five year life-span | g on security target | English | No | External audit (cert | https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/IT-Sicherheiskriterien/CommonCriteria/commoncriteria_node.html |