「ISMAP-LIUクラウドサービス登録規則（案）」等に対する BSA ｜ザ・ソフトウェア・アライアンスからの意見

2022年7月5日

BSA| The Software Alliance[1]（BSA｜ザ・ソフトウェア・アライアンス、以下、「BSA」）は、内閣サイバーセキュリティセンター、経済産業省、総務省、および、デジタル庁（以下、「関係省庁」）が政府全体におけるデジタルトランスフォーメーションの加速化に向けて不断の努力を続けていることを高く評価しています。今回、低リスクの SaaS の採用を促進するために策定された、「ISMAP-LIU（英語名:ISMAP for Low-Impact Use）」に関し、我々の意見を述べさせて頂きます。

総論

BSA は、政府やグローバル市場において、世界のソフトウェア産業を代表する主唱者 です。BSA の会員企業は、最先端のクラウドコンピューティング技術およびサービス提供で世界を牽引しており、各国政府が、ネットワークセキュリティやシステムの可用性を高めながら、その俊敏性、生産性、および革新性を向上することを支援しています。その経験に基づき、以下の提言を述べさせて頂くことで、政府の目標である「クラウド・バイ・デフォルト原則」の実現に貢献したいと考えております。

提言

関係省庁が認識しているように、SaaS は、機密性 2 情報のうち、重要度の低い情報のみを扱うサービスを含め、幅広いサービスを提供しています。過剰なコンプライアンス要件を回避し

[1] BSA の活動には、 Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Dassault, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.が会員企業として参加しています。詳しくはウェブサイト（http://bsa.or.jp）をご覧ください。

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office

たクラウドのセキュリティ評価の仕組みを策定することで、日本の公共部門での SaaS サービスの利用を一層促進することができます。

ISMAP-LIU においては、外部監査対象となる管理策基準数を減らし、また、全統制目標の内部監査実施状況を三年というサイクルで求める年次報告など、公共部門のクラウド導入を促進するのに役立つと思われる、現行制度への変更が加えられています。実際、このような変更を ISMAP 自体に適用することが、非常に有効であると考えます。

現在、意見募集にかけられている ISMAP-LIU においては、以下の推奨事項を採用することで、関係省庁の目標がより達成しやすくなると、我々は考えております。

対象となる業務や情報を透明性を持って示すこと
(「ISMAP-LIU クラウドサービス登録規則（案）」 第 3 章～6 章、附則)

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。

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。

「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。

「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。

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。

審査プロセスの改善
(「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)

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。

- **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。

- **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。

- **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。

- **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。

- **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[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。

  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。

[2] https://jicpa.or.jp/specialized_field/files/2-8-33-2-20200914.pdf
Q15: 19-20ページ

- **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。

- **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。

- **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。

  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。

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。

結論

BSA は、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、BSA と BSA 会員企業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。

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office