日本のデジタルトランスフォーメーションに関して
BSA ｜ザ・ソフトウェア・アライアンスからの提言

2021年10月1日

BSA｜The Software Alliance[1] （BSA｜ザ・ソフトウェア・アライアンス、以下、「BSA」）は、デジタル社会形成の司令塔として機能するデジタル庁（以下、「貴庁」）の発足を歓迎し、国民目線でデジタル時代の官民インフラを作り上げようとする目標を支持します。BSA と会員企業は、世界各国の政府と緊密に連携し、市民サービスの向上に貢献しており、デジタル庁が今後実施していく様々な取り組みを支援するために協力していけることを期待しています。

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 の会員はクラウドコンピューティング、セキュリティソリューション、AI（人工知能）と機械学習、IoT（モノのインターネット）などの最先端の技術やサービスを世界に先駆けて提供し、世界経済の成長と回復を促進するデータ駆動型イノベーションの最前線にいます。BSA の会員は企業顧客にソフトウェアソリューションを提供しており、その事業モデルは顧客データを収益化することに依存していません。実際には、プライバシーやサイバーセキュリティなど、顧客のコンプライアンスを促進するツールを数多く提供しています。日本においては、これらのエンタープライズ・ソフトウェア企業は、中小企業や大企業、中央政府や地方自治体、病院、学校、大学、非営利団体など、さまざまな組織を支え、政府が進めているデジタルトランスフォーメーションの取り組みに寄与しています。

[1] BSA の活動には、Adobe, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, ServiceNow, Siemens Industry Software Inc., Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, Zendesk, Zoom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

「デジタル社会の実現に向けた重点計画」[2]において、貴庁が市民サービス向上のために省庁間でのデータ活用促進を重視する政策を公表したことを我々は歓迎します。中央政府や地方自治体の情報システム及びウェブサイトの刷新に統一性をもたらし、医療・教育・防災分野でデータ連携を促進し、認証制度の整備によりデータの信頼性を確保する取り組みは、いずれも重要であり、我々はこれらの目標を全面的に支持します。このような重点計画によって、より強靭な社会造りが可能となります。我々はこれらの取り組みを推進するために、グローバル市場で利用可能な最先端の技術の恩恵を公共機関が受けられるよう、貴庁との連携について引き続き模索していきたいと考えております。

上記の目標を達成するには、安全なクラウドコンピューティング・サービスの調達と利用がますます重要になっており、以下の提言を述べさせて頂くことで、我々は貴庁の優先事項に貢献したいと考えております。

提言

デジタル社会におけるクラウドコンピューティング普及を成功させるために、「政府情報システムのためのセキュリティ評価制度（ISMAP）」の継続的改善を求めます。

BSA は、貴庁が「クラウド・バイ・デフォルト」原則を公共分野において確実に実践することに注力し、共通的な基盤・機能をを提供する複数のクラウド・サービス（IaaS、PaaS、SaaS）の利用環境である「ガバメントクラウド」の構築に向けた議論を進めていることを歓迎します。また、この取り組みを実現するための土台となる「政府情報システムのためのセキュリティ評価制度（ISMAP）」（以下、「ISMAP」）のさらなる改善が検討されていることを高く評価します。現行の制度は、ISMAP クラウドサービスリストへの登録を希望するクラウドサービスプロバイダー（CSP）に、多大なコンプライアンス負荷と法外な費用を課します。クラウド普及を促進するために、貴庁が関連省庁や影響を受ける産業界のステークホルダーと連携し、以下の点を考慮に入れ、ISMAP を継続的に改善することを奨めます。

- クラウドサービスの責任共有モデル[3]を強調し、周知徹底させること。クラウド導入を成功させるには、クラウド利用者や調達者が、クラウド環境で安全なアプリケーションを開発し、必要に応じて CSP が提供するツールや対策を自ら

[2] http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20210615/siryou6.pdf

[3] https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/

の責任で利用し、セキュリティ・リスクを最小限に抑えることが求められている、ということを理解することが重要です。ISMAP に責任共有の原則を明確に盛り込むことで、クラウドサービスのリスク管理をするための管理基準の設定と維持において、CSP と顧客との間とのクラウド運用に関しての異なる責任が認識されるようになります。また、自らが管理し、責任を負う環境の側面において、可視性の無い環境以外において、どの当事者が説明責任を負うのかを明確にすることができます。これにより、アクセス権を持たない顧客データやシステムに対して、セキュリティ要件や義務を CSP に課すということが回避され、不適切な義務を課せられた場合に、結果的にセキュリティやプライバシーに逆効果となる事態を避けることができます。

- 様々なクラウドサービスのモデル（SaaS、IasS、PaaS）の特徴的な要件を考慮し、 これらのサービスに最も関連するリスクを管理するために最適化された必須のセキュリティ管理を定義することにより、現行の ISMAP をより柔軟に、実施しやすくすること。

- 既に取得済みの国際規格と重複する管理基準の適用を免除することで、反復的な監査手順を削減すること。多くの CSP はすでに国際的に認知された規格（ISMS-JISQ/ISO 27000 シリーズ）の認証を取得していることから、それらを認め、反復的な手続き、及び、過去の認証手続きで提供された証跡の再利用という ISMAP の要求事項を排除することで、政府関係者を含む、全てのステークホルダーの負担を軽減するができます。また、これにより、さらに多くの日本企業が ISMS/ISO 認証を取得することを促進し、積極的にそれらが活用されることで、国際的なビジネス・チャンスの拡大にもつながります。

- また、国際的に認知された第三者機関による認証および監査結果を、ISMAP の関連する管理基準および要件に準拠している証拠として認めることにより、非実用的で反復的な現地監査の必要性が減ります。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。

- ISMAP に登録する監査法人の数を増やすことで、CSP による柔軟な選択を可能とすること。ISMAP で要求される監査手続を満たすために、現在また今後の人材需要の集中と不足を避けるためにも、ISMAP に登録する監査法人の数を増やす方法を検討することを強く推奨します。これにより、監査法人間の公正な競争が実現され、CSP は現行の 4 つの登録監査法人から選択することを強いられず、より多様な選択肢を得ることができます。また、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。

- 国際的なクラウド・セキュリティのベスト・プラクティスに沿った、頻度を減らした 監査スケジュール（例：三年に一度）を設定し、CSP と政府双方の監査作業を削減すること。毎年の監査では、CSP は事実上、連続して監査プロセスを実施しなくてはならず、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すこととなります。調達省庁側にとっても、年度の契約更新の負荷が増すこととなります。

- 申請・登録の受付を、四半期ごとではなく、年間を通じて行うことができるようにすること。年に 4 回の申請・登録に限定されると、ISMAP 登録を目指す CSP にとっては、3 ヶ月以上の遅れが生じる可能性があります。年間を通して継続的に申請・登録を行うことで、ISMAP は急速に進化するクラウドの技術に対応することが可能となります。

最新技術を反映した、最も効果的なセキュリティ・アプローチの採用を推進することを求めます。

今後、地方自治体の基幹システムを含めたシステムの統一・標準化を貴庁が進め、ガバメントクラウド上に構築していくと我々は理解しております。自治体が保有するデータの有効活用が期待される本取り組みの進展に我々は期待を寄せています。自治体が革新的なクラウド技術やサービスを利用して、想定通りのデータ活用を実現するためには、貴庁が総務省と協力し、現行の「地方公共団体における情報セキュリティポリシーに関するガイドライン」[4]（以下、「ガイドライン」）を見直し、更新することを強く要望します。本ガイドラインでは、物理的なネットワーク分離を推奨する三層の対策によるセキュリティ施策が引き続き盛り込まれています。市民のプライバシーと個人情報を保護するという目的を我々は全面的に支持しますが、このような時代にそぐわない方針を維持することは、公的機関によるクラウドコンピューティング・ソリューションの採用を妨げるものであり、データのリスクに相応していません。実際、総務省が最近、意見募集にかけた「クラウドサービス提供における情報セキュリティ対策ガイドライン」の第 3 版では、絶えず進化するクラウド技術環境と複雑化するデジタルプラットフォームの状況を見越し、マルチクラウドインフラと責任共有モデルを考慮しています。このことからも、最新の技術的進歩を反映した政策をデジタル庁にて調整頂くことを求めます。

多くのクラウドサービスは、暗号化や厳格なアクセス管理システムなど、国際的に認められた機能を実装することで、世界水準のデータセキュリティを実現しています。BSA 会員を含む、多くのグローバルな CSP は、データセキュリティへの大規模な投資をしており、利用可能な機密個人情報のために、最も効果的なデータセキュリティを提供しています。これらの最高水準の安全なソリューションの使用を可能にすること

[4] https://www.soumu.go.jp/main_content/000726079.pdf

を、デジタル庁が政策により確かなものとすることが不可欠であると、我々は考えます。

このような最高水準のデータセキュリティ・ソリューションは、リスクベースで成果重視の手法を採用しています。[5]採用されているのは、ゼロトラスト・セキュリティ・アーキテクチャ[6]、高度なユーザーID管理やアクセス制限システム、常時接続の仮想プライベート・ネットワークや仮想ネットワーク・セグメンテーションなどのネットワーク制御、強力なデータ暗号化などのセキュリティ対策です。デジタル庁は総務省と連携し、時代にそぐわない物理的なネットワーク分離要件やデータローカライゼーション要件を撤廃し、代わりに現在の技術に合わせたセキュリティ・ソリューションを採用し、成果重視のリスク管理制御に焦点を当て、「多層防御」[7]の原則に基づいた ベストプラクティスを採用し、安全なクラウドコンピューティングサービスの調達と使用により、政府業務をより効果的に推進させるべきです。これにより、日本のガバメントクラウドの柔軟で堅牢な基盤を構築することができます。このような重要な実践を採用した政府は[8]、クラウドコンピューティングを最も効果的に活用しながら、強力なサイバー脅威に対しても、より効果的に対処することに成功しています。

サイバーセキュリティのソリューションは、官民が連携し、市場主導型のソリューションを採用するときに最も効果を発揮します。[9]日本のデジタルトランスフォーメーションとセキュリティ政策が、セキュリティ対策の最新の進歩の恩恵を受けられるように、BSA と BSA 会員企業はデジタル庁と連携できることを願っています。

公共部門におけるデジタルスキル向上のための官民連携

デジタル庁が、官民のデジタル人材育成の強化に重点を置いていることを我々は高く評価しています。現在のテクノロジーの可能性を十分に活用するために、BSA 会員が提供する様々なトレーニングの機会[10]をデジタル庁が活用することを推奨します。こ

[5] BSA International Cybersecurity Policy Framework
https://bsacybersecurity.bsa.org/report-item/bsa-international-cybersecurity-policy-framework/

[6] Zero Trust Architecture, NIST SP-800-207
https://www.nist.gov/publications/zero-trust-architecture

[7] NISTでは「多層防御（Defense-in-Depth）」は「人、技術、および業務遂行能力を統合して、組織内の階層およびミッションごとに複数の調節可能な防壁を築く情報セキュリティ戦略」と定義されています。
https://www.ipa.go.jp/files/000056415.pdf
https://csrc.nist.gov/glossary/term/defense_in_depth

[8] 米国: https://cloud.cio.gov/strategy/
英国: https://www.gov.uk/guidance/creating-and-implementing-a-cloud-hosting-strategy

[9] https://bsacybersecurity.bsa.org/report-item/bsa-international-cybersecurity-policy-framework/

[10] https://bsa.or.jp/policy/digitalskill/

れらは、公共部門の人材のデジタルスキルを向上させ、政府内でのデータ分析能力を構築するための取り組み、また、民間部門での同様の取り組みの促進を支援するものです。

また、デジタルトランスフォーメーションの方針や戦略を策定、改良、実施する上での定期的な議論に、IT 業界のステークホルダーが積極的に参加できる正式な手続きや制度をデジタル庁が確立することを奨励します。デジタル庁がデジタルトランスフォーメーションの実現に成功するには、オープンで透明性の高いプロセスを実現することが鍵となります。また、民間企業との連携的な場を設けることで、デジタル庁は、産業界の担当者から最新の専門知識やベストプラクティスを得ることができます。

結論

日本のデジタルトランスフォーメーションを推進するために、また、民間企業が提供するサービスへの政府投資の価値を生み出すために、BSA と BSA 会員企業がどのようにデジタル庁と連携していけるか、幅広い議論ができる機会を期待しています。

https://transformyourtrade.org/training-opportunities/