「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（改訂案）」に対する意見

2020年12月 22日

BSA｜ザ・ソフトウェア・アライアンス[1]（以下、「BSA」）は、総務省の「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（改訂案）」（以下「本ガイドライン」）に対するパブリック・コメントの機会に感謝し、以下のとおり意見を提出致します。

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 の会員企業は、クラウドコンピューティング、データアナリティクス、機械学習、AI（人工知能）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、世界各国の政府と緊密に連携して、市民 サービスの向上に貢献しています。

提言

BSA は、地方公共団体の情報セキュリティ対策の改善に向けた、貴省の不断の努力に感謝致します。サイバーセキュリティ政策や法案の策定において、BSA は世界中の政府と緊密に協働してきました。そのことを通し、このような政策や法案が市民のプライバシーと自由を守りながら、サイバーセキュリティの脅威を効果的に抑止・管理するのを可能にするのを直に見てきました。地方公共団体の情報セキュリティ対策を先導する貴省の取り組みを支援するために、以下、我々の意見を述べさせて頂きます。

中央政府と地方公共団体における情報システムの分断の解消

新政権の主導の下でデジタルトランスフォーメーションが進められ、政府業務の高度化が図られる中、安全なクラウドサービスの取得と利用は、その実現に不可欠なものとなっています。この点において、本ガイドラインの見直しが「クラウド・バイ・デフォルト」原則に基づき、テレワークや行政職員の利便性向上を支援するために、以前よりもインターネット接続を可能とする新たな対策が示されたことを、我々は歓迎しています。また、地方公共団体において「クラウドネイティブ」アーキテクチャの方針を推進することで、各府省情報化統括責任者（CIO）連絡会議が中央政府向けに策定した方針[2]と、本ガイドラインとの整合性をより明確にできると考えております。つまり、地方公共団体が LGWAN ベースのシステムを実装するための総コストとクラウド導入の総コストをより適切に評価できるようにすることで、地方公共団体のクラウドアーキテクチャへの移行を促進することができるのです。

---

[1] BSA の活動には、Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workdayが加盟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。

[2] https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf

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

推奨するセキュリティ対策の刷新

貴省が、境界の安全性確保に依存する従来のネットワーク・セキュリティ対策を見直すことを推奨します。地方公共団体が採用すべき具体的なセキュリティ対策を規定するのではなく、様々な利害関係者間で基準となるセキュリティ／プライバシーへの責任の在り方を推奨する、原則ベースのガイドライン策定に注力することを提案します。また、ガイドラインの中で、地方公共団体には、その管轄区域のニーズとリスクプロファイルに最適な情報セキュリティポリシーを企画・実施する自律性があることを明確にすることを推奨します。

さらに、「第３編　第２章　4.1（7）機器の破壊等」に記載されている、市民の個人情報を保存する機器の廃棄に関する詳細な対策の助言を改訂することを推奨します。記憶装置の物理的破壊や地方公共団体職員による現場監視の要件は、オンプレミスの IT システムを前提としています。地方公共団体によるクラウドコンピューティングの革新的活用に対応するために、本ガイドラインでは、詳細な媒体やデータの破棄方法を規定するのではなく、使用しなくなった場合にデータを復元できないようにすることに重点を置くべきです。したがって、暗号的消去（cryptographic erase）等のデータ消去方法を認め、データ復元を不可にする仕組みを明確にすることを推奨します。

場所でなく、データセキュリティ実践に基づくクラウドサービスプロバイダ（CSP）の選定

「クラウド・バイ・デフォルト」原則に基づくガイドラインの見直しを歓迎する一方、クラウドサービスの利用に関する本ガイドラインの説明が、日本国外のサーバにデータを保存・ 処理する CSP の利用を制限しているように読めることを、我々は引き続き懸念しております。データセキュリティの確保は、CSP が維持する技術的・物理的なセキュリティ管理に依存しており、データセンターの場所は、CSP がどのように個人情報を保護するか又は利用者に適用される法律を遵守するかには、ほとんど関係がありません。実際、クラウドサービスの利点の多くは、国境を越えてデータが移転できることにあります。地理的に分散した複数のデータセンター間でデータを移転し、重複的に保存することでレジリエンス（回復力）が高まり、データのセキュリティは向上するのです。このアプローチは、日本政府が G20 大阪トラックの主要な基本概念として提唱した「データ・フリー・フロー・ウィズ・トラスト（DFFT）」とはっきりと合致しています。それゆえに、物理的な場所に焦点を当てた本ガイドラインは、そのような移転を制限することになり、実際には地方公共団体が扱うデータのセキュリ ティが損なわれる可能性があるのです。

以上を踏まえ、貴省に対し、以下のように修正することを求めます。

（iii-142 頁）
第３編：地方公共団体における情報セキュリティポリシー（解説）
第２章 情報セキュリティ対策基準（解説）
8. 外部サービスの利用
8.4. クラウドサービスの利用

「② インターネットを介してサービスを提供するクラウドサービスの利用に当たっ ては、クラウドサービス事業者の事業所の場所に関わらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要がある。具体的には、クラウドサービス事業者のサービスの利用を通じて海外のデータセンター内に蓄積された地方公共団体の情報が、データセンターの設置されている国の法令 により、日本の法令では認められていない場合であっても海外の当局による情報の差し押さえや解析が行われる可能性があるため、住民情報等の機密性の高い情報を蓄積する場合は、~~日本の法令の範囲内で運用できるデータセンターを選択する必要がある。~~**日本の法令を遵守した場所・方法でデータが保管されることを保証できるサービ**

スプロバイダが運用するデータセンターを選択する必要がある。また、データ保全、災害対策等の観点から、海外にバックアップ用のデータセンターを持つことも考慮する必要がある。」

マイナンバーのネットワーク保護のためのクラウド活用推進

マイナンバーを管理する情報システムの保護の必要性を十分認識しつつ、我々は、クラウドコンピューティング・ソリューションの導入を阻害したり、そのメリットを不必要に損なわずに、地方公共団体におけるセキュリティ対策や指針を貴省が継続して見直していくことを奨めます。クラウドサービスは、最も安全なグローバル・インフラの下でシステム構築をしながら、暗号化やストレージ管理など、国際的に認められた機能を活用することで、機密性の高い個人情報を安全に取り扱うことを可能にします。進化し続けるクラウドサービスの性質が、機密な個人情報を守るための最も効果的なデータセキュリティ提供を可能とするのです。[3]このような視点から、現行の LGWAN 対策を修正し、クラウドのこうした特徴を活かして、LGWAN とインターネット接続系の情報システムの分割をしないことを求めます。

官民連携によるセキュリティへの最新対応の導入

上述したように、セキュリティへの対応は、技術の進歩を反映して急速に進化しています。データ・セキュリティのベスト・プラクティスは、リスクベース、セキュリティ成果指向、多層防御、ゼロトラスト・セキュリティ・アーキテクチャといったアプローチを採用しています。これらは、高度なユーザーID 管理や限定的なアクセス、常時安全な仮想プライベートネットワークやネットワーク・セグメンテーションのネットワーク制御、強力なデータ暗号化の実装により可能となります。我々は、貴省が今後も本ガイドラインの見直しを継続し、現在の技術により適合したセキュリティ・ソリューションを採用し、規定的な要件でなく、多層防御の原則に基づく、リスク管理されたコントロールとベスト・プラクティスを重視した、安全なクラウドサービスの取得と利用を通じて、政府の業務をより効果的に推進することを奨励します。

また、サイバーセキュリティ対応に関する国際的なコンセンサスを形成するために、政府と産業界の強固なパートナーシップを強く支持します。貴省が本ガイドラインの中でクラウドの安全性を評価する基準として ISO や SOC といった標準を認識していることを我々は歓迎します。サイバーセキュリティのソリューションは、官民連携を取り入れ、市場主導型のソリューションを促進することで、最も効果的なものとなります。 BSA と会員企業は、貴省と協働し、セキュリティ対応の最新動向を共有していくことを希望します。

結語

BSA は、本ガイドラインに対し意見する機会を頂けたことを感謝致します。提案された対策案に関し、利害関係者間で検討・議論をするための十分な時間を確保する上でも、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希望します。今回の我々の意見が本ガイドラインを完成させる上で有益であることを願っております。日本のデジタルトランスフォーメーションの実現に向け、貴省を引き続き支援していきたいと我々は考えております。本意見について、ご質問、又、詳細について協議の機会を頂けるようでしたら、いつでもご連絡ください。

[3] https://cio.go.jp/sites/default/files/uploads/documents/dp2020_03.pdf