政府クラウドのための原則
セキュリティに関する法律や政策

BSAは、政府と産業界が、現在提供され、クラウドサービスによって継続的に改善されている最先端のソリューションを利用できるような法律や政策を支持するよう、世界各国の政府に求めています。このような法律や政策は、リスクベースで、成果重視で、柔軟で、技術的に中立で、サイバーセキュリティのリスク管理を具体的に改善するものです。

政府や産業界は、クラウドサービスの利点を活用することでデジタルトランスフォメーションを続けています。このデジタルトランスフォメーションにより、組織は市民や顧客により良いサービスを提供できるようになるだけでなく、サイバーセキュリティのリスクをより効果的に管理することができます。クラウドサービスとは、Infrastructure as a Service（IaaS）、Platform as a Service（PaaS）、Software as a Service（SaaS）のことで、政府や産業界は、オンプレミスで運用するよりも費用対効果が高い高度なコンピューティング環境を運用することができます。これらのサービスは、柔軟性をもたらし、生産性を向上し、効率化やセキュリティの向上を実現します。

クラウドサービスプロバイダーは、規模の経済を生かして顧客のコストを最小限に抑えながら、オンサイトのデータストレージのセキュリティ能力をはるかに超える、セキュリティ対策の更新と強化を繰り返すことで、政府や産業界に独自のメリットを提供することができます。これらのクラウドデータセンターは、複数の顧客の要件を満たすように設計されており、そのセキュリティ対策は、単一の組織で通常使用されるものより高いレベルで機能しています。例えばデータセンターでは、多くの場合、バックグラウンドチェック（身元調査）が完了した人員のみにアクセスを制限し、物理的なアクセスを得るために生体認証を要求し、最小限権限ポリシーを適用しています。同様に、大規模な顧客数は、セキュリティに関する重要な洞察をもたらし、クラウドサービスプロバイダーが環境全体のセキュリティ・インテリジェンスを調査することを可能にします。一般的な企業や政府における従来のオンプレミス型インフラよりも多くの情報にアクセスできるだけでなく、ビッグデータのセキュリティ・インテリジェンス・システムによりマルウェアやネットワーク侵入を迅速に発見し、対処することができます。競争の激しいグローバルなクラウドサービス市場において、クラウドサービスプロバイダーは競合他社との差別化のためにセキュリティを活用し、この分野の優秀な人材を採用し、その開発に多大なリソースを投じています。実際、クラウドセキュリティは、オンプレミスのセキュリティと比較して、明らかに大きな優位性を持つことが多いです。クラウドサービスはこのようなセキュリティ改善を達成すると同時に、顧客の機能性向上を実現します。

しかし、政府や産業がクラウドサービスを通じてセキュリティと効率性を十分に向上できるかどうかは、政府が採用を支持（もしくは阻止）する法律や政策にかかっています。それにより、革新的で適応性の高い、回復力のあるソリューションが可能となるか、もしくは、セキュリティの重大な改善をもたらさないまま、選択肢が制限され、競争が妨げられ、コストが増加することになるのです。

Log4jの脆弱性はクラウドサービスの優位性を示すものでした。Log4jへの対応の際にも、クラウドサービスプロバイダーは、オンプレミス型のソフトウェアと比較して、より効率的にクラウド型のソフトウェアにパッチを適用することができ、顧客のワークフローを中断させずにそれを実現したのです。

クラウドサービスが企業や政府にもたらす、このような優位性にもかかわらず、一部の政府は、グローバルなクラウド

サービスが自国産業と競合し、自国のクラウドサービスのエコシステムに不利益をもたらすことに懸念を表明しています。こうした懸念を受けて、一部の政府は、クラウドサービスの調達と運用に大きな障壁を設ける保護主義的な法律や政策を検討または制定しています。こうした保護主義的な法律や政策は、自国のクラウドサービスプロバイダーのエコシステムを短期的には保護するものの、最終的には、国際競争力を低下させ、国内市場に取り込まれることによって、自国のクラウドプロバイダー企業をグローバル市場から孤立させることになり、国内のイノベーションが阻害されてしまいます。さらに、こうした法律や政策は、他の地域の企業や政府が、グローバルに利用可能な最も革新的で安全、かつコスト効率の高いソリューションにアクセスすることを制限することとなります。逆に、グローバルに統合された競争力あるクラウドサービスを法律や政策が受け入れると、政府や産業が、グローバルなサプライチェーンや高度なセキュリティ技術や実践を容易に利用できるようになり、プラットフォーム上でイノベーションを起こす能力が高まるため、経済成長、グローバルな接続性、および国民の信頼を得ることが可能になります。

イノベーションを支援しつつセキュリティも向上させる法律や政策の出発点は、クラウドセキュリティが一般的なサイバーセキュリティと明確に異なるものではないということを認識することです。どちらも、効果的なリスク管理が基本です。クラウドサービスは独自の技術的課題を抱えていますが、これらの課題に対しては、ベストプラクティスの確立と実装に焦点を当てた、リスク管理と成果に基づく姿勢から取り組むのが最適です。

例えば、クラウドセキュリティの法律や政策においては、セキュリティとは本質的にデータの所在地に関連付けるものではなく、アイデンティティや認証情報のアクセス管理等の、クラウドサービスプロバイダーや利用者がデータに適用するセキュリティ管理策に関連付けるものであると認識する必要があります。

政府が企業によるデータ移転を制限した場合、データセキュリティに不必要な障害が発生する可能性があります。国内に保存されているデータでもサイバーセキュリティ上のリスクから解放されるわけではなく、実際、クラウドサービスが受けるサイバー攻撃と同じ攻撃を受けることとなります。さらに、国内に保存されているデータに対する攻撃に対抗するにあたっては、クラウドサービスプロバイダーが注力している、国際的なリソースやセキュリティ対策を直ちに利用できない状態で攻撃に対処しなければなりません。実際、越境データ移転は、物理的アクセスからの保護、冗長性の確保、回復力の向上、遅延の低減などといった複数の理由により、重要なサイバーセキュリティ対策となっています。加えて、越境データ移転では、リアルタイムデータへのグローバルアクセスを利用して、トラフィックパターンの監視、異常の特定、潜在的な脅威の回避を行うことができます。各国政府がローカライゼーションを義務付けている場合や、リアルタイムでのデータ転送・分析を制限すると、意図しない脆弱性を作りだしたり、最新のグローバル脅威情報を入手できない場合があります。

データローカライゼーションなどの政策は、機密性の高い、国の安全保障情報など、非常に限定的な状況においては正当化されるかもしれませんが、こうした状況は、クラウドサービスの使用に幅広い制限を課すのではなく、特定の個別の決定によって対処することが可能です。

BSAは各国政府に対し、現在提供され、クラウドサービスによって改善されている最先端のソリューションを組織が利用できるようにする法律や政策を支持するよう求めます。このような法律や政策は、リスクベースで、成果重視で、柔軟で、技術的に中立であり、サイバーセキュリティのリスク管理を具体的に改善するものです。

BSAは各国政府がクラウドセキュリティに関する法律や政策に取り組む際、以下の原則に基づくことを推奨しています。

1. 国際的に認知された規格の開発・利用の促進
2. 既存の認証結果の援用
3. 役割に応じたセキュリティ責任の支持
4. サイバーセキュリティのための最新のアプローチの採用
5. クラウドセキュリティに関する優れた法律や政策とベストプラクティスの組み合わせ

1 国際的に認知された規格の開発・利用の促進

政府は、クラウドセキュリティの法律や政策を、オープンで透明性のあるコンセンサスに基づいたプロセスで開発され、国際市場で広く採用されている国際的に認知された規格に基づいて、策定すべきです。国際的に認知された規格では、政府、産業界、学界のグローバルなセキュリティの専門知識を取り入れています。例えばISO 27001は、「組織の中で情報セキュリティマネジメントシステムを確立、実施、維持、継続的に改善するための要件を規定」するものであり、ISO 27017は、「クラウドサービスの提供と利用に適用される情報セキュリティ管理策に関するガイドライン」を規定しています。

地域・国・地方の独自の規格や基準はこの状況を断片化し、顧客（政府の顧客も含む）のコストを増加させ、革新的なソリューションを提供する能力を低下させ、顧客を獲得するために競合するクラウドサービスプロバイダーの数を減少させます。残念なことに、クラウドサービスプロバイダーが地域・国・地方の独自の規格や基準を満たすことが要求されるため、市場で競合するクラウドサービスプロバイダーの数が減少することがあり、これは、法律や政策が意図した結果であり、サイバーセキュリティのエコシステム全体に害を及ぼすものです。

地域・国・地方の独自の規格や基準とは対照的に、国際的に認められた規格に基づく法律や政策は、国際的な相互運用性を可能にし、政府と産業界が技術レベルでより良く意思疎通することを可能にします。法律よりも効率的に開発・更新された実績があり、競争力を高め、技術革新を促し、技術の進化を考慮したものとなっています。最終的に、国際的に認知された規格は、より効果的、効率的、かつ革新的なサービスを、より安価に提供することを可能とします。規格開発のプロセスに参加することで、政府は、顧客にコストを転嫁したり、技術革新を妨げたり、競争を制限することなく、懸念を提起し対処することができます。

2 既存の認証結果の援用

政府は、国際的に認知された規格に基づき、外部の認定された評価者によって実施されるクラウドサービスの認証を認めるべきです。既存の認証に追加的かつ重複的な国内の認証を要求することは無駄であり、セキュリティ上の事実上の利点は無く、クラウド導入を遅らすこととなります。政府の認証プロセスでは、可能な限り、同等の国際的な監査や認証を認めるべきです。

国内での認証が必要な場合は、クラウドサービスプロバイダーが、資格ある監査人が国際的に認知された規格に照らして過去に実施した監査の証跡を示すことを可能とし、異なる顧客に対して同じ管理策に対する監査を繰り返させる必要はありません。また、これらの証跡はデジタル形式で受理されるべきです。

既存の認証を認めるもう1つの利点は、政治的な配慮よりもセキュリティへの配慮が高められることです。これにより、すべての関係者が「より安全で豊かな未来」という共通の目標に向けて努力する、より強力なデジタル変革エコシステムの構築を支えられます。

3 役割に応じたセキュリティ責任の支持

法律や政策は、クラウドにおけるセキュリティの責任は、顧客が調達したサービスと顧客がデータをクラウドに移行した範囲に依存することを明確にした、クラウドサービスの責任共有セキュリティモデルを支持すべきです。[1] 効果的なセキュリティプログラムでは、クラウド環境での役割や管理レベルに応じて、プロバイダーや顧客に適切な責任が割り当てられます。この責任共有モデルは、顧客やプロバイダーのニーズに最適な形で調整できるものであり、実際に金融サービスやその他の分野において成功裏に実施されています。

この基本的なセキュリティ責任の分離を認めていない法律や政策は、重要なセキュリティ管理策を強制的に排除し、顧客のクラウド環境のセキュリティ管理能力を減退させ、重要なセキュリティ警告を見逃がす可能性を高めることになるため、顧客のリスクを増大させます。例えば、クラウドサービスの契約当事者同士が、特定のインフラのセキュリティが相手側の責任であると考えた場合、盲点が生じ、それが脆

[1] セキュリティ責任共有モデルについては、複数の重要な文書で説明・支持されています。National Cyber Security Centreの Cloud Computing: Shared Responsibility Security Models（2019年7月）など。

弱性となる可能性があります。各当事者がその責任を自覚し、確実に果たすことが必要です。

4 サイバーセキュリティのための最新のアプローチの採用

法律や政策は、サイバーセキュリティに対する最新のアプローチを認識し、可能にするとともに、次世代のセキュリティ保証ツールを生み出すために研究開発に投資し、イノベーションを促進するべきです。例えば、従来の監査や認証プロセスは、ある時点のセキュリティを測定するものでした。このようなアプローチは、クラウドサービスの規模や継続的な進化にうまく適応できません。法律や政策は、ソフトウェアを用いて遵守状況の監視を自動化し、クラウド環境のセキュリティ状況を柔軟かつリアルタイムに可視化する新たなアプローチを支持すべきです。機械読み取り可能な証跡の受理と処理に移行しようとしている政府、産業界、監査人を支援するため、監査や認証をサポートするための証跡はデジタル形式で受理されるべきです。これにより、他の優先度の高い課題に追加のリソースを投入できるようになります。

同様に、政府や産業界がデジタルトランスフォメーションとクラウドへの移行を進め、Internet of Things（IoT、モノのインターネット）が発展し、より多くのデバイスが接続されるにつれて、アイデンティティ、認証情報、アクセス管理（ICAM）に対する効果的で最新のアプローチの重要性が高まっています。ゼロトラストアーキテクチャ、シングルサインオン、フィッシングに強い多要素認証などの効果的なICAMは、クラウドにおけるサイバーセキュリティリスク管理を改善するための費用対効果の高いアプローチです。

5 クラウドセキュリティに関する優れた法律や政策とベストプラクティスの組み合わせ

各国政府は、クラウドサービスに適用される法律や政策を策定・実施する際は、これらのソリューションをより広範なテクノロジー製品やサービスの流れの中で理解する必要があります。サイバーセキュリティ規制を水平的にアプローチすることで、クラウドサービスだけでなく、あらゆる製品とサービスのセキュリティを強化し、エコシステム間の一貫性を高め、テクノロジーの変化に合わせて進化し、継続的な改善を促進する、リスクベースのアプローチを進展させることができます。

すぐに利用できる商用ソリューションを活用することで、デジタルトランスフォメーションが促進されます。また、すぐに利用できる商用ソリューションは、セキュリティと機能の両方が定期的に更新・改善されるため、そのようなソリューションを活用する組織は、古い、セキュリティの低い、機能性の低い製品やサービスに追いやられてしまうことがありません。

各国政府は、サイバーセキュリティを積極的に幅広く改善し、ベストプラクティスを改善するための国際的な取り組みに参加することでプラスの波及効果を生みだし、エコシステム全体のセキュリティを強化すべきです。このような取り組みとしては、政府が報告を求める主体やサイバーインシデントの種類、報告の時間枠を調和させることも含まれるはずです。

クラウドセキュリティに関する法律や政策の有効性を高めるため、政府や産業界は、「BSA Framework for Secure Software」、「BSA Policy Principles for Building a Secure and Trustworthy Internet of Things」で示す内容も含め、サイバーセキュリティ、ソフトウェアセキュリティ、IoTセキュリティを強化する法律や政策を支持するべきです。政府、テクノロジー、産業、製品の垣根を越えて培われた強固で調和のとれたサイバーセキュリティ環境は、クラウドインフラのセキュリティを強化し、政府やその国民、企業やその顧客にも利益をもたらします。