クラウドサービスの安全性評価に関する検討会 とりまとめ（案）に対する意見

2019年12月25日

BSA ｜ Software Alliance（BSA）[1] は、「クラウドサービスの安全性評価に関する検討会とりまとめ（案）」（以下「とりまとめ」といいます。）について、総務省及び経済産業省に対して以下の通り意見を提出します。

総論

BSA は、総務省及び経済産業省が、政府全体におけるクラウド利用の拡大を目指し、クラウドサービスの安全性評価（以下、「評価制度」といいます）の手順策定に取り組んでおられることを高く評価します。

BSA 会員企業は、最先端のクラウドコンピューティング技術及びサービスを提供しており、これを利用することによって、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、生産性及び革新性を向上することを支援しています。BSA および会員企業は、セキュリティが確保されたデジタリゼーションを政府が加速化していくことに貢献していきたいと考えており、この目標を後押しするため、以下の意見を述べさせて頂きます。

提言

本とりまとめは、評価制度プロセスにおける関係ステークホルダーの役割や責任、また、提出書類やその他の詳細に焦点をあてており、評価制度で用いる基準、また、詳細な運用ルールに関しては 2020 年に公表されるという理解でおります。評価制度の枠組みを最終決定していくにあたり、また、その運用にあたっては、発表前に、引き続き関係ステークホルダーと協議しながら進めていくことを奨めます。BSA 会員企業は世界中の政府と協働しながら、クラウドコンピューティングやその他のソフトウェアを介したソリューションを利用して業務効率の改善をしてきており、検討の過程において、その豊富な経験と知見を共有することが可能です。

この取り組みに貢献するため、以下の提案を述べさせて頂きます。

[1] BSA ｜ The Software Alliance（BSA ｜ ザ・ソフトウェア・アライアンス）は、グローバル市場において世界のソフトウェア産業を牽引する業界団体です。BSAの活動には、Adobe, Akamai, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, SAS Institute, Siemens PLM Software, Sitecore, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, 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。

22F Shibuya Mark City West
1-12-1 Dogenzaka, Shibuyaku,
Tokyo 150-0043, Japan
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office

国際規格の有効活用

本年４月に提出した意見書[2]でも述べておりますが、クラウドサービスプロバイダー(CSP)は、地理的な分散と規模の経済を利用して、効率性や信頼性が高く安全なソフトウェアを介したサービスを提供するため、多くの場合、複数国の市場で同時に事業展開しています。そのため、安全で効果的なクラウドサービスの採用を促進する方針は、他国の公共セクターのクラウドの安全性評価及び認証制度と**相互運用性があり**、また、**国際規格に適合していることが**不可欠となります。

とりまとめの 2.2.では、評価制度の管理基準が国際規格を参照ベースとしており、「政府機関等の情報セキュリティ対策のための統一基準」[3]（以下、「統一基準」といいます。）、又は、調達要件を満たすために不可欠と政府が判断した特有の管理基準が追加されると明示しています。従って、評価制度の中核的な構成要素は国際規格と一致している、と我々は理解しております。

評価制度の中核的な管理基準が国際規格をベースとしてないとなると、国際規格に準拠して監査を受けている日本企業を含む、多くの企業にとっては、重複する管理基準が日本に存在することとなり、混乱をきたします。また、民間分野がクラウドの安全性を評価する際に、本評価制度を参照することが期待されているということからも、国際規格と不整合な重複する要件は、民間分野におけるクラウド導入を抑止し、生産性、安全性、経済成長、雇用創出の阻害となりかねません。

従って、追加の管理基準は慎重に吟味・厳選され、不可欠と政府がみなした統一基準や NIST SP800-53 の項目のみを追加し、国際規格との整合性を保つことを推奨します。

規範的な要件ではなく、リスクベースで結果指向の要件であること

評価制度のプロセスにおいて起用される基準が政府の情報や情報システムを保護するために幅広いセキュリティ対策を網羅する必要性があることを我々は理解しておりますが、実質的にセキュリティ強化に貢献しない、過度な負荷や手間となる、規範的な要件を設けることは非生産的であります。むしろ、そのような要件は長期かつ高コストな手続きとなり、CSP に対して事前投資を行うことを強いることとなります。上記で述べましたように、政府機関におけるクラウド技術の利活用を促進させるのではなく、むしろ、その導入を阻むことにもなりかねません。また、評価制度が民間分野においても活用される可能性を考えますと、そのような要件はイノベーティブな CSP にとっては障壁となります。

どれが不可欠な管理策か優先順位をつけることは、効果的な結果を推進する上で、非常に重要なことです。監査において、そのような優先順位があることで、登録を目指すクラウドサービスのセキュリティ対策を CSP が合理的かつ適切に選択することが可能になります。評価制度のプロセスを能率的にするには、**国際規格で取得された既存の認証を認めることが大変重要**であります。評価制度では既存の認証を有効活用し、敏速に監査と評価プロセスを進めることを強く奨めます。具体的には、監査プロセスにおいて、既存の認証の報告書を認め、その他の報告書作成において使用された証跡の再使用を認めるべきです。

---

[2] 「クラウドサービスの安全性評価に関する検討会　中間とりまとめ（案）」に対する意見
https://bsa.or.jp/wp-content/uploads/20190416j.pdf

[3] 政府機関等の情報セキュリティ対策のための統一基準
https://www.nisc.go.jp/active/general/pdf/kijyun30.pdf

22F Shibuya Mark City West
1-12-1 Dogenzaka, Shibuyaku,
Tokyo 150-0043, Japan
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office

また、とりまとめの 1.5. と 1.6. においては、登録されたクラウドサービスの全てのセキュリティ対策に関し、毎年の監査が必要であると記していますが、CSP への不要な負荷は最小限におさえ、限られた人的資源を有効活用するためにも、最優先の管理策に焦点をあて、頻度を減らした、監査スケジュールを検討されることを奨めます。

日本政府のためにカスタマイズされた新たな管理策に焦点をあてるのでなく、セキュリティ向上をもたらすための管理策をより良く評価するためには、評価制度は結果を重視するべきです。これにより、CSP は新しい技術と情報セキュリティソリューションを継続的に開発し革新することが可能になります。規範的で、カスタマイズされた管理策にもとづいた基準はセキュリティ向上を保障するものではなく、より意義のあるセキュリティ結果に焦点をあてるのでなく、日本特有の管理策に人的資源や努力を集中させることを CSP に強いることになりかねません。従って、評価制度の基準や具体的な運用のルールを策定するにあたり、政府は、**結果達成のための具体的な手順を規定するのではなく、結果を重視した、セキュリティ目標を明確に定義し、柔軟性のある手順で CSP がその目標を達成できるようにすべきです。**その観点では、クラウドサービスにおける目標/管理策と運用ガイダンスで構成されている ISO/IEC27017 は有用な参照資料となるでしょう。

データ保管又は処理の物理的な場所に依存しないセキュリティ

とりまとめの 2. 2.(5)においては評価制度プロセスの一環として、データセンターの場所を含む情報の提出が CSP に求められることが記されております。他方、本制度のレベル２の基準に基づく登録においては、データセンターの国内設置が一律に求められるということではない、と明記いただいております。この点に関して、**国内で保管されたデータに比べ、国外で保管されたデータが安全面で劣ると示唆するではなく、**注視すべきなのは、どこで保管されていようとも、データの安全な保管を確実にする、ということであると理解頂きたいと思います。上記で提案している、セキュリティ目標に焦点をあてることで、日本国外にデータが保管されていても、適切なセキュリティが確保されていることが証明されます。

データの安全性はデータの物理的場所でも、それを支える設備の場所でもないということを認識することは重要です。安全性はデータを保護するために維持されている手順や管理策の質や有効性という機能によって決まります。企業はデジタル設備の設置場所を決める際に、多様な要素を考慮に入れます。その中にはインターネットのスピードやアクセスを最大限に活かすサーバーやゲートウェイ、また、冗長性の実装やバックアップシステムの性能、そして、利用者のデータのために最先端のセキュリティの導入を確実にすることなどが含まれます。

評価制度が政府全体に適用されること

評価制度の目標が、全ての政府機関に安全なクラウドサービスを提供することであることを踏まえますと、評価制度の規範が統一的に導入され、省庁間で分断を生じさせないことが大事です。特に「機密性」、「完全性」、「可用性」をもとにクラス分けされた情報システムにおいて、明確で統一性のとれたアプローチをとり、省庁間の連携を促すことは、評価制度に係る関係ステークホルダーにとって、より混乱の少ない環境をもたらすこととなります。

政府機関のサービスは多様で、評価制度が政府機関の全ての管理策を網羅することは困難です。クラウドコンピューティングの環境では、サービスの管理策は個別のクラウドサービス契約（SLA）で網羅されており、本とりまとめに基づくと、評価制度は中核となる、基本的な管理策をまとめており、その他の管理策については、本評価制度での調達時に、

クラウドSLAにおいて、CSPと調達者間で合意されるという理解でおります。この点を評価制度に係る関係ステークホルダーに明確にして頂きたく思います。

政府内の体制構築・制度利用の実行性確保について

さらに、CSPが監査主体や政府機関と共有しなくてはならない情報には、CSPが保有する企業秘密が含まれる可能性があり、当事者間での守秘義務契約に服する場合があります。この点に関して、登録簿により公開される情報の適切な範囲について慎重に検討することが非常に重要です。

また、評価制度の本格始動が2020年の秋に予定されていることから、政府全体のクラウド導入を進める上での具体的な計画を政府には可視化していただきたく思います。日本のデジタル・ガバメント実現という目標を達成するためには、評価制度の運用は、省庁における認知向上に向けた取り組みと対になっていなければなりません。

結論

BSAは、本とりまとめ（案）に対する意見を提出する機会を感謝します。BSAは、政府機関のクラウド導入を促進させようとする、総務省及び経済産業省の取り組みに引き続き協力させていただきたく存じます。また、本意見に関するご質問、また、意見交換に関し、いつでもご連絡ください。

以　上

22F Shibuya Mark City West
1-12-1 Dogenzaka, Shibuyaku,
Tokyo 150-0043, Japan
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office