2013 年 8 月 30 日

「クラウドサービス利用のための情報セキュリティマネジメントガイドライン改訂版（案)」等に関する意見

BSA ｜ ザ・ソフトウェア・アライアンス

BSA｜ ザ・ソフトウェア・アライアンス[1]（以下「BSA」）は、「クラウドサービス利用のための情報セキュリティマネジメントガイドライン改訂版（案)」(以下「本改訂版」）及び「クラウドセキュリティガイドライン活用ガイド」に関し、以下の通り意見を提出致します（以下「本意見」)。

総論

BSA は、クラウドコンピューティングが、引き続き情報技術分野の中で重要な技術の１つであり、世界におけるクラウドサービスに関する法令及び政策は、クラウドサービスの普及を支え加速させるものであるべきと考えている。

クラウドサービスの普及を支える法令及び政策のうち､データの自由な移転の確保と国際的な規制の協調が非常に重要であるというのがBSAの基本的な考えである。世界中で円滑にデータが移転されるには、異なるクラウドプロバイダー間の移転を含めて、オープンであることと相互運用性が確保されることが必要であり、政府は、世界においてクラウドプロバイダーに課される義務の矛盾を最小限にすべきである。また、本改訂版のように法的拘束力がないガイドラインや、マニュアルその他の商習慣であっても、曖昧又は過度の記載によって利用者の誤解や萎縮を生じさせ、クラウド関連サービスの利用を検討する事業者が実際の利用を差し控えたり、クラウド関連サービスへの投資を検討する海外企業が投資を差し控えることにつながるようなものは取り除いていくべきである。これらの観点から、世界における円滑なデータ移転に悪影響を与えかねない記載に関し、本意見の各論におい

---

[1] BSA ｜ The Software Alliance（BSA ｜ ザ・ソフトウェア・アライアンス）は、世界のソフトウェア産業を代表する業界団体です。70 社を超える BSA 加盟企業は、経済の活性化とより良い現代社会を築くためのソフトウェア・ソリューションの創造に年間数千億円もの投資を行っています。世界各国の政府との意見交換、著作権をはじめとする知的財産権の保護ならびに教育啓発活動を通じて、BSA はデジタル社会の拡大とそれを推進する新たなテクノロジーへの信頼の構築に努めています。BSA のメンバーには、アドビ システムズ、Altium、アップル、ARM、オートデスク、AVEVA、ベントレー・システムズ、CA Technologies、シスコ、CNC/Mastercam、デル、IBM、インテル、Intuit、McAfee、メンター・グラフィックス、マイクロソフト、Minitab、オラクル、PTC、クエスト・ソフトウェア、ロゼッタストーン、シーメンス PLM ソフトウェア、シマンテック、テクラおよび The MathWorks が加盟し、活動を行っています。詳しくは、日本の BSA ウェブサイト（www.bsa.or.jp）、または、BSA 本部（米国、英語）のウェブサイト（www.bsa.org/country.aspx）をご覧ください。

てコメントを述べる。

日本のITインフラ面での強みを活かしつつ、日本におけるクラウド関連サービスを更に発展させていくには、萎縮的な政策環境は取り除いていくべきであり、今後、BSAは、この点に関し、可能となった時点で更なる情報提供と提言を行っていく所存である。

各論

1. 6.2.2 顧客対応におけるセキュリティ

「個人情報保護法などの法令に基づき，クラウドコンピューティング環境上の情報への顧客のアクセスが制限される場合がある」と記載されているが、個人情報保護法によって個人情報へのアクセスが制限されるのはクラウドコンピューティング環境に限ったことではなく、クラウドコンピューティング環境が制限を受けやすいといった誤解を生じるような記載は好ましくない。

2. 7.2.1 分類の指針

「クラウドサービスの関連情報」において、データ分類項目の例として「第三者が不正を防止する義務」が挙げられているが、不正を防止する主体が第三者とも読み取れて紛らわしいため、「第三者による不正を防止する義務」と記載すべきである。

3. 10.3.1 容量・能力の管理

「クラウドサービスの関連情報」において、CPU 利用率などの急激な上昇・降下が発生し、クラウドサービスの安定稼働に影響を及ぼす場合に備え、クラウド事業者にはクラウド利用者がクラウドサービスにおける資源の利用を監視する機能（例えば、クラウド利用者が資源利用率などを確認できる機能）を提供することが提案されているが、そのようなクラウドサービスのリエンジニアリングは、クラウド利用者が得ているクラウドサービスのコストの利点を損ねてしまいかねない。クラウド事業者にとっての最大の関心事は信頼性が高く安定稼働のサービスを提供することであり、実際にクラウド事業者が信頼性の高いサービスを提供しているかどうかは、第三者による事業者の監査レポートなどで十分に確認可能であるため、資源の利用の監視を利用者側の作業事項とすべきではない。

4. 10.6.2 ネットワークサービスのセキュリティ

「クラウド利用者のための実施の手引」において、「クラウド利用者はクラウドービスに含まれるネットワークサービスが，セキュリティを保つ能力を見定め，常に監視することが望ましい」とあるが、クラウドにおけるセキュリティはクラウド利用者とクラウド事業者が協働する事項であって、クラウド利用者が常に監視するとの記載は、利用者が行うべき内容が適切又は明確とは言えない。例えば、Cloud Security Alliance’s Star Registry というプロジェクトでは、クラウド事業者が当該クラウドサービスで行われているセキュ

リティ管理に関する資料を提供することにより、全般的なクラウドのセキュリティ向上と、クラウド利用者がクラウドサービスのセキュリティについて知る機会の提供に取り組んでおり、このようにクラウド事業者と利用者の協働を促進していくべきである。

5. 15.1.1 適用法令の識別

本改訂版では、適用法令の識別に関して、クラウド事業者の実施が望まれる事項の追記が行われ、より詳細に適用可能性のある法令及び規制等について明示することを望ましいとしているが、追記には反対であり削除すべきである。また、改定前の記載も検討し直すべきである。BSA会員企業は、クラウド事業者として法令及び規則の遵守確保の重要性を十分理解しており、また、クラウド利用者にとっても、クラウド上に保存したデータのセキュリティやプライバシーが守られ、法令に則った取扱いが可能となることは確保されなければならない。しかしながら、 政府がクラウドを特異に扱うのは避けるべきである。クラウドコンピューティングはIT革命よりも更に進化したものであるから、そのような視点をもって検討されるべきである。もし、以前の技術革新についても当該要求事項が課されていたら、それらの技術や・サービスはどうなったかを考えてみる必要がある。例えば、電子商取引及びそれにより購入した商品の物流、音楽配信、その他のインターネットサービスのケースを考えてみても、契約当事者間の準拠法の問題とトレーサビリティに関する努力は別として、逐一、利用しているサーバーの所在地、データセンター事業者の名称と所在地、物流の過程で使用する運送会社の国籍、サーバーメンテナンスを行う従業者の所在地などのサービスのバックグラウンド情報を元に、詳細に適用可能性のある法令や規制等全て明示して行うべきとはなっておらず、実社会でもそのように運用されていない。

従って、当該記載はクラウドサービスに対する過度の要求事項であって、クラウドサービスの利用や提供に萎縮効果を生じさせるものであり、改定前の記載についても見直されるべきと考える。

6. 15.1.3 組織の記録の保護

本改訂版は、「他国のクラウド事業者では，特定国内における法律に対応できないクラウド事業者がある可能性もある」と記載している。しかしながら、クラウド事業者の国籍や場所が、利用者に適用される法律に適切に対応できるかどうかを決するものではない。実際、クラウドサービスは世界的に展開されることが多く、他国でサービスを提供しつつも特定国内の法律も十分に遵守することができる場合が多くある。同時に、国内のクラウド事業者であっても、開発力や資金力の不足、情報収集の不十分さ等様々な理由に起因して、単に日本に存在するというだけでは直ちに十分な法律（改正を含む）対応ができない場合がある。従って、日本と海外の事業者を区別するかのような表現は不正確であり、海外のクラウドサービスの利用に萎縮効果を生じさせうる記載は削除又は修正すべきである。

7. 15.1.4 個人データ及び個人情報の保護

個人情報保護法や企業等が定める自己の規程に当該クラウドサービスが合致していない可能性があるとすれば、その可能性自体は、国内のクラウドサービス事業者であっても海外のクラウドサービス事業者であっても変わらない。にもかかわらず、日本と海外の事業者を区別して、海外のクラウドサービスの利用に萎縮効果を生じさせるべきでない。したがって、「国内外の」といった、事業者の国籍が関連するかのような記載は削除すべきである。これを考慮すると、当該箇所の記載は下記程度とするのが妥当である。

「個人情報保護法の要求事項及び当該要求事項の実現のために企業等が定める規程に対応できないクラウド事業者が存在するかもしれない。そのため，個人情報保護に関する基準や手順がクラウド事業者の提供するクラウドサービスに合致するかどうかを検討することが期待される。」

8. 附属書 A（参考）クラウドサービス利用にかかわるリスク：データセンターの所在

様々な国や場所にデータセンターが設置された場合、データセンターに従事する従業者の経験やモラルによる情報の取り扱いの差やネットワークの接続性が抽象的に懸念事項として挙げられている。しかしながら、サービスの質は、むしろ SLA とその達成度、評判及び実績によって判断し、そのリスクを受容するか検討するのが合理的かつ客観的である。また、クラウド事業者は、高可用性を達成するため世界中にデータセンターを設置することが多く、インターネットとクラウド事業者のデータセンターが相互に接続していることから、利用者のデータがどこに存在するか終始常に明確とも言えず、抽象的にデータセンターの所在地と従業者のモラルや経験を結びつけてリスクを想定したり、クラウドサービスの場合の接続性に関わるリスクを抽象的に想定した上で、合理的で客観的なリスクの洗い出しと受容を行うことは困難である。従って、記載は修正されるべきである。

9. 附属書 A（参考）クラウドサービス利用にかかわるリスク：接続性

国内外に事業者がクラウドサービスを提供するためのデータセンターを展開し、それらが連携して運用されているため、ネットワーク構成が複雑になり、接続の信頼性を把握することができないという課題やリスクが抽象的に指摘されている。ユーザーが関連するリスクを理解することはとても重要なことであるが、その場合、全体的なリスク分析を行うべきであり、これにはクラウドサービスプロバイダーが管理していない接続（クラウドサービスプロバイダーから見て第三者である ISP が提供するユーザーによるインターネット接続など）の信頼性も含まれる。従って、サービスの質は、むしろ SLA とその達成実績によって、オンプレミスでの自前のシステム管理との比較考量をして検討するなど、クラウドサービス全体のパフォーマンス（接続の信頼性だけでなく）について正確かつ全体的な視点で判断していくのが合理的かつ客観的であり、クラウドサービスの場合の接続性に関

わるリスクを抽象的に想定した上で利用料の減額との比較考量をするというアプローチは困難かつ合理的ではないと考える。従って、記載は修正されるべきである。

10. 活用ガイド 3.3.1 インフラに関するリスクと対策:データセンタへの不正な入退館への対策

「マルチテナントによる運用ということもあり、利用者が監査などで訪問した場合に、監査対象となる機器などを限定することが難しい場合もあります」とあるが、これは不正な入退館とは関係のない記述であり、この項から削除すべきである。

11. 活用ガイド 3.3.8　人員に関するリスクと対策：クラウド利用者のリテラシーに関するリスクと対策

「(クラウド) サービスの内容や機能について理解しないまま自由に使うことは、プライバシーの侵害や重要な情報の漏えいにつながる恐れがあります」とあるが、クラウドはサービスを提供するためのインフラであって、プライバシー侵害や情報漏えいは、クラウドを利用してもしなくても、理解や対策が不十分な場合には起こるリスクである。現在の記述は、クラウドサービスを使うことがプライバシー侵害や情報漏えいにつながりやすいと利用者の不安を無駄に煽るおそれがあり、こうした問題を未然に防ぐための具体的な対策を併記することで利用者に正しい対策を取るよう喚起すべきである。

12. 活用ガイド　4.4.2.契約面におけるクラウドサービス利用のリスク

「クラウド事業者のサーバーは日本国外に設置されている場合もありますが、仮に、当該地が法制度の十分に整っていない国である場合に、法的に問題のあるサーバーの差押えなどにより、サーバー内のデータが強制的に没収されるなどのリスクをいいます。また、法制度は整っていても、当該地の法律が広範な捜査権を捜査機関に付与していたり、法律の適用に不明確な点があるなどの理由で、予期せぬ形でサーバー内のデータの開示を余儀なくされる、などといったリスクもここに含めてよいでしょう。」とあるが、政府が国外のサーバーに保存されたデータにアクセスする権限は無制限に認められるわけではない。例えば、データへのアクセスを要求する政府は管轄権及びその他の制約を受けることがある。また、データが置かれた国では、他国の政府によるデータ開示要求に対して、たとえそれが他国における正当な法的手続きを踏まえた要求であったとしても、制約を設けていることがよくある。他国に置かれた電子データを取得するには、もっとも適切なメカニズムとして刑事共助条約があり、これは 2 国間または多国間で締結される。この条約を用いると、ある国の政府が、取得したいデータが置かれた国の政府に対して、公式にデータ開示を要求でき、データが置かれた国の政府は、適切な法的手続きに従い、そのデータを扱っているプロバイダーに対してデータ開示を求めることができる。この条約は、公共の利益のため、政府による国境を越えた捜査を可能とするが、データが置かれた国の法律に従うこと

が前提となっている。これは、データの開示請求を受けるプロバイダーが法の抵触によるリスクを負うことを防ぐためである。

「米国愛国者法は（中略）テロリズムやコンピュータ詐欺及びコンピュータ濫用罪に関連する有線通信や電子的通信を傍受する権限、あるいは裁判所の命令によらず電子メールやボイスメール（留守番電話）を入手する権限などが捜査機関に与えられるなど、捜査機関に与えられている権限が大きなものになっています。」とあるが、米愛国者法は米政府が一歩踏み込んで情報を入手できるメカニズムを新設したと一般的に信じられているものの、最近の研究報告[2]によれば、これは誤解であり真実と大きくかけ離れた認識である。愛国者法によって認められた捜査手段は、憲法やその他の法規制の制約を受ける。例えば、米政府がeメールやその他のコミュニケーションの内容の開示を強制する場合、憲法は政府に対し、裁判所が正式に発行する令状又は命令書を取得することを要求している。米愛国者法を使っても、米政府は裁判所の令状や命令書がなければ、（eメールを含む）コミュニケーションやクラウドに保存された情報の内容の知り得ることができない。すなわち、米政府は独立した裁判所に令状や命令書を出してもらうため、求められる法的要件をすべて満たすという十分な証拠を事前に示さなければならない。この求められる法的要件は、憲法やその他の法規制によって定められている。政府が犯罪捜査に必要なデータの開示を要求することは、正当な行為である。プロバイダーが出している各種報告書が示す通り、米政府に限らず多くの国の政府が利用者のデータ開示を要求している。

こうした政府のデータ開示要求によって影響を受けるのは利用者のほんの一部であることがこれまで報告されてきたが、クラウド利用者は十分な理解のもと、どこにデータを保存するか（どこの国のデータセンターを利用するクラウドプロバイバーを使うか）を決めることが大切である。利用者は活動を行う国およびデータが置かれる国においてプライバシー保護に必要な法制度が整備されていることを確認した上で、どのクラウドプロバイダーを使うか決めることが重要である。この観点では、政府による情報アクセスや利用を審査し、必要な令状の発行を行う独立した司法機関の存在が、政府に対して法令上の制約を設け、利用者のプライバシーを保護する上で大変重要である。

以　上

---

[2] Maxwell, Winston, *A Global Reality: Governmental Access to Data in the Cloud*, Hogan Lovells White Paper (2012) *at* *http://www.hldataprotection.com/2012/05/articles/international-eu-privacy/hogan-lovells-white-paper-on-governmental-access-to-data-in-the-cloud-debunks-faulty-assumption-that-us-access-is-unique/*