2014年2月14日

「政府機関の情報セキュリティ対策のための統一基準群」（案）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、「政府機関の情報セキュリティ対策のための統一基準群」（案）（以下「本基準群」）を構成する文書に関し、以下の通り意見を提出致します。

総論

BSAは、政府が、益々重要性を増している情報セキュリティの問題に関し、政府における情報セキュリティの統一基準をより良いものにするために改定をしていく努力について敬意を表する。サイバーセキュリティに関する政策においては、絶えず進化する脅威に直面するなか、デジタル経済の繁栄に欠かせない情報システムを保護するために市場の力を結集して、急速なイノベーションを活用して対応を進めていくことが求められている。

この点、「政府機関の情報セキュリティ対策のための統一基準」（案）（以下「本統一基準」）及び「府省庁対策基準策定のためのガイドライン」（案）（以下「本ガイドライン」）において、「外部委託」の一形態として、クラウドコンピューティングの利用について記載しているため、重要な論点であると考え、意見を述べる。

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。クラウドコンピューティングの利点や特性を考えると、データの自由な移転の確保が非常に重要であり、そのため規制は国際的に出来る限り協調すべき

[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。世界をリードする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には、アドビシステムズ、アジレント・テクノロジー、Altium、アンシス、アップル、オートデスク、AVEVA、AVG、ベントレー・システムズ、CA Technologies、シスコシステムズ、CNCSoftware-Mastercam、デル、IBM、インテル、Intuit、マカフィー、マイクロソフト、Minitab、オラクル、PTC、ロックウェル・オートメーション、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 Math Works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本部のウェブサイト/英語（www.bsa.org/country.aspx）をご覧ください。

であるというのがBSAの基本的な考えである。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ることに留意すべきである。

また、サイバーセキュリティに関しては、脅威が絶えず進化している以上、情報システムを保護する側にはそれ以上のイノベーションが必要であり、政府の政策においては、技術的中立性が重要となる。何らかの理由により技術を固定化させてしまったり、技術の進歩を遅らせるおそれのある政策を採用すべきではない。

さらに、BSAは、現在、世界中において情報セキュリティや個人情報保護の名の下に各国が保護主義に傾くことについて強い懸念を有している。本基準群は、中央省庁のポリシーとして適用され、また、調達の際の仕様にも関わるものであり、政府調達に影響を与えるものであるが、本基準群が、情報セキュリティの名の下に、政府調達に関して保護主義に傾いていないかについても十分考察し、問題があれば修正すべきである。

各論

1. 本統一基準（23 頁及び 25 頁）4.1.1「外部委託」/4.1.2「約款による外部サービスの利用」の目的・趣旨の記載について

本統一基準 4.1.1 「外部委託」の目的・趣旨では、「なお、約款による外部サービスを利用し、行政事務を遂行する場合も外部委託の一つの形態と考えられるが、委託先と特約を締結することが難しく、必要とする情報セキュリティに関する十分な条件設定の余地が無いものについては、4.1.2 項「約款による外部サービスの利用」を遵守する必要がある。」と記載している。また、本統一基準 4.1.2「約款による外部サービスの利用」の目的・趣旨では、「約款による外部サービスを利用し行政事務を遂行する場合、4.1.1 項「外部委託」にて規定する事項を特約として締結するなどし、情報セキュリティ対策に努めるべきである。しかしながら、約款による外部サービスでは特約の締結等ができず、必要とする情報セキュリティに関する十分な条件設定ができない場合が多く、サービスの継続性が保証されていない、データの保管場所やバックアップ方法が不明であるなど、利用に当たってのリスクが高いことから、要機密情報を取り扱う可能性がある場合においては利用すべきではない。」と記述している。これらの記述によれば、クラウドサービスでは、特約、即ち個別の約束が出来ないために、一般的に情報セキュリティリスクが高いように読めるが、これは、クラウドサービスの正当な評価とは言い難く、また要機密情報を取り扱う可能性がある場合に全て利用すべきでないと取れる書き方は行き過ぎであるから、修正すべきである。　即ち、約款の内容（情報セキュリティや個人情報保護に関する約束を含む）は、各クラウドサービスによって千差万別であるから、約款サービスであっても、約款及びサービスの内容を吟味のうえ、セキュリティに関する対策、サービス継続性、データ保管場所、バックアップ方法が明確になっていて十分であれば、要機密情報を取り扱う場合でも利用可能と明記すべきである。また、約款か個別契約かという契約手法の論点と情報セキュリティの水準の問題は全く別物であるため、両者を分けた精緻な議論が必要である。さらに、クラウドサービスのデータ保管やバックアップ方法に関する情報セキュリティ水準については、事業者が提供するクラウドサービスの

情報セキュリティに関する情報、第三者による事業者の監査レポート、情報セキュリティに関連する国際的な規格への準拠及び実績等により判断が可能であるため、これらの情報によりメリットとデメリットを判断するような基準を記載すべきである。クラウドサービスの情報セキュリティ対策技術は日々進化している。もし、国際的に採用されていない日本特異な要求事項を盛り込んだ特約の締結を求める場合には、むしろ、日本におけるイノベーションを阻害し、また、サービス品質、技術水準の高さや機能に基づいて各省庁が合理的にサービスを選択することを妨げてしまうおそれがある。

2. 本統一基準（24 頁）4.1.1 「外部委託」(2)外部委託に係る契約「情報セキュリティ対策の履行状況の確認」

情報セキュリティ対策の履行状況の確認については、第三者による事業者の監査レポート、国際規格への準拠状況、クラウド事業者が提供する様々な資料の活用を推進していくべきである。クラウド事業者に個別のレポート提出・面談を求めるなど、クラウドサービスのコストメリットを減殺するような確認方法を仕様としないようお願いしたい。

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、このような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。

3. 本統一基準（24 頁）4.1.1「外部委託」(2)外部委託に係る契約「情報セキュリティ監査の受入れ」

本統一基準は、必要に応じて、情報セキュリティ監査の受入れを仕様に含めるべきであるとしている。しかしながら、以下の理由により、情報セキュリティ監査を契約当事者である政府担当者が行うことを政府調達の仕様に含めるべきではなく、当該規定は削除されるべきである。

まず、政府の担当者が、情報が保管・運用されているデータセンターにおいて実際に監査する実地監査を要求することは、実効性の観点からも適切でない。政府担当者の情報セキュリティ監査の手間と旅費等の別の制約要因によってデータセンターの日本国内設置義務を規定したのと同様の効果となるので、当該規定は削除すべきである。

政府担当者が単にデータセンターを見聞しただけで得られる情報は非常に限定的であり、そのメリットは少ない。安易に情報セキュリティ監査受入れの名目で、各契約当事者をデータセンターの中に立入りさせる運用自体、情報漏洩のリスクにつながってしまう。さらに、データセンターの日本国内設置義務につながる規定について合理的な根拠なくしてグローバルに展開されるクラウドサービスの利用を阻害することになる。

クラウド事業者が実際に情報セキュリティに関して信頼性の高いサービスを提供しているかどうかは、各契約当事者ではなく第三者による事業者の監査レポートや実績等により十分に確認

可能であるため、各省庁は実地監査ではなく、多様なこれらの情報により確認するのが妥当である。また、複数の利用機関からの監査の受入れは、それ自体が重大なセキュリティ懸念を生じうることから、国際的な機関による代表代理監査を許容可能とすべきである。

4. 本統一基準(25 頁) 4.1.2　遵守事項　(2)約款による外部サービスの利用における対策の実施

「クラウドサービスでは要機密情報が取り扱われないように規定すること」「利用に当たってのリスクを認識した上で約款による外部サービスの利用を申請」と記載されており、これは、クラウドサービスは一般的にオンプレミスの情報システムに比べてよりリスクが高いと誤解を与えるうえ、クラウドにおいて特約が締結されない限り要機密情報を扱ってはならないという規定は設けるべきでなく、これらの記載は修正されるべきである。

約款という契約手法と情報セキュリティの水準に論理的関係性がないことは前記のとおりである。また、クラウドサービスにおいては、大規模なデータセンターを運用する中で日々得られるノウハウに基づきイノベーションが起こっており、最新の情報セキュリティ対策がなされていることから、個々の情報システム担当者や委託先のベンダーがオンプレミスで管理する個別の情報システムよりも高い情報セキュリティ対策がなされていることも多いというメリットがある。従って、クラウドサービスの利用にあたっては、情報セキュリティの観点も含めて、オンプレミスの情報システムとのメリット・デメリットを十分に比較衡量すべきであるが、一般的にクラウドサービスの方がリスクが高いとの記載は、クラウドサービスの正当な評価とは言い難いので修正すべきである。これにより、政府情報システムにおけるクラウドサービスの利用を遅らせ、TCO（Total Cost of Ownership）のメリットを十分に享受できないこととなれば、国民に過大な財政負担を強いることになり適切でない。

5. 本ガイドライン（91頁）遵守事項4.1.1(1)(a)(ア)「委託先によるアクセスを認める情報及び情報システムの範囲」

「特に、委託業務において使用される情報システムが海外のデータセンターに設置されている場合等においては、保存している情報に対して現地の法令等が適用されるため、国内であれば不適切と判断されるアクセスをされる可能性があることに注意が必要である。『行政機関の保有する個人情報の保護に関する法律』で定義する個人情報については、国内法が適用される場所に制限する必要があると考えるため、個人情報を取り扱う委託業務においては、保存された情報等において国内法令が適用されること等を外部委託の際の判断条件としておくべきである。」と規定し、事実上、グローバルクラウドを排除し、個人情報が関係する場合には、国内データセンター設置要件を課している。

しかしながら、本来、クラウド事業者の国籍やデータセンターの場所が、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一番重要なものではない。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、海外に設置されたデータセンターについて殊更リスクを強調することは誤解を招くものであって、かかる理由で利用を禁止することは適切でなく、削除すべきである。

6. 本ガイドライン(95頁)　遵守事項4.1.1(2)(a)(カ)「情報セキュリティ対策その他の契約の履行状況の確認方法」

情報セキュリティ対策その他の契約の履行状況の確認方法として、個別の報告や実地監査の受入れを要求事項とするのは不適切であり削除すべきである。それらの確認は、第三者による事業者の監査レポート、情報セキュリティに関する国際規格への準拠状況、クラウド事業者が提供する様々な資料の活用によるべきであることは、前記各論 2 及び 3 のとおりである。

以　上