2016 年 7 月 4 日

「政府機関等の情報セキュリティ対策のための統一基準群」の改定（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、内閣サイバーセキュリティセンター（NISC）より公表された「政府機関等の情報セキュリティ対策のための統一基準群」を構成する文書（以下「本基準群」といいます。）に関し、以下の通り意見を提出致します（以下「本意見」といいます）。

BSA は、政府機関等の情報セキュリティ対策を改善するために本基準群を改定し続ける政府の不断の努力に敬意を表します。私どもは、健全なデジタル経済の発展を支える効果的な情報セキュリティ戦略が非常に重要であると考え、世界中において効果的な情報セキュリティ戦略のための政策提言活動を行っております。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平成 26 年度版（以下単に「26 年度版」といいます。）に対してもパブリックコメントを提出していますが[2]、本意見においては、再度強調すべき重要な点及び本基準群で追加された新しい記述について意見を述べます。

BSA の意見は、下記に重点を置いています。

- 本基準群が、クラウドサービスについて、従来のオンプレミス情報システムとの比較の観点で、セキュリティ、機能性、サポート及び費用削減効果を正しく認識する形で記述しているか。
- クラウドサービスプロバイダーの評価を、関連する国際規格への準拠・認証に基づき行うよ

---

[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の加盟企業は世界中で最もイノベーティブな企業を中心に構成されており、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・ソリューションを創造しています。ワシントンDCに本部を構え、世界60カ国以上で活動するBSAは、正規ソフトウェアの使用を促進するコンプライアンスプログラムの開発、技術革新の発展とデジタル経済の成長を推進する公共政策の支援に取り組んでいます。BSAの活動には、Adobe, ANSYS, Apple, ARM, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, DataStax, Dell, IBM, Intel, Intuit, Microsoft, Minitab, Oracle, PTC, salesforce.com, SAS Institute, Siemens PLM Software, Symantec, Tekla, The MathWorks, Trend Micro, 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] BSA の政府機関の情報セキュリティ対策のための統一基準群平成 26 年度版に対するパブリックコメントについては、http://bsa.or.jp/files/20140214.pdf をご覧ください。

う規定しているか。

・　情報システムを物理的にインターネットから分離することを求める、不必要な要件が、課され又は推奨されていないか。

本意見は、クラウドコンピューティングなどインターネットにより可能となったサービスが世界経済に大きな影響を与えていることに基づいています。社会が著しい技術進展から受ける恩恵を最大化するためには、政府が、これらのサービスの開発、採用、導入にインセンティブを与える政策を立案することが極めて重要です。BSA が最近発表した報告書[3]の中では、膨大な、そのままでは非生産的である情報の中に潜在する非常に有益な価値を引き出すために、データを収集、蓄積、分析そして変換するデータイノベーションの中枢部分が重要であること、そして、世界中の非常に困難な問題を解決する現場において、データイノベーションが革新的な進歩をもたらしていることが示されています。政府もこの動向を踏まえて、例えば、日本再興戦略 2016 において、クラウドを含む最新のテクノロジーを積極的に利用しつつ、運用コストを削減しながらも国民の利便性を向上する行政サービスの提供を目指しています[4]。BSA 会員企業は、安全で安心なクラウドサービス、データアナリティクス、デバイス、アプリケーション等、この動きを支える先進的なテクノロジー及びサービスを提供しており、BSA も前記のような政府のリーダーシップを支持します。

技術革新の恩恵を最大限に社会に活かすには、サイバーセキュリティを含むあらゆる IT 政策に関し、政府と民間企業が協働してベストプラクティスを共有すること、そして政府が実践において模範を示すことが非常に重要です。また、政府が、サイバーセキュリティ指針を、効果的、柔軟、技術中立かつリスクベースのものとし、かつ、クラウドサービスが従来のオンプレミス情報システムと比較して必然的にリスクが高いという誤解を生じさせないようにすることが重要です。

以上の観点を踏まえ、以下、各論につき、優先順位に従って意見を述べます。

第 5 部　情報システムのライフサイクル

5.2.1「情報システムの企画・要件定義」についてですが、「情報システムのライフサイクル全般を通じて、情報セキュリティを適切に維持する」という目的に異論ありません。セキュリティ要件の曖昧さや過不足が「**過剰な情報セキュリティ対策**（太字追加）に伴うコスト増加」とい

3　「データは何をもたらすのか？～データイノベーションが実現する世界～
http://bsa.or.jp/news-and-events/news/bsa20151221/

4　例えば、国・地方自治体の IT 化・BPR の更なる推進策として、「国の行政機関における業務・システムについては、国民の利便性や公共価値を高める観点から、情報システムの運用コスト削減と行政サービスの改善、業務の効率化に取り組む。」「自治体クラウド未実施の団体においては、業務の共通化・標準化を行いつつ、自治体クラウド導入の取組を加速することにより、当該情報システムのコスト削減を図る」（同戦略 63 頁及び 64 頁）とされている。

う不利益を生じる可能性に繋がるとの記述も着目に値します。

しかしながら、今回、遵守事項(2)「情報システムのセキュリティ要件の策定」において、情報システムセキュリティ責任者は「構築する情報システムをインターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することの要否を判断」することが追加されています。BSA は、情報システムをインターネットから物理的に分離する（これにより、クラウドサービス及びインターネットにより可能となるサービスが除外される）ことは、通常「過剰な情報セキュリティ対策」に該当すると考えます。本基準群は、分離の要否につき、「情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき」判断することとしていますので、必ずしも分離を唯一の選択肢としている訳ではないことは私どもも認識していますが、情報システムのインターネットからの分離は、当該システム内の情報にアクセスし利活用する能力を大幅に低下させるにもかかわらず、それが完全なセキュリティソリューションという訳でもありません。サイバーセキュリティにおいては、多階層な防御方法を採用することによって、インターネット接続から分離を行うことなく、インターネット接続から得られる生産性向上や他の利点を失わずに、効果的にシステムを保護することが可能です。また、最近の調査では、攻撃の 31.5%は悪意を有する従業員または元従業員により行われ、23.5%は攻撃者が善意の従業員の手を介して攻撃を仕掛けるという報告[5]もされています。情報システムをインターネットから分離することは、必要なデータにアクセスし利活用する能力を低下させるだけでなく、BSA 会員企業を含む先進的なクラウドサービスプロバイダーが提供する最先端のセキュリティソリューションから当該政府機関が恩恵を得ることも制限されてしまうことになります。

提言

5.2.1 の遵守事項(2)(a)及び府省庁対策基準策定のためのガイドライン（28 年度版）（以下「本ガイドライン」）（133 頁）における「インターネットやインターネットに接点を有する情報システム（クラウドサービスを含む。）から分離」に関する記述を削除することを求めます。これにより、本基準群が政府職員に対して情報システムのセキュリティを確保するための最も効果的な方法がインターネットからの分離であるとの誤解を生じさせてしまうことを防ぐことができます。

第 4 部「外部委託」

4.1.4「クラウドサービスの利用」

当該項目は、本基準群に新たに追加され、クラウドサービスの利用に特化してセキュリティ上考慮すべき点について記述しています。本基準群は、政府機関がクラウドサービスを進んで活用することの重要性を認めたといえ、クラウドサービスを採用・利用する際に考慮すべき要件につ

[5] IBM 2015 Cyber Security Intelligence Index
http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03073usen/SEW03073USEN.PDF

いてのガイダンスを正しく提供しています。現在、多くの専門家が、主要なクラウドサービスプロバイダーは、洗練された事業者が自らデータを保護するのに比べても、より高いレベルでユーザーのデータを保護するセキュリティを提供していると認めています。多くのクラウドサービスは、ユーザーがクラウドに保管したデータを暗号化することを認めているため、この場合、クラウドサービスプロバイダーであっても、可読可能な形式のデータにアクセスすることはできません。このことから、本基準群が、クラウドサービスがより高いセキュリティをユーザーに提供する点に言及し、クラウドサービスが他の選択肢と比較してセキュリティリスクが高くなるのではないかという印象を打ち消すことが有益であると考えます。

さらに、混乱や誤解を防ぎ、より良いものとするため、下記のとおり修正すべきと考えます。

4.1.1 では、「クラウドサービスの利用に係る外部委託については、クラウド特有のリスクがあることを理解した上で、4.1.4 項「クラウドサービスの利用」についても本項に加えて遵守する必要がある。」と記述されています。前述したとおり、クラウドが「特有の」リスクを有することは事実かもしれませんが、そのリスクが他の選択肢であるオンプレミスの情報システムなどのものよりも高いといった正しくない印象を与えることがない記載とすべきです。

4.1.4 遵守事項(1)(b)は、「情報システムセキュリティ責任者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定すること」を挙げています。BSA は準拠法、裁判管轄、適用される法令・規則を確認することの重要性について同意します。しかし、クラウドサービスプロバイダーが、準拠法に従いデータを安全・適切に扱うことを保証することができれば、データの保存場所を指定する必要はないはずです。クラウドサービスがもたらす優位性の多くは、国境を越えたデータ移動が可能であることによりもたらされます。よって、そのような移動を制限し、データが「特定の場所」にあることの説明を求めることは、データのセキュリティを何ら増すことがないのに、クラウドサービスやプロバイダーを制限することになってしまいます。データのセキュリティは物理的な保管場所に依存するのではなく、データを保護するための品質の高い機能、効果的な手段、制御の行き届いた管理によってもたらされます。

4.1.4 は、情報システムセキュリティ責任者が情報の適切な取り扱いが行われていることを直接確認することが容易ではないことを踏まえ、4.1.4 遵守事項(1)(d)及び(e)において、情報システムセキュリティ責任者に対し「クラウドサービスの特性」を考慮し、「クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定める」ことを適切に記載しているものと考えます。また、情報システムセキュリティ責任者は「クラウドサービスを総合的・

客観的に評価し判断すること」とされています。本ガイドライン 118-119 頁では参考となる認証として、ISO/IEC27017 によるクラウドサービス分野における ISMS 認証の国際規格が挙げられ、また、日本セキュリティ監査協会のクラウド情報セキュリティ監査やクラウドサービス事業者等のセキュリティに係る内部統制の保証報告書である SOC 報告書（Service Organization Control Report）の活用が示唆されています。BSA は、技術製品及びサービスの能力又は品質を確保するための手段として、透明性を有し業界が主導する形で策定された任意の国際規格を活用することを支持します。

提言

委託先のクラウドサービスプロバイダーを選定する上で評価・判断するための要件として、関連する国際規格への準拠や認証を活用する旨、本ガイドラインにとどまらず、本基準群において明示するよう求めます。

また、米国政府が採用している、セキュリティ評価と認証における標準的手法の提供を目指す Federal Risk and Authorization Management Program（FedRAMP）のような、政府機関向けクラウドサービス認証制度の採用を推奨します。

これらを併せて用いることにより、情報システムセキュリティ責任者は、クラウドサービスプロバイダーを包括的に評価することができ、目的に対して、最も費用対効果が高く、安全で、機能に優れたクラウドサービスを選定する確率を高めることができます。また、結果として、公共部門にとどまらず、安全で効果的なクラウドサービスの導入の更なる普及を推進することになります。

4.1.1「外部委託」及び 4.1.2「約款による外部サービス」

異なる種類の外部委託業者についての区別が不明瞭又は混乱を招きがちであるため、外部サービスで取り扱うことのできる情報について余計な懸念を生じさせかねない記載となっています。この点、「要機密情報」が全面的に禁止されているのは「約款による外部サービス」に限定されていると考えます。万一、クラウドサービスが、同時に「約款による外部サービス」に該当する場合があるとすると、4.1.1 及び 4.1.2 の記述により要機密情報を取り扱うことができないという懸念が残ってしまいます。本基準 1.3 節「用語定義」によれば「クラウドサービス」と「約款による外部サービス」は区別されており、本ガイドライン 7 頁に 4.1 節に記述されているそれぞれの外部サービスの関係が記載されているものの、その区別につき政府機関において誤解や混乱が生じる恐れがあります。

また、4.1.1 遵守事項(2)(b)(ア)には、「セキュリティ監査」の受入れについての記述があります。新たに設けられた 4.1.4 遵守事項(1)(e)において情報システムセキュリティ責任者は「ク

ラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し、判断すること」とされています。前回、BSA は 26 年度版に対し、監査プロセスの一環として、政府担当者による現地調査を要件とするか又は奨励しているように思われる点について懸念を表明しました。

提言

「約款による外部サービス」による取扱いを禁止される情報の範囲が過度に広くならないよう、該当する「要機密情報」の適用範囲を最も機微な情報に限定するよう狭めることを提言します。

本基準群中の記載により、クラウドサービスが「約款による外部サービス」ではないことを明示することを求めます。例えば、本ガイドラインの 7 頁に記載されている参考図を用いて、異なる外部委託サービスの関係についての説明を本基準群に含めることを提言します。

「約款による外部サービス」により「要機密情報」の取り扱いが禁止されるのは、当該サービスの約款の内容が要機密情報を扱う要件を満たしていない場合に限られる旨を明確にすべく、本基準群の記載を修正するよう提案します。

最後に、外部委託業者（特にクラウドサービスプロバイダー）が適切なセキュリティ対策を有するか否かを確認するために、政府機関は、利用可能な様々なセキュリティ対策に関する情報（例えば、第三者によるクラウドサービスプロバイダーの監査レポート、情報セキュリティに関する国際規格への準拠状況（上述 4.1.4 に関するコメントにおける国際規格についての記述を参照）等を含みますが、これらに限定されません））を活用すべきことを明確にしていただけるようお願いします。クラウドサービスプロバイダーが政府担当者による直接の現地調査を受け入れることを要件とすべきではありません。そのような要件は現実的でも効果的でもなく、間接的にデータやハードウェアを国内に置かせることを要求する結果を招くからです。

結論

BSAは、重要な本基準群に対する意見提出の機会に感謝致します。本意見が、本基準群を完成させる上で有益であることを願っておりますが、更には、公共及び民間部門における情報システムのサイバーセキュリティ能力の向上並びに経済成長、雇用創出及び困難な社会的課題解決のための有効策であるクラウドサービス等のインターネットにより可能となるサービス採用推進のための政府の継続的な活動に際して有益なものとなるよう願います。本意見について、ご質問等ございましたらいつでもご連絡下さい。

以　上