「政府機関等のサイバーセキュリティ対策のための統一基準群」の改定（案）（令和3年度版）に関する意見

2021年5月13日

BSA｜ザ・ソフトウェア・アライアンス（以下、「BSA」）[1]は、内閣サイバーセキュリティ―センター（以下、NISC）より公表された「政府機関等のサイバーセキュリティ対策のための統一基準群」に対するパブリック・コメントの機会に感謝し、本基準群を構成する文書である「統一基準」（以下「統一基準」）に関し、以下のとおり意見を提出致します。

総論

BSAは、各国政府の前で、また国際的な市場において、グローバルなソフトウェア業界のための主要な提唱者です。BSAは、政府機関等のサイバーセキュリティ水準の斉一的な引き上げのために、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。BSAの会員企業はクラウドコンピューティング、セキュリティ・ソリューション、データアナリティクスや人工知能（AI）等の最先端のテクノロジーやサービスの提供し、政府や社会のデジタルトランスフォーメーションを支えています。

BSAはサイバーセキュリティ政策や立法の策定に関し、世界中の政府と協働しており、その中で、当該政策や立法を通して、市民のプライバシーや人権を保護しながらサイバーセキュリティの脅威を効果的に阻止し、対処することが可能であることを見てきました。これらの経験を踏まえ、BSAでは「International Cybersecurity Policy Framework [2]（以下、「BSA Framework」）」をまとめました。「BSA Framework」では、各国が国内の包括的なサイバーセキュリティ政策を策定する上で推奨できる模範を示し、政府調達を含む国内のサイバーセキュリティ政策において重要となる要素に触れております。この中では、国際規格との整合性、リスクベース、成果志向、技術的中立性といったアプローチに加え、イノベーション促進のために政策の順応性を高めることを提唱しています。

サイバーセキュリティの課題に対処するには、接続環境にあるエコシステムの完全性、機密性、また、回復力を防御するための革新的なツールと実践が必要であり、最良の暗号化技術を適宜使用できることが重要です。そのためにも、政府が民間部門と密接に協力し、セキュリテ

[1] BSAの活動には、Adobe, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Workdayが参加しています。詳しくはウェブサイト（http://bsa.or.jp）をご覧ください。

[2] BSA International Cybersecurity Policy Framework: https://bsacybersecurity.bsa.org/report-item/bsa-international-cybersecurity-policy-framework/

22F Shibuya Mark City
1-12-1 Dogenzaka, Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 530
W bsa.org

Japan Representative Office

ィの取り組みの最新の進歩の恩恵を受けられるように、セキュリティ政策を策定することを奨めます。

本統一基準の目標を支援するため、以下、各論につき、意見を述べます。

提言

第 1 部　総則　/ 1.3 用語定義
第 6 部　情報システムのセキュリティ要件 /　6.1　情報システムのセキュリティ機能

「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見直し（案）について」[3]（以下、「見直し（案）」）は、注力すべき適切な主要なサイバーセキュリティ課題を特定しており、BSA は NISC の検討の方向性を支持しております。情報セキュリティ対策の基盤をより強固にするために、見直し（案）で言及されている「常時アクセス判断・許可アーキテクチャ」や「常時システム診断・対処」などのキーワードを「統一基準」に明確に反映させること、つまり、これらのキーワードを「1.3　用語定義」に追加するとともに、第 6 章 6.1.「情報システムのセキュリティ機能」に反映されることを奨めます（例： 6.1.6 常時アクセス判断・許可アーキテクチャ」、「6.1.7 常時システム診断・対処」）。

また、今回の改定統一基準において、様々な外部の委託サービスに関し、説明が追加がされていることを我々は歓迎します。この中では、クラウドサービスが「外部サービス」に該当することが明確にされ、「外部サービス」は「機関等外の者が、一般向けに情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能を利用して機関等の情報を取り扱う場合に限る」と記されています。政府関係者や関連するステークホルダーが同じ理解を共有するために、どのような場合が外部サービスの「情報を取り扱う」に該当するのかを明確にすることで、この本文はさらに改善されると考えます。また、「外部サービス管理者」が「外部サービスの利用における利用申請の許可権限者から利用承認時に指名された当該外部サービスに係る管理を行う者をいう」と記されていますが、これが政府機関等の職員を指すのか、事業者を指すのかを明確にされることを希望します。

第 4 部外部委託 / 4.2 外部サービスの利用

我々は、政府がクラウドサービスのセキュリティに関する説明を追加したことを支持します。公共部門において「クラウド・バイ・デフォルト原則」（以下「本原則」）を達成するという日本政府が公式に発表している目標に進むには、セキュリティ要件によって政府機関等が革新的なクラウドコンピューティング・ソリューションを採用することが不必要に阻害されないよう、本原則を統一基準に反映させることを奨励します。本原則が各機関で統一的に共有されることが重要です。

加えて、統一基準の改訂において、国際規格を認め、「遵守事項」にセキュリティの責任共有モデルを反映させたことを歓迎します。クラウド環境におけるプロバイダーと顧客の役割と管理レベルに応じて、適切な要件を割り当てるのが効果的なクラウドのセキュリティ政策です。このような基本的なセキュリティ義務の分担を認識していない政策は、重要なセキュリティ管理策を強制的に削除したり、自身のクラウド環境における政府のセキュリティ管理能力を低下させたり、セキュリティに関する重要な前兆を見逃す可能性を高める等、政府機関の作業負荷リスクを高めます。例えば、クラウドサービスの取り決めにおける二当事者間で、インフラの一部のセキュリティがもう片方の当事者の責任であると思い込んでいる場合があります。この

[3] https://www.nisc.go.jp/active/general/pdf/gaiyo2021.pdf

ような盲点がセキュリティ上の深刻な脆弱性となってしまいます。そのためにも、このセキュリティモデルが政府機関全体で理解されることを NISC にて確実にすることを奨めます。

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　（2）情報システムのセキュリティ要件の策定　(a)

前回の 2018 年の意見書[4]でも述べておりますが、BSA は、統一基準の中で、情報システムセキュリティ担当者が「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（外部サービスを含む）から分離することの要否を判断した上で」セキュリティ要件を策定するというガイダンスに引き続き懸念を抱いています。 この判断は、「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け等」に基づき行われるべきであり、デフォルトの選択を意図したものではないと認識していますが、情報システムをインターネットから分離すると、当該システムに保有されている情報へのアクセスや利用が大幅に減少するだけでなく、政府機関が大手クラウドコンピューティング・サービス・プロバイダー（以下、「CSP」）が展開する最先端のセキュリティ・ソリューションの恩恵を受けることも制限することとなります。

多くのクラウドサービスは、暗号化や厳格なアクセス管理システムなど、国際的に認められた機能を実装することで、世界水準のデータセキュリティを実現しています。BSA 会員の多くを含むグローバルな CSP は、データ・セキュリティへの大規模な投資をしており、機密な個人情報の利用を可能にする最も効果的なデータ・セキュリティを提供しており、これらの最高水準の安全なソリューションの利用を日本政府が政策において確実にすることが不可欠です。したがって、我々は日本政府に対し、統一基準の 5.2.1 (2) (a) および「政府機関等の対策基準策定のためのガイドライン （令和３年度版）」（173 ページ）において「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 （外部サービスを含む。）から分離する」という記述を削除することを求めます。これにより、本基準群によって、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いう誤解を政府職員に生じさせるとを防ぐことができ ます。

結論

BSA は、意見提出の機会に感謝致します。本意見が統一基準を確定する上で有用であれば幸いです。本意見に関して、ご質問がある場合又はより詳細に議論をされたい場合には是非ご連絡下さい。

[4] https://bsa.or.jp/wp-content/uploads/bsa_20180628.pdf