特定妨害行為の防止による
特定社会基盤役務の安定的な提供の確保に関する基本指針（案）に対する意見

2023年3月10日
BSA | The Software Alliance

総論

BSA｜The Software Alliance[1]（BSA | ザ・ソフトウェア・アライアンス、以下「BSA」）は、「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針」（案）（以下「基本指針案」）に対する、パブリックコメントの機会に感謝し、経済安全保障推進室に以下の通り意見を提出します。

BSAは、政府やグローバル市場において、世界のエンタープライズ・ソフトウェア産業を代表する主唱者です。BSAの会員は世界で最もイノベーティヴな企業で構成されており、クラウドコンピューティング、データアナリティクス、人工知能（AI）など、政府や企業を強化する最先端のテクノロジーと役務を提供しています。また、BSAの会員はセキュリティ分野のリーダーでもあり、今日、業界全体で使用されているソフトウェアセキュリティのベストプラクティスの多くを開拓してきました。[2]

BSAは、サイバーセキュリティ政策の策定において、世界中の政府と緊密に連携しています。これらの経験に基づき、日本政府の取り組みを支援するために、以下の見解と提言を述べさせていただきます。BSAが先の意見書で[3]述べましたように、我々は、悪意ある行為を効果的に特定し、遮断するために、持続可能で透明性がある政策対応の設計をすることを推奨します。基本指針案は「経済政策を一体的に講

[1] BSAの活動には、 Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.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] *Strengthening Trust, Safeguarding Digital Transformation: BSA's Cybersecurity Agenda* https://www.bsa.org/files/policy-filings/10132021bsacybersecurityagenda.pdf
また、 *The BSA Framework for Secure Software: A New Approach to Security the Software Lifecyle – Version 1.1 (September 2020)* https://www.bsa.org/files/reports/bsa_framework_secure_software_update_2020.pdf
をご覧ください。

[3] https://www.bsa.org/files/policy-filings/jp04262022jpecsec.pdf

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

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office

ずることによる安全保障の確保の推進に関する法律」（以下、「本法」）の第3章に規定された、新たな事前審査制度を実施するための現在の検討方向を示しており、この中には特定社会基盤事業者、特定重要設備、特定重要維持管理等の委託の指定が含まれています。基本指針案で的確に言及されているように、この新たな制度によって、保護しようとする技術や経済活動が阻害されるような意図せぬ結果を最小限に抑えること、また、これらの政策がイノベーションや世界的に利用可能な最高水準の技術へのアクセスを妨げないようにすることが重要です。 BSAは、日本のデジタル経済の安全性、完全性、活力を強化するために、日本政府に協力していけることを期待しています。

第 3 章 特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に当たって配慮すべき事項

第 1 節 特定重要設備に関する基本的な考え方

(1) 特定重要設備に関する考え方

基本指針案の第 3 章第 1 節（1）では、特定社会基盤役務を安定的に提供するための重要な設備、機器、装置、又はプログラムを取り上げていますが、障害や劣化の原因の一つが、妨害行為によるものではなく、供給者やベンダーによるサポートが終了した機器、システム、ソフトウェアの使用であることを理解することが重要です。例えば、電気通信事業者が使用する物理的なネットワーク製品で、ライフサイクルが終了したものは、もはや使用せず、サポートが受けられる最新の製品に交換する必要があります。同様に、サポートが終了したソフトウェア製品も、更新されたバージョンに置き換えるべきです。

したがって、特定重要設備については、製品ベンダーのサポートが終了した機器、システム、ソフトウェアの継続使用を禁止することを推奨します。これにより、そのような旧式の製品に起因する混乱を最小限に抑えることができます。ライフサイクル終了の通知は、通常、サポート終了日の大分前に送られます。 特定重要設備の運営者は、このようなライフサイクル終了の通知を受けて、移行やアップグレードを計画する必要があります。

(2) プログラムの変更に関する考え方

基本指針案の第 3 章第 1 節（2）は、プログラムを含む特定重要設備、機器又は装置に関する方針を示しています。ここでは、提出された導入等計画書に記載されたプログラムに関係する機能に変更を加える場合（新たな機能の追加を含む）、原則、その変更内容を政府に届出または報告することが必要であると規定されています。特定重要設備は今後正式に指定されますが、その対象にクラウドコンピューティングが含まれる場合、クラウドサービスプロバイダー（CSP）とその顧客が当

該方針を効果的に実施するためには、明確かつ実用的なガイダンスが役立ちます。本法において、どのようなクラウドサービスが特定社会基盤事業者による特定重要設備の「導入」または「委託」に該当するのかを定義すること、特に、各担当省庁が定めるクラウドサービスの定義が一貫していることが重要です。このような定義を含む不一致を避けるため、内閣府及び内閣官房が強力なリーダーシップを発揮し、各省庁間で採用されるハイレベルな指針を提供し、多くの産業で一般的に使用されているシステムの安全基準を作成することを奨めます。このような指針は、一致させるべき事項、また、各省庁判断に委ねられる事項を特定する上でも有用です。

また、政策や省令の策定にあたっては、クラウド特有の側面を考慮し、民間事業者を適切に指導するとともに、特定社会基盤事業者が本法の下で円滑にクラウドに移行できるようにすることを奨めます。例えば、基本指針案では、日常的なバグ修正等のアップデートのような軽微な変更については、届出を要しないことを明確にしています。また、クラウドサービスの日進月歩の性質を考えると、定期的なアップデートが CSP によってグローバルかつ同時に実施されていることが理解されていることも重要です。このような変更は、セキュリティを含む、顧客に対する迅速な対応とサービス向上のために必要なものです。もし、機能のアップデートも「プログラムの変更」として届出義務の対象となれば、実際の業務に支障をきたすことになります。指定を受けた事業におけるクラウドユーザーを適切に指導するためにも、届出等を要するのは、リスク管理に実質的な影響を与える変更のみに限定される、と基本方針において明確にすることを求めます。

第 3 節 特定重要設備及び重要維持管理等を定める主務省令の立案に当たって配慮すべき事項

「経済対策を一体的に講ずることによる安全保障の確保の推進に関する基本的な方針」（平成 4 年 9 月 30 日閣議決定）において、自由かつ公正な経済活動との両立を図ることなど、本法の施行に当たって配慮すべき基本的事項が示されました。この基本な方針に沿って、基本指針案の第 3 章第 3 節では、特定重要設備及び重要維持管理等を指定する主務省令の立案に当たっては、特定社会基盤役務の提供に当たって過度な負担を生じないよう、また、適正な競争関係を不当に阻害することのないよう、真に必要な範囲に限定して慎重に判断することとされています。セキュリティレベルを評価する際には、グローバルなセキュリティ・プラクティスや国際的に認知された規格を考慮に入れ、本法や省令を遵守しながらクラウド型システムを円滑に導入できるよう、CSP やその顧客に対して明確な指針を政府から示すことを我々は推奨します。

また、供給者への負担については、新たなサイバー脅威や脆弱性は継続的に出現し、ベンダーが提供するアップデートや対策がタイムリーに適用されることが重要

であることから、脅威に効果的に対処できるよう、対策の適用方法については柔軟性をもたらすことを推奨します。

第 4 章 特定社会基盤事業者に対する勧告及び命令に関する基本的な事項

第 1 節 導入等計画書の届出並びに勧告及び命令に関する考え方

（4） 審査に当たっての考慮要素

第 4 章第 1 節（4）では、事前審査におけるリスク評価の考慮事項として、「我が国の外部にある主体から強い影響を受けている事業者からの設備の導入等について慎重な審査を行う必要がある」と示されています。外国政府からの影響力が審査の対象となることは理解できますが、考慮要素に、本社と日本の子会社・関連会社間の関係のように、現地の主体に影響を与える海外主体と関係をもつ供給者も含まれてくるのかを明確にすることは、関係者の理解に役立ちます。

また、日本の外部の主体からの影響の審査については、単一のステークホルダーに不必要に負担を強いることのないよう、潜在的に関与し得る様々なステークホルダーの責任の範囲や限界について明確化することが有用です。

(5) リスク管理措置

第 4 章第 1 節（5）では、特定社会基盤事業者が特定重要設備の導入及び重要維持管理等を委託する際のリスクを軽減するために講じることができるリスク管理措置の例を挙げ、これらの措置は特定重要設備が特定妨害行為の手段として用いられるおそれを審査するに当たり必要な要素であるとしています。業界特有のシステム等がある一方で、電気通信等を含む多くの業界で一般的に使用されているシステムがあることにも留意する必要があります。このような一般的に使用されるシステムについては、リスクの管理や評価方法、提出を求められる情報の種類など、規制上の共通要件を設けることを強く推奨します。さらに、これらの要件が、可能な限り国際的に認められた規格に基づくことを奨めます。

また、コンフィデンシャル・コンピューティングやゼロトラスト原則など、費用対効果の高いアプローチによってデータ保護を強化し、サイバーセキュリティを向上させるクラウドサービスの可能性を考慮することが必要となります。また、リスク評価の指標には、既存の国際的なベンチマーク、ベストプラクティス、認証フレームワークを取り入れることを推奨します。クラウドサービスの場合、ISO/IEC 27001、27017、27018、ISMAP、その他の関連規格や第三者認証の取得などが考えられます。さらに、適切なサイバーセキュリティのリスク管理プロセスが実施されているとして、米国政府の Federal Risk and Authorization Management

Program（FedRamp）等、有志国による認証を評価することも推奨します。本制度の効果的な運用を可能とするためには、特定社会基盤事業者及びその供給者の過度な負担となるような、重複する規制を避けることが重要です。リスク評価において国際的に認知された規格やその他のプログラムを統合することは、事前審査の効率的かつ効果的な実施を促進し、この新たな制度の対象となり得る多様な事業者に対して、より明確で確実な情報を提供することになります。

リスク評価指標の目的は、事業者がリスクの基準値を設定し、リスク許容度を理解しようとする際の指針となることです。リスクの審査においては、特定重要設備のリスクレベルの評価も含め、事業者がそのリスクレベルに応じて必要な緩和策を講じる責任を負うということを、基本指針に明記すべきです。リスクレベルに応じた義務が課されれば、重要でないリスクや低レベルのリスクを管理するために事業者が過剰なリソースを費やす必要がなくなります。この点については、事例を盛り込み、また、それが単なる例示であり、断定的な判断ではないことを明確化することを奨めます。

第 5 章 特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関し必要な特定社会基盤事業者その他の関係者との連携に関する事項

第 3 節 関係者等の意見の適切な考慮

第 5 章第 3 節では、「内閣総理大臣及び事業所管大臣は、政令及び主務省令の策定に当たっては、平時から関係事業者等と必要なコミュニケーション・連携を図ることに加え、経済団体、学識経験者、関係行政機関等の知見を有する者の意見を十分に聴くとともに、パブリックコメント制度を活用し、多様な意見を適切に考慮する」とあります。ステークホルダーの意見を聴くという強いコミットメントを我々は歓迎しますが、今回の意見募集のように、1 ヶ月という短い期間は、ステークホルダーが十分に理解し、実質的な意見を検討するには十分な時間ではないことにも留意が必要です。外国事業者が英訳を準備するには、相当の時間を要することから、意見募集期間として、少なくとも 2 ヶ月確保するとともに、意見募集の開始時に原案の英語版を提供するよう強く要望します。

結論

BSA は、経済安全保障を効果的に推進するという日本政府の目標を支援するために、協力してゆきたいと考えています。本意見書の提出に加え、検討された方向性をよりよく理解し、さらなる提言や提案を通じて、政府の目標達成に貢献するためにも、引き続き意見交換ができる機会をいただけることを期待しています。