2025 年 11 月 21 日

重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針（案）に関する意見

Business Software Alliance（ビジネス・ソフトウェア・アライアンス、以下 BSA）[1]は、「重要電子計算機に対する不正な行為による被害の防止に関する法律」[2]（以下、本法）に基づく施策を適切に機能させるための基本的な事項を示した「重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針（案）」[3]（以下、方針案）に関して意見する機会を得られたことに感謝します。国民生活・経済活動を脅かし、増え続けるサイバー攻撃に対し、日本の対処能力を向上させるという政府の目標を我々は全面的に支持します。

BSA は、エンタープライズソフトウェア業界を代表するグローバルな業界団体であり、サイバーセキュリティ、人工知能（AI）、クラウドコンピューティング、量子技術、その他の先進的技術をリードする企業を代表しています。BSA の会員企業は最先端のセキュリティツールを提供し、政府や産業界全体で採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。BSA は会員企業と共に、世界各国の政府と緊密に連携しながら、サイバーセキュリティ政策の策定に取り組んでいます。こうしたグローバルな経験に基づき、経済安全保障推進法[4]で指定された特定社会基盤事業者[5]の被害を防止し、役務の継続を確実にするという政府の目的を支援するため、以下の意見を提出します。

---

[1] The Business Software Alliance (https://bsa.or.jp/（日本語）、www.bsa.org（英語）)は、アメリカ合衆国、ヨーロッパ、アジアの 20 を超える市場で活動し、あらゆる分野の産業また一般消費者がイノベーションの恩恵を受けられるよう、テクノロジーに対する信頼を構築する政策を推奨しています。BSA の会員には以下の企業が含まれます： Adobe, Alteryx, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

[2] https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/houritsu.pdf

[3] https://public-comment.e-gov.go.jp/pcm/download?seqNo=0000301883

[4] https://www.japaneselawtranslation.go.jp/en/laws/view/4716

[5] https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_gaiyou.pdf

我々の提言は、日本政府及び国内企業が最良かつ最も安全なクラウドサービスを利用できることで、日本国民と顧客へのサービスが向上されることを目標としています。制度運用方針の策定においては、他の国際的な慣行との整合性、既存および新たなビジネス慣行や技術的配慮との一貫性を保つことを推奨します。また、本法に基づき指定された事業者（「特別社会基盤事業者」）が、最高水準のセキュアなソフトウェア技術を導入することを促進するのではなく阻害する可能性のある、意図しない影響を最小限に抑えること奨めます。

方針案に記された目標を達成するには、**具体的な方針案について、実施前に十分な意見照会をし、実施後は方針を頻繁に見直し**、法律や施行規則が目的に合致していることを確実にし、特別社会基盤事業者によるデジタルトランスフォーメーションやクラウド導入といった他の重要目標を阻害しないようにすべきです。

我々が下記で推奨しているのは、以下の事項となります。

- ***「特定重要電子計算機」の届出***
- ***インシデント（侵害事象）の報告***
- ***脆弱性開示と脆弱性対応の強化***

特定重要電子計算機の届出

方針案では、日本における特別社会基盤事業者のレジリエンス強化を目的とした官民連携の促進策の一環として新たに導入される、特別社会基盤事業者が使用している特定重要電子計算機の届出義務について説明がされています。特定重要電子計算機には重要設備だけでなく、クラウドコンピューティングサービスを含む情報システムも含むとされています。特定重要電子計算機の対象範囲については、来年公布予定の政令・省令で詳細が定められると理解していますが、我々の以前の提言[6]でも述べたように、特定重要電子計算機の指定に際しては、リスクベース・アプローチを採用し、特別社会基盤事業者が提供する重要役務の継続的な提供に不可欠な特定のシステムに焦点を当て、特別社会基盤事業者が使用するその他の重要でないシステムは指定対象としないことを求めます。

方針案の第 4 章第 2 節(1)で述べられているように、特別社会基盤事業者が使用する機器の数を考慮すると、届出は膨大となり、手続きに多大な時間を要すると予想されます。本方針を実現可能なものとするためには、高度なコンピューティングシステムを導入する特別社会基盤事業者、また、届出を管理する政府機関の負担を最小限に抑えることが重要です。この点において、クラウドコンピューティングサービスの対象範囲を、特別社会基盤事業者のテナントのうち重要機能を支えるサービスに絞り込むことを推奨します。

[6] https://www.bsa.org/files/policy-filings/jp04112025recccyberdef.pdf

本方針が関連するステークホルダーにおいて効果的に実施されるためには、合理的な制度設計が必要であり、この点において、個別事業者向けの専用設計品等に関しては届出を不要とすることや、機器更新等の重要電子計算機の変更に伴う届出の負担を配慮した方針案の考え方を我々は支持します。

また、本法及び方針案に沿い、クラウドサービスプロバイダーではなく、特別社会基盤事業者によって直接さまざまな対策が継続的に実行されるようにすることも重要です。

そして、届出手続においては、過度に詳細な情報の開示を義務付けることは避けるべきです。特に、企業秘密やシステム・セキュリティー関連情報など、供給者が特別社会基盤事業者と共有することが困難な情報を収集することを特別社会基盤事業者に求めないことが重要です。

侵害事象（インシデント）の報告

方針案の第 4 章第 2 節(2)では、特定重要電子計算機に影響を及ぼすおそれがある特定侵害事象について、特別社会基盤事業者に報告を求める新たな義務についての考え方が示されています。BSA は「サイバーインシデント報告の国際的調和化に向けた 10 原則～グローバルな課題に対するグローバルなソリューション」[7]において、政府が自国のニーズを満たしながら、サイバーインシデントに対応・回復する企業の能力を過度に妨げずに、サイバーインシデント報告におけるエコシステムを構築するためのアプローチを提示しています。方針案において、報告様式の統一化や官民連携基盤による報告窓口の一元化等、影響を受けるステークホルダーの負担軽減を図る考え方が示されていることを我々は高く評価しています。特別社会基盤事業者と政府双方にかかる追加的な作業負担を最小化し、恩恵を最大化する侵害事象（インシデント）報告要件の在り方を今後も継続的に模索することを推奨します。特別社会基盤事業者に課される義務は、BSA 会員企業を含む、重要な IT サービスを提供している事業者に直接的・間接的に影響を及ぼす可能性があります。

この点において、サイバー侵害事象報告要件に関し、国内では省庁横断的に、国際的には新たな国際的動向と整合させる方向性が方針案において示されていることを歓迎します。多くの大規模なサイバーセキュリティインシデントが分野横断的・国境横断的な性質を持つことを踏まえれば、日本政府の制度が他の主要法域の制度と整合すればするほど、国内企業も多国籍企業も、より調和した、効果的かつ迅速な対応ができるようになります。その目的は、日本にある企業に独自のコンプライアンス義務を課すことではなく、重大な侵害事象を迅速に特定・緩和して被害を最小化することであるべきです。

---

[7] BSA「サイバーインシデント報告の国際的調和化に向けた 10 原則～グローバルな課題に対するグローバルなソリューション」
https://www.bsa.org/files/policy-filings/jp02182025bsacyberincidreporting.pdf

特に、サイバーセキュリティ侵害事象が「報告対象」であるか否かを判断するためのリスクベースの閾値を設定する際には、BSA 会員を含む、産業界のパートナーや関連するステークホルダーと緊密に連携することを推奨します。報告対象となるサイバー侵害事象は、重大な損害をもたらし、企業の重要な機能の提供能力を損なう実際のサイバー侵害事象のみが含まれるように狭く定義する必要があります。侵害事象が疑われる場合や、単にリスクを伴ったり、危険にさらしたり、もしくは、その他の方法でサイバー侵害事象が発生する可能性を高める場合等は含まれないようにするべきです。この点において、ファイアウォール等のインターネットとの接続点となる機器については、平時から大量の攻撃性通信をブロックしており、そのような事象まで含めて一律に報告を求めると、特別社会基盤事業者に過度な負担を強いることが方針案において認識されていることを高く評価します。

また、報告義務の開始および関連する時間軸は、特別社会基盤事業者が報告義務の対象となった侵害事象を認識した（すなわち、判断した）時点とすべきです。方針案において、明確に侵入を検知した後の事象のみを対象とする方向性が示されていることを我々は支持します。特別社会基盤事業者が侵害事象に遭遇したという疑いまたは確信に基づいて義務を課すべきではありません。この点は、本法第５条において規定されている「特定侵害事象の原因となり得る事象」を今後、定義する上で特に重要となります。最近公表された、「官民連携の強化に向け今後具体化が必要な論点」[8]においては具体的な事象の痕跡を認知した場合に報告を求める対応とする考えが示されています。侵害事象報告制度を実用的かつ効果的にするために、「痕跡」とみなされる範囲を絞りこむことを推奨します。

方針案では、報告の期限について「諸外国での同様の報告手続きを設けている国の例や、官民で有効な対処を行う観点も踏まえて期限を設定することとする」と記されています。政府が様々な国際基準を参照していることを我々は高く評価します。報告対象侵害事象に該当すると事業者が判断した後でも、侵害事象の性質を理解するのには時間がかかることがよくあります。多くの場合、企業は簡易な通知を迅速に提供できるものの、米国の重要インフラ向けサイバーインシデント報告法（Cyber Incident Reporting for Critical Infrastructure Act、CIRCIA）のように 72 時間以下にならない基準を課すことで、特別社会基盤事業者は、１） 侵害事象の理解と対応に集中し、２）政府にとって有用な報告を提出する時間を確保することができます。企業の限られたリソースをインシデント対応からコンプライアンス義務にシフトさせることは逆効果です。企業は、政府関係者に可能な限り最新の情報を確実に提供することに尽力しています。そのため、速報を提出するための十分な時間を設けることを強く推奨します。

特定侵害事象等の報告内容については、不確実な内容も含めて報告時点で判明した事項を記載すれば速報として足りることとするという考え方が方針案では示されています。速報に必要な情報を政

[8] https://www.nisc.go.jp/pdf/council/cyber_anzen_hosyo/cyber_anzen_hosyo-03shiryo03.pdf

府が詳しく定義する過程においては、特別社会基盤事業者が把握している 1）悪意のある行為者についての情報（戦術、手法、手順を含む）、2）脆弱性（どのように悪用されたかを含む）、3）影響を受けた情報および情報システム、といった情報に限定すべきです。特別社会基盤事業者が供給者から収集した侵害事象報告情報は、特別社会基盤事業者の従業員、その産業を所管する省庁や内閣府など、関連組織の幅広い主体と共有される可能性があることを考慮し、こうした情報には企業秘密や機密性の高い専有情報が含まれるべきではありません。

さらに、方針案第 5 章第 5 節で述べられているように、侵害事象に関連する情報は、漏えいした場合に悪用される可能性があり、本法に基づく政府の情報取得等に対する国民の信頼を損なうおそれがあることから、公表前に適切な措置を講じるべきです。情報取扱者の特定、研修の実施、保管庫の施錠等の物理的な安全管理措置、電子ファイルのアクセス制御等の技術的な安全管理措置の確保といった組織的な安全管理措置を講じるという方針案の考え方を我々は支持します。

この方針に従い、政府は、上記のサイバー侵害事象報告で得られた情報を、一般市民に情報公開を義務付ける法律や政策から保護し、サイバー侵害事象報告から収集した匿名化された分析結果のみを他のサイバーセキュリティ関係者と共有すべきです。これにより、企業が情報を共有する際の障壁が低減され、企業被害のさらなる拡大の可能性が低減され、他の企業のサイバーセキュリティが改善されます。

脆弱性の公表と脆弱性対応の強化

方針案第 4 章第 3 節(1)では、特定重要電子計算機の届出、脆弱性、特定侵害事象等の報告等、種々の情報を内閣府が収集し、データベース化等による整理や、各種の情報間の照合等の分析を行うことで、サイバー攻撃の予防措置や重要電子計算機を防護する組織（民間事業者を含む）における戦略的な意思決定・判断に効果的に活用できるようにすると説明しています。また、内閣府から当該情報（「総合整理分析情報」）の提供を受けた行政機関が、必要に応じて当該情報を加工し、関係機関・関係者と共有することで、情報受領者が具体的な措置を講じることを促すとしています。しかし、当該情報が公表されていない場合、情報共有はサイバーセキュリティに実質的なプラス効果をもたらさず、悪用される機会を増やす可能性があります。そのため、政府内での情報の発信に安全策を講じ、遅延させることを推奨します。

また、方針案第 5 章第 2 節（6）において所管省庁からの要請を受けた際に電子計算機等供給者が講じなければならない「必要な措置」については、その要請が確認された脆弱性に焦点を当て、体系化された情報開示の慣行に沿った形で、その脆弱性に見合った適度な範囲にとどまるようにすることを強く推奨します。

さらに、第 5 章第 2 節(4)では、政府が特定した公表前の脆弱性情報が、守秘義務および安全管理

措置を課せられる協議会の構成員である特別社会基盤事業者と共有されると記されています。しかし、どのような公表前脆弱性情報が想定されているのか、また政府がどの主体から当該情報を取得するつもりなのかは不明確です。提案されている制度の運用意図をより的確に理解するためには、情報の範囲および取得・共有プロセスに関する一層の明確化が望まれます。

さらに、方針案第 5 章第 2 節(5)では、マルウェア感染等により一般利用者の通信機器を利用して攻撃が行われることが増加していることを踏まえ、脅威情報に必要な加工を行った上で、重要電子計算機を使用する者に限らず、特定不正行為に用いられるおそれのある電子計算機を使用する者にも周知のために政府が情報を提供し得ると記されています。本措置の意図には賛同するものの、特に脆弱性に対するパッチが未提供の場合、政府が脆弱性を公に早期に開示するのは避けるよう求めます。

ソフトウェアやハードウェアの脆弱性は避けられるものではありませんが、多くの場合、独立したセキュリティ研究者によって特定されています。そのため、このようなコンピューティングシステムのベンダーが、特定された脆弱性に関する第三者からの報告を処理するための手順を維持することが不可欠となります。この点に関して、情報セキュリティコミュニティは、「協調的脆弱性開示」（coordinated vulnerability disclosure、CVD）[9]と呼ばれる一連の手順を開発しました。これは、ベンダーが第三者の利害関係者と協力し、一般への潜在的なリスクを軽減するのを支援するものです。すべての CVD 要件は、既存の国際的に認められた標準規格である ISO/IEC 29147 および 30111 に準拠する必要があります。CVD の指針は、脆弱性を修正できるベンダーに直接報告し、ベンダーが根本的な脆弱性を軽減するためのパッチを開発、テスト、展開する機会が得られるまで公開を延期することで、セキュリティが最大限に保護されるというものです。この基本原則を具体化するため、ソフトウェアベンダーは、第三者からの脆弱性報告に対応するための CVD プログラムを維持しています。これは、悪意のある攻撃者が未修正の脆弱性を悪用してシステムに侵入するリスクを最小限に抑える方法です。

したがって、特定された脆弱性、特に特別社会基盤事業者が使用する重要なコンピューティングシステムに関連する脆弱性が検証され、確実に修正されるまで、公表されないようにすることを我々は政府に強く求めます。

また、セキュリティ研究者、顧客、あるいは政府によって発見されたものであるかどうかに関わらず、新たに発見された脆弱性の報告をコンピューティングシステムベンダーが容易に受け取れるよう、ベンダーに対し、脆弱性開示ポリシーの公表を奨励します。脆弱性開示ポリシー は、特に製造業者が日本国外に所在する場合、所管大臣が製造業者に連絡を取り、脆弱性情報を共有する方法

[9] 「協調的脆弱性開示（CVD）に関する指針（Guiding Principles for Coordinated Vulnerability Disclosure）」
https://www.bsa.org/files/policy-filings/2019globalbsacoordinatedvulnerabilitydisclosure.pdf

を提供するため、所管大臣にとっても有益です。製造業者が新たに発見された脆弱性を可能な限り迅速に是正できるよう、関係者が新たな脆弱性を内密に直接ベンダーに報告することを奨励するような方針とすべきです。

結論

BSA からの意見をご検討頂けることに感謝します。BSA は、サイバー対処能力の強化という日本政府の目標を支援するため、引き続き、政府と協力していきたいと考えています。本意見の提出に加え、能動的サイバー防御を実施するための具体的な施策をよりよく理解するため、基本方針に関して対話の機会をいただければ幸いです。