2026 年 8 月 18 日

サイバー対処能力強化法に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する制度の解説（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、政府が特別社会基盤事業者のサイバー防御・対処能力の強化に向けて取り組みを継続していることを高く評価するとともに、「サイバー対処能力強化法」[2]に基づく届出および報告義務をより明確にするために本解説案 [3]が公表されたことを歓迎します。

BSA は、エンタープライズソフトウェア産業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）、クラウドストレージサービス、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、以下のとおり、意見を提出します。

提言

制度の実効的な運用を支援する観点から、BSA は、特別社会基盤事業者とテクノロジー提供事業者との間の責任分担について、さらなる明確化を行うとともに、侵害事象報告要件についても、リス

[1] Business Software Alliance（ https://bsa.or.jp/（日本サイト）、www.bsa.org（グローバルサイト））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する業界団体です。BSA の会員には以下の企業が含まれます：Adobe, Alteryx, Amadeus, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Morisawa, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., TrendAI, 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=0000317900

クベースで、リスクに見合った比例的かつ国際的なベストプラクティスと整合した制度となるよう、追加的な見直し・改善を求めます。

法定の届出・報告義務を負う主体が特別社会基盤事業者であると明確化すること

本解説案においては、クラウドサービスが特定重要計算機に含まれることも踏まえ、特定重要計算機の届出および特定侵害事象等の報告義務が特別社会基盤事業者に課されるものであることを明示すべきです。

本解説案では、特別社会基盤事業者が、クラウドサービス事業者、回線事業者、システム運用や監視等を担当する委託先事業者等の外部関係者から提供される情報に依拠し得ることを適切に認識しています。他方で、法令上の義務はあくまでも特別社会基盤事業者に課されるものであり、対象となる製品やサービスを提供していることのみを理由として、その義務がテクノロジー提供事業者に及ぶものではないことを明確にすべきです。

クラウドサービス事業者やその他のテクノロジー提供事業者は、契約上の取決めや運用面での連携を通じて、顧客による法令遵守やセキュリティ対応を日常的に支援しています。しかしながら、法制度上、届出や報告に関する責任の所在が不明瞭になることは避けるべきです。規制対象となる社会基盤事業者とテクノロジーやサービス提供事業者間の責任分担を明確化することは、制度の実効性向上、侵害事象発生時の混乱防止、さらには重複した報告の回避にもつながると考えます。

そのため、本解説案に以下の文言を含むことを推奨します。*「クラウドサービス、委託事業、その他の第三者サービスが特定重要電子計算機として特定された場合であっても、法第2条、第4条および第5条に基づく届出・報告義務は、特別社会基盤事業者が負う。テクノロジーやサービス提供事業者は契約上の取決め等を通じて必要な協力を行うが、それらを提供していることのみを理由として、これらの義務を負うものではない。」*

報告対象となる特定侵害事象等の「痕跡」の範囲を明確化すること

BSA は、特別社会基盤事業者に影響を及ぼすサイバー脅威を早期に把握できるよう支援しようとする政府の取組を支持します。しかしながら、「特定侵害事象の痕跡」および「特定侵害事象の原因となり得る事象」に関連する義務については、さらなる明確化が望まれます。

現行の解説案では、ランサムウェア、不正アクセス、DDoS 攻撃といった確認済みの侵害事象だけでなく、特定重要設備等に関連して、一定の攻撃の試み、マルウェアの送達事象、認証情報の窃取、さらにはそれらが発生した可能性を示す痕跡が存在する場合についても報告対象となるように読めます。しかし、こうした試みや事象は、実際のセキュリティ侵害ではなく、未確認の、失敗に終わった、あるいは自動的に防御・遮断された挙動を示しているにすぎない場合が多いことに留意することが重要です。

今日の脅威環境においては、最新のセキュリティオペレーションセンター(SOC）は、遮断された接続試行、認証の失敗、無害化されたマルウェアなどを含む数百万件の「事象」を日々処理してお

り、こうした件数は AI を活用したサイバー脅威の進展に伴い、今後さらに増加すると見込まれます。こうした事象は、確認済みの侵害事象とは本質的に区別されるべきです。

現代のセキュリティ監視システムは大量のアラート、指標、および潜在的な検知結果を生成するため、報告義務が発生する前に、どの程度の分析、確信の度合、または検証が求められるのかについて、さらなる明確化が必要です。

定常的なスキャン、侵入未遂、自動的に遮断された接続、無害な異常検知、重複検知、誤検知などは、いずれもセキュリティ監視システム上に証跡や痕跡を残す可能性があります。しかし、そのような検知結果は、必ずしもマルウェアが実行されたこと、不正アクセスが発生したこと、あるいは事業運営に影響が生じたことを意味するものではありません。

報告制度の実効性を確保するとともに、過剰な報告件数の発生を防ぐ観点から、報告対象となる痕跡については、実際に侵害事象が発生した、又は合理的にみて発生した可能性が高いと判断される場合に限られることを明確化するよう推奨します。

この考え方は、他の法域で採用されているリスクベースのインシデント報告制度とも整合性があります。こうした制度では、合理的な調査を通じて確認され、かつサイバーセキュリティリスク管理上重要なインシデントに報告対象を限定しています。これにより、政府の対応能力を圧迫し、報告情報全体の有用性を損なうような、実質的な価値の乏しい報告の大量発生を防ぐことができます。

5-5 では、フォレンジック調査や脅威ハンティングによる確認など、侵害事象の発生を認知する事例が示されていますが、以下の点を明確化することを推奨します。

「特定侵害事象の痕跡については、特別社会基盤事業者が合理的な評価を行った結果、当該痕跡が、特定侵害事象又は特定侵害事象を引き起こすおそれのある事象が発生したと結論づけるための信頼できる根拠を提供すると判断した場合に、報告対象となる。」

さらに、解説において、以下を区別する実務上の具体例を示すことを推奨します。

- 報告対象となる、特定侵害事象の発生が疑われる痕跡
- 報告対象とならない、定常的な活動、不成功に終わった攻撃の試み、又は自動的に遮断・緩和された活動

加えて、「痕跡」について正式な定義を設け（例：「対象となる侵害事象を裏付ける技術的証跡として認識されるもの」）、併せて、客観的な認識基準を示すことを奨めます。

リスクに応じた、国際整合性を踏まえたインシデント報告制度の推進

本解説案は、システムの分類、報告対象事象、および報告義務について詳細な整理をしています。BSA は、サイバー脅威に関する状況認識の向上という解説案の目的を評価する一方で、報告要件の

簡素化を継続的に進め、適切な範囲で既存の国際的に確立されたサイバーセキュリティインシデント報告制度との整合を図ることを推奨します。

国際的な実務との整合性を高めることにより、以下の効果が期待されます：（1）コンプライアンス対応の複雑さの軽減（2）より効率的なインシデント対応（3）組織が重要なサイバーセキュリティ事象にリソースを集中することによる、報告の質の向上（4）グローバルに統合されたシステム全体における、より効果的なサイバーリスク管理の促進。

このため、BSA は、運用・機密性・完全性・可用性に実質的な影響を及ぼす事象に重点を置いた、リスクベースのアプローチを採用するとともに、サイバーセキュリティ上の結果に実質的な影響を及ぼさない低リスク又は推測的な事象については報告義務の対象外とすることを推奨します。

また政府が、報告義務の目的が重大なサイバーセキュリティリスクの把握及び低減を支援することにあることを明確化するとともに、その運用が国際的に認知されたインシデント報告の実務およびリスクの大きさに応じた適切な原則に沿ったものとなるよう、指針を示すことを推奨します。

結論

BSA は、本解説案の目的を支持しつつ、（1）特別社会基盤事業者とテクノロジー提供事業者との間の責任分担（2）侵害事象の痕跡の扱い（3）国際的実務と整合した比例的かつリスクベースの考え方に基づく侵害事象報告義務の運用について、さらなる明確化を推奨します。

これにより、本制度の実効性を高めるとともに、規制対象事業者及び提携するテクノロジー提供事業者にとっての不確実性を低減することができます。我々は、日本のサイバー対処能力の更なる強化に向け、今後も政府と連携していけることを期待しています。