2025 年 4 月 11 日

日本のサイバー対処能力の強化に向けた法律案に関する提言

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案」[2]（以下、法案）を策定し、サイバー安全保障分野での対応能力の向上に向けて日本政府が取り組んでいることを高く評価します。質・量の両面で急増傾向にあるサイバー攻撃の脅威に対し、重要となるインフラ事業者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。

この目標達成に向け、法案においては、一連の新たな権限、制度、義務等が導入されています。特に重要な点として挙げられるのは、法案において、脅威把握やインシデントの調査を含む多様な目的のために、基幹インフラ事業者の同意に基づく、また、同意によらない通信情報の取得権限を政府に付与していることです。さらに、法案は導入した「特定重要電子計算機」を政府に届け出ることを基幹インフラ事業者に義務付けており、この対象にはクラウドコンピューティング・サービスのようなソフトウェア対応システムも含まれると我々は理解しております。また、基幹インフラ事業者は、このような特定重要電子計算機に影響を及ぼすサイバーインシデントを所管省庁に報告することも義務付けられています。さらに同法案は、日本の基幹インフラ事業者への攻撃への関与が疑われるコンピュータ・システムやサーバへのアクセスや無害化を含む、攻勢的サイバーセキュリティ措置にあたる権限を政府に付与しています。

政府が法案を改善、また、今後の制度運用における規定を整備する上で一助となることを願い、我々は本提言をまとめております。上記の新たな権限と義務を実施する上では、これらが他の国際慣行、また、既存および新たなビジネス上の実務や技術を考慮に入れた整合性を確保していることが大切です。加えて、基幹インフラ事業者や日本の他の事業者が安全な最先端ソフトウェア対応技術の採用をするこ

---

[1]BSA の会員企業は、政府機関や重要なインフラ供給者を含むあらゆる種類の企業や組織の顧客に、エンタープライズ ・ソフトウェアを利用したサービスを世界各国で提供しています。BSA 会員企業は、イノベーションに多大なリソースを投資し、クラウドコンピューティング、ビジネスソフトウェア・アプリケーション、人工知能などの分野で最先端のテクノロジーとサービスを提供しています。また、最先端のサイバーセキュリティ・ソリューションを顧客に提供しています。

BSA のメンバーは以下の通り：Adobe、Alteryx、Amazon Web Services、Asana、Atlassian、Autodesk、Bentley Systems、Box、Cisco、Cloudflare、Cohere、Dassault Systemes、Databricks、DocuSign、Dropbox、Elastic、EY、Graphisoft、HubSpot、IBM、Informatica、Kyndryl、MathWorks、Microsoft、Notion、Okta、OpenAI、Oracle、PagerDuty、Palo Alto Networks、Rubrik、Salesforce、SAP、ServiceNow、Shopify Inc、Siemens Industry Software Inc.、Trend Micro、TriNet、Workday、Zendesk、Zoom Communications Inc.

[2]「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案」
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/houan.pdf

とを促進するのではなく、抑止するような意図せざる影響を最小化することも重要です。これらの目的を達成するために、法の制定前、施行中、そして施行後の頻繁な政策の見直しを通じて、法律と施行規則が目標に適合し、目標を達成し、デジタルトランスフォーメーションや基幹インフラ事業者によるクラウド導入といった他の重要な目標を妨げないように、適切な意見聴取を行うことを政府に奨励します。

我々の提言は以下の項目に言及しています：

- **通信情報の取得と利用**
- **官民連携**
  - *「一定の重要電子計算機」に関する届出*
  - *インシデント報告*
  - *脆弱性の開示と脆弱性対応の強化*

通信情報の取得と利用

法案では、同意に基づく、また、同意によらない通信情報を基幹インフラ事業者やその他の事業者から取得・利用するための新たな権限を政府に付与することを規定しています。この権限の目的は、日本に対するサイバー攻撃の実態をよりよく把握することとされています。

しかし、国際的な例として挙げられている法令、例えば米国の外国情報監視法、英国の調査権限法、豪州の通信情報傍受及びアクセス法などは、一般的に国家安全保障や法執行に関連するはるかに広範な権限であり、どのような主体が、どのような状況下で、どのような手続きを要求して、そのような権限の対象となり得るかについて、実質的な規則を定めています。今回の法案では、この権限はサイバーセキュリティの脅威の監視に特化したものであり、提案されている権限の利用において同様の手続き上の保護措置が規定されていないように思われます。

このように、この広範な提案は、日本政府による私的通信へのアクセスを可能にすることで、プライバシーと市民の自由という重要な問題に関わってきます。政府がこの新たな権限を創設する場合、**それがどのように創設され、どのように適用されるかを知らせるために、しっかりとした公開対話の場を設けることを強く求めます。**特に、**本法律では、新たな法的義務および権限の範囲に明確かつ意義のある制限を設け、プライバシーの促進を目的とした制度的および技術的な保護策を整備し、この新たな権限の行使を独立機関による厳重な監視の対象とすべきです。**

<u>通信情報の取得と利用に関する具体的な提言</u>：

1) **独立した司法機関による厳格な監視を確保すること。**我々は、この法律において、司法機関のような真に独立した監督機関を設立し、新たな法的権限の全般的な運用を審査することを推奨します。法案で想定されている機関であるサイバー通信情報監理委員会は、内閣総理大臣が委員を任命することとなっています。これは真に独立した審査機関の創設にはなりません。独立した審査機関は内閣総理大臣や他の行政官に対して説明責任を負うべきではありません。これらの新たな権限によって影響を受ける重要な権利に鑑み、真に独立した機関には、法制度全体の監督を行う

権限を与えるべきです。この役割は、特定の通信へのアクセスを求める個別の要請を審査する新たな機関の役割とは別となります。これは、適切な保護措置が実際に機能していることを保証し、法案で提案されている権限の誤用を回避するのに役立ちます。さらに、新たな権限を行使する省庁も、定期的かつ厳格な内部審査の対象となるべきです。

2) **取得するデータの種類を明確に制限すること。**政府による取得・利用の対象となる通信の種類を厳格に制限し、そのデータの分析を制限する保護措置を設けるべきです。さらに、法案では、この新たな法的権限が意図された範囲（サイバー攻撃の調査や対応）を超えた目的で悪用されることを防ぐための強固な仕組みを盛り込むべきです。法案においては、データアクセス権限を「メタデータ」とよく呼ばれる「機械的情報」（例えば、意思疎通の本質的内容ではないデータ）に限定し、また、本データは、サイバー攻撃に関係があると判断された場合にのみ使用され、取得されたデータは自動的な方法によってさらなる分析のために選別されると読めます。これが実際にどのように機能するのか、また、このデータの集合体を特定するために、より広範なデータセット（コミュニケーションの本質的内容を含む）を最初に取得しなければならないのかどうかは、法案からは完全に明らかではありません。しかし、日本政府が、この新たな権限によるプライバシーや個人情報その他の機微情報への影響を最小限に抑える方法を積極的に検討しているのは心強いことであり、このような取得が実際にどのように実施されるかについて利害関係者と協議することを奨励します。

3) **政府によるデータへのアクセス権限の対象となり得る主体を明確に規定すること。**通信データを取得・利用する政府の権限の対象となり得るのはどの主体なのか、また、当該主体が当該取得・利用に同意するか否かは依然として明らかではありません。法案ではデータ要求の対象を基幹インフラ事業者に限定していないですが、政府が電気通信サービスプロバイダー、クラウドサービスプロバイダー（CSP）、また基幹インフラ事業者に提供されるその他の IT サービスからの通信情報を要求する権限を持つ場合、これはさらなる重大な懸念を引き起こし、そのようなプロバイダーを複雑な法の抵触の状況に陥れる可能性があります。この権限の対象となる指定事業者を法案で明確に規定すること、CSP などの第三者が管理する基幹インフラ事業者の情報は、たとえ CSP が電気通信事業法の下で電気通信事業者とみなされる可能性があるとしても、基幹インフラ事業者のみがアクセスし政府に提供しなければならないことを明記することを強く求めます。言い換えれば、通信情報へのアクセス権限は、基幹インフラ事業者を顧客とするエンタープライズ・ソフトウェアサービス・プロバイダーには直接適用されるべきではありません。

4) **同意によらない通信データの取得と利用に関して、影響を受ける利害関係者と緊密に協議すること。**基幹インフラ事業者やその他の事業者の同意なしに政府が通信情報を取得・利用する権限をいつ、どのように行使するのかは、依然として明らかではありません。政府がこの新たな仕組みの実施を検討する際には、すべての関連事業者および影響を受ける事業者と緊密な協議を行うことを強く推奨します。

5) **データ取得のための強力な手続き要件を採用すること。**法案には、政府が通信情報を入手する際に満たすべき高い法的基準を設けるなど、具体的かつ強固な保護措置を含むべきです。また、法

案には、先に述べた広範な監視機関に加え、政府による通信情報の取得・利用要請を審査・承認する独立した司法機関を設置すべきです。

6) **取得データの利用に関する具体的な手続きを確立すること。**法案においては、取得した情報の利用は、新たな法的枠組みで対処することとされているサイバーセキュリティと国家安全保障の目的に限定し、厳格な手続きを確立すべきです。例えば、国内の刑事訴訟手続きやその他の追加的な用途で取得情報を利用することは制限されるべきです。

7) **データ取得後の保護措置の実施を確保すること。**法案においては、データ取得後に政府が実施することが求められる明確かつ具体的な保護措置を定めるべきです。例えば、取得されたすべてのデータに厳格なデータセキュリティ対策を適用すること、取得目的が達成された後にデータを削除することを義務づけるデータの最小化手続きを採用すること、取得された情報が不適切にアクセス、開示、または取得された目的以外の目的のために利用されないよう、保存データを保護するための保護措置を講じること等、法案において義務づけるべきです。このような保護措置においては、国家および国家によらないサイバースパイ活動に関連するリスクや取得データが盗まれる可能性を考慮すべきです。

官民連携

法案では、民間部門、特に 基幹インフラ事業者と政府との間の情報共有を強化するための新たな義務や自主的な仕組みをいくつか導入しています。増大するサイバーセキュリティの脅威に直面する上での準備体制、対処能力、回復力を強化するために、民間部門と公共部門間で情報共有を強化する仕組みを BSA は支持します。情報共有は定義上、任意であり、適切なインセンティブを生み出すように、その仕組みを慎重に調整する必要があります。基幹インフラ事業者 や彼らの情報技術（IT）サービス・プロバイダーに不要な負担をかけたり、一般的な技術やビジネス慣行と対立する意図しない結果を生じさせないようにすべきです。また、このような仕組みは、国際的な相互運用性を促進するために、可能な限り他の主要な法域の仕組みと整合させることが重要です。

軽減しようとしている脅威に対する政策の有効性を理解するには、影響を受ける利害関係者との緊密な協議が必要になります。実施に向けた政策を策定するための会合や意見聴取を通じて、BSA 会員を含む民間部門と政府が連携することを強く求めます。民間部門および BSA 会員は、急速に進化し加速するサイバーセキュリティの懸念に対する効果的な対応策を日本政府が策定できるよう支援することができます。したがって、**法案の施行後、定期的な見直しを含め、サイバーセキュリティのリスク管理のベストプラクティスを活用した、緊密かつ一貫した官民連携のための創造的な機会を活用することを我々は政府に推奨します。**

「特定重要電子計算機」の届け出

法案には、日本国内の基幹インフラ事業者の強靭性を高めるために官民連携を促進するさまざまな措置が盛り込まれており、基幹インフラ事業者に対し、「特定重要電子計算機」の導入を所管大臣に届け出る義務が導入されています。政府関係者とのこれまでの対話に基づき、この「電子計算機」には、仮想

プライベート・ネットワーク、認証システム、クラウドコンピューティング・サービスを含む特定のソフトウェア・ソリューションが含まれる可能性があると我々は理解しています。指定された基幹インフラ事業者が使用している重要な IT システムの可視性を高めたいと考えるのは理解できます。しかし、このような制度が、既存のセキュリティ保証制度と重複したり、ソフトウェア対応システムやクラウド・コンピューティングなどのサービスを含む先進的なコンピューティング・システムを基幹インフラ事業者が採用する意欲をそぐような不要なコストを生じさせないことが重要です。

この「導入届け出」制度の意図しない結果を最小限に抑えるため、法案においては、以下のようにすることを推奨します。

- **基幹インフラ事業者が提供する重要な役務を継続的に提供するために要する特定のシステムに焦点をあて、リスクベースのアプローチを採用し**「特定重要電子計算機」が定義されるようにすることを奨めます。このようなアプローチは、政府と企業の限られたリソースを「重要」とみなされるシステムのみに集中させることにより、「重要」システムを含む高度なコンピューティングシステムを採用する基幹インフラ事業者の負担を最小限にします。
- 最先端技術プロバイダーが基幹インフラ事業者への製品・サービス提供を躊躇することのないよう、導入届け出に関する**不要または機微性の高い情報の開示を最小限にとどめること**を奨めます。届け出手続においては、過度に詳細な情報の開示を義務付けることを避けるべきであり、特に、企業秘密やシステム・セキュリティー関連情報など、プロバイダーが基幹インフラ事業者と共有することが困難な情報の収集を基幹インフラ事業者に義務付けないことが重要です。
- **既存の認証を活用し**、報告やその他の文書の不要な重複を避けることを奨めます。例えば、「政府情報システムのためのセキュリティ評価制度（ISMAP）」や、その他広く認知されているクラウドセキュリティの保証制度や標準に基づく認証を受けているクラウドコンピューティングシステムに関しては、情報開示要件を軽減すべきです。

インシデント報告

法案では、特定の重要な「電子計算機」に影響を及ぼす可能性のある特定のサイバーセキュリティインシデントについて、基幹インフラ事業者に報告義務を課すことを導入しています。これは妥当な要件ですが、影響を受ける事業者および政府にとっての利益を最大化し、同時に不要なコンプライアンス負担を最小化するような方法でインシデント報告要件を設計することが非常に重要となります。基幹インフラ事業者に課される義務は、BSA 会員企業を含む重要な IT サービスを提供する企業に直接的または間接的に影響を与えることとなります。この点において、政府が以下の提言を採用するよう強く求めます。詳細は、BSA の「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」[3]を参照ください。

1) **サイバーインシデントの通知・報告要件を、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こと。**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、より調和した対応ができるようになります。その目的は、重大なインシデントを迅速に特定・緩和して被害を最小化することであるべきであり、日本にある企業に独自のコンプライアンス義務を課すべきではありません。

2) **サイバーセキュリティインシデントが「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こと。**日本政府は、BSA 会員企業を含む産業界のパートナーやその他の関連利害関係者と緊密に協力して、何を「報告対象インシデント」とみなすかを定義すべきです。報告対象となるサイバーインシデントは、重大かつ企業の重要な機能を提供する能力を損なう実際のサイバーインシデントのみとし、インシデントが疑われる場合や、単にリスク伴ったり、危険にさらしたり、もしくは、その他の方法でサイバーインシデントが発生する可能性を高める場合等は含まないように狭義に定義されるべきです。

3) **通知または報告義務の開始時点を、実際の認識基準に基づいて明確に定めること。**報告義務の開始および関連する時間軸は、基幹インフラ事業者が報告義務の対象となったインシデントを認識した（すなわち、判断した）時点とすべきです。基幹インフラ事業者がインシデントに遭遇したという疑いまたは「合理的な確信」に基づいて義務を課すべきではありません。

---

[3]「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

4) **速報のための十分な時間を設けること（報告主体が通知すべきインシデントを認識してから最低72時間）。**タイムリーな報告は重要ですが、インシデントが通知対象であると事業者が判断した後でも、インシデント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、企業はより迅速に情報を提供できますが、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、基幹インフラ事業者（およびそのITサービス・プロバイダー）は、a) インシデントの理解と対応に集中し、b) 政府に妥当な速報を提出する時間を確保することができます。企業の貴重な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。

5) **速報の「合理的な情報量」を明記し、必要とされる情報を国際慣行と整合させ、報告に際して多様な形式を認めること。**政府は、BSA会員企業を含む産業界のパートナーおよびその他の関連利害関係者と緊密に協力しながら、報告に必要な時間枠に合わせて情報量と詳細度を調整し、合理的かつ適切な報告義務を定めるべきです。72時間以内の速報については、インシデント発生後数週間以内に基幹インフラ事業者が要求される可能性のある、より詳細な報告に比べれば、量も詳細度も比較的少なくて済むはずです。さらに、政府が求める情報は、複数の地域に影響を及ぼす事故への対応を合理化するために、他の主要な管轄区域が求める情報と一致させることが重要です。**報告書に求められる情報は、基幹インフラ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**（それがオンプレミスシステムで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、に限定されるべきです。**基幹インフラ事業者がプロバイダーから収集したインシデント報告情報は、基幹インフラ事業者の従業員、その産業を所管する省庁、政府内に新設されるサイバーセキュリティ戦略本部など、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。**

6) **報告義務はインシデントを経験した主体にあることを明記すること。**インシデントの影響を受ける重要な情報サービスを提供するITサービスプロバイダーは、顧客である基幹インフラ事業者と緊密に連絡を取ることになりますが、インシデントの対象となる基幹インフラ事業者が、インシデントを報告する責任を負う主体であることは、法律上明確であるべきです。サービスプロバイダーは、インシデントに関する重要な情報を有しているかもしれませんが、サービスプロバイダーである性質上、顧客である基幹インフラ事業者に対する具体的な影響や、インシデントによって影響を受けるデータやシステムに関する知識は限定的です。

7）**すべてのサイバーインシデント報告を受ける責任を負う単一の機関を設けること。**政府は、日本におけるすべてのインシデント報告義務について、単一の機関への報告で足りるようにし、インシデント報告要件を合理化すべきです。これにより、基幹インフラ事業者の重要な IT サービスプロバイダーが、何百もの基幹インフラ事業者を所管するいくつもの関係省庁に過剰に詳細な報告書を提出することを防ぐことができます。オーストラリアやシンガポールのような一部の法域では、サイバーセキュリティインシデントを報告するための単一のウェブポータルを導入しており、これによって企業が規制上の義務を果たすためのプロセスが簡素化されています。

8）**インシデント報告で受け取った情報の利用は、サイバーセキュリティに関連する用途のみに限定すること。**サイバーセキュリティのインシデント報告で開示される情報は機密性の高い内容であることが多いため、そのような情報が、特定のサイバーセキュリティ目的（インシデントに対するインシデント対応の調整、重要なインフラへの重大なリスクの防止・軽減など）のみに利用され、その他の目的には利用されないことを政府は確保すべきです。[4]日本政府は、報告制度からの情報漏えいを回避するため、強固で効果的な制度化された枠組みを確立すべきです。

9）**インシデント報告で得られた情報を一般公開から厳格に保護し、完全に匿名化された分析結果のみを共有すること。**政府は、サイバーインシデント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、サイバーインシデント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。将来の攻撃を検出するために使用される可能性がある戦術や技術に関する情報（例えば、侵害の兆候（Indicator of Compromise、IOC））は、機密情報として扱われるべきです。そのような情報を広く共有すると、攻撃者が検出を回避するために行動を調整するため、それらの IOC が攻撃を特定できなくなる可能性が高くなるからです。

脆弱性対応の強化

法案では、「脆弱性対応の強化」のための手続きを策定しています。新法案第 8 章第 42 条では、内閣総理大臣及び所管大臣が、重要システムに使用される電子計算機の脆弱性を認識した場合、「電子計算機等の供給者に情報を提供」し、「対応方法を公表・周知」し、当該電子計算機等の供給者に対し、脆弱性への対処又は軽減のために「必要な措置を講ずるよう要請」する権限を付与しています。この制度がどのように機能することを意図しているのか、内閣総理大臣や所管大臣がどのように脆弱性を認識す

[4]最近成立した「サイバーセキュリティ法 2024」において、オーストラリア政府は同様の「限定的利用義務」を実施しました。本法の下では、重大なサイバーインシデントの影響を受けた主体が、インシデントに関する情報を国家サイバーセキュリティ・コーディネーターに開示した場合、国家サイバーセキュリティ・コーディネーターは、「許可されたサイバーセキュリティ目的」のためにのみ、その情報を利用または開示することができます。「サイバーセキュリティ法 2024」第 38 条を参照ください。
https://www.legislation.gov.au/C2024A00098/asmade/text

ることを期待されているのかが明確ではありませんが、理解していることに基づき、以下の提言をします。

- **脆弱性を早期に一般公開することは避けること。**対応方法についての公表や発表に関する記載は懸念すべき点です。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）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。[5]

  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、特に基幹インフラ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。

- **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すること。**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規制とすべきです。

---

[5] 「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

- 所管大臣がベンダーにそうした脆弱性に関する報告書の提出を求める場合、**ベンダーが複数の主体に報告することを避けるため、サイバーインシデント報告書を受け取るのと同じ主体に、そうした脆弱性報告書を受け取る権限も与えるべきです。**

結論

BSA からの意見と提言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、政府と協力していきたいと考えています。本提言の提出に加え、本法案の具体的な目標とその達成のための具体的な仕組みについて、さらに理解を深めるために、継続的に対話の機会をいただければ幸いです。今後、詳細が明らかになりましたら、さらなる提言や提案を通じて、政府の目標達成に貢献していけることを期待しています。