

2026 年 10 月 30 日

デジタル大臣
サイバー安全保障担当大臣
古川 俊治 様

立憲民主党
政務調査会長 徳永 エリ

サイバーセキュリティ対策の強化に関する緊急要請

我が国に対するサイバー攻撃により、企業の情報はもとより、個人情報漏えいしたり、財産を奪われたりする事態に直面し、国民の間で恐怖ともいえる不安が広がっています。フェーズは既に大きく変わり、いつ何時、金融や交通、医療など重要インフラが攻撃され、社会経済に混乱を招かないとも限りません。

事実、世界中で不正アクセスが急増し、9月からの約1カ月間で、少なくとも延べ3億人超の個人情報の漏えいが公表され、国内で公表された個人情報の漏えいも過去最悪のペースとなっており、新しい有事の前夜というべき状況です。

サイバー攻撃は、もはや一部の大企業や国家機関の問題ではなく、国民生活そのものを脅かす存在です。政府は、セキュリティインシデントに関する統計情報の一元化と対策共有の仕組みを早急に構築するとともに、注意喚起にとどまらず、事業者が講じた対策の報告・フォローアップを行う体制を可及的速やかに整えるべきと考えます。また、国民の不安を払拭するため、国民に伝わる情報発信を行うとともに、被害の救済について検討を進める必要があります。

立憲民主党は、AI開発・利用は「人間中心のAI社会原則」を基本とする方針の下、国民の暮らし・経済を守るサイバーセキュリティ対策として、基本的かつ必要最小限の項目に絞り、以下の対策を速やかに講じるよう緊急に要請いたします。

記

1. 実態を正しく把握し、備える体制の整備

政府及び民間のサイバーセキュリティインシデントの実態を正確に把握し、被害の拡大防止と再発防止につなげるため、政府の司令塔機能を明確化するとともに、民間企業、学識経験者等の専門的知見を結集し、情報共有・分析体制を強化すること。

特に、2026年10月16日の参議院予算委員会での議論も踏まえ、サイバーセキュリティ政策を推進する関係府省庁や重要インフラ所管省庁が縦割りを排し、相互に連携して対応できる体制を構築すること。その際、新たな会議体の設置ありきではなく、既存のサイバーセキュリティ戦略推進体制を十分に機能させ、機動的かつ実効性のある対応を実現すること。

（１）潜在的な「隠れたインシデント」の存在の把握と公表しやすい環境の整備

現在、表出しているセキュリティインシデントは、被害を受けた組織が事案を把握し公表に至ったものに限られ、「氷山の一角」ともいわれており、公表されていない潜在的な「隠れたインシデント」を把握しなければ、今後に備えた効果的な対策を講じることはできない。このため、インシデントを公表することによる批判や責任追及への懸念が、事案の隠蔽や報告の遅れにつながることを防ぐよう、報告者の保護や適切な情報の取扱いに配慮しつつ、インシデントを積極的に報告・公表できる環境を整備すること。

（２）手口・手法に関する情報共有の強化

サイバー攻撃の発生状況、攻撃者の手口・手法、被害の内容及び対応状況等を組織間で共有することは、同様の攻撃による被害を未然に防止し、被害の拡大を抑止する上で極めて重要であることから、NCO（国家サイバー統括室）、JPCERT/CC（一般社団法人 JPCERT コーディネーションセンター）等の関係機関の役割を明確にし、政府及び民間のインシデント情報を収集・分析・集約し、必要な情報を迅速に関係組織へ提供できる体制を早急に整備すること。

（３）インシデントに関する統計情報の一元化と対策共有の仕組みの構築

政府及び民間におけるインシデントについて、発生件数、被害の状況、攻撃の手口・手法等に関する統計情報を一元的に集約・分析し、個人情報や機密情報の保護に十分配慮した上で、可能な限り公表・共有する仕組みを構築すること。

また、分析結果を踏まえ、各組織における対策の必要性や推奨される対応を具体的に示し、対策の実施状況を把握・検証することで、社会全体のサイバーセキュリティ水準の向上につなげること。

２．社会全体のセキュリティ投資を促進するための税制等の支援

セキュリティ強化対策に関する費用負担に関しては、中小企業では難しい側面がある一方、サプライチェーンを構成する中小企業がサイバー攻撃をひとたび受ければ、その被害は大企業にも波及し、結果として、国民生活や社会経済活動に多大な影響を生じることとなる。また、クラウドサービスへの攻撃や障害は、これを利用する地方自治体、中小企業、医療機関等に広範な影響を及ぼす可能性がある。2026年10月22日にデジタル庁が公表した情報漏えい事案等も踏まえ、個々の組織の自助努力に委ねるのではなく、社会全体でセキュリティ対策を支える仕組みが必要である。

そのため、中小企業等のセキュリティ対策に対する補助・助成制度の拡充に加え、サプライチェーン全体の安全確保に取り組む大企業に対する税制上の優遇措置など、企業間の連携を促進する仕組みを検討すること。特に、取引先や委託先を含めたセキュリティ対策の導入・強化を促すとともに、地方自治体、医療機関・介護事業者等の公共性の高いサービスを担う組織への支援を充実させることにより、社会全体のセキュリティ水準の底上げを図ること。

3. データの適正利用と必要な法整備の推進（個人を守り、企業を守る）

政府は、規制緩和の側面からデータ利活用を推進してきたが、これほど多くのセキュリティインシデントが深刻になった今、個人を守り、企業を守る観点から法制度を抜本的に検証し、必要な法整備を推進すること。

具体的には、EU で導入されている一般データ保護規則（GDPR）を参考に、データ最小化の原則を徹底し、事業者が利用目的の達成に必要な範囲で個人情報を取得・保有するとともに、必要な保存期間を超えて保有し続けることのないよう、適切な保存期間の設定と不要な情報の定期的な削除を促す制度を整備すること。個人情報の保有量を必要最小限に抑えることは、情報漏えい等が発生した場合の被害を軽減するとともに、管理コストや経営上のリスクの低減にもつながることから、事業者に対して、保有する個人情報の定期的な点検・整理、保存期間の適正化及び不要情報の削除を求めるなど、実効性のある法改正を検討すること。

実際の大規模な個人情報漏えい事案の多くは安全管理体制の不備によって発生していることから、個人情報保護法の課徴金制度に安全管理措置義務違反を対象とするなど、消費者が安心して個人情報を預けることのできる環境を構築すること。個人情報漏えい事案の多発に鑑み、情報漏えい時の本人通知義務の緩和について、本人の権利利益の保護の観点から、早急に再検討を行うこと。

4. セキュリティ人材の確保と研究開発予算の拡充

（１）研修・教育体制の充実

サイバー攻撃の高度化・巧妙化に対応するため、情報システムやネットワークの管理・運用に携わるデジタル人材が必要なセキュリティの知識と対応能力を身につけることができるよう、研修・教育体制の充実を図ること。また、高度な情報セキュリティ技術を有する専門人材の育成・発掘に加え、専門人材の確保と継続的な能力向上を支援する施策を推進すること。

（２）研究開発環境の整備と予算の拡充

サイバー攻撃への対処能力の向上や新たな防御技術の開発に向け、産学官の連携を強化するとともに、継続的かつ安定的に研究開発を推進できる環境を整備すること。情報セキュリティ分野における研究開発の予算を拡充し、継続的かつ安定的に研究開発を推進できる環境を整備すること。

以上