

「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項について」 ヒアリング結果要旨

ヒアリング実施概要

第1回 令和7年3月21日（金）

- ・ 国立研究開発法人情報通信研究機構
- ・ 日本商工会議所

第2回 令和7年3月26日（水）

- ・ 一般社団法人日本経済団体連合会
- ・ 特定非営利活動法人日本ネットワークセキュリティ協会
- ・ 独立行政法人情報処理推進機構

第3回 令和7年4月9日（水）

- ・ 公益社団法人経済同友会
- ・ 総務省・地方公共団体情報システム機構
- ・ 一般財団法人日本サイバー犯罪対策センター
- ・ 八雲法律事務所

「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項について」 ヒアリング結果要旨

1. 新たな司令塔組織を中心とした政府機関・重要インフラ等の対応能力の抜本的強化

ヒアリングにおいて示された意見

- サイバー攻撃に関する一次情報を自ら収集・分析できる能力を構築する必要がある。
- サイバーセキュリティ機関とインテリジェンス機関とが連携し、安全保障等の観点も含めた視点での分析を行うべきである。
- 発展的に改組されるNISCの司令塔機能を強化し、サイバーセキュリティに係るその他政府機関等、それぞれの役割と責任範囲を明確に整理すべき。

有識者からのコメント等

- クロスドメインでの分析という観点が非常に重要。
- 担当官庁の差異等があったとしても横に繋いで活動できるような役割分担・連携体制を考えることが必要。

「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項について」 ヒアリング結果要旨

2. 巧妙化・高度化するサイバー攻撃に対する官民の対策・連携強化（1/2）

ヒアリングにおいて示された意見

- 政府と民間の双方向からの情報共有を基軸とした、新たな官民連携の枠組みを構築すべき。
- 情報提供に係る負担軽減や、政府からの情報のフィードバック、提供された情報の保全体制の確保等を通じて、民間事業者にとっても参画しやすい枠組みとすべき。
- 業界横断で継続的に議論する場を確保し、政府関係部局とも双方向で連携が可能な場を設けるべき。
- 業界・分野固有等の課題についても考慮し、ガイドライン整備や人材育成等を通じて、リスクベースで優先度をつけて対策を推進していくべき。
- 人材面のサポートや共通基盤の提供といった方法を通じて、地方公共団体のサイバーセキュリティの底上げを図るべき。
- IoT機器の増加を踏まえ、問題が起きた際の対応に係る責任の整理等を進めるべき。

有識者からのコメント等

- 民間の情報収集・対処能力と国の役割との連携のあり方についても考えるべき。
- 官民連携・情報提供等における「民間事業者のインセンティブ」を高める施策がどのようなものかを考えるべき。
- 金銭的な支援のみならず、信頼できるソフトウェア・サービス等を政府が提供することも考えられる。
- 地方自治体のサービスについては、災害時等にも提供を継続できるかどうかも重要である。
- 経営層のリーダーシップが重要であるのと同様、地方自治体トップのリーダーシップも重要である。
- IoTデバイスに関する責任の所在について、考慮する必要がある。

「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項について」 ヒアリング結果要旨

2. 巧妙化・高度化するサイバー攻撃に対する官民の対策・連携強化（2/2）

ヒアリングにおいて示された意見

- 重要インフラ事業者等を顧客とする事業者等についても、影響や責任のあり方を検討すべき。
- サプライチェーン全体のレジリエンス向上のためには中小企業の対策強化が必要であり、中小企業でも実施可能かつ効果的な対策について、具体的な目安や方法を伴って浸透を図る等、必要な支援を行うべき。
- 金融機関等の既存のコミュニケーションパスを通じて、中小企業の経営者に向けた周知・広報活動を行ったり、中小企業を外部の専門家と結びつけたりする取り組みが必要である。
- 実務者向けに、詳細対策やワンストップソリューションの提供についても検討していくべき。

有識者からのコメント等

- 中小企業のレジリエンス向上を最重要課題とし、スピード感をもって実施していくことが必要。
- 中小企業の相談窓口となる金融機関等から、中小企業に伝えるべきことを整理するのも有効である。
- 中小企業への支援とセットで、サイバーセキュリティ意識の向上についても考慮する必要がある。
- 地方の中小企業等において、デジタル化の推進・生産性向上とセキュリティとをセットで考えるべき。

「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項について」 ヒアリング結果要旨

3. サイバーセキュリティを支える人的・技術的基盤の整備

ヒアリングにおいて示された意見

- 官民での情報や危機感の共有、連携に必要な信頼関係の醸成を図るため、政府機関と民間の人材交流を図るべき。
- 高度人材からプラス・セキュリティ人材まで、幅広い人材の確保を図る取組を行うべき。
- 官民連携した対処能力の向上を図るため、平時から演習・訓練等の取り組みを官民一体となって推進すべき。
- 我が国独自の情報収集、分析能力を高めていくため、国内のセキュリティ産業の育成を図るべきである。
- 生成系AIのセキュリティ対策を後押しする仕組みを検討すべき。
- PQC移行に向けた方針を定め、取り組みを進めるべき。

有識者からのコメント等

- PQC移行に関しては、重要度に応じたプライオリティを設けて進めるべき。