(ア) 重要インフラ分野を含め、**民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有**や、**政府から民間事業者等への対処調整、支援等の取組を強化**するなどの取組を進める。

- 金融ＩＳＡＣ及び電力ＩＳＡＣから、それぞれの活動と「議論の整理」に対する受止めについてプレゼンテーション。

（金融ＩＳＡＣ）

- 金融ＩＳＡＣは、金融業界のサイバーセキュリティ分野における共助を実現するための組織。
- サイバーセキュリティに係る脅威に対する防衛力を向上・維持するために、２つの活動の柱（コレクティブインテリジェンス、リソースシェアリング）のもとで日々活動。
- 組織の規模によって情報を活かす能力は異なるため、ＩＳＡＣによるトリクルダウン的な機能も対応を全体に浸透させていくための一助になると考えられる。

（電力ＩＳＡＣ）

- 電力ＩＳＡＣは、会員間で信頼と互助の精神に基づきサイバーセキュリティに関する情報等を交換・分析し、電気の安定供給及び電気事業に係る情報の安全性や業務の継続性の確保に資することが目的。
- 諸機関や他ＩＳＡＣからの情報収集、情報分析を行い、会員各社との情報共有を実施。
- 国民生活の基盤をなす経済活動や社会の安定を守るため、高度な侵入・潜伏能力を持つサイバー攻撃への対策の有効性確保に向けた、官民連携強化の必要性を理解。電力分野含め、行動計画に定める重要インフラ事業者は社会基盤を担う事業者であり、攻撃者による侵入・潜伏のターゲットともなり得るため、実効性のある対策が必要。

テーマ別会合「官民連携」（第３回）　議論の概要

● 事務局から、提言素案について説明。

（サイバーセキュリティ戦略本部の活用を含めた検討について）

- 提言案では、能動的サイバー防御の**法整備を待たずに実行可能なものもある**ことから、できるところから始める必要がある。**サイバーセキュリティ戦略本部の活用**も含めて、政府で主導的にまとめ、実行すべき。

（サイバー攻撃が発生した場合の対応能力向上のための官民連携の必要性について）

- 官民連携の対象となる**「民」とは具体的にどのような業種業態を指すのか**をイメージし、**その輪郭がはっきりするような書き方**としていただきたい。

（高度な攻撃に対する支援・情報提供について）

- 「セキュリティクリアランス制度の活用や、情報共有ポリシーの設定により、**適切な情報管理と情報共有を両立する仕組みを構築すべき**」との記載について、**これらの役割分担等について、もう一歩整理**があると良いと思う。

（ソフトウェア等の脆弱性対応）

- 国内で悪用されている**脆弱性情報について触れられているが、これは非常に重要な領域**である。企業のセキュリティ関係者はこういった情報を是非とも入手したいと考えているが、現在、**日本に関するこうした情報は入手が困難**であり、**政府が入手した情報を提供いただけることは非常に重要**。

（基準・ガイドライン等の実効性確保について）

- 重要インフラ事業者の行動を規律する基準・ガイドライン等において細かく書くことには限界があり、安全な仕組みとするためには、**評価・検証を実施し、適時適切に見直すべき**。

（人材の育成・確保について）

- 人材育成については、**政府が中心となって**、**各省庁の取組や業界の取組全体を俯瞰した上で**、官についても一歩踏み込みつつ、取り組んでいくべき。