情報セキュリティに関する新たな基本戦略の策定に向けて

総務省 Ministry of Internal Affairs and Communications

参考２

サイバー攻撃の変化

サイバー攻撃は、高度化・複雑化が進むとともに、愉快犯的なものから経済犯・組織犯的なものに移行し、社会的な脅威が高まっている。

総務省の取組

以下の４つを軸に総務省として取組を推進。

政府自身の防御体制の構築

国会や行政機関など官公庁に対するサイバー攻撃が多発している現状を踏まえた体制づくり。CSIRTの構築など。

【具体的な取組】

政府共通プラットフォーム（クラウド化）における拠点の分散整備及びサイバー攻撃の検知機能等の一元的な提供。

官民連携

社会経済活動の基盤であるインターネットの安心・安全に向けて共同対処を図るなど官民連携を強化。

【具体的な取組】

「サイバー攻撃解析協議会」において、経済産業省等と協力して高度解析を行い、サイバー攻撃の実態等を把握。（平成24年7月～）

国際連携

サイバー攻撃のボーダーレス化を踏まえ、各国の取組の共有化や連携を推進。

【具体的な取組】

国際連携プロジェクト（PRACTICE）の面的な広がりなど戦略的な連携の推進（欧米やASEAN諸国との連携強化）。

技術開発・人材育成・周知啓発

高度化・複雑化が進むサイバー攻撃に対応可能な技術開発、人材育成及び周知啓発。

【具体的な取組】

サイバー攻撃への防御モデルの検討を行うとともに、官民参加型の実践的な防御演習を実施。

今後の方向性

○ **新たな基本戦略では、グローバルな視点を重視し、サイバー攻撃の動向等を踏まえた強化策について検討していくことが必要。**

○ 総務省では、情報通信ネットワークの安心・安全の確保のために議論を行う「情報セキュリティ アドバイザリーボード」を立ち上げ、検討に貢献。