

今後の課題

サイバー攻撃事案の実態解明に係る取組の強化

サイバー攻撃への対処能力を強化するためには、**サイバー攻撃の手口等に係る実態を解明し**、これに応じた対策を講じる必要があります。

このため、警察では、情報通信に関する技術的な分析能力やサイバー攻撃事案に関する捜査能力を高めるとともに、平素より**関係省庁、外国治安情報機関等との情報交換**に努めるほか、国境を越えて行われたサイバー攻撃に対しては、**国際捜査共助**の枠組みを積極的に活用することとしています。

官民連携した被害の未然防止に係る取組の強化

サイバー攻撃による被害の未然防止を図ることは、警察の力のみでは不可能であり、**関係省庁、民間事業者等による官民を挙げた連携・協働**が重要です。

このため、警察では、先端技術を有する事業者等に対して、サイバーインテリジェンス情報共有ネットワークへの参加を働き掛けるとともに、ネットワーク等を通じて集約・分析した情報のうち、提供可能なものについて、関係省庁と共有することとしています。これに加え、重要インフラ事業者等への個別訪問や事案の発生を想定した共同訓練を行うほか、業務を通じて得た不正プログラムに関する情報を情報セキュリティ関連事業者等に提供するなど、**官民で情報を共有し社会全体で対処**するための取組の更なる推進が重要です。

今後も、我が国の政府機関や先端技術を有する企業等に対するサイバー攻撃の発生が懸念されることから、警察では、**サイバー攻撃事案の実態解明及び被害の未然防止**を対策の2本柱として、引き続き、違法行為に対する捜査を推進するとともに、官民連携の更なる強化に努めることとしています。