サイバーテロ

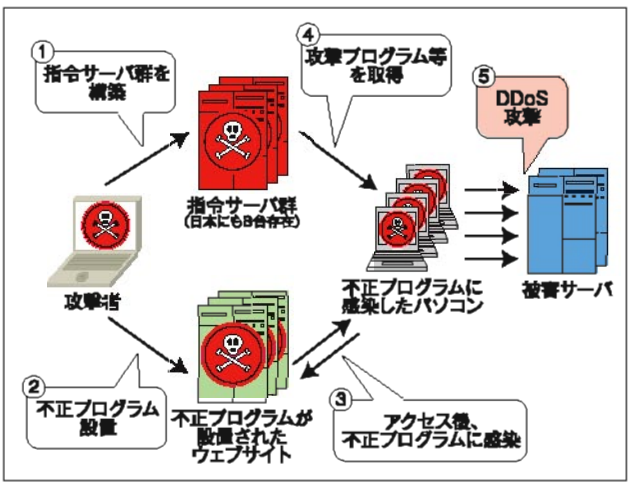
情勢

情報通信システムは、サイバー攻撃を受けて過剰な負荷が掛かったり、コンピュータ・ウイルスに感染したりすると、正常に動作しなくなってしまいます。**政府機関等の重要インフラ事業者の基幹システム**がサイバー攻撃を受け、国民生活や社会経済活動に甚大な支障が生じる事態は、**サイバーテロ**と呼ばれています。サイバーテロは、**攻撃者の特定が難しい**上に**容易に国境を越えて実行することが可能**です。こうした中、次のような事案が発生しており、我が国でもサイバーテロの脅威が現実のものとなっています。

「中国紅客联盟」と称する者が、尖閣諸島の中国領有を主張する民間団体「中国民間保釣联合会」のウェブサイト上で、我が国の政府機関等に対するサイバー攻撃を呼び掛けました。（事例１参照）。

【事例１】平成二二年九月、尖閣諸島周辺領海内における中国漁船衝突事件を受けて、**中国のハッカー集団**である「中国紅客联盟」と称する者が、**我が国の政府機関等に対しサイバー攻撃**を行うよう呼び掛け、警察庁のウェブサーバに対してこれに関連したとみられるアクセスが集中しました。

【事例２】二一年七月、**米国・韓国の政府機関等に対するサイバー攻撃**が発生し、我が国所在の複数のコンピュータが攻撃に利用されていたことが判明しました。



【事例３】二二年九月、イランの原子力発電所等のコンピュータ約三万台が、**電力、ガス等の産業用システムを標的とするスタックスネットと呼ばれる不正プログラム**に感染した旨が報じられました。我が国では、産業用システムにおける被害は確認されていませんが、複数のコンピュータが感染したとされています。

対策

サイバーテロの未然防止や事案発生時の的確な対処のためには、国内の関係機関・団体や事業者が連携することはもとより、国際的な取組みを進めることが重要です。

警察では、内閣官房を中心とする政府全体の取組みに積極的に参画するとともに、**重要インフラ事業者等への個別訪問、サイバーテロ対策協議会**の開催を通じて、情報セキュリティに関する情報提供や意見交換を行っているほか、重要インフラ事業者等と事案発生を想定した**共同訓練**を実施し、緊急対処能力の向上を図っています。また、外国治安情報機関との情報交換を行うなど、**国際連携の強化**に努めています。

神奈川県警察と重要インフラ事業者との共同訓練の状況。疑似インターネット環境を構築し、APEC首脳会議で使用する会議場がサイバー攻撃を受けたとの想定で訓練を行いました（9月、神奈川）。

さらに、警察庁には、サイバーテロ対策の技術的中核として**サイバーフォースセンター**が設置されています。ここでは、サイバー攻撃の発生を早期に把握するため、**リアルタイム検知ネットワークシステムを二四時間体制で運用**するとともに、サイバーテロ発生時には緊急対処の技術支援を行う拠点として機能します。

24時間体制でサイバーテロの予兆把握に当たる警察庁のサイバーフォースセンター。リアルタイム検知ネットワークシステムには、インターネットとの接続点に設置した警察のセンサーからの情報が集約されます。