サイバーテロ対策の推進

サイバーテロとは

重要インフラ(※)の基幹システムに対する電子的攻撃又は重要インフラの基幹システムにおける重大な障害で電子的攻撃による可能性が高いものとされ、一般的には、政府・行政機関を含む重要インフラ事業者等の基盤を機能不全に陥れ、社会機能を麻痺させてしまう行為をいい、サイバー犯罪のうち最も甚大な被害を及ぼす危険性があるものです。

※　重要インフラとは

情報通信(テレビ、ラジオ、電話等)、金融、航空、鉄道、電力、ガス、政府・行政サービス(地方公共団体を含む。)、医療、水道及び物流の10分野があり、私たちの日常生活に不可欠な社会基盤のことです。

サイバーテロの脅威

インターネットや情報システムが社会基盤として定着し、今や、サイバー空間は、私たちの日常生活や社会経済活動に不可欠な存在となっています。 しかし、その一方で、近年、国内でも多数のサイバー攻撃事案が発生しており、重要インフラの基幹システムに対してサイバー攻撃が実行された場合、国民・県民の生活や経済活動に甚大な支障が生じるおそれがある等、サイバーテロの脅威はますます現実のものとなっています。

サイバー攻撃の特徴

コンピュータとインターネットへのアクセスさえ確保できれば、簡単に世界中にアクセスすることができ、また、通信は直接目に見えないことなどから、サイバー攻撃には、

- ○　攻撃の実行者の特定が難しい
- ○　攻撃の被害が潜在化する傾向がある
- ○　国境を容易に超えて実行可能である

等の特徴があります。

サイバー攻撃の手口

サイバーテロに用いられる手口としては、攻撃対象のコンピュータに、複数のコンピュータから一斉に大量のアクセスを行って負荷を掛けるなどして、そのコンピュータのサービス提供を不可能にするDDoS攻撃が代表的です。

また、サイバーインテリジェンス(※)の代表的な手口として、業務に関連した正当なメールを装って、ウイルス入りの添付ファイルを付した電子メールを送信し、コンピュータを不正プログラムに感染させて、機密情報を外部へ送信させ、情報の窃取を図る標的型メール攻撃があります。

※　サイバーインテリジェンスとは

政府機関や先端技術を有する企業のシステムに侵入して、機密情報を窃取する攻撃のことです。

サイバーテロ対策

県警察では、県民生活に大きな被害を与えるサイバーテロの未然防止と発生時の被害拡大防止を目的として、官民一体となったサイバーテロ対策を推進していくため、平成22年7月29日、県内の重要インフラ事業者等から賛同を得て「群馬県サイバーテロ対策協議会」を設立しました。

サイバーテロ対策プロジェクト研修会の開催について

平成24年11月5日（木）、警察本部において、「サイバーテロ対策プロジェクト研修会」を開催しました。

この研修会では、サイバー犯罪の現状や電子メールの仕組みに関する講義を行ったり、セキュリティ関連事業者を講師に招いて、サイバーテロ対策のためのセキュリティ技術に関する講演会を開催して、捜査員の対処能力の向上を図りました。

研修会の開催状況

第4回群馬県サイバーテロ対策協議会の開催について

平成25年7月25日（木）、警察本部において、「第4回群馬県サイバーテロ対策協議会」を開催しました。

この協議会では、サイバー攻撃の現状と対策について情報提供及び意見交換を行ったり、独立行政法人情報処理推進機構職員を講師に招いて「近年のITシステムを取巻く脅威と対策」と題する講演会を開催して、警察と参加事業者との連携強化を図りました。

協議会の開催状況