特集：サイバー攻撃をめぐる情勢とその対策

昨今、サイバー攻撃が世界的規模で頻発する厳しい情勢にあります。

このような中、我が国は、平成28年に伊勢志摩サミット、32年に東京オリンピック・パラリンピック競技大会の開催を控えているところ、その対策に万全を期す必要があります。

警察では、サイバー攻撃の実態解明や被害の未然防止等を推進しており、外国治安情報機関との捜査や情報収集に関する協力を強化したり、民間事業者等との協力関係を確立して被害の未然防止を図ったりするなど、サイバー攻撃をめぐる新たな情勢に対処するための対策に取り組んでいます。

サイバー攻撃の概要

サイバー攻撃の特徴

インターネットが国民生活や社会経済活動に不可欠な社会基盤として定着し、今や、サイバー空間は国民の日常生活の一部となっています。こうした中、重要インフラ(注1)の基幹システム(注2)を機能不全に陥れ、社会の機能を麻痺させる**サイバーテロ**や、情報通信技術を用いた諜報活動である**サイバーインテリジェンス（サイバーエスピオナージ）**といったサイバー攻撃が世界的規模で頻発するなど、その脅威は、国の治安、安全保障及び危機管理に影響を及ぼしかねない問題となっています。

サイバー攻撃には、**①攻撃の実行者の特定が難しい、②攻撃の被害が潜在化する傾向がある、③国境を容易に越えて実行可能である**といった特徴があり、我が国において、この脅威に対する対処能力の強化が求められています。

	サイバーテロ	サイバーインテリジェンス（サイバーエスピオナージ）
用語の意味	○　重要インフラの基幹システムに対する電子的攻撃 ○　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	情報通信技術を用いた諜報活動
目　的	社会機能の麻痺	機密情報の窃取
対　象	重要インフラ事業者等 （情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油の13分野）	政府機関や先端技術を有する企業等

サイバーテロ、サイバーインテリジェンスの概要

（注1）：情報通信、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、物流、化学、クレジット、石油の各分野における社会基盤

（注2）：国民生活又は社会経済活動に不可欠な役務の安定的な供給、公共の安全の確保等に重要な役割を果たすシステム

サイバーテロ

情報通信技術が浸透した現代社会においては、私たちの生活に不可欠な電力、ガス、水道等の重要インフラも、情報システムによって支えられています。

重要インフラの基幹システムに対する電子的攻撃によりインフラ機能の維持やサービスの供給が困難となり、国民の生活や経済活動に重大な被害をもたらすサイバーテロの脅威は現実のものとなっています。海外では、金融機関のシステムや原子力発電所の制御システムの機能不全を引き起こす事案が発生しています。

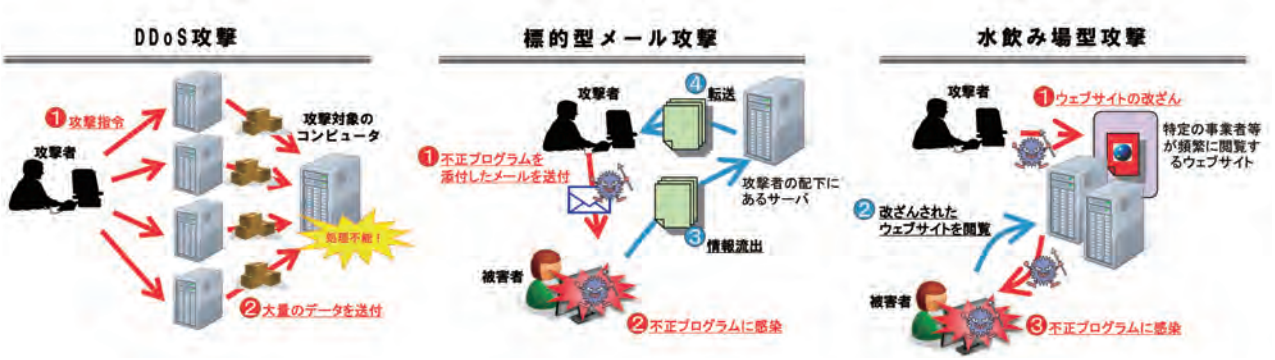
サイバーテロの手法としては、複数のコンピュータから一斉に大量のデータを送信して負荷を掛けるなどして、攻撃対象のコンピュータによるサービスの提供を不可能にするＤＤｏＳ（ディードス）(注1)攻撃や、コンピュータに不正に侵入したり、不正プログラムに感染させるなどにより、管理者や利用者の意図しない動作を当該コンピュータに命令する手法等があります。

サイバーインテリジェンス

近年、情報を電子データの形で保有することが一般的となっている中、**軍事技術への転用も可能な先端技術や、外交交渉における国家戦略等の機密情報の窃取を目的として行われるサイバーインテリジェンス**の脅威が、世界各国で問題となっています。

サイバーインテリジェンスに用いられる手口としては、業務に関連した正当なものであるかのように装った、市販のウイルス対策ソフトでは検知できない不正プログラムを添付した電子メールを送信し、これを受信したコンピュータを不正プログラムに感染させるなどして、情報の窃取を図る**標的型メール攻撃**が代表的です。

また、こうした標的型メール攻撃のほか、対象組織の職員が頻繁に閲覧するウェブサイトを改ざんし、当該サイトを閲覧したコンピュータに不正プログラムを自動的に感染させる手口による**「水飲み場型攻撃」**も発生するなど、サイバー攻撃の手口はますます巧妙化・多様化しています。



サイバー攻撃の手口

（注１）：Distributed Denial of Serviceの略