サイバーテロ対策

1 サイバーテロの脅威

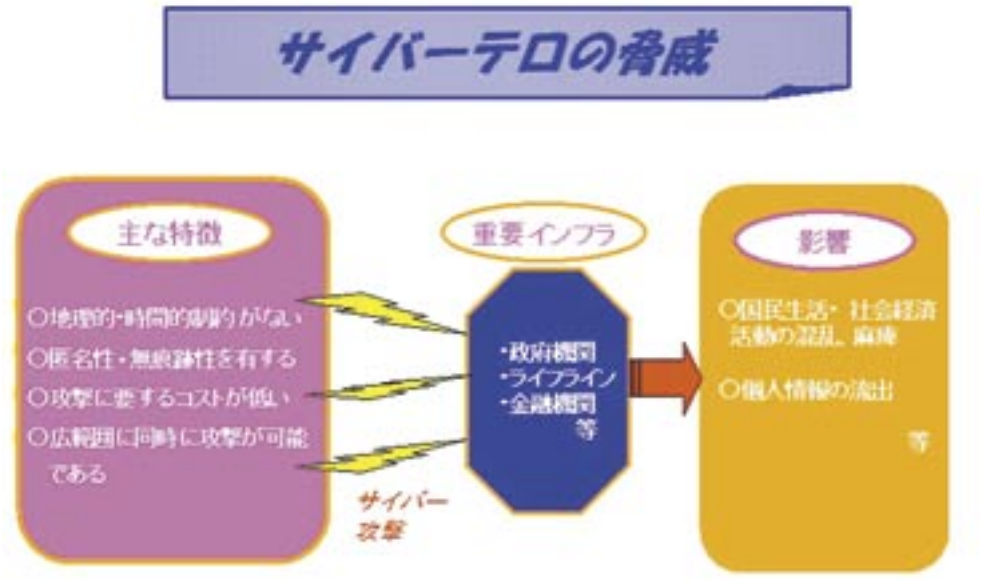
平成一四年一〇月、インターネットの流れを制御する世界各地のルートＤＮＳサーバへのサイバー攻撃が発生したほか、一五年一月、特に韓国で甚大な被害が生じたスラマーワーム（注一）によるインターネット接続障害が発生、さらに、同年八月には特定のサーバに対し、ＤｏＳ（Denial of Service（サービス拒否）攻撃を行うようプログラムされていたブラスターワーム（注二）がまん延するなど、国内外を問わず重大な被害を被るウイルス事案、サイバー攻撃事案が発生しており、サイバーテロの脅威が正に現実のものとなってきています。

一三年九月に発生した「米国における同時多発テロ事件」以降、テロ対策は国際的にも最重要課題となっていますが、とりわけ、サイバーテロについては、

① 地理的・時間的制約がない
② 匿名性・無痕跡性を有する
③ 攻撃に要するコストが低い
④ 広範囲に同時に攻撃が可能である

などの特質があり、国の内外や、動機・主張の如何を問わず、さらには団体、個人を問わず敢行されるため、その対策は急務となっています。

警察庁セキュリティポータルサイト（@police）



このような情勢下、一五年五月に開催されたＧ８司法・内務閣僚会合においても、重要情報インフラ防護が主要議題の一つとして取り上げられ、国際的な連携強化や政府と民間部門との関係強化が重要な課題とされています。

2 サイバーテロ対策

警察では、サイバーテロ事案発生の未然防止、事案発生時の被害拡大防止及び事件検挙を目的に、警察庁と各管区警察局に所属する技術系職員の中から高度な技術を有する者を選抜の上、機動的技術部隊としてサイバーフォースを創設して二四時間体制でサイバーテロの予兆の把握、事案の早期認知に努めているほか、警察庁にサイバーテロ対策推進室を、全国の都道府県警察にサイバーテロ対策プロジェクトを設置し、様々なサイバーテロ対策を推進しています。特に、重要インフラ事業者等の基幹となるシステムがサイバー攻撃を受けた場合、国民生活や社会経済活動に重大な影響を及ぼすおそれがあることから、警察と重要インフラ事業者等との連携が重要であります。そのため、重要インフラ事業者等を個別に訪問するなどして、セキュリティ水準向上のための自主的な取組み、事案発生時等における警察への迅速な通報、捜査への協力等について要請するとともに、スラマーワームやブラスターワームのようなコンピュータ・ウイルス発生時等には、適宜、注意喚起や対策に関する助言を行うなど、連携の強化に努めています。

今後も、高度化するサイバー攻撃手法に対応するため、装備資機材の高度化、外国治安情報機関等との連携強化、国内外のサイバーテロに関する情報収集体制の強化、情報のデータベース化、サイバーテロの物理的・電子的攻撃手法の収集・分析能力の強化、要員の能力向上のための教育訓練等を行い、緊急対処体制及び捜査活動のための体制の充実、強化に努めることとしています。

（注一）スラマーワーム
Microsoft SQL Server 2000 SP2等の脆弱性を利用してサーバに侵入し、さらに、ほかの任意のサーバへ同様の侵入を繰り返すことによりネットワークのトラフィックを増大させ、システムダウンを引き起こすワーム。

（注二）ブラスターワーム
マイクロソフト社の提供するＯＳ、Windows XP等の脆弱性を有するコンピュータに侵入した後、そのワームのプログラムが実行されるとコンピュータの異常終了を生じさせ、さらに、ほかの脆弱性を有するコンピュータを探し、同様の感染を繰り返すことにより感染が拡大するワーム。このワームは、マイクロソフト社の特定のサーバに対し、ＤｏＳ攻撃を行うようプログラムされていた。


サイバーフォースセンター