「サイバー攻撃」

近年、クラウド監視（No224 号掲載「よく見かける下水道用語」）のように、下水道システムにおいてもインターネットが活用されています。今回は、下水道用語ではありませんが、インターネットを活用した下水道システムの安定した運営のためにも正しく理解しておくべき用語として、「サイバー攻撃」についてご説明したいと思います。

サイバー攻撃とは、インターネットやデジタル機器を絡めた手口で、個人や組織を対象に、金銭の窃取や個人情報の詐取、あるいはシステムの機能停止などを目的として行われる攻撃です。組織を対象にした攻撃は、不正アクセスにより企業が保有する機密情報や顧客情報を窃取する、あるいは Web サービスやシステムをダウンさせるなどして何かしらの被害を与えることを目的に行われます。組織には企業や団体だけでなく、国家や行政機関なども含まれます。攻撃の類別も、特定の組織を標的とした攻撃と不特定多数を狙う攻撃が存在します。次に、よく目にするサイバー攻撃について、説明します。

１）標的型攻撃

標的型攻撃とは、特定の組織を狙ったサイバー攻撃です。2015 年には国内の特殊法人が狙われ、125 万人分の個人情報が窃取されました。標的型攻撃の際に使用されるメールは極めて巧妙に偽装されているものが増えています。事前に不正に取得した情報をもとに、組織内で実際に用いられている役職名を使い、業務に関係する内容を記載する場合もあるため、受信者は判別が難しくなります。また、送られてきたメールに記載された URL（ショートカットファイルを含む）をクリックしただけでマルウェア※に感染するケースもあります。

※ マルウェアとは、コンピュータウイルスやスパイクウェアなど悪意で作られたプログラムです。近年話題となった Emotet（エモテット）もマルウェアのひとつです。Emotet は、本物のファイルに見えるショートカットファイルをメールに直接添付することが多く、そのファイルを開くだけで Emotet に感染してしまう可能性があるので注意が必要です。

２）ランサムウェア攻撃

ランサムウェアの「Ransom」とは、日本語で身代金を意味します。ランサムウェアに感染すると、所有するデータが勝手に暗号化されてしまいます。従来のランサムウェアの攻撃は、明確な標的を定めずに感染を試み、運悪く感染した被害者から身代金を引き出そうとしていました。しかし最近では標的型サイバー攻撃と同様に、特定の企業や組織を狙う攻撃も増えています。攻撃者は暗号化したデータの復号と引き換えに、金銭を要求します。暗号化されたデータが機密情報であったり、顧客の個人情報であったりする場合、被害はより深刻になります。近年では、「機密情報の暴露」を加えた二重脅迫、「顧客や取引先への嫌がらせ」、後述する「DDos 攻撃」を含めた四重脅迫のケースも出ています。

３）DoS 攻撃／DDoS 攻撃

DoS 攻撃とは「Denial of Service attack」の略であり、日本語に訳すと「サービス拒否攻撃」となります。DDoS 攻撃は「Distributed Denial of Service attack」で「分散型サービス拒否攻撃」と訳されます。いずれも、Web サイトやサーバーに負荷をかけてダウンさせることでサービスを妨害する攻撃です。2020 年 3 月には自治体の公式サイトが DDoS 攻撃を受け、閲覧できなくなるという事件が発生したほか、2022 年 9 月 6 日にはロシアのウクライナ侵攻を支持するサイバー攻撃集団「キルネット」が日本政府のサイトに攻撃をしかけました。

警察庁が発表した 2022 年度上半期の「サイバー空間をめぐる脅威の情勢等について」において、ランサムウェア被害が前年同期比で 8 割増加したとの報告がありました。国内の被害は幅広い業種に及んでおり、ウクライナ情勢をはじめ国際情勢が変化する中、政府機関や重要インフラ関連企業に対するサイバー攻撃も頻発しています。

サイバー攻撃を防ぐためには、まず業務にかかわる 1 人ひとりの個人が正しい知識を持って対策にあたることが必要です。また個人だけでなく、組織としてもセキュリティ対策をとる必要があります。年々手口が巧妙になっているサイバー攻撃ですが、下水道システムにおいても個人と組織が一丸となって、常に最新のセキュリティ対策を導入することを心がけましょう。

（DX 戦略部システムマネジメント課）