ニューノーマル処方箋（第31回）

IoTがサイバー攻撃を招く！？「ボットネット」の恐怖

2024.01.26

＜目次＞

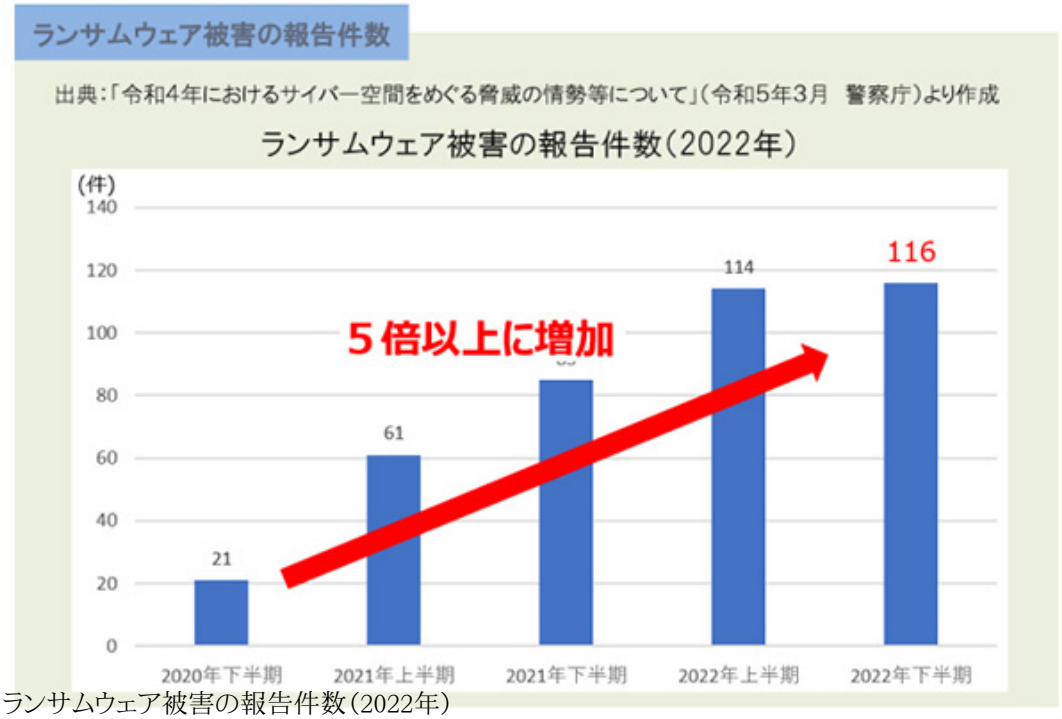
コロナ禍で情報通信の依存度が高まった中、サイバー攻撃も増えている

総務省のサイバーセキュリティタスクフォースは、2023年8月、サイバーセキュリティに関する最近の動向や、今後取り組むべき施策をまとめた「ICTサイバーセキュリティ総合対策2023」を公開しました。

同資料によると、サイバー攻撃のリスクは日々拡大しているといいます。例えば、2022年のランサムウエア被害の報告件数は、2020年（下半期）と比較して5倍以上、フィッシングメール／フィッシングサイトの報告件数についても、4年前の2019年と比較してそれぞれ約17.4倍／約14.7倍と、大幅な増加を見せています。

一方で、新型コロナウイルス感染症の感染拡大などにより、社会の情報通信ネットワークに対する依存度は高まっており、日本のインターネットにおけるトラフィック量はここ5年で約3倍に増加しているといいます。

もしサイバー攻撃によって情報通信ネットワークの機能に支障が生じた場合には、国民生活や社会経済活動に多大な影響が及ぶことになります。このことから本資料では、総務省の役割について「社会経済活動を支える情報通信ネットワークの安全を確保し、サイバー空間を利用する全ての国民のサイバーセキュリティの向上を図ること」とし、「情報通信ネットワークの安全性・信頼性を確保することは一層重要」と明言しています。



ランサムウェア被害の報告件数（2022年）

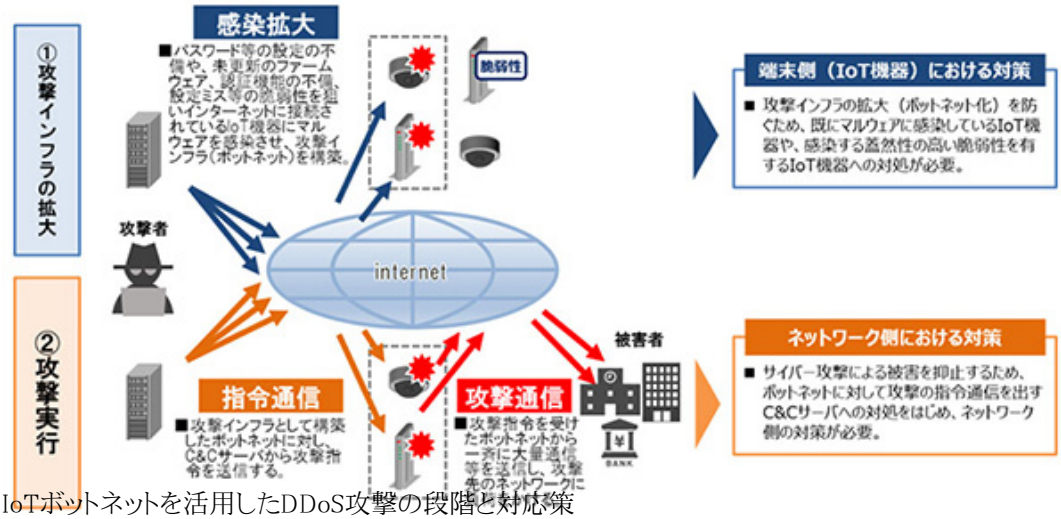
IoTがサイバー攻撃を招く！？「IoTボットネット」の恐怖

それでは、情報通信ネットワークの安全性・信頼性を確保するためには、具体的にどのような取り組みを行うべきなのでしょうか？本資料の中で特に大きく取り上げられているのが「IoTボットネット対策」です。

「ボットネット」とは、ボット（自動化プログラム）に感染したコンピューターと、攻撃者の命令を送信する指令サーバーによって構成されたネットワークのことです。つまりIoTボットネットとは、悪意のある攻撃者の支配下にあり、攻撃インフラとして活用される恐れのあるIoT機器のことをさします。

IoTボットネットが、DDoS攻撃のように大規模なサイバー攻撃を引き起こす流れとしては、まずIoT機器にマルウエアが感染し、攻撃の踏み台として悪用できるようIoTボットネット化されます。その後IoTボットネットに対し、C&Cサーバーからネットワークに対して指令が出され、大量の通信で攻撃が実行されます。

そのため、大規模サイバー攻撃を防ぐためには、【A】IoT機器側（端末側）における対策と、【B】攻撃の指令通信を出すネットワーク側の対策という、2つの側面におけるIoTボットネット対策を講じることが必要になります。



IoTボットネットを活用したDDoS攻撃の段階と対応策

IoTボットネットで最も狙われるのは「ルーター」… 続きを読む