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＞

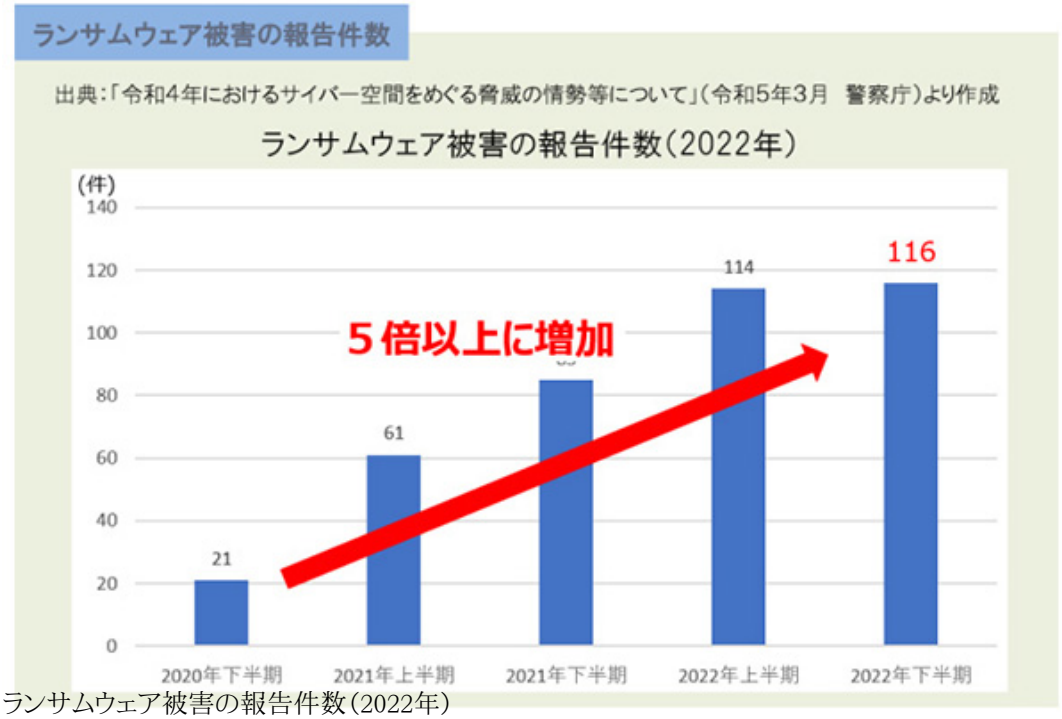
コロナ禍で情報通信の依存度が高まった中、サイバー攻撃も増えている

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）

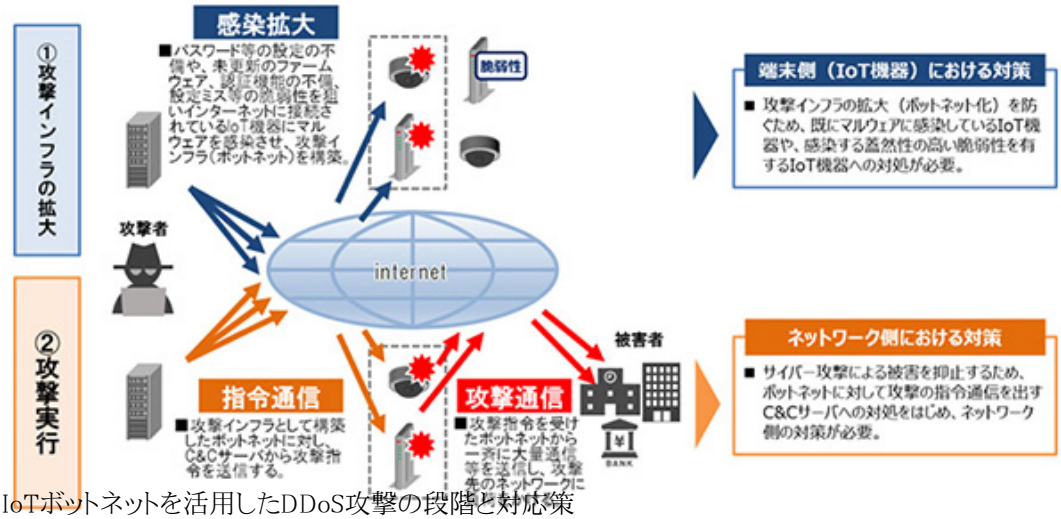
IoTがサイバー攻撃を招く！？「IoTボットネット」の恐怖

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」

このうち【A】IoT機器側の対策としては、総務省やNICT（情報通信研究機構）らが主体となり、「NOTICE」（ノーティス）というプロジェクトを実施しています。具体的には、以下の1～4の流れで行われています。

1. 脆弱性等のあるIoT機器の調査の延長・拡充

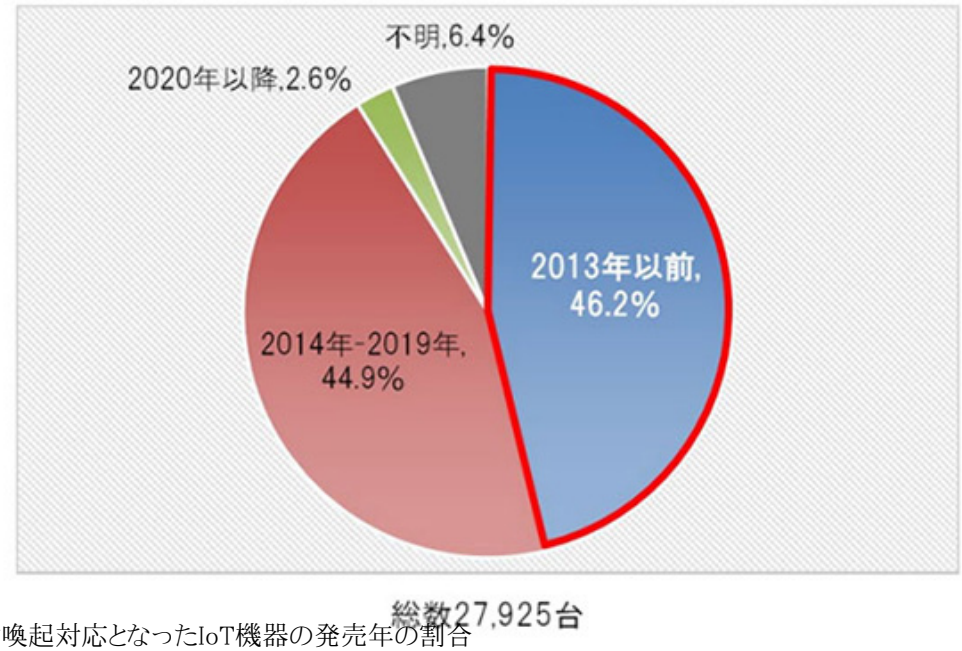
2. 利用者への注意喚起等の実効性向上

3. メーカーやSIer等の幅広い関係者との連携による総合的な対処

4. 1～3を効果的に実施するためのNOTICEの運営体制の強化

1の「IoT機器の調査」に関しては、すでにNICTが国内の1.12億のIPアドレスを対象に、脆弱性に関する調査を実施しています。それによると、機器のID・パスワードに脆弱性があるとしてISP（インターネットサービス事業者）に通知されたIoT機器の数は、直近では月平均4000件程度で推移しており、現在まで累計で8万件以上の通知を実施しています。注意喚起の対象となった機器で最も多かったものは「ルーター」で、全体の90%以上を占めています。

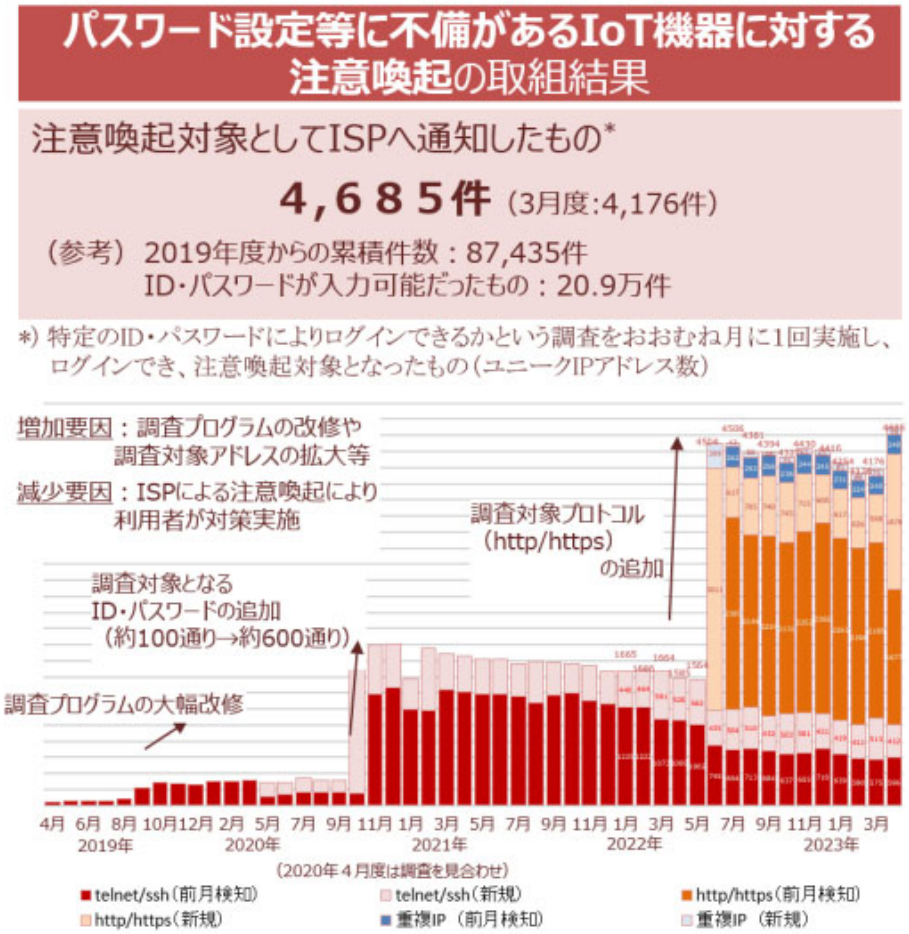
このようなNOTICEの取り組みを実施しているものの、資料によればID・パスワードに脆弱性があるIoT機器は、現在でも一定数残存しており、特に注意喚起対象となった機器のうち、10
年以上前に発売された機器は4割以上という高い数値となっています。



注意喚起対応となったIoT機器の発売年の割合

現在、総務省・NICTでは「NOTICE サポートセンター」という窓口を設置し、問い合わせ対応や機器別の脆弱性解消マニュアルの作成等、注意喚起を受けた利用者のサポートなどの取り組みを行っています。

今後は、引き続きサイバー攻撃の踏み台となり得るIoT機器の観測を続け、利用者に対し、注意喚起だけにとどまらない“プッシュ型支援”を強化していくとしています。さらに、IoTボットネットの全体像を可視化するための観測網として「統合分析対策センター（仮称）」を立ち上げることも明記されています。



パスワード設定に不備があるIoT機器に対する注意喚起対象件数の推移

Beyond 5G・6Gに求められるセキュリティの考え方とは

資料ではこの他にも、さまざまなサイバーセキュリティ対策を推進することを訴えています。

例えば電気通信事業者に対しては、フィッシングサイトなど悪性Webサイト情報の収集・分析を行い、得られた知見を普及・啓発するなど積極的なサイバーセキュリティ対策を推進することを呼びかけています。

さらに、2030年代に導入される予定の次世代情報通信インフラ「Beyond 5G・6G」のセキュリティ対策についても言及しており、Beyond 5G・6G で開発・採用される技術について、企画・設計の段階からセキュリティ仕様を取り込んで行うシステム開発手法である「セキュリティ・バイ・デザイン」の考え方を反映することを訴えています。

情報通信技術は日々進化していますが、それに伴い、セキュリティの穴を狙うサイバー攻撃も進化しています。サイバー攻撃の被害から自社を守り、ビジネスを安定的に続けるためにも、本資料に目を通し、自社のIoT機器の安全性を確認してみてはいかがでしょうか。