IoT機器調査及び注意喚起プロジェクト（NOTICE）の取組み

総務省
サイバーセキュリティ
統括官室
参事官補佐
梅城（うめき）　崇師（たかのり）

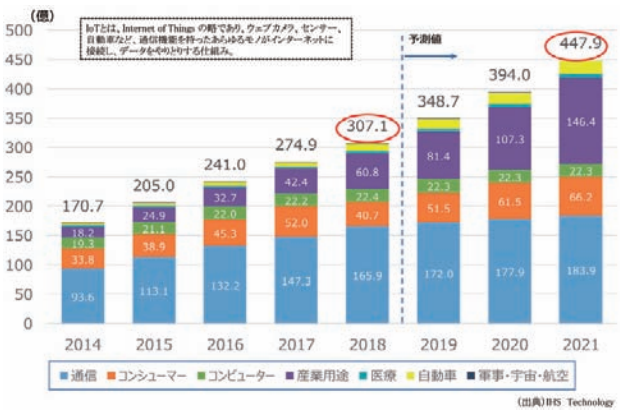
総務省
サイバーセキュリティ
統括官室
主査
黒田（くろだ）　淳（じゅん）

総務省
サイバーセキュリティ
統括官室
係員
山下（やました）　恵一（けいいち）

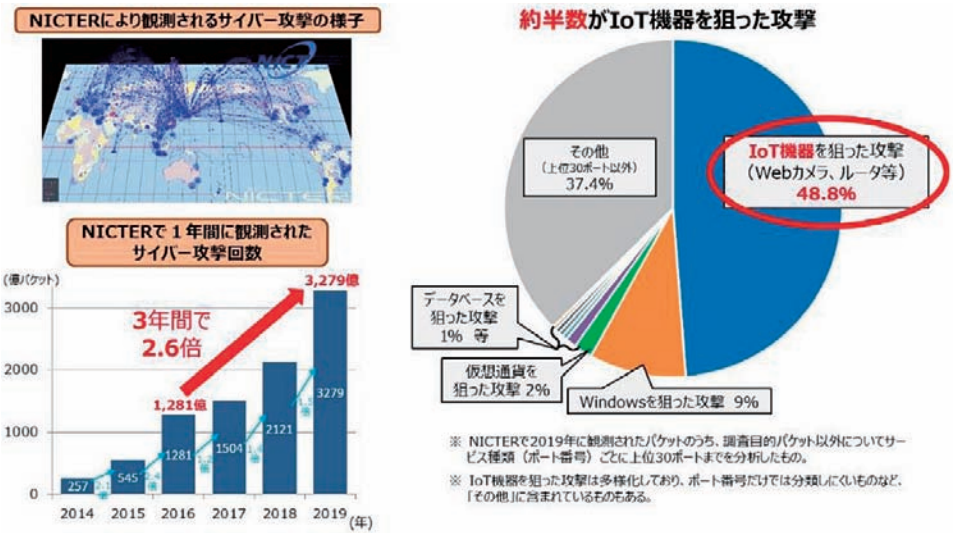
1. 背景

インターネット技術や各種センサー、テクノロジーの進化等を背景に、パソコンやスマートフォンといった従来のインターネット接続端末に加え、家電や自動車、ビルや工場など世界中のあらゆるモノがインターネット等のネットワークに接続され、その数は爆発的に増加している。民間調査会社の推計によれば、IoT機器は、2018年時点では約307億個であったが、2021年には約1.5倍の約448億個まで増加する見込みである。

多くのIoT機器が普及している現在においては、これらのIoT機器を狙ったサイバー攻撃も多発している。こうした攻撃を捉えるため、国立研究開発法人情報通信研究機構（NICT）では、大規模サイバー攻撃観測網である「NICTER」を開発している。このNICTERは、未使用のIPアドレス約30万個から構成されている。これらのIPアドレスは通常のインターネット利用においては使用されないため、通常は当該IPアドレス宛に通信が発生することはないが、マルウェアに感染した機器が感染を広げるために無差別に通信を行った際には、当該IPアドレス宛にも通信が発生することがある。NICTERでは、こうした通信を捉えることで、サイバー攻撃の状況を観測している。この結果を、2016年と2019年とで比較すると3年間で約2.6倍に増加しており、Webカメラやルータ等のIoT機器を狙ったサイバー攻撃が全体の約半数を占めていることが報告されている。



■図1. IoT機器の急激な増加

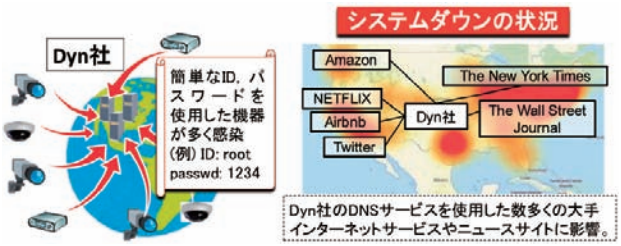


■図2. IoT機器を狙った攻撃の急増（NICTERによる観測）

このようなマルウェアに感染したIoT機器を踏み台として、大規模なサイバー攻撃が行われた例が実際に存在する。2016年10月に米国のDyn社のサーバーに対して大規模なDDoS攻撃が2回発生し、同社からDNSサービスの提供を受けていた多数の企業のサービスにアクセスしにくくなる等の障害が発生した。これは、Miraiというマルウェアに感染した10万台を超えるIoT機器を踏み台にして、最大1.2Tbpsの大量の通信が発生したことが原因とされている。

また、東京2020オリンピック・パラリンピック競技大会のような国家を挙げての大規模イベントは、攻撃側にとっても格好の標的となりやすい。実際に過去のオリンピック・パラリンピックにおいても、様々なサイバー攻撃が行われており、東京大会においても、関係機関が協力して対策が進められているところである。

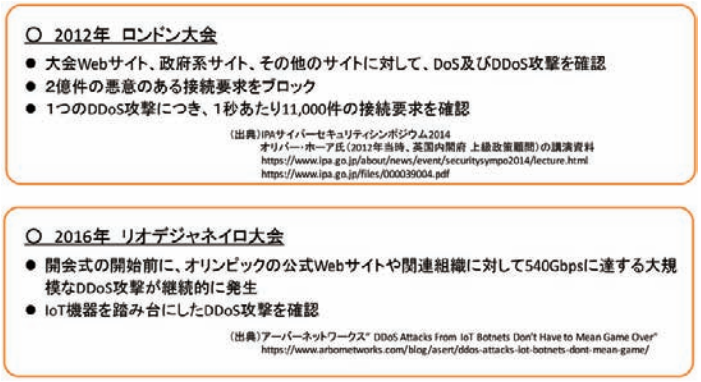
このように、サイバー攻撃は大きな被害をもたらすことが想定されることから、その対策は安心・安全な国民生活の保護や社会経済活動の保護など、あらゆる面から必要不可欠であり、喫緊の課題となっている。



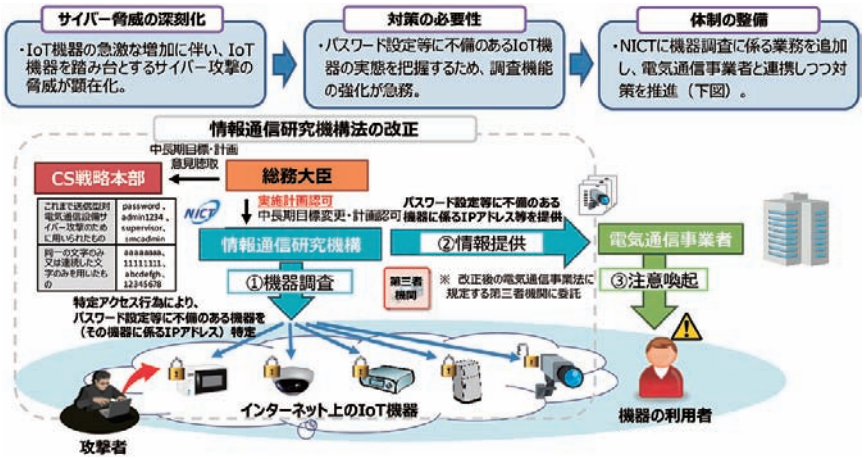
■図3. IoT機器を踏み台とした大規模DDos攻撃

2. 国立研究開発法人情報通信研究機構法の改正

このようにIoT機器を踏み台とするサイバー攻撃の脅威が顕在化している状況を踏まえれば、パスワード設定等に不備のあるIoT機器（例えば「password」や「123456」等の容易に推測されるパスワードを設定しているようなもの）の実態を把握し、対応を行うことが急務である。このため、NICTの業務に、パスワード設定等に不備のあるIoT機器の調査等を追加する国立研究開発法人情報通信研究機構法の改正を行い、2018年11月1日に施行した。



■図4. 過去のオリンピック・パラリンピック時のサイバー攻撃



■図5. 国立研究開発法人情報通信研究機構法の改正概要

①特定アクセス行為に係る業務に従事する者の氏名、所属部署及び連絡先
②特定アクセス行為の送信元の端末設備又は自営電気通信設備に割り当てられるアイ・ピー・アドレスその他のこれらの設備に関する事項
③特定アクセス行為に係る識別符号の方針及び当該方針に基づき入力する識別符号
④特定アクセス行為の送信先のアクセス制御機能を有する特定電子計算機である電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備に割り当てられるアイ・ピー・アドレスの範囲その他のこれらの設備に関する事項
⑤特定アクセス行為により取得する通信履歴等の情報の安全管理措置その他の当該情報の適正な取扱いを確保するために必要な措置に関する事項
⑥送信型対電気通信設備サイバー攻撃のおそれへの対処を求める通知先に求める特定アクセス行為により取得する通信履歴等の電磁的記録に記録された情報の適正な取扱いを確保するための措置に関する事項
⑦その他必要な事項

■図6. NICTの実施計画で規定する内容

この法改正により可能となる調査は、NICTがインターネット上のIoT機器に対して、例えば「password」や「123456」等の容易に推測されるパスワードを入力する等により、サイバー攻撃に悪用されるおそれのある機器を特定するものである。

調査の実施に当たってIDやパスワードを入力する行為が必要となるが、NICTが調査に当たって実施する場合にはこの行為を「特定アクセス」と呼称する。この特定アクセス行為に当たっては、NICTは総務大臣の認可を受けた実施計画に基づいて実施することとされており、特定アクセス行為を含む調査によって得られた情報についても厳格な安全管理措置を講じることとされている。こうした措置を講じた上で、5年間の時限措置として調査を実施するものである。

3. NOTICEによる注意喚起

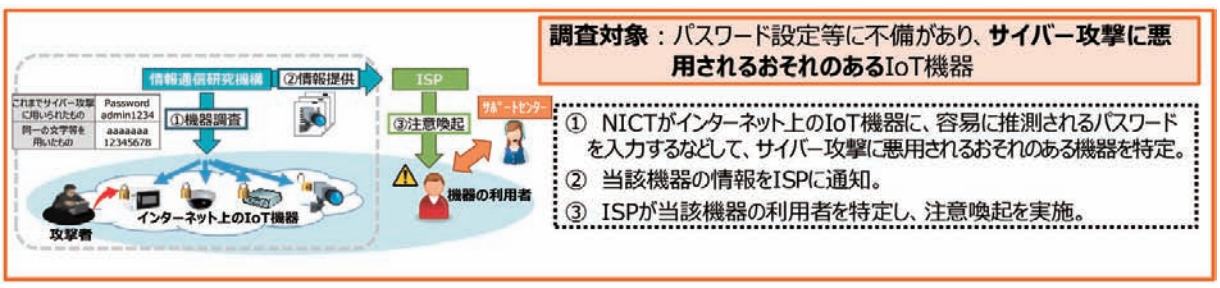
上記改正法に基づき、総務省及びNICTは、インターネット・サービス・プロバイダ（ISP）と連携し、2019年2月から、脆弱なID・パスワード設定等のためサイバー攻撃に悪用されるおそれのあるIoT機器を調査し、利用者への注意喚起を行う取組みである「NOTICE（National Operation Towards IoT Clean Environment）」を実施している。

具体的には、①NICTがインターネット上のIoT機器に対して、例えば「password」や「123456」等のこれまでにサイバー攻撃に用いられたパスワードや同一の文字列等を用いたような容易に推測されるパスワードを入力するなどにより、サイバー攻撃に悪用されるおそれのある機器を特定する。②その特定した機器の情報をNICTからISPに通知する。③通知を受けたISPがその機器の利用者を特定し注意喚起を行う、といった流れで進めている。

また、NOTICEの実施に当たって、総務省は「NOTICEサポートセンター」を開設し、ウェブサイト（https://notice.go.jp）や電話（0120-769-318（無料・固定電話のみ）・03-4346-3318（有料））により、利用者からの問合せ対応を行い、適切なセキュリティ対策を案内している。

4. マルウェアに感染しているIoT機器の利用者に対する注意喚起（NICTER注意喚起）

NOTICEは「サイバー攻撃に悪用されるおそれのあるIoT



■図7. NOTICEの概要

■図8．NICTER注意喚起の概要

機器」を対象としていたが、これと並行して、2019年6月から、総務省、NICT、一般社団法人ICT-ISAC及びISP各社が連携して、「既にマルウェアに感染しているIoT機器」の利用者に対し、ISPが注意喚起を行う取組みを実施している。本取組みは、NICTが前述のNICTERで得られた情報を基にマルウェア感染を原因とする通信を行っている機器を検知し、ISPにおいて当該機器の利用者を特定することにより行っている。

5．これまでの実績

2019年12月時点で調査に参加しているISPは41社であり、当該ISPが保有する約1.1億の国内IPv4アドレスに対して調査を実施した。

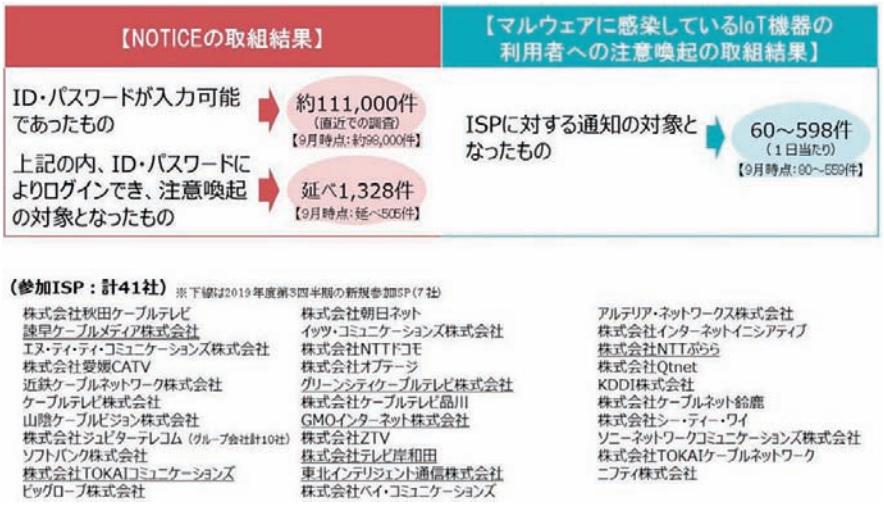
NOTICEの取組結果として、調査対象となったIPアドレスのうち、ID・パスワードが入力可能であったものが直近での調査において約111,000件であり、このうち、特定のID・パスワードの入力によりログインでき、注意喚起の対象となったものは延べ1,328件となっている。

また、マルウェアに感染しているIoT機器の利用者への注意喚起の取組結果として、ISPに対する通知の対象となったものは、1日当たり60件～598件となっている。

6．今後の取組みについて

現時点では容易に推測されるID・パスワードを設定している、または既にマルウェアに感染していると判明したIoT機器の数は少ない状況と考えられるが、今後もIoT機器へのマルウェアの感染活動は継続することが見込まれる。このため、利用者においては、引き続き適切なID・パスワードの設定やファームウェアの最新版へのアップデート等のセキュリティ対策の徹底に努めることが重要である。

また、今後ともより多くのISPと連携しながら上記取組みを継続し、引き続きIoT機器のセキュリティ対策の向上やIoT機器を悪用したマルウェアの活動状況の把握等に取り組んでいく予定である。



■図9．IoT機器調査及び利用者への注意喚起の実施状況（2019年12月）