ITの過去から紡ぐIoTセキュリティ:

政府のIoT機器調査、無差別の「力業」に踏み切った背景は

https://www.itmedia.co.jp/news/articles/1902/14/news059.html

政府が、サイバー攻撃に悪用される恐れのあるIoT機器を洗い出し、ユーザーに注意喚起を行う「NOTICE」を始める。なぜ、こうした力業に踏み切ったのか。

2019年02月14日 07時00分 更新

[高橋睦美, ITmedia]

総務省は2月1日、脆弱な設定のままインターネットにつながっており、サイバー攻撃に悪用される恐れのあるIoT(Internet of Things)機器を洗い出し、インターネットサービスプロバイダー(ISP)を介してユーザーに注意喚起を行う「NOTICE」(National Operation Towards IoT Clean Environment)という取り組みを発表しました。実際に調査を担うのは国立研究開発法人情報通信研究機構(NICT)で、2月20日から実施予定です。

政府によるIoT機器のセキュリティ調査「NOTICE」を周知するポスター=総務省のニュースリリースより

この取り組みを巡っては一部の報道で「無差別の侵入」と表現された他、ネット上でも「国がわざわざ、各戸のドアが施錠されているか確かめるのはやりすぎでは」「これを機に、なしくずし的に侵入範囲が広げられるのではないか」など、否定的な意見も上がりました。大半のユーザーにとっては「寝耳に水」の話ということもあり、不安に感じるのも無理はないでしょう。

実はこのNOTICE、2018年11月に施行された「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」を踏まえて準備が進められてきた取り組みで、決して突然浮上したものではありません。

けれど猶予があったにもかかわらず、「どのような法律の枠組みの下で、具体的にどんな調査が行われるのか」が十分に伝わっていなかった上に、「なぜ、こうした力業に訴えてでも対策を進める必要があるのか」についても、まだあまり認識されていないようです。今回はその背景を考察したいと思います。

連載:ITの過去から紡ぐIoTセキュリティ

家電製品やクルマ、センサーを組み込んだ建物そのものなど、あらゆるモノがネットにつながり、互いにデータをやりとりするIoT時代が本格的に到来しようとしています。それ自体は歓迎すべきことですが、IoT機器やシステムにおける基本的なセキュリティ対策の不備が原因となって、思いもよらぬリスクが浮上しているのも事実です。

この連載ではインターネットの普及期から今までPCやITの世界で起こった、あるいは現在進行中のさまざまな事件から得られた教訓を、IoTの世界に生かすという観点で、対策のヒントを紹介していきたいと思います。

MiraiとNOTICEの特定アクセス、何が違う?

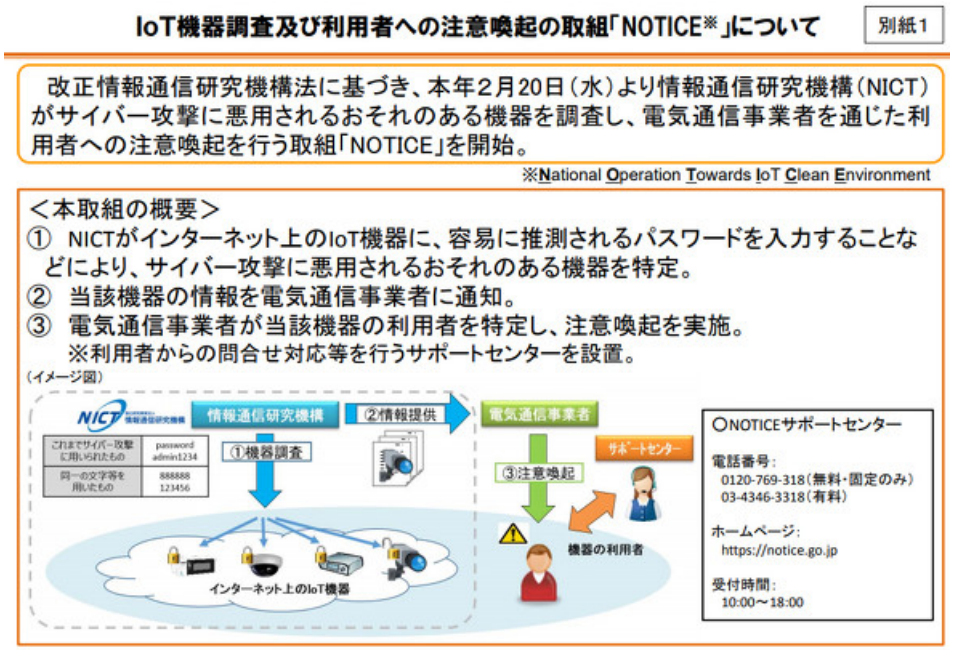
既にさまざまな報道で指摘されてきましたが、家庭用ルーターやWebカメラ、その他の組み込み機器やIoT機器の中には、脆弱な状態のままインターネットに接続されているものが少なくありません。

ここ数年、サイバー攻撃者はこうした機器を格好のターゲットと捉え、さまざまな形で悪用してきました。その最も有名な例が、IoT機器に感染してbot化し、他者に対するDDoS攻撃の踏み台にする「Mirai」です。そろそろ風化してきたきらいもありますが、Miraiが登場し、1Tbpsクラスという、文字通り「桁違い」の規模のDDoS攻撃が起きた際のインパクトは大きなものでした。

Miraiは、インターネットにスキャンをかけてtelnet、すなわちtcp/23ポートで接続可能な状態のデバイスを探索し、見つかると「admin」と「123456」「password」といったいくつかの安易なIDとパスワードの組み合わせでログインが可能かどうかを試しました。ログインに成功すればさらに別のマルウェアをダウンロードし、攻撃者の指令に応じて動く「bot」に仕立ててDDoS攻撃を実施します。

そう、この挙動だけ見れば、途中までは「NOTICE」において、NICTが行う調査活動、いわゆる「特定アクセス行為」の動きとそっくりです。

NOTICEの特定アクセスでは、まず約2億件に上る国内のIPv4アドレスに対して1日1回の間隔でポートスキャンを行い、サービスが公開され接続できる状態にあるかを確認します。そして公開ポートがあると判断した対象に対してのみ、容易に推測できたり、過去の攻撃に用いられたりしたIDとパスワードの組み合わせを約100通り入力し、ログインが成功するかどうかを試します。もし成功すれば、Miraiのようなマルウェアに感染するリスクが高い脆弱な機器と判断できるわけです。



NOTICEの概要＝総務省のニュースリリースより

しかし、その後は違うと説明されています。NOTICEの特定アクセスでもしログインに成功した場合は、機種特定のための情報とIPアドレス、タイムスタンプ、ポート番号を記録した上でそのまま退出します。そもそも機械的なアクセスのためグラフィカルユーザーインタフェース（GUI）にアクセスして機器の設定を変更したり、コンテンツや画像を盗み見たりといった操作は行いませんし、別途保存するログによってそのことを担保するといいます。もし、スキャン行為によって機器の動作に何らかの副作用が生じた場合にも、このログを基に調査できると期待したいところです。

他にも違いはいくつかあります。まずは目的です。NOTICEは、Miraiやその亜種のようなマルウェアに侵入される恐れのあるIoT機器を特定し、ユーザーに注意喚起を促し、対策を進めてもらうことを狙っています。ですからNICTでは特定ログインによって得た情報をISPに提供し、ISPから機器の利用者に設定変更やファームウェアのアップデートといった対策を取るよう注意喚起を行う流れです。いきなり「対策してください」とメールが来ても具体的にどうしたらいいか分からないユーザーのために、手順などを案内するコールセンターも用意します。

何より、Miraiなどのマルウェアは堂々たる（？）不正アクセスですが、NOTICEの特定アクセスは改正法によって、5年間の時限立法措置として、「不正アクセス禁止法」でいう不正アクセス行為から除外されることになります。

「特定アクセス」という力業に至った背景とは

けれど、わざわざNOTICEのような取り組みをする前に、IoT機器についても皆がセキュリティ対策をすればいいじゃないかーーといいたいところです。それが理想なのですが、なかなか対策は進んでいません。

PCの場合は「常に最新のアップデートを適用する」「安易なパスワードは設定しない」といった基本的なセキュリティ対策を認識し、実施する人が増えてきました。OSが搭載するセキュリティ機能や対策ソフトを活用すれば、ある程度攻撃を防

ぐことも可能です。

しかしIoT機器の場合、リソースの制約から対策が難しい上、こうした記事を積極的に読まない普通の人々にとっては「家電の延長」といった意識が強く、「セキュリティ対策を実施すべき対象」と見なされていないケースが多いのが実情です。今回のNOTICEに関する報道によって多少は危機感が伝わったかもしれませんが、それ以上に機器の絶対数の方が多く、インターネットにつないでいることすら忘れられている機器も少なくないでしょう。

しかも人間、自分に直接害が及ばない脅威については対策のスピードも鈍りがちです。仮にMiraiがランサムウェアのようにデータを暗号化し、利用できなくしてしまうマルウェアだったら、NOTICEのような取り組みがなくても対策が進んでいたかもしれません。けれど、手元の機器が感染した結果被害を受けるのが第三者、それも例えば海の向こうの事業者――となれば、なかなかすぐには手を打とうとはならないのではないでしょうか（PCのbot対策の場合も、「なぜ私がどこかの誰かのために対策しなければならないのか」を納得してもらうまでに時間がかかったと聞きます）。

その上、IoT機器の場合、分かりやすい管理インタフェースやアップデート機構が備わっているものばかりではありません。後述するように、古い機器の場合はそもそものパスワード変更すらできない仕様になっていることもあります。対策の必要性を感じても、実行が難しい場合があるのです。

ならばメーカー側に対策を求めるのがスジ、という声もあるでしょう。その通りですし、メーカー側もこの1～2年、設定や脆弱性対応に留意して機器を開発するようになってきました。

ただ、世の中に出回っているのは、こうしたセキュリティリスクが認識されてから出荷された新しい機器ばかりではありません。数年前に開発された古い機器もまた多数インターネットにつながっており、メーカーですら利用実態が分からないのが実情です。ユーザーの心情からいっても、壊れたわけでもない限り、機器は使い続けるものですよね。そんな、古いけれど現役の機器も含めて対策しなければ根本的な解決には至りません。これらへの対処や意識醸成も含めると、まさに、数年単位で取り組む必要があるといえるでしょう。

脅威は目の前に、いつ対策するかというと、今でしょ？

IoT機器のセキュリティ対策が難しいのはこうした背景があるからです。だからといって、対策をしないわけにはいきません。IoT機器に対する脅威が現に存在しているからです。

このことは、NICTが2月6日に発表した「観測レポート 2018」からも明らかです。NICTERの観測結果によると、この1年間で、1つのIPアドレスに対し約79万のパケットが届いたことになります。内訳を見ると、Telnet（23/TCP）を狙った攻撃パケット数は大きく減りましたが、その他のさまざまなポートを狙った攻撃パケットの比率が増えており、結果として「全体の約半数がIoT機器で動作するサービスや脆弱性を狙った攻撃」ということです。

年	年間 総観測パケット数	観測IPアドレス数	1 IPアドレス当たりの 年間総観測パケット数
2009	約35.7億	約12万	36,190
2010	約56.5億	約12万	50,128
2011	約45.4億	約12万	40,654
2012	約77.8億	約19万	53,085
2013	約128.8億	約21万	63,655
2014	約256.6億	約24万	115,323
2015	約545.1億	約28万	213,523
2016	約1,281億	約30万	469,104
2017	約1,504億	約30万	559,125
2018	**約2,121億**	**約30万**	**789,876**

図1. NICTERダークネット観測統計（過去10年間）

NICTが発表した「観測レポート 2018」より

この状況下でユーザーの善意に任せた対策を待っていては対応が遅れ、大きな被害が生じるかもしれません。第三者に対するDDoS攻撃も深刻な問題ですが、例えばドイツテレコムで発生したインシデントのように通信に大規模障害が発生したり、あるいは個人の情報やコンテンツが侵害されたり、破壊的な被害が生じてしまってからでは遅いのではないか――PCのbot対策時のように、マルウェア感染端末を特定した上で対処を依頼する方がスジだとは思いますが、感染していない機器も含めて調査するNOTICEが立ち上がった背景には、そんなのっぴきならない危機意識があるのだと思いま

す。

NICTは今後、特定スキャンの結果に基づいたポートの公開状況や、取り組みの効果を示せるデータをWebサイトで公表していく方針です。この枠組みが適切に運用されるのかを見守る意味でも、IoTボットの全体像を捉える上でも、またこの先何らかの事態が起きたとしても事実に基づいて対策する上でも注目したいところです（ちなみにNOTICEについてはこちらのPodcastが参考になります）。

蛇足ですが、もう1つ気になることがあります。この名前を悪用したさまざまな「詐欺」の登場です。フィッシング詐欺かもしれませんし、偽のセキュリティ警告を表示するアドウェア、電話による詐欺かもしれません。これらを防ぐための手だてもぜひ講じていただきたいところです。

関連記事

「政府がIoT機器に無差別侵入調査へ」　その方法は？　資料をチェック
政府がサイバー攻撃対策の一環として、国内のIoT機器に無差別侵入――こんな計画が物議をかもしている。計画の詳細は、公表された資料から読み解くことができる。

国によるIoT機器"侵入"調査、その名も「NOTICE」サイト公開　「不正アクセスではない」と理解求める
弱いパスワードを使ってIoT機器へのログインを試み、ログインできた機器のユーザーに注意喚起する試み「NOTICE」を、総務省が2月20日から始める。「国による事実上の不正アクセス行為では」といった批判もあるが……

史上最悪規模のDDoS攻撃　「Mirai」まん延、なぜ？
インターネットの普及期から今までPCやITの世界で起こった、あるいは現在進行中のさまざまな事件から得られた教訓を、IoTの世界で生かせないか――そんな対策のヒントを探る連載がスタート。

ソフトバンク障害は"他人事"ではない　デジタル証明書のヒヤッとする話
12月6日、ソフトバンクで大規模な接続障害が発生。原因は「デジタル証明書の有効期限が切れたため」。エンジニアの方々の中には、他山の石と捉える人が多かった印象です。

ITmedia Inc.