CIAJ セキュリティ Information

総務省：IoT 機器調査及び利用者への注意喚起の取組み
「NOTICE」の実施状況概要

2020 年 3 月 25 日

CIAJ 通信ネットワーク機器セキュリティ委員会

はじめに

現在、様々な産業分野において IoT 機器や関連システムの利用が進んでいます。しかし、インターネットの世界のセキュリティ事故、セキュリティ事件が絶えず、ますます猛威を振るっている状況です。安全安心なインターネット環境にしていくことが、大変重要になってきています。

総務省では、上記状況を踏まえて、NICT（国立研究開発法人情報通信研究機構）の業務にサイバー攻撃に悪用されるおそれのある機器の調査等を追加（5 年間の時限措置）するため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 日に改正法が施行されています。

上記改正法に基づき総務省及び NICT では 2019 年 2 月 20 日から、インターネット上の機器に対する脆弱性の調査及び当該機器の利用者への注意喚起を行う取組み「NOTICE（National Operation Towards IoT Clean Environment）」の運用を開始しました。また、6 月中旬に NICTER プロジェクトによりマルウェア（※）に感染していることが検知された機器に対して注意喚起を行う取組みの追加を行い、2019 年 6 月 28 日に実施状況の発表を行っています。その後、2019 年度第 2 四半期分の実施状況を 2019 年 10 月 25 日に、第 3 四半期分を 2020 年 1 月 28 日にそれぞれ発表を行っています。

本書は、NOTICE や NICTER による注意喚起取組の概要説明と、現在までの実施状況について紹介いたします。

（※）マルウェアとは、不正な動作をさせるための悪意あるソフトウェアの総称で、感染した機器は、データが改ざんされたり、消去されたり、意図しない動作をします。

NOTICE とは

2019 年 2 月に開始された NOTICE とはどのようなものなのか、簡単に説明します。

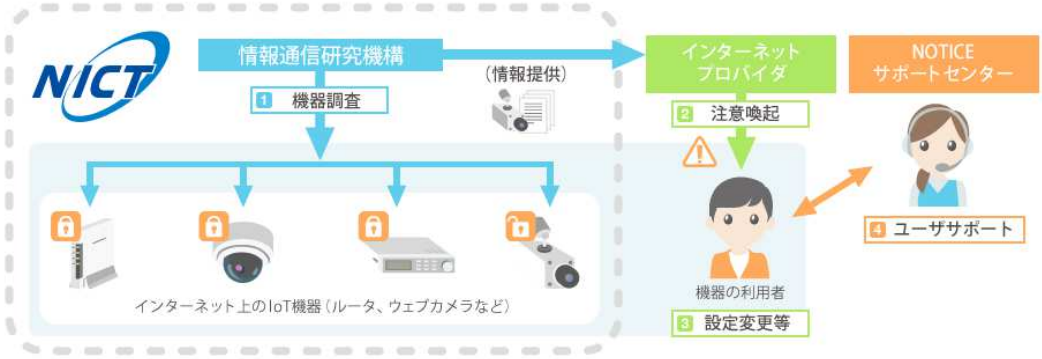
インターネットにつながっている機器、例えば、家庭で利用しているルータや、街中に設置されている IP カメラ等は、インターネットの「住所」にあたるグローバル IP アドレスを 1 つ、または、複数持っています。NOTICE では、このグローバル IP アドレスを持っている機器が対象となります。ちなみに、家庭内で、ルータ経由で接続する機器は、家庭内で閉じたプライベート IP アドレスを持っていますが、こちらは対象外です。

NOTICE では、このグローバル IP アドレスについて、約 100 種類のユーザ ID、パスワードの組み合わせでログインを試み、ログインできてしまう機器を脆弱性のある機器と識別しま

す。グローバル IP アドレスは、インターネットプロバイダに割り振られており、NOTICE に参加しているインターネットプロバイダの機器を対象としています。

脆弱性があると識別された機器は、そのグローバル IP アドレスを管理するインターネットプロバイダに通知され、さらにそこから、機器の利用者に設定変更等の注意喚起が行われる仕組みになっています。

NOTICE では、ホームページで取組みの紹介やよくある質問を掲載し、電話サポートが必要な利用者には NOTICE サポートセンターで問い合わせできる取組みも行っています。

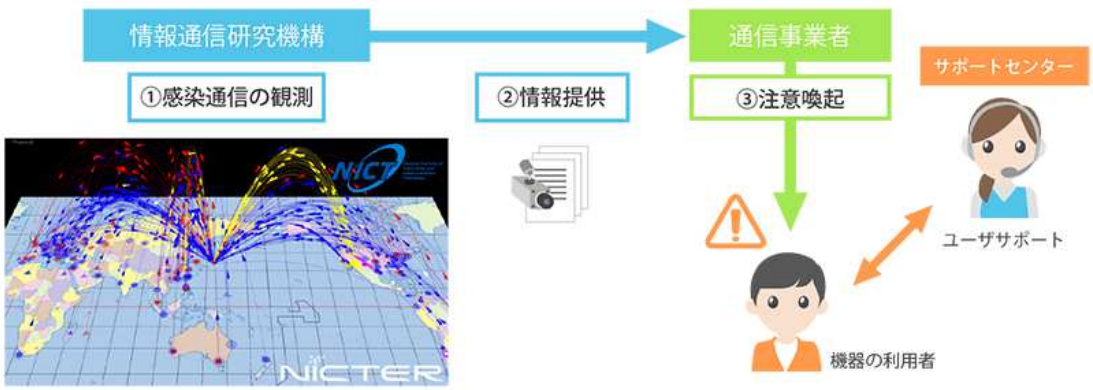


(出典：NOTICE ホームページより　https://notice.go.jp/)

NICTER プロジェクトとは

2019 年 6 月中旬より追加で開始された注意喚起の取組みにおいて活用されている NICTER プロジェクトとはどのようなものなのか、簡単に説明します。

NICTER プロジェクトでは、インターネット上のサイバー攻撃観測・分析システムを用いて、サイバー攻撃の大規模観測を実施しています。その対象は NOTICE と同様にグローバル IP を持った機器になります。その中で、既にマルウェアに感染している機器を特定し、利用者に対して注意喚起を行います。注意喚起、サポートセンターは NOTICE と同様に行われています。



(出典：NOTICE ホームページより　https://notice.go.jp/nicter)

NOTICE の実施状況

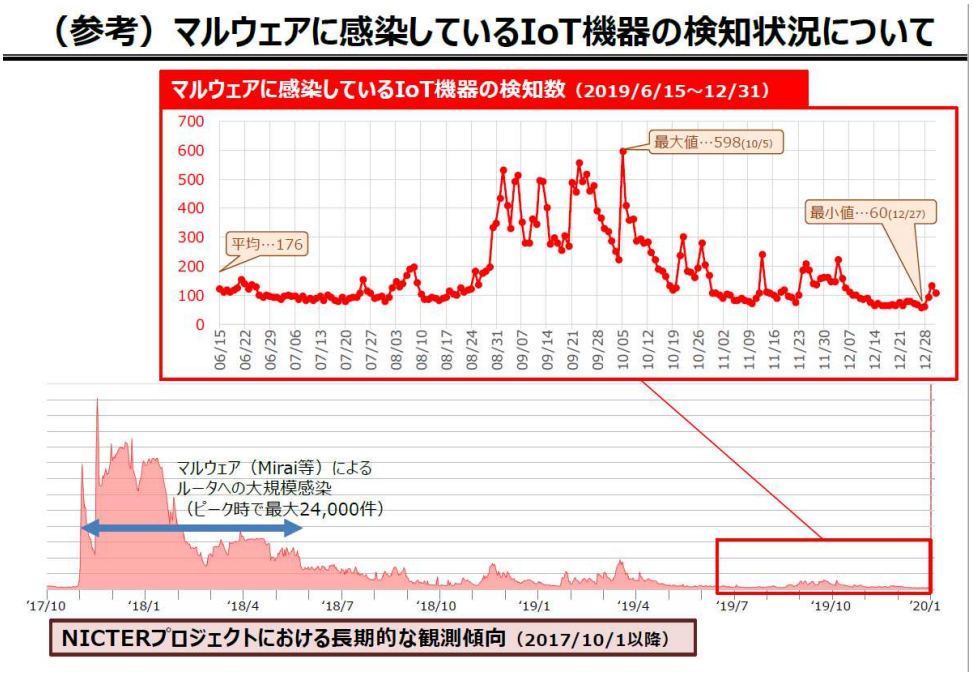
2019 年 6 月、10 月、2020 年 1 月に総務省から発表された実施状況を紹介します。

調査対象となったグローバル IP アドレスは、6 月時点においてインターネットプロバイダ 33 社で合計約 9 千万個、9 月時点においてインターネットプロバイダ 34 社で合計約 1.0 億個、さらに 12 月時点ではインターネットプロバイダ 41 社で合計 1.1 億個のアドレスまで増やされています。毎月 1 回程度の全数調査を行い、結果は以下になります。

No	項目	2019 年 6 月	2019 年 10 月	2020 年 1 月
(1)	ID、パスワードを入力可能な機器	約 42,000 件	約 98,000 件	約 111,000 件
(2)	No(1)のうち、ログインできた機器 ＝注意対象となった機器	延べ 147 件	延べ 505 件	延べ 1,328 件
(3)	NICTER によりマルウェアに感染していることが検知され、インターネットプロバイダに通知された機器(1 日あたり)	112～155 件	80～559 件	60～598 件

(1),(2)の件数が増えていますが、これは、参加プロバイダの増加に伴う調査対象グローバル IP アドレスの拡大、また、調査対象ポートの追加によるもので、脆弱な機器の割合については大きな変化はないと考えられています。

(3)も件数が増えていますが、長期的に見ると過去に数千件、数万件の時期もあり、数百件という数字は、大規模感染といった状況ではないと考えられています。



（出典：総務省　脆弱な IoT 機器及び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実施状況（2019 年度第 3 四半期）
https://www.soumu.go.jp/main_content/000665799.pdf）

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又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ています。しかしながら、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ため、利用者においては引き続き以下の適切なセキュリティ対策の徹底に努めることが重要とされています。

・最新のファームウェアに更新をする。

・適切な ID、パスワードの設定を行う。

総務省では、こうした実施状況を踏まえながら、NOTICE や NICTER による注意喚起の取組みを継続して行い、IoT 機器のセキュリティ対策の向上に取り組んでいくとのことです。

また、CIAJ も、インターネット、IoT を構成する通信ネットワーク機器提供者の業界団体として、適切なセキュリティ対策機能の提供を考察しています。そこで、当該機器ユーザを対象に、通信ネットワーク機器のセキュリティ対策機能の取り扱いに関して、その必要性をご理解いただき、適切な設定/運用を実施頂くため、「通信ネットワーク機器セキュリティ・ユーザーガイドライン」を策定しています。本ガイドラインでは、通信ネットワーク機器特有のセキュリティ対策も紹介されていますので、ご参照ください。

著者

CIAJ 通信ネットワーク機器セキュリティ委員会

【参考文献】

・総務省報道資料

○IoT 機器調査及び利用者への注意喚起の取組「NOTICE」の実施（2019 年 2 月 1 日）
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00011.html

○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の実施（2019 年 6 月 14 日）
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00025.html

○脆弱な IoT 機器及び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実施状況（2019 年 6 月 28 日）
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00033.html

○脆弱な IoT 機器及び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実施状況（2019 年度第 2 四半期）（2019 年 10 月 25 日）
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00043.html

○脆弱な IoT 機器及び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実施状況（2019 年度第 3 四半期）（2020 年 1 月 28 日）
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00058.html

・CIAJ 発行資料

○「通信ネットワーク機器セキュリティ・ユーザーガイドライン Ver.1.0」の発刊（2019 年 3 月 29 日）
https://www.ciaj.or.jp/common_issue/technical/guidelines_v1.html