第1章　はじめに

ケーブル業界では、インターネットサービス加入者が 900 万世帯を超えており、同時にスマート家電等の普及により多くの IoT 機器が宅内につながり、ネットを介し機器、アプリ、サービスが相互接続する環境となってきた。お客様に寄り添うべきケーブル事業者は、安全・安心なインターネット環境をお客様に提供しながら、これら宅内の IoT 機器も外部のセキュリティ脅威から守っていかなければならない。

実際の脅威としては、たとえば IoT 機器を狙うマルウェアである“Mirai”がある。Mirai は通常のマルウェアと同様に、いくつかの経路で侵入を試み、「辞書攻撃」と呼ばれるサイバー攻撃を仕掛けた上で対象の IoT 機器に侵入し、その制御を乗っ取る。その後、Mirai は、感染した IoT 機器を使って巨大な「ボットネット」を形成し、「C&C サーバー」として指示を出すことで、DDoS 攻撃に移行する。ネットワークカメラや家庭用ルータといった家庭内のオンライン機器（IoT デバイス）を主要ターゲットとしている。

このようなセキュリティ脅威に対処するための公的な動きとして、NOTICE や NICTER がある。

(1) NOTICE（National Operation Towards IoT Clean Environment）

「NOTICE」は、総務省、国立研究開発法人情報通信研究機構（NICT)、およびインターネットプロバイダが連携し、2019 年 2 月に開始された。パスワードが初期設定のままでマルウェア感染などの危険性のある脆弱な IoT 機器の把握と、その機器の利用者に設定確認などの注意喚起を行うことが目的である。

総務省が 2019 年 6 月に発表した「NOTICE」プロジェクトの実施状況によれば、国内約 2 億の IP アドレスのうち、約 9,000 万アドレスに対してポートスキャンを行い、接続可能かつ認証要求のあった機器について、過去のサイバー攻撃などに用いられた 100 通りの ID とパスワードの組み合わせを使ってログインを試行した。

その結果、

・ID とパスワードが入力可能だった IP アドレスは約 3 万 1000～約 4 万 2000 件

・このうちログイン試行の状況から注意喚起の対象となったアドレスは延べ 147 件

・ISP への通知対象になったアドレスは 1 日平均 112～155 件

という結果が得られ、対象利用者への注意喚起が 6 月に開始された。「NOTICE」は今後 5 年間継続する予定となっている。

(2) NICTER（Network Incident analysis Center for Tactical Emergency Response）

NICT のネットワークセキュリティ研究所が開発した、攻撃トラヒックの観測／分析システムで、インターネットを流れるトラヒックに基づいたマクロ的な解析と、マルウェア分析