サイバーデブリ、IoT普及の壁に

ネットに接続、放置の機器 犯罪の温床、官民で対策

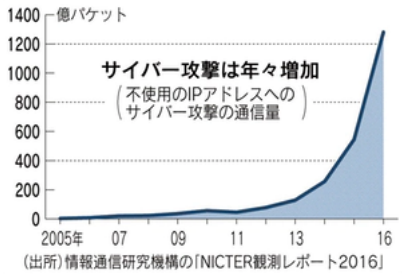
日本経済新聞　朝刊
2018年1月21日 2:30 ［有料会員限定］

あらゆるモノがネットにつながる「IoT」が広がるなか、ネットに接続したまま放置された機器「サイバーデブリ（ごみ）」がウイルス感染や犯罪の温床となる危険性がでてきた。IoT機器が攻撃され、SNS（交流サイト）の接続が途切れた米国の事例もある。IoT普及の足かせともなりかねず、官民での対策が必要になっている。

冷蔵庫などの家電やメガネ、産業機器やごみ箱――。様々なものがネットにつながればビジネスも暮らしも便利になると期待される。調査会社IHSテクノロジーによるとIoT関連の機器は世界で2020年に530億個に達する見通しだ。

IoT機器が犯罪者に狙われている

だがIoT機器は犯罪者の標的になっている。情報通信研究機構（NICT）は2017年12月中旬、IoT機器を狙うサイバー攻撃が日本国内で急増していると明らかにした。16年秋に世界で猛威を振るった「ミライ」と呼ぶコンピューターウイルスを改変した亜種が活動しているという。



（出所）情報通信研究機構の「NICTER観測レポート2016」

ミライはIoT機器から別のIoT機器へ自動的に感染する。16年の攻撃では米ネットフリックスなどのサービスが一時的につながらなくなり約40万個が感染したとされる。米マカフィー日本法人（東京・渋谷）のスコット・ジャーカフ氏は「ミライに感染したIoT機器の多くはパスワードが適切に設定されておらず、管理が行き届いていない」と指摘する。

こうした無防備な機器がサイバーデブリ。使わなくなったネットワークカメラやウエアラブル端末も今後は増えるとみられる。NICTによると使われていないIPアドレスへのサイバー攻撃の通信量のうち、IoT機器を狙う攻撃が前年比約3倍のペースで増えている。ウイルス感染すると監視カメラが乗っ取られたり医療機器やエンジンが動かなくなったりする可能性もある。

こうした現状を受け、総務省はIoT機器のセキュリティー対策に本格的に乗り出す。来年度の予算要求で一定の要件を満たした機器に認証マークを付与し、事業者間で情報を共有できる仕組みを構築する。

日本の法制度ではセキュリティー対策の費用を誰が負担し、責任を取るか明確でない。サイバーデブリから大規模攻撃が起こった場合、被害者が救済されない恐れもある。NTTコミュニケーションズの境野哲氏は「セキュリティー対策は民間企業だけでは到底無理だ」と話す。「重要インフラなどIoTのサービスごとに段階を分け、どれくらいの対策を実施し料金がかかるのかを決める必要がある」と言う。

官民のIoT対策は欧米が先行する。ドイツでは電力などのインフラに使うIoT機器に最新の対策が義務付けられ、罰金もある。シーメンスなどはIoTのセキュリティーの標準化を視野に入れているとされる。

情報セキュリティ大学院大学の後藤厚宏学長は「日本の事業者にIoTのセキュリティーでいちはやくデータやノウハウを蓄積してほしい」と話す。爆発的に増えるIoT機器は次の産業を生み出すきっかけともなる。安全面の対策がおざなりのままでは成長する市場のブレーキになりかねない。

（大西綾）