日本経済新聞

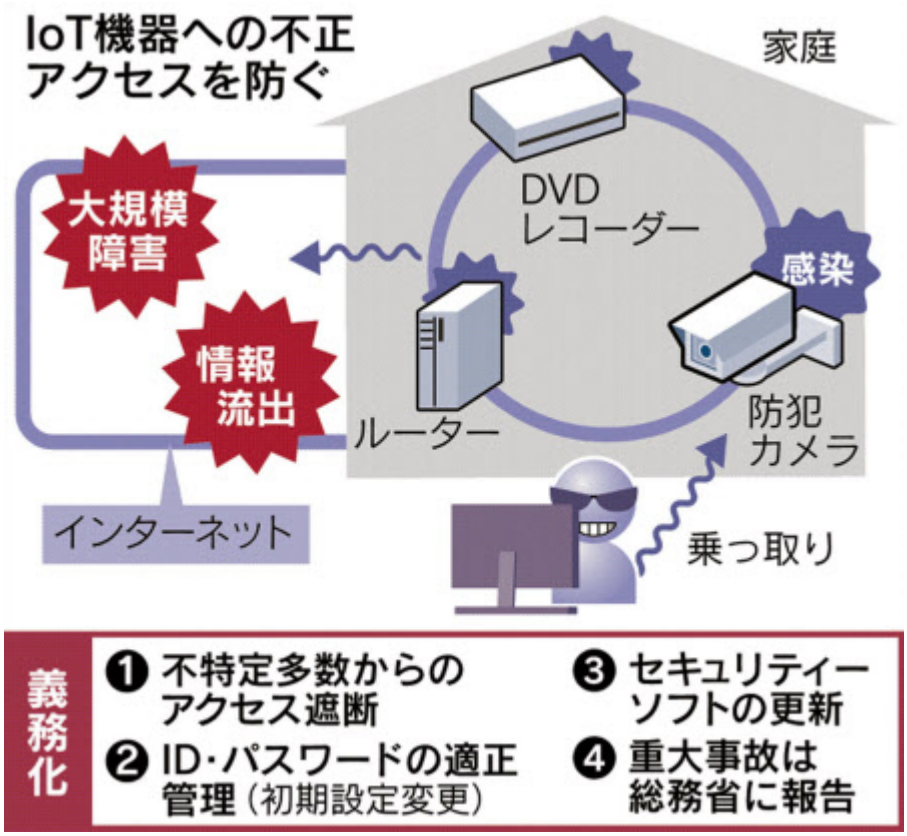
IoT機器、防御を義務化　サイバー攻撃入り口封じ
【イブニングスクープ】

2019/1/31 18:00｜日本経済新聞　電子版

総務省はあらゆるモノがネットにつながる「ＩｏＴ」の普及を踏まえ、端末機器に不正アクセスを防ぐ機能を設けることを義務付ける。2020年４月から適用する。ＩｏＴでは無数の機器がネットにつながり、大規模な障害を生む不正アクセスの入り口になりかねない。ネットを通じて連鎖するサイバー攻撃のリスクは飛躍的に増しており、対策を徹底する。

■ソフトやパスワード更新促す

電気通信事業法に基づいて端末機器の技術基準を定める省令を改正し、ＩｏＴ向けのセキュリティー対策を盛り込む。不特定多数からのアクセスを遮断する制御機能と、ＩＤやパスワードの初期設定の変更を促す機能、ソフトウエアを常に更新する機能を求める。基準を満たすと認定される機器だけが販売できる。



ＩｏＴでは街角の防犯カメラや家庭の家電など膨大な機器がインターネットでつながる。どれか１台でも乗っ取られればウイルスが拡散し、電力や交通機関などのインフラに影響を与える恐れがある。パソコンやスマートフォンなど特定の機器がネットにつながる現状よりも、対策を一段と強めなければならない。

総務省が対策を義務付ける対象はネットにつながる防犯カメラやＤＶＤレコーダー、ルーターなどだ。防犯カメラなどはパソコンと違って普段は人が操作しないため、ウイルスに感染しても気づきにくい。

不正アクセスを受けて障害が起きた場合に、すぐに把握して対応するためのルールも設ける。「３万人の利用者に12時間以上」もしくは「100万人に２時間以上」の障害があった場合、ＩｏＴサービスを展開する通信事業者に「重大事故」として総務省に報告させる。従わない場合は行政指導などをする。電気通信事業法の施行規則を今春に改正する。

これまでのセキュリティー対策は民間の自主的な対応に委ねてきた。通信網の一部にでもサイバー攻撃を許す穴があると、被害が一気に拡大する。総務省は法令で安全対策を徹底する必要があると判断した。

■利用者に注意喚起も

世界ではすでにマルウエア（悪意あるプログラム）による大規模な通信障害が起きている。

16年には米国で防犯カメラなど10万台以上の機器が感染して、米ツイッターや米ネットフリックスなど大手のサイトが長時間アクセスしにくくなった。ドイツでも家庭用ルーターへのサイバー攻撃でネット障害が起きた。スウェーデンでは17年に交通当局のシステムがマヒし、列車の運行停止・遅延が生じた。

既に企業や家庭にある機器の対策にも乗りだす。情報通信研究機構（東京都小金井市）が２月から、セキュリティーに不備のある端末を洗い出す。端末にひもづくネット上の住所（ＩＰアドレス）に対し、簡単なパスワードでアクセスできるようになっていないか接続を試みる。

不備のある機器は通信事業者を通じて利用者に注意喚起する。ＩｏＴ機器の設定操作に不慣れな一般ユーザーが少なくないと考えられるため、パスワード変更の仕方などを教える相談窓口も新設する方針だ。