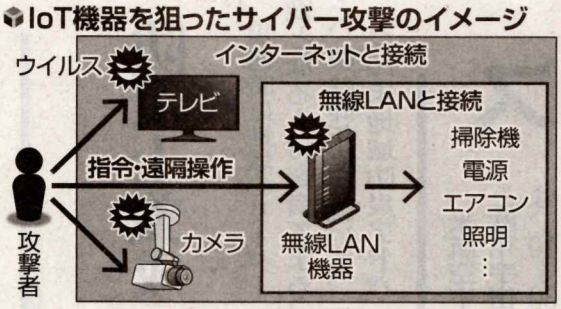
狙われるサイバー空間 5

ウイルス 家電も破壊

ネットワーク化 新たなリスク

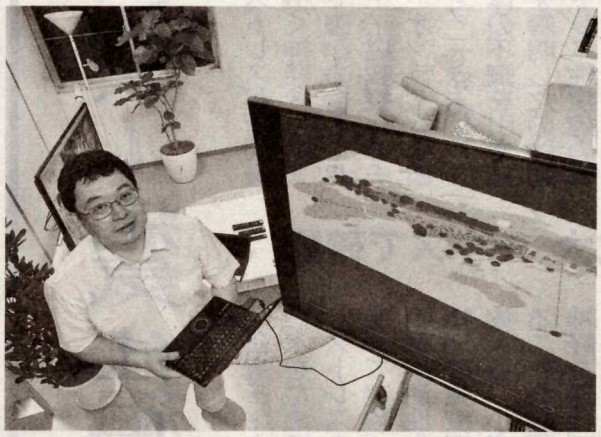


150か国で感染

「攻撃は前例のないものだった」。英ロンドン市内で病院を運営する医療グループ「バーツ・ヘルス・トラスト」の担当者は読売新聞の取材にこう答えた。

5月12日午前11時58分、異常は突然現れた。グループ病院の一つで、機器がサイバー攻撃を受けたとの一報があり、病院側は7分以内にすべてのネットワークの遮断を開始。しかし、約1万2000台あるパソコンの17%とサーバー2台がダウンし、407件の手術を延期せざるを得なかった。

世界中を震撼させたランサム（身代金）ウェアと呼ばれるウイルス「WannaCry（ワナクライ）」。インターネットや社内LANなどを通じ、数日間で150か国、30万台の機器が感染した。日本でも、日立製作所でメールシステムに障害が発生。茨城県日立市の日立総合病院も被害を受けた。翌月には、ホンダの国内外の工場で生産を管理・制御するパソコンが同種のウイルスに感染し、国内の工場の一部で一時操業を止める事態となった。



IoT機器を集めた実験室で、世界各地からの不審な通信をモニターする吉岡准教授（横浜市の横浜国立大で）

今回の被害が世界中で爆発的に広がったのは、ウイルスがネットワーク内を勝手に動き回り、メールの添付ファイルなどを開かなくても、最新の状態に更新されていないパソコンなどを次々と感染させたためだ。

情報セキュリティー会社マカフィーの佐々木弘志氏は「工場などの制御システム自体が大丈夫でも、そこにつながった管理・監視機器などが攻撃されれば、何かしらのダメージが生じる」とし、こう警告する。

「あらゆるものがネットワーク化された時代の新たなリスクだ」

目に見える被害

「ウイルス感染させたWi-Fiルーターに攻撃指令を出します」。学生がパソコンを操作した。スマートフォンで遠隔操作できる電源につながった照明が消える。「無線LANにつながっている機器は遠隔操作される恐れがあるんです」

横浜国立大と民間企業が合同で6月、同大に開設した実験室。一般家庭のリビングを再現し、ネットにつながったゲーム機やカメラ、テレビのほか、スマホで操作できる掃除機など、20種類の市販機器が並ぶ。そうした機器を誤作動させるサイバー攻撃について研究している。

家電製品など生活のあらゆるものがネットにつながる「IoT」。実験室で研究する同大の吉岡克成准教授は今年1月、これまで見たことのないタイプのウイルスの出現に気が付いた。ウイルスを市販の機器に感染させてみると、電源が入らず、機器のプログラムが破壊されていた。IoT機器に感染して他の機器に攻撃を仕掛ける従来のウイルスとは違い、感染した機器自体を壊す能力を持っていた。吉岡准教授は、「これまでの攻撃とは明らかに目的が違う。新たな脅威が広がりをみせている」と危機感をあらわにする。

従来はパソコンなどの情報を狙うケースが多かったサイバー攻撃が、形態を巧妙化させている。あらゆるものがネットでつながり、病院や工場の稼働を止めたり、日常生活で使う家電を誤作動させたりと、目に見える被害を生じさせられる時代になりつつある。情報流出や単なるいたずらにとどまらず、重要インフラを狙うテロや人的被害にもつながりかねない。

吉岡准教授はこう指摘する。「現状は、玄関の前まで泥棒が来ているのと同じ。鍵を開けられ、侵入される前にどんな対処ができるか、データの蓄積や対策を急がなければならない」

（おわり。村山誠、大沢帝治、田中洋一郎が担当しました）

IoT Internet of Things（モノのインターネット）の略。家電や自動車、医療機器、工場のセンサーなど、あらゆるものがネットにつながり、遠隔操作や情報収集ができるようにする仕組み。情報通信白書によると、2015年にIoT機器は全世界に154億個あり、20年までに304億個に増える見込み。