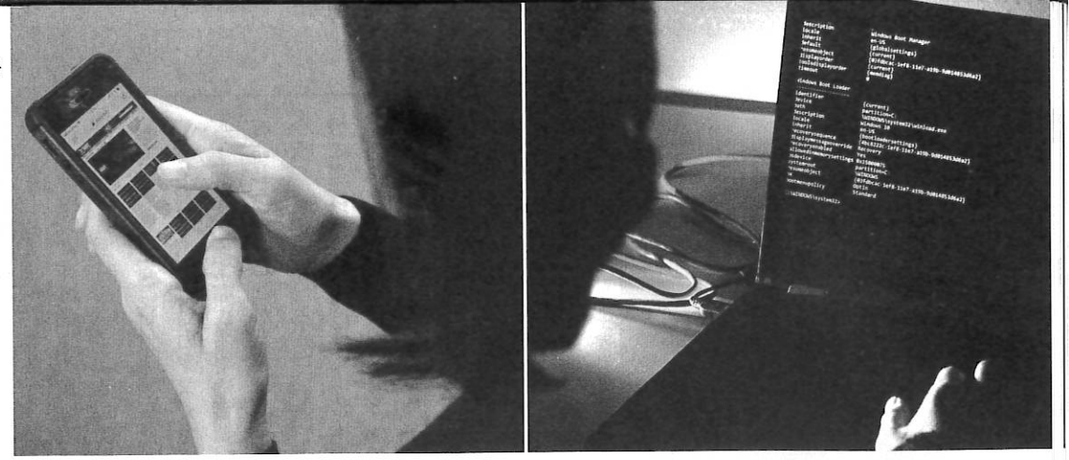
世界中の悪玉国家が「顧客」に

「監視・盗聴」ハイテク企業が大繁盛



需要増にあわせて業界全体が隆盛に

十月、中東バーレーンの反体制派活動家ら四人が、英国の有名サイバー系企業を訴えることが明らかになり、話題となった。

反体制派側の訴えによれば、四人が二〇一一年の「アラブの春」に参加した報復として、バーレーン政府は彼らに厳しい弾圧を続けてきたという。そして、政府が行動を徹底的に監視するために使っていると名指しされたのが、英国企業のガンマ・グループが販売しているスパイウェア(監視ソフト)だった。

ガンマがバーレーン政府に販売したとされるスパイウェア「フィンフィッシャー」は、世界的に悪名高い。これまでも各地の国家による弾圧に手を貸していると指摘されてきた。バーレーンのケースでは、反体制派だけでなく、ジャーナリストや弁護士なども重点的に監視対象にされているという。

セキュリティ業界では、世界にはいくつもの監視システムを開発・販売しているメーカーが存在し、水面下で独裁国家などを支えている実態はよく知られている。そして今回、バーレーンの反体制派らが同社を訴えたことで、改めてスパイウェア業界にスポットライトが当たっているのだ。

日本の公安調査庁も興味

ガンマのフィンフィッシャーを秘密裏に導入してきた国は数多い。判明しているだけで、エジプト、ヨルダン、サウジアラビア、カザフスタン、トルクメニスタン、バングラデシュ、インドネシア、トルコ、スペイン、イタリア、ベルギーなどがある。同社から流出した内部文書によれば、こうした国の警察当局や情報機関などが監視システムを利用しているという。

フィンフィッシャーは、インターネットが人々の生活に深く根付いている近年、クリックだけで徹底した監視を可能にする現代の「秘密警察」のようなものだと言える。このシステムは、パソコンやスマホのユーザーが導入しているセキュリティソフトを飛び越えてマルウェアをインストールし、標的のデバイスに「侵入」する。そしてユーザーのキーストロークを記録し、会話を盗聴したり、電子メールを窃視したりでき、さらにデバイスを監視カメラや盗聴器のように自在に不正操作できてしまう危険なソフトだ。しかも操作性も良く、利用者に優しい「ユーザーフレンドリー」なシステムとして知られている。

実は最近、こうした監視システム業界は成長が著しく、今後も拡大が見込まれている。欧米のセキュリティ専門家によれば、「いま、スパイウェア業界は『ゴールドラッシュ』状態にあると言っていい」。事実、監視システム業界は一四年に二億五千百万ドル(約二百八十億円)規模だったが、二二年には三十三億ドル規模に膨れ上がると予測されている。

世界ではガンマ以外にどんなスパイウェア企業が暗躍しているのか。例えばガンマと並んで知られている企業に、イタリアの「ハッキング・チーム」がある。フィンフィッシャー同様、徹底した監視に使われる同社のシステムは、遠隔で操作ができる「Galileo(ガリレオ)」「Da Vinci(ダ・ビンチ)」などとイタリアらしい名前が付けられている。内部資料によれば、独裁的なロシアやウズベキスタン、ベネズエラなどが顧客リストに挙がっており、米CIA(中央情報局)も同社のスパイウェアを購入している。

実は日本の公安調査庁も一五年にこのシステムに興味を示していた。公安関係者によれば、「職員が東京都内で製品の説明を受けていたのは事実だが、結局導入はされていない」と言う。またお隣の韓国も、国家情報院が「5163部隊」という偽名を使って、このスパイウェアを購入していた。「韓国の国情院はメッセージングアプリの『LINE』を監視できると豪語している」(公安関係者)と言うが、韓国製アプリであるカカオトークなどもハッキング・チームのシステムで監視していた。

そのほか、英軍事・セキュリティ企業のBAEシステムズはデンマークの子会社を通じて人権蹂躙で批判されているアラブ諸国にスパイウェアを販売している。サイバーセキュリティ先進国と言われるイスラエルにはNSOグループをはじめいくつかのスパイウェア企業があり、強権的とも言われるメキシコやニカラグア、マレーシアなどが顧客だと暴露されている。

イタリアには「ラクシア」「RCSラボ」という企業があり、ドイツには「ウルフ・インテリジェンス」というスタートアップ企業もある。インドにも「アグラヤ」と呼ばれる怪しい企業がある。

規制のない無法状態

こうした企業の顧客は、なにも国の治安や情報当局だけではない。英テレコムやバークレイズ銀行、ドイツ銀行、高級ブランドのグッチなども導入していたことが判明し、顧客の調査などに利用されてきたと見られている。世界的に、政府による監視から、民間企業の調査活動まで幅広くスパイウェアが使われているというわけだ。

もちろん、こうした監視ソフトは合法的に節度を持って事件捜査や調査などで使われる分には有効だろう。ただ現実には強権国家がバレないように導入しているというのが実態だ。前出の公安関係者は、「こうしたシステムに対する規制は世界的にもなく、無法状態にある」と指摘する。

今年十月二日、イスタンブールにあるサウジアラビア総領事館で、サウジアラビア人記者が殺害された事件は記憶に新しい。いまだにトルコが情報を小出しにするなど、米CIAを絡めてサウジアラビアを刺激しているが、この事件はトルコ政府によるサウジ総領事館やその関係者らに対する監視活動がなければ、ここまで大事にはならなかったと言えよう。

トルコは、フィンフィッシャーだけでなく、ハッキング・チームのシステムも導入している。さらに別のハッキング手法を複数駆使してデバイスに侵入している形跡も発見されている。トルコはこれまでも、例えば一六年のクーデター未遂事件では米国亡命中のイスラム教指導者ギュレン師のシンパらを監視し、粛清してきた実績がある。

こうした監視システムを駆使して、サウジアラビア人記者の殺害の顛末を、トルコ当局はつぶさにモニターして記録することができた。そして同じイスラム教スンニ派の国として歴史的にもライバル関係にあるサウジアラビアの評判を、世界的に貶めることに成功したと言える。監視システムがトルコのような国家にとって、いかに有効なツールであるのかが証明されたわかりやすい事例だろう。

すでに世界中の治安・情報当局で常識となっているスパイウェアだが、多くの国がトルコのケースを興味深く観察しており、こうした監視システムが今後さらに広く利用される可能性は高い。システム自体もさらにステルス性が高くなり、巧妙化していくことが予想されている。日本でも、実は誰かが密かに監視を始めているかもしれない。