日本企業は「機密情報」盗まれ過ぎ

サイバー攻撃「スパイ天国」の惨状

二〇二〇年に入ってから、相次いでスパイ工作事件が明るみに出ている。

最初に話題になったのは、日本が誇る先端技術の大手メーカー、三菱電機。サイバー攻撃によって、自社の持つ情報だけでなく、同社が付き合いのある内閣府や防衛省、原子力規制委員会、資源エネルギー庁などの官公庁に加えて、重要インフラを担う電力や通信会社、JRや私鉄などの情報も盗まれた可能性が指摘された。

このニュースのすぐ後、今度はソフトバンクがロシアのスパイ活動の餌食となっていたことが発覚。元社員が次世代通信システムの5Gに関連する機密情報をロシア人スパイに渡していたとして起訴された。KGB時代から科学やテクノロジー分野のスパイ工作を担ってきたスパイ集団が暗躍していたとされる。

さらにNECや神戸製鋼所なども サイバー攻撃に晒されていたことが相次いで発覚した。もっとも、こうしたケースはたまたま表面化しただけで、日本に対するスパイ工作のほんの一端に過ぎない。国防やインフラなど日本の機微情報が、多層的な手法で盗まれ放題となっているのが実情だ。

NEC顔認証システムも被害に

NECのケースでは、サーバーに不正アクセスがあったことが発表されたが、同社は「情報流出などの被害は確認していない」と語っている。物は言いようだが、実際には情報が流出したかどうかも把握できていないのだ。

日本に進出している国外のサイバーセキュリティ企業の幹部は、「過去十年以上にわたって日本の軍事やインフラ、先端技術などを担う大手民間企業は軒並みサイバー攻撃などによるスパイ活動の餌食になっている。大手企業が本当に、今になってようやくそれに気がついたとしたら間抜けにもほどがある」と指摘する。

また、こんな戦慄の事態が水面下で起きているとも証言した。NECが力を入れている先端技術の顔認証システムが、中国政府系ハッカー集団にサイバー攻撃で盗まれてしまっているというのである。

NECの顔認証システムは、二〇一九年に米国国立標準技術研究所(NIST)による顔認証技術のベンチマークテストで世界一位の評価を得るほどレベルが高い。中国側からしてみれば、喉から手が出るほど欲しい技術だ。

中国は、サイバー攻撃などを駆使したスパイ工作で世界から先端技術を盗んで国内企業を成長させてきた過去がある。有名なのは一〇年に発覚した中国政府系ハッカーらによるグーグルへのサイバー攻撃で、ハッカーらはグーグル検索のソースコードを盗んで、中国の検索エンジン「百度」に提供したと言われている。

さらに憂慮すべきは、NECの顔認証システムが七月に開催予定の東京オリンピックで使われる事実である。NECの技術が、約三十万人の大会関係者が会場に出入りするのを管理する。

国外のサイバーセキュリティ企業関係者たちはこれまで、中国のハッカーらが東京オリンピックを妨害するためにサイバー攻撃による工作を仕掛けるだろうと警鐘を鳴らしている。中国政府系ハッカーらにしてみれば、史上最もハイテクな大会を喧伝する東京オリンピックで日本が失態を晒せば、ライバル国である日本の評判を落とすことができる。もちろんシステム構造を盗み取ったNEC顔認証システムも格好の攻撃ターゲットとなる。

こう見ていくと、問題はもはや日本がスパイ活動の格好の標的になっていることではない。それよりも、スパイ活動の主流がサイバー攻撃になるにつれ、盗まれた側が、何を、いつ盗まれたのかもよくわからなくなっていることだ。

そもそも、三菱電機は社内の八千人分ほどの個人情報(社員や退職者、就職志願者)や社内情報が流出した恐れがあると発表しているが、本当はどこまでの情報が盗まれているのか把握していない可能性が高い。事実、三菱電機は軍事やインフラの情報が漏れていないと発表した後、防衛機密情報が流出した可能性に気が付いた。結果的に、被害の全容を把握していないことを露呈した。

取り締まる法律が存在しない

日本の技術系大手企業を狙うのは圧倒的に中国政府系ハッカーが多い。中国のハッカー組織は二〇〇〇年頃から、先進国の政府や軍、大手民間企業を広範囲に攻撃してきた。米国では政府機関や軍部、民間企業まで中国からの執拗な攻撃が報告されているが、日本でこれまで表面化したものを挙げると、三菱重工業や日立製作所、日本年金機構など、数は多くない。これは明らかに不自然で、単に被害を把握できていないだけというのがもっぱらの評判である。

NECのケースも然りだ。同社が今回、サイバー攻撃を受けていた事実を発表した理由は、一八年に社外からサイバー攻撃を受けていると指摘されたからに過ぎない。結局、独自にはサイバー攻撃を受けたことも、自社の看板技術である顔認証システムのプログラムが盗まれていることも気が付かないのである。

官民揃って意識が低く脇が甘い

敵国からのスパイ工作は、こうしたサイバー攻撃によるものだけではない。サイバー攻撃のような電子的な活動とヒューミント(人によるスパイ活動)を合わせたハイブリッドな工作が行われている。今回の三菱電機はその典型だ。

技術大国を目指す中国は現在、技術者などの人材を国外から集めようとしている。三菱電機から入手した社員や退職者、就職志願者の情報をもとに、中国の技術系企業に取り込もうとスパイ工作を実施することは間違いないだろう。

またソフトバンクのケースもハイブリッドな活動だと言っていい。捜査関係者によれば、ロシアのスパイは街で偶然ソフトバンク元社員と知り合ったということだが、諜報活動の現場では偶然などというものは存在しない。サイバー攻撃などで周到に標的企業の内部情報や個人情報を集めて分析し、対象を絞ってから接触を試みる。そこから居酒屋などで親しくなり、金銭を渡して情報を企業から持ち出させる。サイバー攻撃からヒューミントに繋がるパターンだ。

残念ながら、日本にはこうしたスパイ活動を取り締まる法律が存在しないため、やられ放題になっているのが現実だ。

自民党は、情報を提供してくれる米国の要請もあって、何度かスパイ活動自体を犯罪とする、いわゆる「スパイ防止法」を作ろうとしてきたが、野党の反発でことごとく失敗してきた過去がある。それでも、一四年に情報をスパイなどに盗まれないようにするために、なんとか特定秘密保護法を施行して米国側へのアピールはできたが、スパイ活動の防止に役立っていないことは、ここ数件のケースだけ見ても明らかだ。

日本が「スパイ天国」という汚名を返上することは、当分の間できないだろう。前出の捜査関係者は言う。「国が震撼するくらいの事件が起きなければ日本は目が覚めないだろう」。