在宅勤務に3つの脅威　サイバー攻撃にどう備える

2020/7/27 2:00 | 日本経済新聞　電子版

NIKKEI BUSINESS DAILY 日経産業新聞

新型コロナウイルスの感染拡大が長期化するなか、多くの企業が在宅勤務向けのIT（情報技術）環境の見直しを模索し始めている。ただ、4月の緊急事態宣言の前後にオフィスから在宅勤務に急きょ切り替えた結果、サイバー攻撃への対策はなおざりになっていないか。突貫工事で整えたITシステムを標的にする3つの脅威に備える必要がある。

「サイバー対策の方針をどう変えればよいか」「どれだけの対策をすれば取引先にも納得してもらえるのか」――

■問い合わせ増加

6月から在宅勤務のサイバー対策の無料相談を期間限定で始めたNECには、業種や規模を問わず様々な企業から、在宅勤務のサイバー対策に関する問い合わせが寄せられている。

淵上真一サイバーセキュリティ戦略本部長代理は「在宅勤務が大幅に増え、既存の方針が通用しなくなったと悩む声が想像以上に多い」と話す。

これまでは従業員がオフィスで仕事をするという前提のもと、オフィスのサイバー対策に力を入れるケースが大半だった。だが、在宅勤務が当たり前となった今、「従業員宅など、侵入を防ぎきれない場所

があることを前提に対策を練る必要がある」（ファイア・アイ日本法人の岩間優仁副社長）。

では在宅勤務を続けるうえで、どのようなサイバー攻撃への対処に重点を置く必要があるのか。専門家に聞いたところ、大別すると、3つの脅威に備える必要があることがわかった。

1つ目は仮想私設網（VPN）への不正侵入だ。在宅勤務に対応するため、多くの企業はVPNと呼ぶ仕組みを整えた。業務システムが稼働するオフィスと従業員宅の間に専用トンネルをつくり、遠隔からのやり取りをできるようにした。

だが、VPNを形作る機器がサイバー犯罪者の標的になることが多いという。その背景には、2019年9月に複数のVPN機器にセキュリティー上の欠陥が発覚したことがある。欠陥の修正プログラムを適用せずにVPN機器を利用し続ける企業はVPN機器から社内ネットワークに不正侵入され、情報を盗まれる可能性がある。

実害も出ている。サイバー対策を啓発する民間団体のJPCERT（JPサート）コーディネーションセンターは3月末までに国内の複数企業から被害の報告を受けた。新型コロナの第1波の襲来で、企業がVPNの整備を急いでいた時期と一致する。

対策としてはVPN機器に欠陥が見つかったら、速やかに修正プログラムを適用することだ。ただ、専門家によると欠陥に気づいていなかったり、海外拠点まで対策が行き届いていなかったりする企業が少なからずある。

野村総合研究所傘下のNRIセキュアテクノロジーズ（東京・千代田）の大谷佳裕上級セキュリティエンジニアは「サイバー対策のクラウドサービスの活用が有効だ」と助言する。欠陥が見つかった場合にはクラウド事業者が責任を負ううえ、国内・海外を問わず、共通の対策方針で監視を任せられるためだという。

2つ目の脅威が自宅に持ち帰ったパソコンへの攻撃だ。ホンダが6月、身代金要求ウイルスとみられるサイバー攻撃を受けたことは記憶に新しい。同社は詳細を明らかにしていないが、社員によると在宅勤務のパソコンにも被害が出たという。

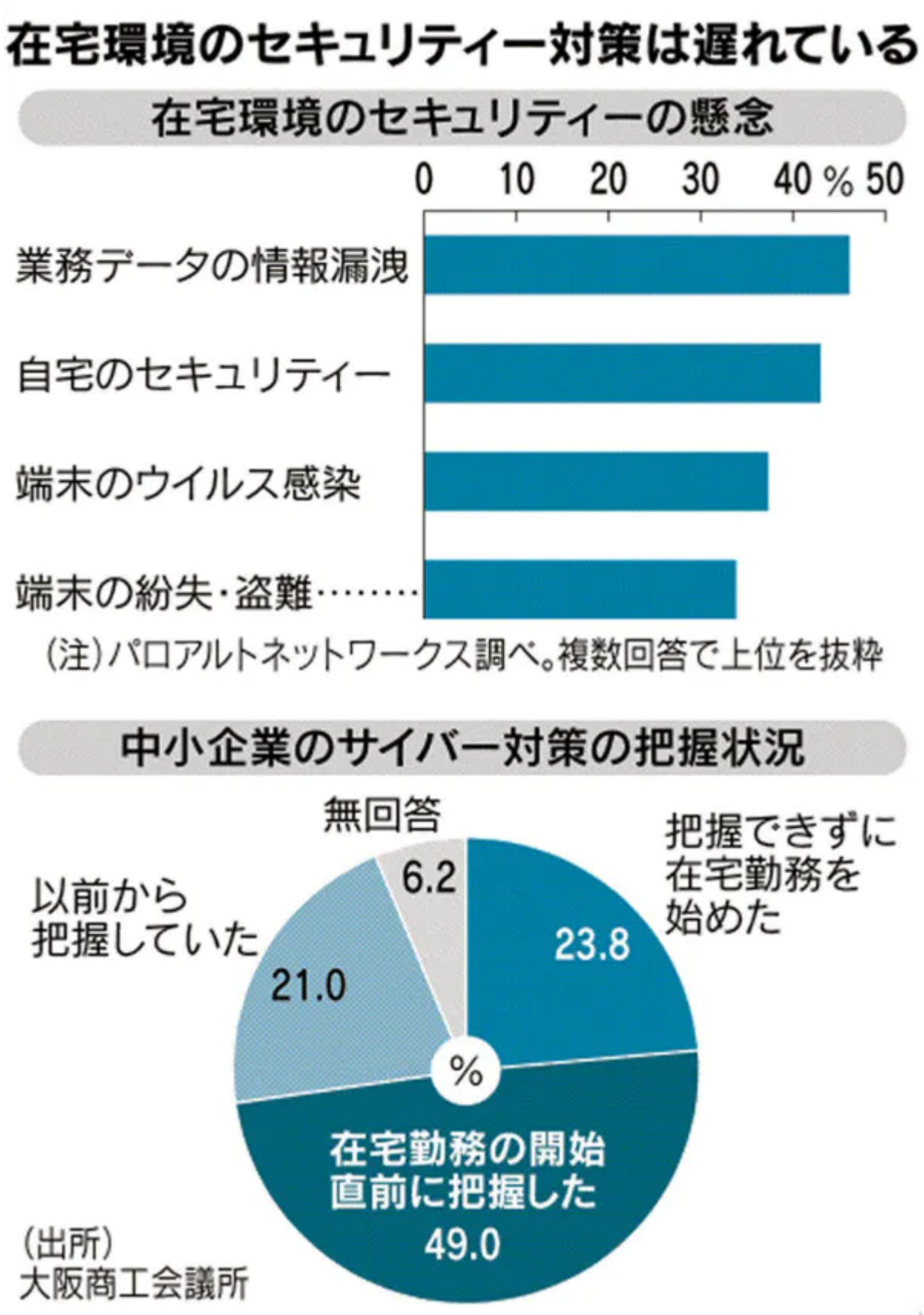
オフィスでサイバー攻撃にあえば、システム管理者がすぐに対処できるが、在宅勤務など遠隔にいる環境では難しい。

サイバー被害の緊急対応サービスを手がけるラックの仲上竜太デジタルペンテストサービス部長は「不審な振る舞いを検出し、遮断する仕組みが必要」と指摘。具体的にはEDR（エンドポイント検知・対応）と呼ぶツールを導入するのが効果的としている。

ウイルス対策ソフトで検知できないウイルスでも、データを無断で送信するなど不審な振る舞いを起こせばEDRで気づけるという。早期に発見すれば被害の拡大を食い止めやすい。

調査会社IDCジャパンによると、EDRを導入済みの国内企業は3割に満たない。ソフトの導入費用がネックになりやすいためとみられる。

サイバー対策企業S&J（東京・港）の三輪信雄社長は「ウィンドウズ10のパソコンであれば、市販のウイルス対策ソフトの利用をやめ、浮いたコストでEDRを導入する手もある」と話す。標準のウイルス対策機能の精度が市販ソフトに引けを取らないためとしている。



最後の脅威は新型コロナ禍で企業の活用が最も進んだツールともいえるビデオ会議の悪用だ。米ズーム・ビデオ・コミュニケーションズの「Zoom（ズーム）」の1日当たりの利用者数は延べ3億人を突破。利用者数が増えるにつれ、サイバー攻撃の被害が目立つ。

■学生装い乱入

米国ではビデオ会議を授業に利用する学校で、不審者が学生になりすまして乱入する「ズーム爆撃」が相次いだ、3月末には米連邦捜査局（FBI）が警告を発したほどだ。

なりすましによる侵入には特に注意を払いたい。会議を盗聴されれば機密情報の漏洩など深刻な被害につながる。特に大人数の会議に紛れ込まれると、不審者に気づきにくくなる。NRIセキュアの大谷氏は「会議の開始前は氏名の入力を求めたり、顔を確認したりする仕組みも取り入れる必要がある」と助言する。

トレンドマイクロの岡本勝之セキュリティエバンジェリストは「偽の会議招待状も要注意」と指摘する。招待状のメールのリンクをクリックすると、本人認証に使われるIDやパスワード、個人情報をだまし取るフィッシング詐欺のサイトにつながる仕組みだ。同社はズームのほか、米シスコシステムズの「ウェブエックス」でも偽の招待状を見つけている。

在宅勤務向けのサイバー対策でも完璧な防御策を整えるのは難しいのが実情だ。まずは人もシステムも信頼しきらないとの発想に立ち、対策を充実することが肝要だ。（企業報道部　島津忠承）

日経産業新聞の記事一覧へ

クリックするとビジュアルデータへ