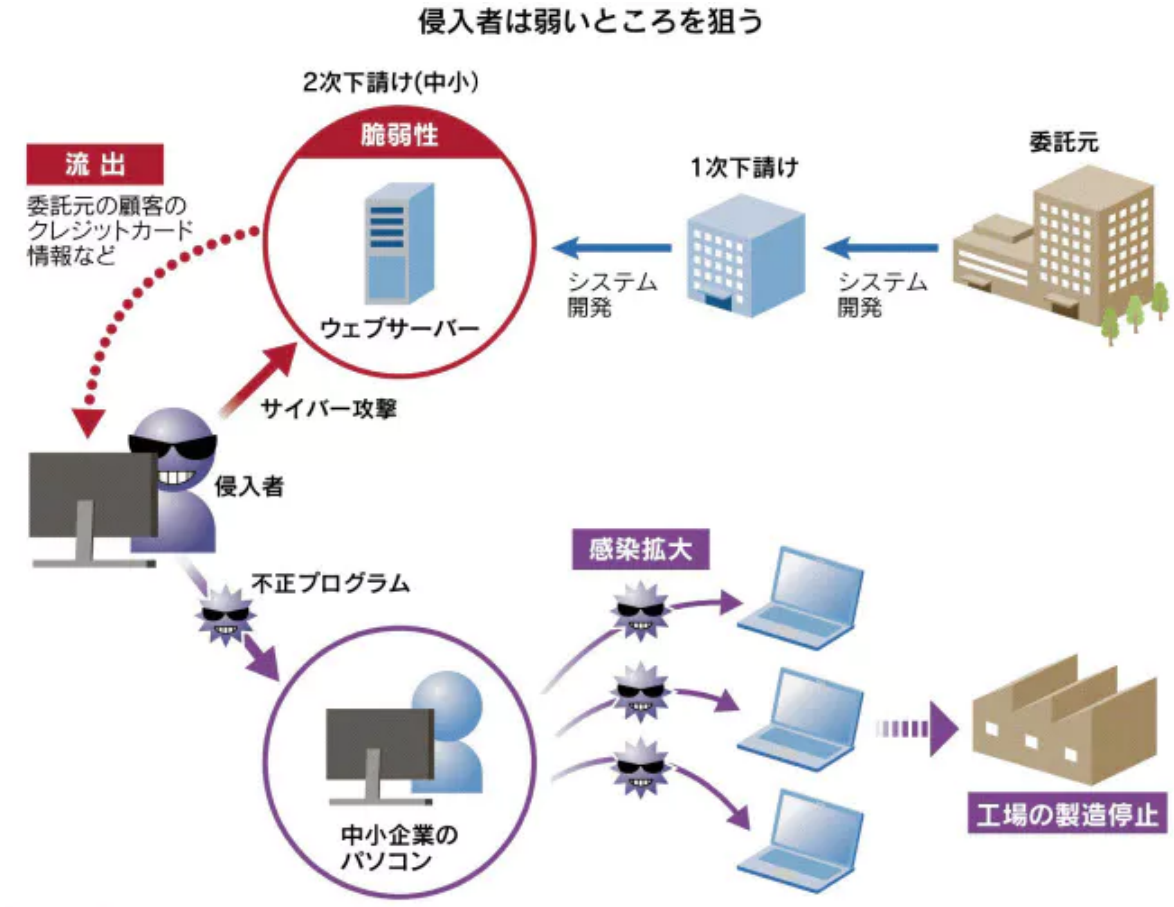
日本経済新聞

サプライチェーンに死角
中小のサイバー対策徹底４％

2019/7/2付 | 日本経済新聞　朝刊

中小企業による情報セキュリティー対策の遅れがサプライチェーン（供給網）に与える影響に懸念が強まっている。民間の調査によると、公的機関がまとめた指針に沿った対応をできている中小企業は４％にとどまる。ほぼすべての企業が不正アクセスを受けている実態も分かってきた。サプライチェーンが進化すればするほど、大企業の営業秘密が中小企業を経由して海外に漏れるリスクが増す。



「貴社のパソコンから不審なメールが届いた」。都内で自動車部品をつくるある中小企業は受注先の完成車メーカーから注意を受け、パソコンがウイルスに感染していたことが分かった。この企業は完成車メーカーから受発注に伴う重要なデータを受け取る立場にあった。ＩＴ（情報技術）担当者がいなかったこの企業は完成車メーカーが指定するシステム会社に駆け込み、再発を防ぐ対策を急いだ。

攻撃、30社全てに

中小企業のサイバー被害は調査が少なく、実態はよく分からない。その中で、全国の中小企業団体のなかでもいち早く1971年からＩＴ関連の部署を持つ大阪商工会議所は2018年９月、神戸大学などと共同で中小企業の実情の調査を始めた。

調査対象の30社と外部の通信を約３カ月にわたって監視したところ、全社で不審な通信が記録され、なんらかのサイバー攻撃を受けていた。あらゆる企業が被害を受けている可能性が示唆されたが、中小企業にとっては被害を受けているかどうかの把握すら難しいことも分かった。大商などは近く、調査内容を精査して詳細を公表する。

侵入者はなぜ中小企業を狙うのか。ソフト検査会社のデジタルハーツ（東京・新宿）セキュリティ事業部の大芝大氏は「大手自動車メーカーの設計図を、セキュリティー対策が手薄な下請けの中小企業から抜き取るといった狙いがある」とみる。いくら大手企業が対策を進めても、製造などの委託先が脆弱であれば共有している重要な情報が危険にさらされる。

2017～18年に米デル日本法人（川崎市）とＥＭＣジャパン（東京・渋谷）が実施した調査によると、情報処理推進機構（ＩＰＡ）の指針に準拠したセキュリティー対策ができている中小・中堅企業は４％どまり。デル日本法人が18年12月から19年１月にかけて実施した別の調査では、ＩＴ担当者が１人以下の中小・中堅企業は38%に達し、19%の企業では専任の担当者がいなかった。

ＩＰＡは17年に、サプライチェーンにおけるセキュリティーリスクについて1249社に聞いた。取引先が仕事を頼む「再委託先」など、直接の取引はないが自社と関係する企業のサイバー対策を把握できている企業は47%にとどまった。大企業から見ると事業の委託が連鎖するほど、状況の把握は難しくなる。

海外から侵入も

侵入者は対策が弱い中小企業にフィッシングメールを送ったり、ウイルスに感染させたりしてサプライチェーンへの侵入を試みる。ＭＳ＆ＡＤインターリスク総研サイバーリスク室の土井剛室長は「特定はできないが海外からの攻撃が多く、政府が関与していることもあるようだ」と指摘する。

実態を把握しようとする試みはある。デジタルハーツは経済産業省やＩＰＡなどと組み、20年２月までに宮城・福島・岩手の各県にある100～200社程度の被害を調査する計画だ。中小企業に専用の機器を設置し、外部との通信をＡＩで分析する。

現場に駆けつける必要があると判断すれば、同社の仙台の拠点から技術者が派遣される。同社の宮崎輝樹セキュリティ・コンサルタントは「実際の事業ではどのくらいの価格設定にすれば中小企業の利用が広がるかも確かめたい」と話す。

ＩＰＡの情報セキュリティービジネスにおける10大脅威19年版によると「サプライチェーンの弱点を悪用した攻撃の高まり」が初めて４位に入った。

欧米ではすでにサプライチェーンを意識したサイバーセキュリティーの強化が進んでいる。米国では17年、防衛調達に参加する全ての企業に対してセキュリティー対策を義務化した。ＩＰＡの横山尚人氏は「セキュリティー対策が不十分な事業者はサプライチェーンからはじき出されることになりかねない」と警鐘を鳴らす。

（石橋茉莉）