中小企業におけるサイバーセキュリティのリアルな実例と現実的対策

大阪商工会議所　経営情報センター　課長
野田　幹稀

サイバーセキュリティに関する啓発情報やマスコミ報道は、中小企業に対するメッセージ性がやや稀薄なケースが散見される。とりわけ公表される被害事例は大企業や政府関係機関、外国企業のものが中心であり、中小企業の被害事例が紹介されることは滅多にない。これでは中小企業は当事者意識を持ちにくい。本稿では、中小企業におけるサイバーセキュリティのリアルな実例と現実的な対策方法につき紹介する。

サイバー攻撃の「攻撃する側」は、個人ハッカーによる愉快犯から、犯罪組織（国家を含む）による経済犯に変化してきている。経済犯である以上、攻撃者は「黒字」を前提としているので、一種のビジネスであり、一定のビジネスモデルに基づき利益が最大化するよう、分業して効率的に実施しているものと考えられる。

「攻撃される側」も変化している。IoT の急増により、攻撃対象の絶対数自体が増えてきている。IoT は物理的に小さいため、ウイルス対策ソフト等を入れられないケースが多く、視界に入らない場所に置かれている場合も少なくないため、多くの場合、資産管理されていない。よって、サイバー攻撃の恰好のターゲットになる。横浜国立大学の調査によると、セキュリティを講じていない IoT をインターネットに接続したところ最短 38 秒でコンピュータウイルスに感染したとのことである。もはや、サイバー空間は「リスクがある」などという次元ではなく「無法地帯」といえよう。

では実際のところ、中小企業にサイバー攻撃がどの程度来ているのか、ということだが、2018 年に大阪府内の、業種・規模などがまちまちの 30 社の中小企業にご協力を頂き、大阪商工会議所、神戸大学、東京海上日動火災保険㈱と共同研究調査をしたところ、実に 30 社全て（100％）で攻撃が確認された。2019 年度に独立行政法人情報処理推進機構（以下、IPA）から請け負い実施した「サイバーセキュリティお助け隊実証事業（以下、お助け隊実証）」では、1 社あたり平均で月 56 件の「外→内」の攻撃、月 4 件の「内→外」の不正通信が観測された。

次に、サイバー攻撃の対象に地域的差異や業種的差異があるのだろうか。2019 年度、2020 年度のお助け隊実証で大阪商工会議所が日本電気㈱などと共同調査したところ、大都市圏である大阪・京都・兵庫と、大都市圏以外の滋賀・奈良・和歌山との比較では有意差が見られなかった。また、業種による有意差も見いだせなかった。「うちみたいな業種は、狙われることはない」といった認識の中小企業経営者は少なくないが、根拠なき過信といえよう。

ここで IPA の「情報セキュリティ 10 大脅威」の上位案件を、中小企業に関連づけながら見てみよう。

2023 年の「組織」における脅威の 1 位は「ランサムウエア」である。ランサムウエアの身代金の額は比較的少額であるケースもあり、被害者の 32％が身代金を支払ったという調査結果もある。数年前にＮＨＫがランサムウエアの犯罪者集団「REvil」に取材したシーンがニュースで放映された。記者が「身代金を払ったらデータを元に戻すか？」と質問すると「必ず戻す。我々は信用を失ったら終わりだ」と回答していた。パソコンの画面の向こう側にも“必死のパッチになっている血の通った人達”がいるのである。最近は「RaaS（Ransomware as a Service）」なる言葉も登場し「悪のエコシステム」が“円滑に”回っているとさえ言われている。

数年前、ある中小企業の経営者が大阪商工会議所に相談に来られた。直接的な相談内容は「ビットコインって何ですの？」といったものだった。

相談員は仮想通貨の概要と入手方法について淡々と説明したが、帰り際に「そもそも、なぜビットコインが必要になったのですか？」と質したところ、「いや～実はなぁ、パソコンやってたら、いきなりパソコンが動かなくなったんや。ビットコインで払ったら直りますって出てきてん。どうやったらビットコインが手に入るんか知りたいんですねん。パソコン動かんと仕事にならへんねん」と。民話のような話だが、これは実話である。

次に脅威２位の「サプライチェーン攻撃」について。サプライチェーンの頂点に君臨する大企業に対し、「貴社の取引先中小企業が受けたサイバー攻撃被害が貴社（大企業）にも及んだ経験があるか」を聞いたアンケート調査（2019 年 5 月、大阪商工会議所が大企業 118 社に実施）によると、25％の大企業が、取引先中小企業が受けたサイバー攻撃被害に起因して大企業側もサイバー攻撃被害を受けていることが分かった。

そして、今後同じようなことが起きた場合、「その原因を作った中小企業に対してどういう対応を取るか？」との質問に対し、実に 47％は「損害賠償請求をする」と回答し、29％は「取引停止も辞さない」と回答している。要するに、中小企業がサイバー攻撃を受けるということは、「被害者なのに加害者になってしまい、最終的には事業継続が困難になることもありうる」ということである。これは中小企業にとっては耳の痛い話である。

2020 年 1 月に下請法の下請け振興基準が改正され、「下請事業者の努力」として「必要なセキュリティ対策を行うこと」、「それに対する親事業者の協力」として「セキュリティ対策の助言・支援を行うこと」が明記されたものの、依然として、大企業側がその優越的地位を濫用して特定のセキュリティサービスの利用を下請け先等に強要することは法律上許されていない。また大企業側が下請け中小企業側にセキュリティ対策の実施を“依頼”した場合、当該コストが（自社への）納入価格に転嫁され、結果として仕入原価が上がるケースもある。この場合、下請け中小企業側のセキュリティ対策投資は、結果として元請け大企業が実質的に肩代わりするのと同じになってしまう。だから大企業側の調達部門は、下請け中小企業に対しサイバーセキュリティ対策の推進を求めたがらない傾向にある。これは同じ大企業の情報システム部門やコーポレートガバナンス部門の思惑と相反しがちである。

次に脅威３位の「標的型攻撃」についてだが、中小企業の経営者と話をしていると、大抵は「うちみたいな中小企業は狙われへん。標的になんかされへんって」と仰る。しかし、先述の通り、最近のサイバー攻撃の多くは経済犯罪ゆえ、攻撃者側も効率性を重視する。したがって、よほど世界レベルの高度な技術を有する会社は別として、通常、攻撃者は、中小企業のことを１件１件個別に事前調査して、特定の会社を狙い撃ちしたり、狙いから外したり、といった“１tol マーケティング”はやっていないと思われる。そんなことをやっていてはペイできないからである。よって、標的型攻撃メールといっても、その実態はバラマキ型の絨毯爆撃メールであり、「うちなんて、標的になるほど、有名な会社ではない」と、油断すべきではない。どんな中小企業でも、広く浅く「標的」になり得るという意識が必要である。

また「うちには値打ちある情報なんてない」と言う経営者が多いが、情報の価値を決めるのは「情報を持っている側」ではなく「情報を盗む側（又は買う側）である」と認識すべきであろう。

私は事あるごとに IPA の担当者などに「標的型攻撃」という言葉を何か別の言葉に変えるように進言しているが、なかなか取り合ってもらえない。「標的型攻撃」というのは、攻撃対象が大企業であることを想定したネーミングであるように感じる。このフレーズは、中小企業のサイバーセキュリティ意識をかえって阻害しているようにすら感じる。「特定の属性を狙った攻撃」などに変更できないものだろうか。

ここからは、中小企業へのサイバー攻撃の事例

（上記の共同研究調査、実証事業等）を幾つか紹介する。

従業員約 10 人の金属製品製造業 A 社では、ラトビアという旧ソ連の国から、管理者パスワードでログインされ、パソコンが長期間にわたり遠隔操作されていた。同社の社長は調査前には「うちなんて、狙われる技術もないし、値打ちのある個人情報も持っていない」と言っていた。ラトビアに取引先、現地工場、出張経験もなく、同国に関係する IT サービスも受けていない。この会社について、とりわけショックだったのは、社長の息子である専務が IT 企業出身者であった点である。そんな企業ですらやられている。

従業員約 80 人の土木工事業 B 社では、社内端末が、深夜を含め、外部の悪性サイトと通信していた。こうした事象は多くの中小企業で日常的に発生しているものと推定されるが、気付いてすらいないのが現状であろう。蛇足ながら、同社の社長は工学博士である。そんな社長がいる会社ですら課題の存在に気付いていないのである。

従業員約 40 人の建築材料卸売業 C 社では、外部の大量のゾンビ化したパソコンから大量の通信が送られ、通信が飽和状態になり営業妨害を被る DDos 攻撃に遭っていた。

従業員約 80 人の化学品卸売業 D 社は、ウイルス感染に伴い、社員のメールアドレスで迷惑メールが多数の取引先に送信されてしまい、取引先のメールサーバが同社からのメールを遮断してしまった。

従業員約 900 人の事務用文具製造販売業の E 社では、自社運営の通販サイトに不正アクセスを受け、顧客のクレジットカード情報が漏洩。同通販サイトは 4 ヵ月間閉鎖を余儀なくされ、4 千万円の逸失利益が発生した。

このように増加・巧妙化するサイバー攻撃の現状に対し、中小企業では、実際、どの程度の対策をしているか、について、先述の 2019 年度、2020 年度のお助け隊実証参加企業での調査結果を紹介する。

先ず「人」の現状だが、専任担当者がいると回答した企業は 1 割未満であり、6 割の中小企業で、専任担当者はもとより兼任担当者すら不在というのが実態である。一般的に問題視される「ひとり情シス」どころか「ゼロ情シス」である。

少し話が横道に逸れるが、「ひとり情シス」は常に孤独であり、重責であり、陽が当たらないポジションである。人事考課という点でも「何も問題が起こらなくて当たり前。せいぜい平均点がもらえる程度。何か問題が起こったら大減点」といった、“美味しくない”立場である。情シスの離職率は高く、ある IT ベンダーの調査によると、従業員 100 人～ 1000 人未満の中堅企業の離職率は 21％と非常に高い。IT 人材の不足が懸念されている今後のわが国にあって、また今後一層サイバー攻撃が激烈化する可能性があるなかにあって、こうした情シス担当者の「地位や処遇の低さ」「離職の多さ」は由々しき問題だといえよう。情シスは、本来、戦略部門として遇されるべきである。

情シスのメンタルを更に悪化させるであろう調査結果が IPA の「中小企業の従業員へのアンケート調査（2021 年 12 月）」で明らかになった。「会社の情報管理ルールに違反した従業員が、その事実を、会社や上司に報告したか」という質問項目で、43％が「1 度も報告を行わなかった」と回答している。経営者や情シスが把握していない「かくれサイバートラブル」が一定数発生しているかもしれない可能性を示している。

次に、サイバー攻撃対策にかけている「お金」についてだが、お助け隊実証参加企業（従業員数中央値：約 10 人）では、地域に関係なく、8 割の中小企業で年 10 万円未満というのが実情である。つまり、月 1 万円未満しか拠出できておらず、経済安全保障という観点からみると、実に心許ないと言わざるを得ない。

では、お金も、人も、時間も不足がちな中小企業は、どのように対策をしていけばいいのだろうか？

先ず、中小企業の経営者に持って頂きたい視点として、サイバー対策を「金食い虫の費用」でな

く「将来の金稼ぎのための投資」と捉えて頂くことである。サイバー攻撃を完全に防ぐことはできないが、リスクをかなり低減することは可能であろう。100 万円の売上を新たに創ることは非常に難しいが、100 万円の新たな (そして無駄な) 支出を防ぐことは比較的簡単であろう。100 万円の非生産的な支出を防ぐために、何らかのセキュリティ対策をすることは、多少の出費とはなるが、中長期的にはそれを相殺して余りある売上と信用の向上をもたらすことだろう。

ここで、サイバー攻撃被害に遭った中小企業の被害額つまり「無駄な支出」の実例を紹介する。

社員 30 人のサービス業である F 社は、受信メールに添付されていたワード文書のマクロを有効にしたところ、PC 1 台がウイルスに感染し、外部に対し偽装メールが送信された。その結果、原因や被害範囲調査費用に 364 万円、再発防止のコンサルティング費用 44 万円、再発防止のセキュリティシステム導入費用 214 万円、計 622 万円の被害があった。このうち、原因調査の 364 万円と再発防止コンサルの 44 万円は、もし、このインシデントが発生していなかったら、支払うことのなかったコストなので、この 400 万円は「無駄な支出」というべきだろう。一方で、セキュリティシステム導入費の 214 万円は「無駄な支出を未然に防ぐための投資」と位置づけられるので、もし、この企業が予め 214 万円の投資をして予防線を張っていたなら、400 万円の「無駄な支出」も発生しなかった、という計算になる。つまり「200 万の投資で 400 万の被害を防止する」ということだ。

こういった計算方法は「後付けの結果論」かもしれないが、サイバーセキュリティに関する「費用と投資」の関係性を考えるうえでの参考事例にはなろう。

中小企業の悩みは「何から始めたらいいか分からない」「どこまでやったらいいか分からない」といったものである。そんな中小企業は IPA の「中小企業の情報セキュリティ対策ガイドライン」の一読から始めるべきだろう。あわせて、同じ IPA の「5 分でできる！情報セキュリティ自社診断」で足元のチェックし、スコアに応じた「やるべきこと」を確認する。次に読んだり調べたりというフェイズから一歩進み、実践フェイズとして「情報セキュリティ 5 か条」に取り組むこと。

「何かに頼りたい」「少しだけしかお金は出せない」という中小企業は、経済産業省・IPA が実証事業を経てその事業スキームを構築し、現在は国の登録制度となっている「サイバーセキュリティお助け隊サービス」を利用するのも一考であろう。人もお金も時間も不足がちな中小企業に特化した、格安で、導入・運用ともに簡単なサイバーセキュリティのワンパッケージサービスである。国に登録されたサービスゆえ、ユーザ企業は「わが社は、中小企業として、最低限のセキュリティ対策をやっています」と公言することもできよう。また、「お助け隊サービス」を利用していたにもかかわらずサイバー攻撃被害に遭ってしまったとしても「中小企業に求められるべき現実的な対策（国に登録されたサービス）をやっていたのですから（取引停止等は）許して下さいよ」というエクスキューズを述べていただくこともできよう。