サイバー攻撃の脅威と中小企業が取るべき経営防衛策に関する報告書

全日本溶接材料商業連合会（全溶連）経済委員会　専門委員（リスクマネジメント・ITセキュリティ担当）

1. はじめに：今そこにある経営リスク

今この瞬間も、あなたの会社のシステムには誰かがアクセスを試みています。これは「海外の犯罪組織による遠い出来事」ではありません。自動化されたプログラムが、インターネット上のあらゆる企業を片っ端からチェックしているという冷酷な現実です。多くの中小企業経営者が抱く「うちは狙う価値がない」という認識は、致命的な誤解です。攻撃者は「価値」ではなく「入りやすさ」を見ています。空き巣が「鍵のかかっていない窓を探す」のと同様、セキュリティの甘い中小企業こそが格好のターゲットとなるのです。我々経済委員会は、会員企業の経営基盤を守る立場として断言します。「狙いやすさ」こそが、現代における最大のリスクであるという現実を、全経営者は今すぐ受け入れなければなりません。

2. 客観的データ：交通事故の19倍という遭遇率

サイバー攻撃を「運が悪ければ起こる事故」と片付けるのは、もはや経営放棄に等しいと言えます。客観的な数値が、その日常的なリスクを裏付けています。

- **異常な遭遇率の証明**
- IPA（情報処理推進機構）の調査によれば、中小企業における情報セキュリティ事故の発生率は年間約5.7%に達します。
- これに対し、交通事故による死傷率は約0.3%です。
- **「大丈夫」という根拠なき過信の払拭**
- サイバー攻撃に遭遇する確率は、交通事故の約19倍という極めて高い数値です。
- 我々の業界が「高圧ガス保安教育」において主観的な「大丈夫」を捨て、徹底した安全管理を行うのと同様、サイバーリスクも客観的数値に基づいた危機管理が不可欠です。
- 「自分だけは大丈夫」という正常性バイアスは、経営を破壊する最大の脆弱性です。

3. 実例に基づく検証：被害の現実と倒産への道のり

ソース資料が示す実例は、サイバー攻撃が企業のブランドと存続をいかに一瞬で奪い去るかを物語っています。

大手企業の悔恨（アスクルの事例）

大手通販企業アスクルを襲ったランサムウェア攻撃は、システムの高度化が孕むリスクを浮き彫りにしました。

- **甚大な被害とブランドの崩壊：** 74万件弱の個人情報が流出し、受注・出荷サービスが全面停止。吉岡晃社長は、効率的なシステムが「功」であった一方で、サイバー攻撃への体制不足を「罪」と表現しました。
- **消えない傷跡：** 物流システムが「本格復旧」を宣言した後も、出荷能力は金額ベースで従来の6〜7割に留まりました。最大の特徴であった「明日来る（翌日配送）」というブランドの根幹は崩壊し、信頼回復には気の遠くなるような時間を要する事態となりました。

中小企業の倒産実例（15名規模の会社）

業績が安定していた社員15名の地方企業が、たった一つの感染からわずか数ヶ月で消滅したプロセスです。

1. **発症：** ある朝、全PCがロック。画面には1,000万円相当のビットコインを要求する脅迫文が表示される。
2. **防御の瓦解：** 唯一の希望であったバックアップ（外付けHDD）をシステムに繋ぎっぱなしにしていたため、同時に感染・暗号化され、復旧が不可能になる。
3. **取引停止：** 業務停止から2週間、主要取引先から契約を停止される。
4. **終焉：** 顧客情報の流出による信用失墜が追い打ちをかけ、数ヶ月で資金ショート。廃業。「事前準備ゼロ」が、そのまま「企業の死」に直結しました。

4. 最悪の想定シナリオ：加害者への転落と社内崩壊

攻撃の被害は、自社のデータ紛失だけに留まりません。以下に示す二次・三次被害こそが、真の地獄を招きます。

- **サプライチェーンの破壊（加害者への転落）** 自社のメールが乗っ取られ、取引先へウイルス付きの見積書が送付されます。これは、**「医療用酸素ボンベにウイルスを混入させ、病院中に流す」**ようなものです。長年の信頼関係という「容器」を信じ切っている相手にとって、そこに含まれるウイルスは回避不能な猛毒となります。信頼関係そのものが凶器となり、自社は「被害者」から、業界全体を汚染する「加害者」へと転落します。
- **社内情報の流出と人間関係の崩壊** マイナンバーや給与情報の流出に加え、最も致命的なのは「接待費の実態（特定の担当者への風俗店や高級クラブでの接待履歴等）」の露呈です。誰が、どこで、いくら使ったか。社内の「知られていなかった不都合な真実」を全従業員が目にした時、職場環境は崩壊します。システムは復旧でき、お金も取り戻せるかもしれませんが、一度壊れた人間関係は二度と元には戻りません。
- **法的・社会的責任の連鎖** 個人情報保護委員会への対応、顧客からの賠償請求、SNSでの炎上、そしてマスコミ報道。これらが同時並行で押し寄せ、経営者は法的・社会的な追及に晒され続け、最終的な企業破綻へと追い込まれます。

5. 必要な備え：企業生命を守る「2つの柱」

「感染を100%防ぐことは不可能である」という現実を直視してください。感染した後に、パニックで時間を浪費し、資金を枯渇させないための「2つの柱」を準備することが経営者の責務です。

1. **専門家による24時間サポート：** 発症時、パニック状態の経営者に「まず何をすべきか」を即座に指示し、伴走してくれる専門窓口。
2. **莫大な復旧費用の確保：** PCの買い替え、システムの初期化、専門業者による調査費用など、数百万から数千万円規模に膨れ上がるコストを賄う確実な手段。これらがない場合、ただ時間だけが経過し、復旧の目処が立たないまま資金が尽きるという、最悪の結末が待っています。

6. 結びに代えて：理想的な対策への期待

経営者の皆様は、対策の必要性を痛感しながらも、以下のような不安を抱いているはずです。「サイバー保険は検討したいが、申し込みの書類や審査が極めて面倒ではないか？」「保険料が高く、一度でも使えば翌年から保険料が跳ね上がるのではないか？」本委員会としては、会員企業の皆様がこうした不安に煩わされることなく、本業に邁進できる環境を整える義務があります。我々は市場に対し、**「24時間365日の専門家サポートがあり、数千万円の費用をカバーでき、かつ面倒な書類や審査なしで即座に導入できる」**という、中小企業にとって極めて都合の良い解決策を強く求めます。一晩にして事業が崩壊するリスクは、今この瞬間も存在します。我々経済委員会は、会員企業の皆様が、一夜にしてすべてを失うことのない実効性のある防衛策を確立することを強く期待し、本報告書を締めくくります。