自社でのセキュリティ対策には限界あり！
専門家との協力がカギ

インフォフラッグ株式会社　代表取締役　神戸　仁

現代の中小企業において、情報セキュリティの重要性は誰もが認識しているでしょう。サイバー攻撃の標的は大企業だけではなく、サプライチェーンの一環として中小企業も含まれることが増えています。こうした状況に対処するために、安価なセキュリティツールを導入し、最低限の対策を取るべきだという声もありますが、それでは本質的な問題解決に至りません。

本稿のテーマは、「自社だけでのセキュリティ対策には限界があり、やった気になってはいけない」という現実的な視点です。ツールを導入すれば安心だと思うかもしれませんが、その運用には専門的な知識と体制が必要であり、これを社内でまかなうことは多くの中小企業にとって非現実的です。むしろ、専門家との協力体制を築くことこそが、真に安心できるセキュリティ対策となり得ます。

1　ツールの導入だけでは解決しない現実

セキュリティ対策は、ツールを導入すれば解決するのかというと、これは大きな誤解です。多くの中小企業では、ＩＴの専門知識を持つ人材が不在であり、ツールの適切な選定や運用ができる環境が整っていません。そのため、以下のような問題が発生します。

【ツールの選定基準が不明確】

ＩＴベンダーに勧められるままにツールを導入してしまう企業が多く、そのツールが自社のセキュリティニーズに合っているかどうかを十分に判断できていないことがほとんどです。結果として、導入したツールが十分に活用されず、セキュリティ対策が中途半端なものに終わるケースが散見されます。

【ネットワーク構成図や資産台帳がない】

企業内のＩＴインフラがどのような状況にあるのかを把握していないため、合理的なセキュリティ対策の優先順位をつけることができません。仮にこれらの資料が存在しても、更新されておらず、現状に即したものではないことが多く意味をなしません。

【ツールを運用するリソースがない】

セキュリティツールを導入したとしても、その管理やメンテナンスを行うためのリソースがない企業が多く、結果的にツールが放置され、効果を発揮しないままになっています。

ここから導き出される中小企業が抱える最大の問題は、“ツールの運用に関わる人材の不足”です。多くの中小企業では、ＩＴの専門人材が不在であり、セキュリティ担当者も他の業務と兼務していることがほとんどです。このため、ツールの選定、導入後の設定や管理、更新といった日常的な運用が疎かになり、結果的にセキュリティ対策が機能しなくなるケースが多々あるのです。

2　IT担当者の採用は危険！受け入れ体制が整わない現実

中小企業の経営者の中には、ＩＴに詳しい人材を採用し、自社のセキュリティ対策を強化しようと考える方もいるでしょう。しかし、これは慎重に考えるべきです。たとえＩＴ運用の経験や知識を持つ人材が採用できたとしても、それが必ずしもセキュリティ対策の成功につながるわけではありません。その理由は以下の通りです。

【人事考課制度が整備されていない】

ＩＴ担当者をどのように評価すべきかの基準がない企業が多く存在します。売上や顧客対応など、他の職種に比べて目に見える成果が出にくいため、適切に評価されることが難しい。そのため、ＩＴ担当者が成果を上げても報われる機会が少なく、モチベーションが低下する可能性が大となります。

【キャリアプランが描けない】

ＩＴ担当者に対する評価基準が不明確であるため、企業内でどのように成長していくべきかのキャリアパスを描くことが困難です。昇進やスキルアップの機会がないまま業務を続けることは、担当者にとっても不安要素となります。

【相談できる上司や同僚がいない】

多くの中小企業では、ＩＴに詳しい同僚や上司がほとんどいないため、ＩＴ担当者は孤立します。問

題が発生した際に相談できる相手がいないという状況は、心理的な負担を大きくし、担当者の離職につながる可能性が大きい。

【売上への貢献が見えにくい】

ＩＴ担当者の業務は、直接的に売上を上げる業務ではないため、経営層からの評価が低くなることが多い。セキュリティの強化やシステムの安定稼働といった成果は、日常業務の一部として捉えられ、十分に評価されない（評価するという概念すらない）ケースが多々あります。

このように、たとえ有能なＩＴ担当者を採用できたとしても、受け入れ体制や評価制度が整っていない企業では、担当者も企業も不幸になる可能性が高い。

3　専門家との協力体制が成功の鍵

問題の解決で重要な視点は、「自社で全てのセキュリティ対策を完璧にこなす必要はない」さらに強調するならば、「ＩＴの専門知識がない自社の要員だけで、自社のセキュリティ対策をしてはいけない」ということです。ＩＴ業務は専門知識が必要な業務だと認識するべきです。中小企業が限られたリソースの中でセキュリティ対策を行うには、専門家との協力が不可欠となります。セキュリティの知識や運用能力が不十分なまま、ツールの導入に走るのではなく、まずは信頼できる専門家に相談し、現状を正確に診断してもらうことが重要です。

【的確なツールの選定】

セキュリティの専門家は、企業の規模や業種、リソースに応じた最適なツールを選定する知見と経験を有しています。これにより、過剰な投資を避け、必要最低限の対策で最大限の効果を得ることが可能となります。

【運用サポートの充実で兼務の負担を軽減】

ツールの導入だけでなく、その後の運用やメンテナンスも専門家に任せることで、常に最新のセキュリティ対策を維持することができます。また、アップデートや脆弱性への対応について適切なタイミングで誘導してくれます。ＩＴ担当者が他の業務と兼務している場合、セキュリティ対策に十分な時間を割くことは難しい。情報の収集と精査など、社内リソースを圧迫することなくセキュリティの強化ができます。

4　最後に…セキュリティ専門家の正しい定義

中小企業が情報セキュリティ対策を進める際、専門家のサポートは非常に重要です。しかし、その専門家を選定する際には慎重さが求められます。一般的に、中小企業はＩＴベンダーを専門家として頼ることが多いと思われるが、ここに一つの問題があります。それは、ＩＴベンダーが自社製品やサービスの販売を通じて利益を得る立場にあるという点です。このようなベンダーに依頼すると、彼らが提供するソリューションが自社製品に偏った提案になる可能性があります。つまり、ベンダーは利益のために自社製品を自然と推奨しがちであり、結果として中小企業にとって最適なセキュリティ対策が講じられないリスクが高まります。中小企業の立場に立った客観的な提案が期待できるかどうかが重要となります。

したがって、本当に中小企業にとって有益なセキュリティ対策を進めるには、第三者の立場で企業のニーズに合った解決策を提供できる専門家を選定することが肝心です。セキュリティ対策の目標は単にツールを導入することではなく、実際のリスクを減らし、企業を守るための長期的な戦略を構築することにあります。そのためには、独立した視点を持ち、特定の製品に依存しないアドバイスができる専門家と協力することが求められます。

- ＩＴ関連製品を販売、開発をしない
- ＩＴ業界歴が１０年以上
- 経営経験がある

この３条件が揃えば、中小企業のセキュリティ対策をサポートする強い味方となるでしょう。中小企業の経営者は「製品を売ることが目的ではない」専門家を選び、信頼できるパートナーシップを築くことが、真のセキュリティ対策への第一歩となります。大阪府中央会では、セキュリティに関する各種相談に対応しています。自社に不安や悩みを抱えている方は、相談窓口に問い合わせをするなど第一歩を踏み出していただきたいです。

＼ 大阪府中央会では中小企業組合等の事業活動に関する支援を行っています ／

お問い合わせ先

大阪府中小企業団体中央会　連携支援部　連携支援課
TEL（06）6947−4371