IT担当者がいない中小企業のセキュリティ対策（第2回）

一人情シスや兼務の場合、セキュリティ対策は外部の専門家に任せよう

2022.02.28

中小企業のIT担当者は、人数が少なかったり、兼務であったりと多忙なケースが少なくありません。業務過多で、セキュリティ対策まで手が回らない場合、どうすればよいのでしょうか。

IT担当者の業務過多は危険！

DXという言葉をよく耳にするようになり、業務のデジタル化を推進している企業は、これまで以上に増えています。一方で、ITを導入するということは、それを管理する人材も必要になることを意味します。新たな機器やサービスを導入した場合、それらが正しく機能しているか否か、日々監視し続ける人材が必要になります。

しかし中小企業の場合、こうした情報システムを担当する十分な人員を確保できず、別の業務との兼任で担当していたり、専任であっても、自社の情報システム全般を一人で担当したりする、いわゆる「一人情シス」というケースも少なくありません。

一般的に情報システムに関連する業務は膨大で、少人数や兼務で対応するのは負担に感じるかもしれません。担当者がオーバーワークになってしまう可能性も十分に考えられます。

特に懸念すべき問題は、日々の業務に追われ、セキュリティ対策がおろそかになってしまうことです。サイバー攻撃によってその隙を狙われ、情報漏えいなどを起こしてしまえば、その責を問われ、損失を被るのは企業なのです。

セキュリティ対策の人員も時間も足りないなら“おまかせ”すればよい

セキュリティ対策に手を付けたくても、人員も時間も足りない場合は、専用のサービスに“おまかせ”する方法があります。その一つが、NTT西日本の提供する「セキュリティおまかせプラン」です。

セキュリティおまかせプランは、サイバー攻撃など不測の事態を未然に予防し、万が一の場合にも専門部署が迅速にサポートを行うサービスです。特徴は、企業のセキュリティ対策をNTT西日本に“おまかせ”できる点にあります。

提供するセキュリティ対策は大きく2つ。ゲートウェイ装置（UTM）とエンドポイントセキュリティによる多層防御で脅威を未然に防ぐ「事前対策」と、不正な通信やウイルス感染などのセキュリティインシデントを検知した際、サポートセンターより主体的に連絡して遠隔駆除などで支援を行う「事後対策」です。

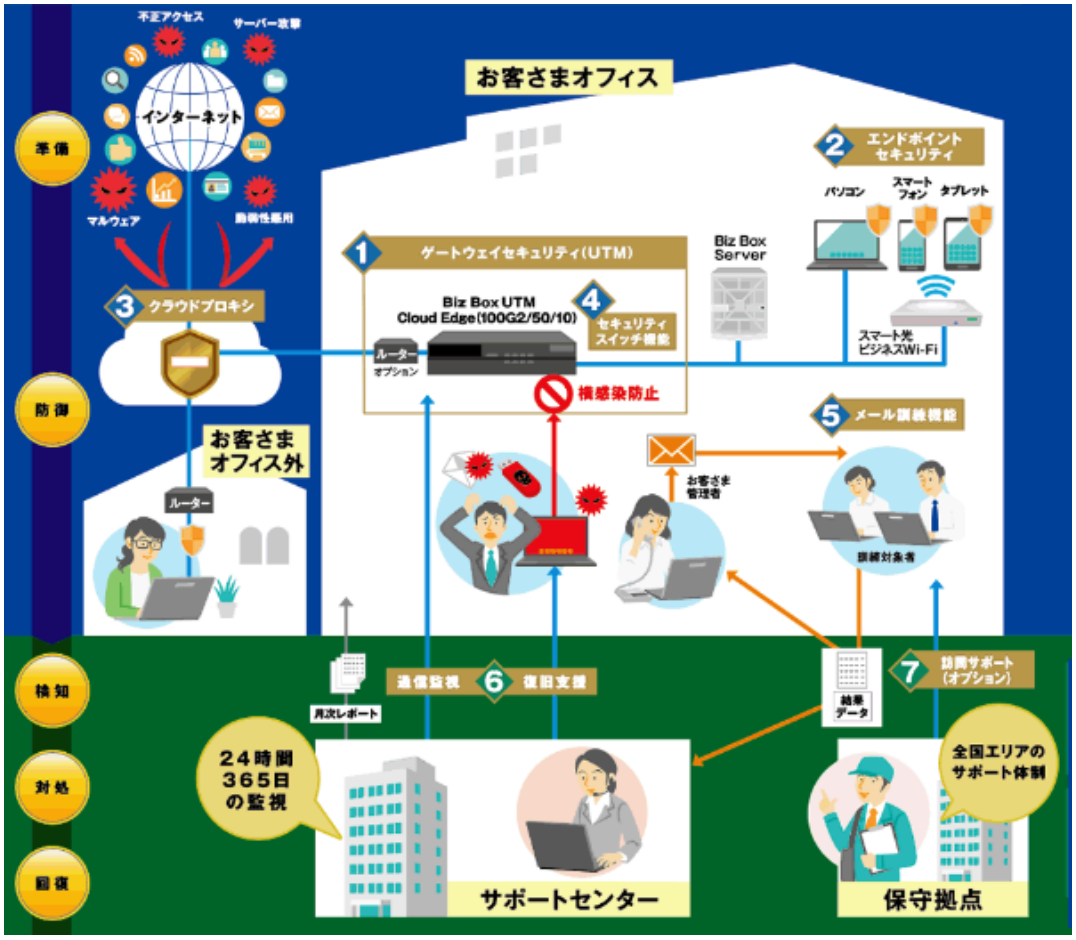
こうした脅威に対する「事前」と「事後」の対策を、自社の業務に負担をかけることなく、NTT西日本におまかせできるサービスです。

具体的には、まず外部からの脅威をブロックするために、オフィスのIT機器とインターネットの境界にゲートウェイ装置を設置します。これにより、悪意のあるメールやウイルス、不正な通信を検知し、外部からの脅威を水際でブロックします。

さらに、従業員が使用するパソコンやスマートフォンなどの端末には、脅威を検知できるよう、エンドポイントセキュリティをインストールします。もし異常が発生した場合は、監視を行っているサポートセンターが電話またはメールでその旨を通知し、仮にウイルス感染など不測の事態が発生した場合は、遠隔でウイルス駆除などの支援を行います。

もし被害を受けてしまい、パソコンの初期化などが必要になった場合は、西日本エリアに約200拠点ある保守拠点からスタッフが駆け付け、復旧支援を行います。

つまり、セキュリティおまかせプランを用いることによって、企業のセキュリティ対策を全て「おまかせする」ことが可能になるわけです。



情シスの負荷軽減とセキュリティ強化を同時に達成できる

複雑で多様化するサイバー攻撃に、十分でない人員で対応するのは不可能です。もし、セキュリティ対策まで手が回らないのであれば、技術とノウハウを持った専門企業に任せてしまうのも一つの方法です。

今回紹介した、セキュリティおまかせプランのようなサービスを導入すれば、企業と情報IT担当者はセキュリティ対策に対する懸念が軽減されます。その分、業務の負担が軽減され、他の業務に集中できるようになるでしょう。

一人情シスや兼務で、システム周りの稼働がひっ迫しており、セキュリティ対策に稼働を割けていない企業は、一度検討してみてはいかがでしょうか。ビジネスインフラの一つである、情報システム関連業務が円滑化することで、企業全体の生産性向上にもつながるはずです。