サイバーセキュリティ最前線

企業の大小を問わず万全のセキュリティ対策が必要!!

AIの進化を背景に、企業の大小を問わず、サイバー攻撃の被害が急拡大している。では、中小企業はどのような対策を講じるべきなのだろうか。長年にわたって、サイバーセキュリティに携わってきた㈱アイ・ティー・ワン ソリューション事業本部 ソリューション営業部のふたりに話を聞いてみた。

時代の変化に対応して20年ほど前からセキュリティに注力

御社は三菱総研のグループ会社だそうですね。

堀口正哉・アイ・ティー・ワン ソリューション事業本部部長　2011年に三菱総研グループに参画し、㈱三菱総合研究所や三菱総研DCS㈱と連携しながら、SIer（システムインテグレーター）としてビジネスを拡大してきました。

どのようなビジネスを展開しているのでしょうか。

堀口　当社はもともとシステム開発を主軸とし、SEサービスなどを展開してきました。主な顧客は銀行・保険・カードを中心とした金融関係ですが、そのほかにも旅行業など、幅広い分野のシステム開発・運用に携わっています。

事業の一環としてセキュリティ対策の支援にも取り組んでいるそうですね。

堀口　20年ほど前からセキュリティ分野にも取り組んでいます。日本でも個人情報保護が大きく注目されはじめた時期で、当社としてもセキュリティに関するソリューションに注力していくことになり、私に白羽の矢が立ったのです。

その後、「アプリケーション単位の隔離」と「封じ込め」に特化したエンドポイント保護ソリューション「HP Sure Click Enterprise（SCE）」の取り扱いをはじめたそうですが、その経緯についてお聞かせください。

堀口　セキュリティ対策の支援に取り組むなかで、セキュリティ専門会社である㈱ブロード（東京都千代田区）とご縁ができ、同社が取り扱っていたSCEに関心を持つようになったのです。

どのような点に関心を持ったのでしょうか。

堀口　なんといっても「隔離技術をセキュリティに活用する」という画期的なアイデアに惹かれました。そもそも、隔離技術はひとつのコンピュータで複数のOSを稼働するために用いられていたのですが、その隔離空間でメールや添付ファイルを開くことによって、マルウェアなどの攻撃を無害化することに成功したわけです。そのため、マルウェアがどんなに悪さをしても、PC本体は何の被害も受けませんし、仮想空間を閉じれば、すべてのマルウェアとその痕跡を一掃することができるのです。もちろん、すべてのファイルを隔離空間で開くというわけではなく、当該ファイルを「信頼する」と設定することで、本体で開くこともできるようになります。

実に素晴らしいソリューションだと思います。こういったソリューションが日本でも開発されるようになると最高ですね。

堀口　日本の場合、携帯電話しかり、システム開発の分野においてもガラパゴス化する傾向があり、なかなかグローバルにヒットするソリューションを生み出せないでいます。しかし、一方で日本はウォークマンをはじめ、独創的な製品を生み出してきたモノづくり大国でもありますし、技術力はもちろん、発想力や着眼点には大きなポテンシャルがあるはずです。あらゆる規格や仕様がグローバルに統一された今こそ、日本の技術力の真価を発揮してほしいですし、当社としても独創的な開発に取り組んでいきたいと思います。

エンドポイントの保護とともに脆弱性の客観的な把握を

日本では「中小企業のセキュリティ意識が低い」といった問題が指摘されていますが、そのあたりについてはどう感じていますか。

堀口　たしかに、そのようなイメージがあります。かつては自分たちで少しずつ内製化しようという動きがあったようにも思いますが、クラウド型のビジネスやソリューションが台頭してきた頃から、クラウドベンダーが提供するソリューションを利用するのが気軽で安価ということで、それが主流になってきたのです。最近はそこにノーコードでプログラミングができる環境が整ってきたものですか

左からソリューション事業本部ソリューション営業部部長（情報処理安全確保支援士）の堀口正哉（ほりぐちまさや）氏、ソリューション営業部営業担当の松尾大史（まつおひろし）氏

ら、結果的にＩＴ人材も減少してしまっているように思います。しかし、ＡＩの進化にともない、世界中により多くの情報が飛び交うようになることを想定すると、企業は規模の大小を問わず、セキュリティ対策にこれまで以上に力を入れなければなりません。そういったことを論理的に伝えるのも、当社の重要なミッションだと考えています。

どのようなことに注意すべきなのでしょうか。

堀口　エンドポイントの保護だけであれば、前出のＳＣＥだけでも十分にセキュリティレベルを維持できるのですが、今の時代、サーバーやネットワークのセキュリティレベルにも注意を払う必要があります。最近は大手企業の関連会社や取引会社などの脆弱性が狙われ、大規模な情報流出につながる例も増えているので、取引先などともセキュリティレベルの足並みを揃えることが重要になっています。

セキュリティレベルをシッカリとチェックする必要がありそうですね。

松尾大史・アイ・ティー・ワンソリューション営業部営業担当　脆弱性をチェックするという観点では、ＡＩを活用して自動でセキュリティを検証してくれるソリューションも世の中にはあります。攻撃対象領域の検出、脆弱性検査、ペネトレーションテストをワンストップで行うことができるため、外部からの脅威に対しても効率的な管理をすることができます。

最近は医療機関などがランサムウェア（身代金要求型ウイルス）による被害を受け、しばらく稼働できなくなるといったケースを目にすることも増えてきました。

松尾　そうですね。いかにセキュリティレベルを高く維持していても、人為的なエラーなどが原因となり、被害が生じてしまうことがあります。そういう意味では、何かあったときのレジリエンス（復旧）の準備もしておいたほうがよいでしょう。

システムの強化もさることながら、社員のＩＴリテラシーを高めることも大切でしょうね。

堀口　ご指摘の通りです。今や誰もがＩＴを活用する時代ですので、情報を取り扱ううえでの最低限のリテラシーが必要ですし、社内できちんとパスワードやアクセス権限の管理を行う必要があります。今は些細な脆弱性や行動が大規模なサイバー被害につながりかねない時代です。そのことを経営陣はもちろん、社員一人ひとりに認識いただけるよう、引きつづき啓発活動に力を入れていきたいと思います。

昨今のセキュリティ事情と中小企業が注意すべきポイントがよくわかりました。