特 集

大切な情報資産を守るため、今求められる“本気のセキュリティ対策”

ストーンビートセキュリティ株式会社 代表取締役 佐々木 伸彦氏

顧客情報をはじめ、営業情報、商品情報など、事業を行う上で不可欠な情報は、企業の重要な“資産”である。これらの情報資産は、紙ベースの書類として企業内に保管されているほか、デジタルデータとしてパソコン内やクラウド上に保存されている。そして目に見えにくいデジタルデータは、日々、サイバー攻撃の脅威に晒されているのが現状だ。大切な情報資産を攻撃から守るにはどうすればよいのか？　情報セキュリティの専門家、佐々木 伸彦氏に、サイバー攻撃の実態や情報セキュリティ対策のポイントを伺った。

事業を行う上でなくてはならないのが情報資産
漏えいすれば事業継続が困難になる危険性も

――佐々木さんが率いるストーンビートセキュリティは情報セキュリティを包括的にサポートする専門会社とのことですが、どのような事業が中心なのですか。

佐々木　情報セキュリティの研修や、リスクアセスメント、脆弱性診断、ペネトレーションテスト（侵入検査）などを行っています。ISOに関しては、ISMSの構築･認証取得支援も行っています。

――過日は私どもベターリビングのISMS審査員研修の講師も務めていただきました。ほかに、国のお仕事もされているそうですね。

佐々木　中央省庁等で使われるシステムに関して、調達から運用までのライフサイクルにわたり、セキュリティの観点からアドバイスを行っています。

――本日のテーマは「情報資産を守るためのセキュリティ対策」なのですが、“情報資産”と聞くと、IT企業のような限られた業種の事業者が保有している特別な資産のような印象も持ちます。まず、改めて、情報資産とはいったい何なのでしょうか。

佐々木　情報資産とは、企業や組織が事業を進めていく上でなくてはならない大事な情報と考えていただければよいと思います。わかりやすいところでは、お客様についてのデータや営業機密などです。これらの情報がなければ仕事を進めていくことはできません。つまり、すべての企業は情報資産を保有

しているのです。

われわれ情報セキュリティの専門家は、機密性、完全性、可用性といった観点から情報資産の価値やリスクを評価しますが、もっと身近に社員自身の観点で、仕事上必要な情報を識別していけば、自社にとって最も守るべき情報資産がはっきり見えてくると思います。

情報資産管理の先にあるのは、お客様との信頼関係の構築です。情報資産をきちんと守っていかなければ、企業の信頼を失墜してしまったり、事業の継続が困難になったりする事態を引き起こしかねません。情報資産はそのような側面を持っています。お客様の情報を意識して大事に扱っていかないと、お客様の信頼を得ることができず、事業を継続することが難しくなるのです。

今日、情報資産の多くがパソコンの中やクラウド上にあって、目に見えにくくなっています。この見えにくい情報資産をどうやって守っていくかという情報セキュリティが、事業継続のために重要な要素のひとつとなっています。

――顧客リストなどの社外秘文書であれば誰もが取扱いに注意を払いますが、例えばお客様や取引先と日常的にやり取りしているメールの中にも、重要な情報が含まれていますよね。これもサイバー攻撃のターゲットになりますか?

佐々木　なります。例えば、2020年に大流行したEmotet（エモテット）というコンピュータウイルスは、メールを介して次から次へと拡散されて被害が広がっていくタイプのマルウェア※です。コンピュータウイルスに感染した端末からメールデータを盗み出し、そのメールデータをそっくりそのまま悪用してメールを送り、また次の人を感染させるのです。メールを受け取った人は、知っている人から見覚えのあるメールが送られてくるので、違和感を覚えつつも危険とは思わずにクリックして開いてしまう。そうするとコンピュータウイルスに感染してしまうのです。

私の周りにもEmotetに感染したという人が少なからずいました。あるお客様は、取引相手から、過去に受け取った内容と同じメールが来たので、不審に思って相手に「こんなメールが来ましたけど送りましたか」と電話をかけた。相手が「送った覚えはないけれど確かに私が以前書いた内容ですね」と応じ、「添付ファイルが付いているということですが、どんなファイルですか」と聞かれたのでファイルを開いてみたら、その瞬間に感染したということでした。不審に思って確認するという行為をした人が、コンピュータウイルスに感染してしまう。感染リスクは身近なところに巧妙に仕組まれているのです。

※ユーザーのデバイスに不利益をもたらす悪意のあるプログラムやソフトウェアの総称

――コンピュータウイルスに感染するとどうなるのですか。

佐々木　コンピュータウイルスにはいろいろなタイプがあります。例えばランサムウェアというのは、パソコンのデータを暗号化してしまうマルウェアで、感染するとファイルが勝手に書き換わってしまったり、パソコンが使えなくなったりします。

一方でEmotetのような情報を盗むだけのタイプのマルウェアは、パソコンにわかりやすい症状が出ないので、気づかないうちに淡々と攻撃が進行している場合が多いです。盗まれたメールデータが

悪用されて、外部の人から「あなたからメールが届いたけれど、これは何ですか」という通報があり、そこで初めて自分のパソコンがウイルスに感染していたことに気づくケースが何件もあります。

攻撃者は当人になりすまして盗んだ情報を次の攻撃に使うほか、その情報自体をどこかにリークしたり売ったりすることで経済的利益を得ているといわれています。お客様とのやり取りが外部に公開されてしまうというのは重大な情報漏えいになり、企業の情報管理の責任が問われます。

――大企業だけでなく中小企業も攻撃の対象になるのでしょうか。

佐々木　ITを利用している限りにおいて、サイバー攻撃のリスクは、企業規模の大小にかかわらずすべての企業が負っています。攻撃者は明確にターゲットを絞って攻撃を仕掛けることもありますが、ほとんどの場合、無作為に攻撃を仕掛けては、セキュリティの弱いところを見つけて侵入し、それを足掛かりに攻撃を広げていきます。そこに大企業、中小企業という括りはありません。

情報資産の識別と、基本的対策の徹底
これだけでもかなりのリスクを軽減できる

――情報セキュリティ対策推進のポイントを教えてください。

佐々木　ポイントはたくさんあるのですが、これから取り組むという方に、特に２つのことをお伝えしておきたいと思います。

１つは、まず、自社にとって最も重要な情報は何で、どこにあるかをきちんと把握すること。情報資産の識別と管理状態の確認です。コンピュータウイルスソフトやファイアウォールなど、いろいろなセキュリティ対策がありますが、何を守るのかが明確になっていないと効果的な対策がとれませんから、まずこれを把握することが情報セキュリティの出発点になります。

２つ目は、基本的な対策を徹底することです。例えばパソコンのOSをアップデートする、コンピュータウイルス対策ソフトを更新する、最新バージョンのセキュリティパッチを適用するなど、これらを徹底するだけでも、セキュリティ対策の多くの部分をカバーすることができます。

基本的な対策として忘れてならないのは、パスワードを強固なものにしておくことです。サイバー攻撃の被害は、パスワードが脆弱であることが原因で起きていることが非常に多いです。よくいわれるのが、アルファベットの大文字･小文字、数字、記号を入れて、１０文字以上にするといったことですが、あまり複雑だと覚えておけませんので、私は、自分が好きなフレーズを１つ作っておいて、それに数字なり記号なりをプラスするという方法をお勧めしています。

――メールで添付ファイルを送るときに、別メールで開封用のパスワードを送る方法がありますが、セキュリティ対策として効果がないという意見もあります。これはいかがですか。

佐々木　万一、メールデータが覗かれている場合、ファイルとパスワードを同じ経路で送れば両方見られてしまうので、意味がないという話ですね。機密データをメールで送るのであれば、パスワードは

ショートメールや電話、対面など別の経路で送ったほうが良いです。

弊社がよく使う方法は、プロジェクトがスタートする前にあらかじめパスワードルールを決めて、お伝えしておくのです。そうすればメールでパスワードを送り合う必要がないので、パスワードが漏れる心配はありません。

――基本的対策を徹底するために、注意しておいたほうがよいことはありますか。

佐々木　構成管理、つまり、社内のパソコンがどのようにつながっているか、誰がどこでどういったシステムを使っているかということを、今一度確認したほうがいいかもしれません。例えば経理などの特定業務用に導入したパソコンがあるという場合などは、全台OSのアップデートやウイルス対策ソフトの更新をしているつもりが、管理不足により抜け漏れていたということになりやすいですね。

――パソコン以外にもコピー機やカメラなど、ネットワークにつながっている機器があります。これらのセキュリティはどう考えたらよいでしょうか。

佐々木　業者の方に設置だけをしてもらって、セキュリティ管理はお願いしていないというケースも少なからず見受けられます。初期パスワードのまま使い続けていたり、そもそもパスワードを設定していなかったり、使用者を制限するアクセス権を設定していなかったりと、このあたりの管理はしっかりする必要があると思います。

過去の弊社のお客様で、人事部専用のプリンター複合機でスキャンしたデータがネットワーク上に残っていて、一般社員も見ることができたという例がありました。特定の人だけが使うプリンターであれば、パスワードを入れないと使えないようにするなど認証やアクセス制限を厳重に行う必要があります。

監視カメラの映像がパスワードの管理やアクセス制限などが不十分で外部から覗かれているといったこともありますし、ネットワークにつないで使用する電化製品などもパスワードの管理やアクセス制限を正しく設定して管理することが必要です。

情報セキュリティは企業リスクと表裏一体の関係
経営判断ができる幹部がトップに立つことが望ましい

――情報セキュリティ対策推進のための社内の体制づくりについてお伺いします。情報管理責任者は、どういう立場の、あるいはどういうスキルを持った人がふさわしいですか。

佐々木　情報資産の責任者は企業であって、事業やリスクにかかわる判断をするのも企業です。情報セキュリティは企業経営上のリスクに直結し、事業計画にも密接にかかわる事柄ですから、経営判断ができる幹部の方がトップに立って推進していくべきだと考えます。そういった方が情報システムなど技術に明るくないという場合も当然ありますので、そういった技術や情報セキュリティに詳しい方が横でサポートする体制をとることが望ましいのではないかと思います。

――しかし実際には、情報システム管理担当者が社内に１人しかいないという企業もたくさんあります。中には、すべて外部に任せていて、社内にはわかる人が１人もいないというケースもあります。事業を行う上で情報セキュリティ対策がいかに重要かという認識を社内で共有して、体制を再構築する必要がありますね。

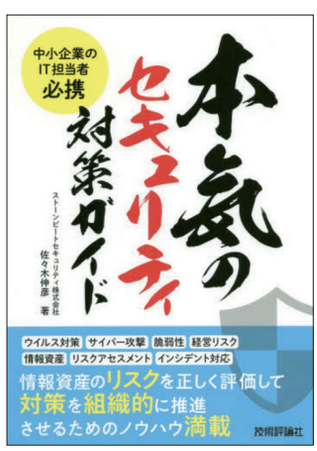
佐々木　社内に情報システム管理責任者がまったくいないというのは問題です。システム管理をまるごとアウトソーシングしているからといって、何か起こったときに外部の人が責任をとるわけではありません。技術的な点に対応する人材についても、社内に最低でも１人は担当者を置く必要があると思います。その担当者に学びの機会を提供して、大事に育てていくといった姿勢が大切なのではないでしょうか。

もちろんすべてを１人でできるわけではないですから、例えば私たちのような情報セキュリティの専門サービスを利用するのもひとつの方法だと思います。自社内でやっていると、他社がどういった対策をしているかがわかりません。外部の専門家を使うことで、他社はどうやっているか、世の中がどうやっているかを知った上で、専門的知見を活用しながら、効率的に有効な対策をとることが可能になります。

――佐々木さんが2020年にお書きになった『本気のセキュリティ対策ガイド』にも、取り組みの参考になる情報がたくさん掲載されていますね。

佐々木　これを執筆したときも、社内で１人とか２人で頑張っている情報セキュリティ担当者を、読者として想定していました。周りに相談する人がいない、何から進めていいかわからない、自分がやっていることが正しいか確証が持てない――。日々疑問を持ちながら奮闘している方々の指針や参考になればといいと思い、書かせていただいたものです。

世の中には情報セキュリティ対策を推進する上で参考になる情報やガイドラインが結構あるのですが、そういったものがあること自体もあまり知られていませんので、それらもこの本で紹介しています。一から始めるとなると「たくさんのことを勉強しなくてはいけない」と身構えてしまいますが、活用できるものをうまく活用していくことで、取り組みやすくなると思います。



『本気のセキュリティ対策ガイド』
佐々木 伸彦（著）／技術評論社

日本のセキュリティ意識はまだまだこれから
サイバー攻撃の恐ろしさを正しく知ることが必要

――企業の情報セキュリティ対策の中で、ISMS（ISO/IEC27002:情報セキュリティマネジメントシステム認証）はどのような位置付けにあるとお考えですか。

佐々木　ISMSを活用するメリットはとても大きいと思っています。情報セキュリティ対策といわれても何から始めていいかわからないという企業は本当に多いです。このマネジメントシステムは情報セキュ

リティを体系的に整備し、何から始めるべきか、どう推進すべきかということを具体的に指し示しています。先ほど私が申し上げた情報資産の識別から、管理·運用までをどのように進めていけばよいかが網羅されていますから、これらに沿って対策を推進し、運用していくことで、企業に情報セキュリティの文化を根付かせていくことができると思います。

――情報セキュリティの先にあるお客様との信頼関係の構築という点からも、認証取得のメリットは大きいでしょうか。

佐々木　認証を取得しているということは、第三者である認証機関に認証を受けた情報セキュリティ対策をしっかりやっているという対外的なアピールにもなり、お客様との信頼関係を生むことにつながります。実際に取引開始に当たって、取引先からISMSの認証取得を求められるケースも増えています。

――業種や規模でいうと、情報セキュリティへの関心が高い企業はどのようなところが多いのでしょうか。

佐々木　業種業態や規模にかかわらず、あらゆる企業でセキュリティの意識が高まっていると感じています。しかしそれでも、世界的に見ると、日本のセキュリティの意識は総じてまだまだ低いです。

その理由はやはり、日本が安全な国だからだと思います。例えばアメリカやロシア、イスラエルなど戦争をしている国では、サイバー防衛という意識でセキュリティ対策に取り組んでいます。それに対して日本人のセキュリティの意識は、自動車の安全運転講習会ぐらいのノリだと思いますよ（笑）。

インターネットは、世界中の人々がつながっています。マンションの隣の部屋に、テロリストや悪質な犯罪集団が住んでいたら、ものすごく怖いですよね。インターネットでも同じことです。すぐ隣に怖い人がいるかもしれないのです。しかし日本には、そういった危機感を持ちにくい文化、特性があるのではないかと思います。

――サイバー攻撃の恐ろしさを正しく理解して、対策を日々継続して実行していくことが大切なのですね。

佐々木　セキュリティはどこまでやってもこれで完璧ということはありません。いくら努力しても、残念ながら、必ずインシデントは起こります。そういったときに、業務を行っている担当者を叱りつけたり、だめだと諦めたりするのではなく、どうしてインシデントが起きてしまったのか、どうすれば起きなかったのかということを究明し、教訓を得て、次の対策に生かすこと。それが、セキュリティ対策を強くしていくための重要なポイントです。

私たちストーンビートセキュリティ株式会社の創業からのミッションは、インターネットを安心安全に使える社会を実現することです。セキュリティの重要性、必要性をお伝えしながら、これからも日本全国に情報のセキュリティを行き届けたいと思っています。

――本日はありがとうございました。

佐々木 伸彦氏　プロフィール

ストーンビートセキュリティ株式会社、代表取締役。国内大手SIerにて、セキュリティ技術を中心としてシステムの提案、設計、構築などに10年ほど従事。2010年に世界最大のセキュリティベンダー、マカフィーに入社。セキュリティエバンジェリストとして脅威動向や攻撃手法の調査･研修、普及啓発に尽力したのち、2015年にストーンビートセキュリティを設立。2016年から外務省最高情報セキュリティ責任者（CISO）補佐官を務める。ストーンビートセキュリティを率いる経営者のかたわら、ペネトレーションテストやセキュリティコンサルティング、トレーニング講師など幅広く活躍中。国内で開催されたCTFでの優勝経験やペネトレーションテスト（侵入検査）のスキルを試すHack The BoxでHacker称号を持つ。CISSP、CISA、CISM、GCFA、LPIC-3 Security等、情報セキュリティに関する認定資格を多数保持。著書に『中小企業のIT担当者必携　本気のセキュリティ対策ガイド』『【イラスト図解満載】情報セキュリティの基礎知識』（いずれも技術評論社）などがある。