サイバーリスクといかに対峙するか いまこそ考えるセキュリティ対策

新型コロナウイルス感染拡大により在宅勤務やリモートワークの導入が進みました。外部からネットワークに接続する頻度が増加したことで、企業がサイバー攻撃を受けるリスクも高まっています。企業や工場の基幹システムが標的にされれば、情報漏洩やデータ消失にとどまらず、事業継続の危機につながります。サイバーセキュリティの専門家であるSBテクノロジー株式会社の辻伸弘様に、サイバーリスクとの向き合い方についてお話を伺いました。

インタビュー

SBテクノロジー株式会社 プリンシパルセキュリティリサーチャー

辻 伸弘 様

Nobuhiro Tsuji

―― リモートワークの普及で、社外から企業の情報システムへの接続が増えています。サイバーリスクが高まるのではないでしょうか。

辻　最近になってリモートワークを導入した企業やシステムを刷新した企業なら、あまり心配はないでしょう。むしろ、リモートの仕組みを持っていながらこれまで運用していなかったり、使用に制限をかけていたりした企業は、システムに脆弱性がある可能性を否定できませんので、注意が必要です。

―― 自社のシステムが安全かどうかを見極める方法はありますか。

辻　一概には言えません。使用する製品やサービスによって品質が違いますし、導入したときにはほぼ100％安全とされていたシステムでも、翌日どうなるか分からないのがセキュリティ対策です。一つ言えるのは、急激に多くの人が使い始めたサービスは標的にされやすいということ。注視したいのは、狙われやすさや脆弱性の有無ではなくて、サイバー攻撃を受けてからの対応方法、問題発生から改善までに要した時間です。例えば、オンライン会議システムのZoomは、脆弱性が指摘されたものの、対処が非常に早く、通信障害もほとんど起きていないので、その点は評価できます。

一般にリモートワークはクラウドサービスやVPN※などに支えられています。いつ、どこからでもメールやファイルを閲覧できるのがメリットですが、言い換えれば、そこがセキュリティ上の穴になり得ます。これは単にシステム担当者が穴を塞げば済むという話ではありません。アクセスに必要なパスワードが漏洩すれば、そこが穴になるわけですから、リモートワークの加速で、アタックポイントが増えた、という見方もできます。

―― 自社のネットワークと外部システムを接続してサービスを受けることがありますが、これもアタックポイントになり得るのでしょうか。

辻　セキュリティ監視システムやクラウドサービスのように信用して接続している所を狙うケースがあります。日本でもクラウドホッパーといって、MSP（マネージドサービスプロバイダ）サービスを狙った事例や、メンテナンス業者が利用するアクセス経路を経由して企業のシステムに侵入した事例がありました。対策としては、自社が利用しているサービスのセキュリティレベルをチェックしておくこと。一方、サービスを提供する事業者にとっては、自社サービスのセキュリティ対策が他社との差別化につながります。

セキュリティの穴に注意！ 二要素認証の導入で安全性を向上

―― IoTや5Gといった新しい通信技術を活用する場合、セキュリティ対策は変わりますか。

辻　基本的に変わりません。今まで必要といわれていた対策に改めて向き合うことが必要です。例えば、個人が設定したパスワードがそもそも弱いとか、仕事用のパスワードを私用でも使い回しているといったことはよく聞く話です。仮に自組織は全員のリテラシーが高いと判断するならば、ユーザーに管理・運用を委ねるのも一つの方法でしょう。しかし、私は可能な限りシステムで解決し、ユーザー任せにすべきではないと思います。パスワードの危険度をチェックする仕組みや、クラウド利用に「二要素認証※」を導入すれば、コストは掛かっても安全性は高まります。

セキュリティ対策はユーザー任せにせず仕組みで解決しよう

―― 二要素認証とはどういったものですか。

辻　認証要素には、IDやパスワードなどの「あなたが知っているもの」、スマホアプリに表示される数字や銀行から配布される数字が一定時間で変更されるワンタイムトークンなどの「あなたが持っているもの」、静脈など「あなたであること」の3種類があります（図1）。同じ要素を使う「二段階認証※」に対し、2種類の要素を組み合わせることで、セキュリティレベルを高められるのが「二要素認証」です。

図１　認証要素の種類

知識認証	所有物認証	生体認証
what you know	*what you have*	*what you are*
		
IDとパスワード、秘密の質問など	スマホアプリに表示される数字や銀行から配布される数字が一定時間で変更されるワンタイムトークンなど	静脈、瞳の光彩など

―― セキュリティ上の穴からサイバー攻撃を受けた場合、どういった被害が起こり得ますか。その際、どのような対策が必要となるのでしょうか。

辻　攻撃を受けた場合、最初にすべき処置は、攻撃を受けた端末をネット回線から切り離すなどして物理的にネットワークから遮断すること。被害の拡大防止です。放っておけば自社のネットワークが汚染され、全ての工場や物流センターが稼働停止せざるを得ない事態に陥る可能性がありますし、ほかの会社にも迷惑を掛けることになりかねません。これは以前から行われているセキュリティ対策の基本で、自宅でも会社でも共通の対策です。

その上で被害の実態を調べるわけですが、最近問題になっているのは「ランサムウエア※」というウイルスによる被害です。感染すると、多くの場合はファイルが暗号化されてシステムが使えなくなり、攻撃者から「元に戻したかったらカネを払え」などと要求されます。ビットコインのように匿名性の高い支払い方法を指定されることが多いです。

守りたいものの価値と失うことによる損失を把握していますか

ランサムウエアは外に出せない情報やシステムを止められない業種・業態を狙う

―― ランサムウエアに感染したら、自社で復旧させることはできないのでしょうか。

辻　企業では一般にメインとバックアップの2つのシステムを用意し、メインでトラブルが起きても、事業が継続できるようにしています。しかし海外の病院で実際に起きた事例では、犯罪グループは、まず一般には公表されていないバックアップシステムを、次にメインシステムを攻撃しました。先にメインを攻撃すると、すぐに気付かれてしまう可能性があるからです。このようなケースでは、被害を受けた側が気付いたときには既にバックアップが暗号化されているので、短期間でシステムを復旧させるのは困難です。

しかも、ランサムウエアにはいろいろな種類があり、工場の制御系コンピュータに特化したタイプもあります。制御系は一般のコンピュータにはない特殊なアプリケーションが入っています。それをターゲットにして攻撃するのです。ネットワークを遮断して自分に都合がよい環境を作ってからファイルを暗号化するので、システム管理者が状態を監視することができず、何が起きているのかが分からないまま全体を止めざるを得ない。その結果、事業全体に影響が及んでしまうのです。

―― 復旧と引き換えに“身代金”が要求されるとのことですが、実際に支払われているのでしょうか。

辻　水面下で解決している事案もあるので、全体像は分かりませんが、あるサイバー犯罪グループは2年間で600万ドル（6億4,200万円／1ドル＝107円）を稼いだそうです。

被害金額は必ずしも件数に比例しません。影響が事業全体に広がりやすい工場や、トラブルが人命に直結する病院が狙われ、多額な身代金が要求される傾向にあります。弁護士事務所や会計事務所など、個人情報や機密情報を扱う職種も同様です。

―― 企業の担当者からは「セキュリティ対策をしなければならないことは分かっているが、何から始めればよいのかが分からない」との声もあります。

辻　まずは、自社が守りたいものは何かを明確にすることです。私は、一律に「セキュリティ対策をしなければならない」とは考えていません。やるか、やらないか、どこまでやるかは、経営判断だと思うからです。例えば、1枚の100円硬貨を守るために、100万円の金庫を用意する必要はないですよね。でも、守りたいものがあって、それが自分にとって価値が高いものならば、それにふさわしい金庫を用意するはずです。自社が守りたいものは何か、それを失うことによる損失はどの程度か、回復できるものなのか、そこを踏まえた上で、セキュリティ対策が必要かどうかを考えてみてはいかがでしょうか。

事例を1つご紹介しましょう。誰もが知る大企業の会員向けポイントサービスに、不正ログインがありました。そのシステムはパスワード設定が数字4桁の簡単なもの。なりすましにより、会員が持っていた日本円にして70万円弱のポイントが盗まれました。事件を受けて、その企業は強固なパスワードを設定できるようにシステムを全面改修しました。

コストでいえば、ポイント被害分を補てんするほうが安上がりでしょう。しかし同社は改修を選びました。不正行為が再発した場合、システム上の不具合を放置していたことによるブランド力の失墜や顧客からの信頼感の低下と、セキュリティ対策費用とを天秤にかけ、改修に投資すべきだと判断したのです。

セキュリティ対策の理解に役立つキーワード

VPN（Virtual Private Network）
仮想プライベートネットワークの略称。暗号化などの技術を組み合わせて、インターネットや公衆回線網を自社の専用線のように扱うための技術のこと。既存のネットワークを使うため、専用線を構築するよりもコストは抑えられるが、公共の環境ゆえのリスクもある。

二要素認証
個人認証において種類の異なる2つの認証要素を用いること。個人認証にはIDとパスワードを用いるケースが多いが、認証要素を複数にすることでセキュリティレベルを高めることができる。

二段階認証
異なる種類の要素を組み合わせる二要素認証に対して、同じ要素を使うのが二段階認証。例えば、「IDとパスワード」と「秘密の質問」はどちらも「あなたが知っているもの＝what you know」なので二段階認証となる。二要素認証よりもセキュリティレベルは低い。

ランサムウエア（Ransomware）
コンピュータウイルスの一種。感染するとパソコン内部のデータの暗号化などにより操作が不能になる。その状態を解除するために多額の費用を請求される。ランサムとは「身代金」の意味。

ノルウェーの企業に学ぶリスク対応5つのポイント

―― もしもサイバー攻撃を受けた場合にはどう対処すべきでしょうか。

辻　ノルウェーに本社を置くノルスク・ハイドロ社（以下、ハイドロ社）の対応は、素晴らしいものでした。同社はアルミニウム生産や再生可能エネルギーなどの事業を展開する企業です。2019年3月18日深夜にサイバー攻撃を受け、翌19日には異常が起きたことを公表しました。何か事故が起きた場合、多くの企業は被害の範囲や程度を把握してから公表しますが、ハイドロ社は事態の公表を優先しました。

公表にあたってはFacebookなどのSNSの公式アカウントを総動員しています。通常、企業や団体のホームページがダウンすると、ユーザーがSNSで騒ぎ始めますから、臆測や噂が拡散する前に公式情報を発信するのは重要なことなのです。

そして同社はウェブキャスト（ウェブを使った動画配信など）で記者会見を配信しました。会場に集まったマスコミだけでなく、ウェブキャストの視聴者からも質問を受け付け、透明性を確保しました。

―― ハイドロ社の顧客や取引先にとっても、事態の成り行きは気になるところですよね。

辻　そうです。事態公表から頻繁に発信されたプレスリリースには毎回、「アルミニウム生産現場の復旧状況は70％」「手動で対応し、通常通りの稼働率を実現」といったセクターごとの復旧状況が記載されていました。

また、リリースにはCFO（最高財務責任者）の顔写真と署名入りのメッセージがありました。「当社はこういう状況ですが、外部の優秀な専門家に支えられながら自分たちの優秀なスタッフが頑張っています。私たちは早期にこの問題を解決することができると信じています」という内容です。リーダーシップが可視化された好事例です。

サイバー攻撃に遭わないに越したことはありませんが、もはや想定外は通用しない時代です。しっかり有事に備えていただきたいと思います。そして、事故対応ではハイドロ社の「迅速性」「SNS活用」「透明性」「頻繁な情報発信」「リーダーシップの可視化」という5つのポイントが参考になるはずです。

―― 素晴らしい対応ですね。とはいえ、やはりトラブルが起きないに越したことはありません。攻撃者に狙われないように自衛することはできますか。

辻　攻撃対象を決めるのは相手なので、狙われないようにすることはできません。まずは対策を取ること、その上で被害を最小限に抑える「ダメージコントロール」の手段を考えておくこと、この二段階の備えが大事です。そして、同業者や近しい業界が攻撃されたときには、「自組織は大丈夫だろうか」と考えてほしいのです。

辻 伸弘（つじ のぶひろ）

1979年生まれ。SBテクノロジー株式会社で法人公共事業統括プリンシパルセキュリティリサーチャーを務める。企業から依頼を受けて、外部から実際にシステムを攻撃してセキュリティ上の弱点を発見するペネトレーションテストを担当。新聞、テレビ、雑誌などさまざまなメディアで活躍するほか多数の講演に登壇。