



高橋教授の

この人に 会いたい

Vol.68

ゲスト

松田孝裕

氏

株式会社サイバージムジャパン取締役COO

身代金要求型ウイルス「ランサムウェア」によるサイバー攻撃を受け、診療停止に追い込まれる事件が起き、医療界に衝撃が走ったことは記憶に新しい。サイバー攻撃はいつ、どこで起きても不思議ではないだけに、対策は待ったなしの状況だ。巧妙化するサイバー攻撃の現状、病院が取るべき対策などについて、株式会社サイバージムジャパン(本社・東京都港区)の松田孝裕取締役COOと意見を交わした。

“サイバー先進国”イスラエルに学ぶ 万全なセキュリティ構築への第一歩

年間4億回の攻撃を受ける サイバー空間での戦争

高橋 今回は、病院にとって大きな関心事であり、喫緊の課題になっているサイバーセキュリティをテーマに、松田さんにおうかがいしたいと思います。まず、サイバージムという社名ですが、ボクシングジムと同じように、トレーニングしてサイバー攻撃に耐えられる人材を育てるイメージを思い浮かべ

ればいいですか。

松田 そうですね。サイバーのジム、トレーニング施設で、われわれはアリーナと呼んでいます。サイバージムジャパンは日本のサイバーセキュリティを強化するため2018年に創業しました。アリーナは国内主要都市の10カ所があり、APT(持続的標的型)攻撃の実践的な対処法などを身につける多彩なプログラムを用意し、企業のセキュリティ、システム開発部門担当者や経営者らに受講し

ていただいています。

ももとは13年に、イスラエル電力公社のもと、従業員へのサイバーセキュリティトレーニングやセキュリティオペレーション(SOC)を担う会社として誕生しました。同社は世界で最も多い、年間4億回ものサイバー攻撃を受けています。それにもかかわらず電気が消えないのは、トレーニングをしつかりとやっております。攻撃をきちんと検知できているからです。

高橋 サイバー攻撃を4億回も受けているとは衝撃的です。いったい、どのような人、あるいは組織が攻撃してくるのですか。

松田 ご承知のとおり、イスラエルは周りを敵国に囲まれていて、そうした国がサイバー攻撃をしかけてきます。コンピューター制御システムが攻撃を受けることがあり、2年ほど前にはイスラエルの水道局が狙われました。水道水の塩素濃度を規制値より高くする攻撃です。

逆に、イスラエルは、サイバー



攻撃によってイランの核施設建屋に火災を起こさせたことがありません。まさに、サイバー空間で戦争をしていると言っても過言ではありません。

中国のハッカーは20万人 世界情勢の混沌化で急増

高橋 世界的にハッカーの数はど

の程度増えているのですか。
松田 世界が混沌とするなかで、ハッカーも増えてきました。たとえば中国は20万人、北朝鮮には2万人いると言われています。00年

はほぼゼロでしたが、国を挙げてITやDXに力を入れてきた結果です。日本国内には、ホワイトハッカーでさえ1万人もいません。これからはハッカーの養成が急務です。

高橋 最近ではホワイトハッカーという言葉をよく耳にします。医療界においても、ICT化が進んでいる病院がホワイトハッカーを雇い、自分の病院を実際に攻撃してもらってセキュリティシステムの脆弱性を調べたという話を聞きました。「病院もそういう時代になったのか」とつくづく感じました。

松田 弊社でも病院のセキュリティ脆弱性を診断しています。医療機関の課題でもありますが、パソコンやネットワークのバージョンをはじめ、さまざまな医療機器がどうつながっているか、ソフトウェアに脆弱性がないかなどの全体像を把握している病院は、多くありません。脆弱性診断は人間ドックや健康診断と同じ。数値が悪く治療しなければならぬ場所を見つけて出し、どこから手を打つべきか、順位を決めるようなイメージです。



DX化でハッカー対策は急務

—— 松田

高橋 病院の規模にもよると思いますが、最初の「健診」と、実際にハッキングして脆弱性を調べる場合、費用はどれぐらいですか。

松田 100床程度の病院であれば50万円ほど。対処方法によっても変わってきますが、大病院になると200〜300万円です。パソコン、ネットワークを最新バージョンにアップするだけで簡単な

サイバー攻撃の80%は防げますが、それすらやっていないためにハッカーに侵入されてしまいます。

アップデートしていれば 大半のサイバー攻撃を撃退

高橋 100床クラスが50万であれば、十分手が届く範囲ですね。VPN回線でインターネットとつ

松田孝裕

Takahiro Matsuda
株式会社サイバージュムジャパン
取締役COO

まつだ・たかひろ ●1983年、慶應義塾大学経済学部を卒業し、富士通入社。39歳でプロセス産業第一部長就任。2003年、営業支援ソフトなどを提供するソフトブレン株式会社に入社。数百社超の顧客の営業改革に貢献した。05年、同社長に就任（08年退任）。総合寝具メーカーの株式会社エアウィーブ代表取締役社長などを歴任し18年、セキュリティ事業などを手がける株式会社バルクホールディングス取締役COO就任

なぐのは基本的なことですが、VPNの脆弱性となるとわからない世界になっています。病院経営者は、VPNの信頼性をどのようにとらえればいいでしょうか。

松田 ある程度VPNは信じていいと思います。しかし、VPNに接続するための機器やソフトに脆弱性があると、それは結局VPNではないのです（笑）。これからVPNを使った遠隔医療が進んでいくと思いますが、DXが進めば進むほど、セキュリティ対策をしっかりと講じなければいけません。たとえば、自分のパソコンに「バージョンアップしてください」とアラームが出ているにもかかわらず、バージョンアップする人はあまりいません。医療従事者のなかでも、I



サイバージュムジャパンの赤坂アリーナ。実践形式かつ最先端のサイバーセキュリティのノウハウを提供している

ITリテラシーのある人は多くないようです。

高橋 バージョンアップするとうなるのか、イメージがまったくできないことが大きいと思います。そもそも、脆弱性とは何なのでしょう。

松田 コンピューターのプログラムは、ウィンドウズなどのOS(コ

ンピューターを動作させる基本プログラム）が提供する機能を組み合わせて活用しながら作業をします。脆弱性とは、OSのなかのウイルスプログラムが悪用できるプログラム部分のことです。

マイクロソフトは「ウィンドウズをアップデートしていれば、大半のサイバー攻撃は防げる」と言っています。古いバージョンのウィンドウズには、ウイルスプログラ

ムが悪だくみに活用可能なプログラムが残っており、ハッカーはそこを利用して攻撃してくるので、バージョンをきちんと上げていけば防げるわけです。

高橋 OSの感染や感染拡大を誘発した原因となつているプログラム部分を悪用できないよう書き換えているのが、OSのバージョンアップと考えればいいですね。

松田 そうです。

病院は積極的に脆弱性診断を

—— 高橋

「ITリテラシーを高める」「治療の順位づけも大事

松田 セキュリティ対策のもう一つの柱は、ITリテラシーを組織全体で高めていくことです。攻撃者にとって一番簡単なのはパソコンに何かを潜ませることで、そこを踏み台にします。リテラシーがあれば、怪しいメールをクリックしてパソコンにウイルスを取り込んでしまうようなこともありません。

高橋 医療機関にとってセキュリティへの投資は高額です。全体のバランスを考えた場合、どこまで投資すべきなのか、病院経営者にとっての目安、指針のようなものはありますか。

松田 厚生労働省が出している医療情報システムの安全管理に関する

ガイドラインをきちんと履行することが基本ですが、治療の順番も大事です。身体全体を診察してどの臓器から治療したらいいのか。いきなり移植手術をする費用が高額になります。ほかに方法がなければ考え、治療の順位づけをきちんとすることが大事です。そのうえで現場のリテラシーを高めれば、サイバー攻撃の8〜9割は防げます。

実はちょうど今、国内企業20社がイスラエルを訪問し、サイバージムのトレーニング施設やイスラエル電力公社などを視察する見学ツアーを行つています。今後、医療機関を対象とした見学ツアーの開催も検討したいと思います。サイバー先進国の実態を自分の目で確かめれば、考え方も変わるでしょう。

高橋 まずは血液検査をして、おかしかったら身体全体を診断してもらおうということです。病気の進行を防ぐために手順を追って治療方針を立てるといっても、医療関係者にとってはわかりやすいです。本日はありがとうございます。



高橋 泰

Tai Takahashi

国際医療福祉大学教授

たかはし・たい●1986年、金沢大学医学部卒業、東京大学病院第1第3第2内科・麻酔科で研修。92年、同大学医学部医学系大学院医学博士課程修了（医学博士）後、米国スタンフォード大学に留学。94年、ハーバード大学公衆衛生校に武見フェローとして留学。97年4月、国際医療福祉大学医療福祉学部医療経営管理学科教授。2016年9月より21年3月まで安倍内閣未来投資会議の構造改革徹底推進会合医療福祉部門副会長を務めた