病院情報システム管理担当者＆CYLLENGE

複雑化・巧妙化・多様化が進むサイバー攻撃へのセキュリティ対策には仕組みと“人”の両輪が重要

大阪で高度な医療を提供している公益財団法人田附興風会 医学研究所北野病院では、情報システムのセキュリティ対策に力を入れている。同院で情報システム管理運用を担当している医療情報部 システム管理課 主任の平山洋輔氏と、国内セキュリティベンダ「CYLLENGE（サイレンジ）」代表取締役社長 津島 裕氏に、日本のサイバー攻撃対策の現況と課題について語ってもらった。

公益財団法人田附興風会 医学研究所北野病院
医療情報部 システム管理課 主任
ひらやま ようすけ
平山 洋輔氏

1989年大阪府出身。2012年近畿大学理工学部卒。医療システムズ株式会社を経て、2015年4月より北野病院勤務、現在に至る。

公益財団法人田附興風会 医学研究所北野病院（大阪市北区）

田附興風会は、田附政次郎氏が医学に関する総合研究に資することを目的に、京都帝国大学（現・京都大学）医学部に提供した寄附金を基に1925年に創立。3年後の1928年に、同財団の事業達成のために医学研究所北野病院を設置した。同院では、最新かつ高度な医療を提供し続け、現在は病床数685床、職員数約1700人の市内有数の大規模病院として地域医療に大いに貢献している。2025年は財団創立100周年を迎え、地域住民の健康を守る「予防医学棟」の建設をはじめ、さまざまな取り組みを展開している。

URL：https://100th.kitano-hp.or.jp/

――「ガイドライン6・0版」※1への改定から2年近くになりますが、未だにセキュリティに関する医療機関での事故・トラブルが多発しています。

平山洋輔氏（以下、平山氏）：事故・トラブルが多発している理由は、サイバー攻撃が巧妙化しているというイメージが強いのです。しかし、セキュリティ全般に言えることですが、最大の問題点は、やはり〝人〟です。サイバー攻撃という言葉だけを聞くと、狙われたら防ぎきれないイメージがありますが、実際に被害を受けた医療機関での事故・トラブルのレポートを拝見すると、実はファイアウォールやファームウェアが最新のバージョンになっていなかったり、運用ルールで禁止されている事項が周知徹底されていなかったり、結局、セキュリティに精通していない人が聞いても「それはおかしい」と思うようなことが原因になっているケースがほとんどです。

当院では、ガイドラインで提示されている病院情報システムに対する要件の見直しや、運用等に関する規程のチェックを行っています。また、診療報酬の面でもサイバー攻撃対策を実施している医療機関に対して診療録管理体制加算1が新設され、職員教育がその条件に定められていることから、多くの医療機関で教育が為されているはずです。

しかし、その職員教育について、個人の認識から集団全体の規範にまで高めているかというと、それにはまだ時間が掛かると感じています。

――セキュリティ対策を怠った際のリスクをサイバー攻撃に対するセキュリティ対策の専門家の立場からお聞かせください。

津島 裕氏（以下、津島氏）：平山様が仰ったとおり、最近のサイバー攻撃は、より巧妙化・悪質化しています。一般的には、システム内に侵入してファイルやデータをロックしたり、情報を搾取して身代金を要求するケースが知られています。日本では個人の権利利益を害する恐れがある個人データの漏洩等が発生した場合は速やかに個人情報保護委員会に報告する義務があるのですが、当社がダークウェブをチェックすると、それらの事故やトラブルについて報告されていない企業や団体がたくさん見つかります。先述したデータロックや情報搾取による身代金

※1：2023年5月に策定された「医療情報システムの安全管理に関するガイドライン6.0版」を指す。

の要求だけでなく、このような報告義務違反についても身代金を要求するケースも出ているようです。

また、サイバー攻撃は一種のビジネスになっており、パスワードを搾取する集団や企業や団体のサーバを攻撃する集団などに分業化が進んでいます。我々ベンダとしても、そのようなサイバー攻撃を防ぐ対策システムを提供していますが、仕組みだけで100%防ぐことは難しいのが現状です。当社も、サイバー攻撃に対する防御については、仕組みの構築と意識の徹底が両輪となって機能するべきと考えており、セキュリティに対する職員全員のリテラシーを向上させていかなければなりません。自然災害だけでなく、セキュリティ対策やサイバー攻撃対策もBCP対策の1つとして、サイバー攻撃を受けた際の訓練等を実施して職員の危機意識を高めることが必要です。

平山 洋輔氏（左）と津島 裕氏（右）。

――職員の入退職が多い医療機関では、教育も難しくないですか。

平山氏：職員教育の観点から述べると、ランサムウェア等の攻撃が巧妙化したとはいえ、結局、職員に要求することは本質的にさほど変わっていません。つまり「怪しいメールや添付ファイルを開いてはいけない」のです。このようにセキュリティ対策の在り方は変わっていないのにも関わらず、その被害ははるかに大規模なものになっており、このギャップを埋めるのがとても難しいと感じています。基本的なルールを守っていれば、大部分の攻撃は防げるのですが、ずっと同じ話を聞かされることで慣れが生じてしまい、それが危機意識の低下に繋がってしまっているのではないでしょうか。

当院では、入職時に個人情報を絡めて教育を行っていますし、先述した診療録管理体制加算1の要件どおり、年に1度、講師を招いて講習会を開催しています。

北野病院のセキュリティ対策―利便性に配慮した高度な対策を実施

――職員教育以外に、北野病院でのセキュリティ対策を具体的にお聞かせください。

平山氏：当院では電子カルテ端末等のエンドポイントにおけるウイルス対策や記憶領域を持つUSBメモリの接続制限、それと操作ログの収集や仮想インターネットやSPAMメール対策、不正接続の検知などを行っています。

ウイルス対策及びUSB対策では、DLP（Data Loss Prevention）ソリューションによって機密情報や重要なデータの漏洩や消失を防ぐ対策を構築しており、USBメモリはシリアルナンバーで管理し、それ以外のUSBメモリを受け付けない環境となっています。

また、中央監視できるタイプのウイルスセキュリティソフトも導入しており、ウイルスを検知した際には、システム管理課の警告灯が点くことにより即時対応できるよう工夫しています。ただ、システムでは自動的にウイルスの処理が行われるので、警告灯が点いた時点で対策が完了しているケースがほとんどです。

――電子カルテ端末でインターネットを使用できる工夫もされていますね。

平山氏：他の医療機関では、厳しいセキュリティ対策を徐々に緩和して利便性を高めるという方向性で進化しているのに対し、当院は緩かったセキュリティ対策を徐々に高めていくという方法で進めている点が大きな違いです。

2015年に私が当院に入職した頃は、恐ろしいことに電子カルテ端末でインターネットを直接使用することができていました。直ちにインターネットと電子カルテ系のネットワークを分離したかったのですが、学会の資料準備等のために院内でインターネットを活用したいという要望は強く、当時、システム管理課で情報インフラを担当していた職員が中心となって、専用の仮想サーバ上で仮想ブラウザを稼働させ、業務ネットワークとは分離した上で、電子カルテ端末上でインターネット検索やWeb閲覧が可能な仮想インターネットを導入しました。現在、仮想インターネット環境は2023年に更新・バージョンアップしており、その際にはCYLLENGEの「Smooth File」を導入してファイルのウイルスチェックに役立てています。

――電子メールの送受信環境についてはいかがでしょうか。

平山氏：電子メールについても、電子カルテ端末上で送受信が実行可能な環境となっています。2024年には、膨大なSPAMメールによってSPAM対策システムがパンクしてしまうトラブルを防ぐためにクラウド式のSPAM対策システムを導入し、成果を出しています。現在は、クラウドによるグループウェアの導入を進めており、外部とのメールの送受信はそちらに限定するなどの対策を図っています。

――セキュリティ向上と利便性を両立させることは難しいですね。

津島氏：以前は、そこまでランサムウェアなどサイバーセキュリティへの意識が全体的に低い時代でしたので、利便性が高い方向に流れることはよくあります。サイバーセキュリティ対策に本腰を入れるとなると、利便性とセキュリティは相反関係にあるので、如何に利便性が高い

状態でセキュリティを担保するかが大きな課題です。

――PPAP※2対策についてはいかがでしょうか。

平山氏：SPAMメール対策の1つとして、PPAPで添付ファイルを受けとれないようにしたのですが、職員より厳しいお言葉をいただいております。銀行や一部の企業では、自社のソリューションによって自動で暗号化する仕組みのため、PPAPでなければメール送信ができないなど、PPAP以外の手法に切り替えていただくようお願いすることが難しいということも少なくありません。信頼できる送信元のみ受信を許可するなどして個別対応している状態です。

――日本でPPAPが広まったのはなぜでしょう？

津島氏：PPAPは日本だけで起きている問題です。海外にはPPAPという概念は全く無く、何故か日本だけ、〝PPAPはセキュリティが高い〟という誤った認識が広まってしまい、後で問題となりました。当社もPPAPは安全なセキュリティ対策とは考えておらず、PPAPを利用しない、セキュリティを更に高めるソリューションを提供しています。送信側が工夫すればPPAPの送信を防ぐことは可能ですが、PPAPが送信されてくることは防ぎようがありません。今後は、社会全体でPPAPにリスクがあることを啓発していくことが、我々ベンダ側の課題であると考えています。

サイバー攻撃の脅威―リモート環境・地政学的対策も重要

――「情報セキュリティ10大脅威」がPAから発表され、「サプライチェーンや委託先を狙った攻撃」や「リモート環境を狙った攻撃」がランクインしました。

平山氏：〝電子カルテはクローズ〟という認識を改める必要がありますね。リモート保守のサービスはどこのベンダでも普通に提案してきますし、厚労省が電子処方箋や電子カルテのデータをクラウド上で共有するように指導し始めていることもあって、院内のシステムに関する外部接続点は増加し続けています。

情報システムベンダのリモート保守に対しては、当院が提供するファイアウォールの環境を使うよう指示し接続状況の管理に努めていますが、ベンダの中には自社の規程で独自の閉域網を利用する企業もあり、必ずしも守れているわけではありません。

2024年度に厚生労働省が「医療機関におけるサイバーセキュリティ確保事業」を実施した際、当院も参加したのですが、その時、当該事業担当のベンダが驚くくらいの接続点が見つかり、また、システム管理課でも把握しきれていないことが明らかになりました。事情を調べると、システムではなく医療機器にもリモート用の外部接続点があり、管理の難しさを痛感しましたね。

調査では幸い、致命的な問題点は見つからず、一部システムでファームウェアを最新バージョンに更新するなどの対応程度で済みましたが、システムではない機械や装置の更新までシステム管理課が関われるわけではありません。そのため、全てのリモート環境を使った攻撃を検知したり、防ぐことは現状では難しいと考えており、どのような対策が必要かを検討しているところです。

津島氏：ファームウェアが最新のバージョンになっていても、修正プログラムが提供される前に攻撃を行う「0日目（Zero Day）」攻撃という手法があり、必ずしもファームウェア等を最新バージョンにすることも決して万全の対策とは言えません。セキュリティ対策については、今後の流れとして「ゼロトラスト」の考え方に基づき、個々で防衛することが主流になると考えています。しかし、ゼロトラストの考え方は重要ですが、それだけのセキュリティを担保するためには、コストが必要なため、現実的に取り組めるかは難しい問題だと言えます。

平山氏：セキュリティは突破されて非難されることはあっても、セキュリティ強度を高めた結果の評価を得ることは難しいのが現状です。あるとき、SPAMに関して、医療情報委員会に当院に送信されてくるメールの件数とその内訳を報告しましたが、その件数の多さ、比率の高さに皆驚いていました。コストについても、セキュリティ対策ソフトは価格と機能が必ずしも比例している訳ではないので、理解を得ることが難しいです。

しかし、最近の物価高騰により、サイバー攻撃を受けてハードウェアの買い替えを余儀なくされることも大きなリスクです。すぐに品物が納品されなかったり、価格高騰で同レベルの製品を導入できなかったり、従来は買い切りだったソフトがサブスク対応になってコストが上昇するなどのリスクもあり得ます。このようなリスクを丁寧に説明して、経営層の理解を得る必要があると考えています。

――大阪万博開催で、大阪方面をターゲットにしたサイバー攻撃が増えることが予想されています。

平山氏：「10大脅威」にも挙げられている「地政学的リスクに起因するサイバー攻撃」が2025年に初選出されましたが、まさにこれが当てはまると言えます。

情報セキュリティ 10大脅威2025［組織］

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサムウェアによる攻撃	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

独立行政法人 情報処理推進機構（IPA）発表資料より

※2：「メールでパスワード付きのZIPファイルを送り、別メールでパスワードを送る」ファイル共有の方法。「Passwor d（P）付きファイルを送ります。」「Password（P）を送ります」「暗号化（A）」「Protocol（P）」の頭文字が由来。

先ほど、津島社長から「サイバー攻撃はビジネス」というお話がありましたが、攻撃を実施するだけでお金を得ることができるというビジネスモデルがすでに存在しています。これは、泥棒と放火犯の違いに似ていて、例えば航空会社の予約システムをダウンさせても直接的な利益はありませんが、航空会社は大きな被害を受けてしまいます。

実は当院でも、２０２１年に開催された東京オリンピックや２０２３年に開催されたG７大阪・堺貿易大臣会合の開催前後で大量のＳＰＡＭメールが送られ、メールの送受信が滞る事態が起きました。また、ファイアウォールに対する不正アクセスの大量攻撃を受けたこともあります。このような不正アクセスやＳＰＡＭメールの受信は現在も起こっており、万博期間中も心配しているところです。

津島氏：過去のオリンピックの事例に見られるとおり、イベントに関連してサイバー攻撃の件数が急激に増えることは多く、今回の関西万博でも増えることが予想されます。平山さんが述べたとおり、「10大脅威」の１つである分散型サービス妨害攻撃（DDoS攻撃）が増え、データロックや情報の搾取が目的ではない、システムを停止させて混乱を誘発するタイプの攻撃も増えるでしょう。

病院・システムベンダも含む医療界全体での交流も必要

――セキュリティの話題で、病院間での交流はありますか。

平山氏：病院間でシステムの話をする際は、やはり自施設にとって業務の効率化といった機能面での話題が中心で、セキュリティに関する話はあまりしませんね。セキュリティ対策製品は効果が分かりにくいため、経営層に対する評価を得にくいのは、先ほども述べたとおりです。

津島氏：ゼネコン業界は、セキュリティ対策に関する交流を積極的に行っています。特にスーパーゼネコンは定期的な情報交換を実施しており、それらのスーパーゼネコンが採用した製品が中堅以下の企業に普及しているという流れがあるようです。

しかし、医療業界はそうではないという話でした。医療業界でサイバー攻撃を受け、多くの事故やトラブルが発生しているところを見ると、医療業界でもセキュリティ対策に関する交流が必要なのではないかと感じています。

――セキュリティ対策を進めたい医療機関に対してアドバイスがあればお聞かせください。

平山氏：サイバーセキュリティ対策は重要、という点については１００人が１００人、そのとおりと答えるでしょう。しかし、現在はスマートフォンに代表されるように、人々が利用するサービスは多様化して、非常に便利に、しかも安価となっています。そのため、よりセキュリティに配慮している病院のシステムは、それに比べて利便性の面でどうしても見劣りがしてしまいます。

「医療情報システムの安全管理に関するガイドライン６・０版」では経営管理・企画管理・システム運用の３編に分かれて策定されています。なぜ、今回分かれて提示したのかを踏まえて、医療情報に関するセキュリティを各医療機関が考えていかなければなりません。

津島氏：当社としては、セキュリティ対策は、医療機関だけではなく、その先にいる患者を守るためにもたいへん重要な課題だと考えておりますので、医療系のイベントに出展してセミナーの開催や、医療ＩＳＡＣでの研修支援などを行いながら、セキュリティ対策の重要性に対する啓発活動に取り組んでいきたいと考えています。

津島 裕（つしま ゆたか）氏

1973年京都府出身。1999年株式会社プロット入社、同社のインターネット事業の立ち上げに参画。2003年より「企業間コミュニケーションをセキュアにする」というコンセプトの下、セキュリティ関連製品開発に着手、同社の売上規模を5倍以上に成長させる。2006年同社代表取締役社長に就任、2024年社名を株式会社「CYLLENGE」に変更、現在に至る。

株式会社CYLLENGE（サイレンジ）

株式会社CYLLENGEは、1968年に写植組版の企業として創業した「株式会社プロット」を前身としており、1999年にインターネット事業部を設立、2003年よりセキュリティ分野に事業を集中していき、2024年1月5日に社名を現在の「CYLLENGE」に変更した。「CYLLENGE」は、同社の事業領域でもある「Cyber」と、創業当初から大切にしている開拓者の精神である「Challenge」を組み合わせた造語で、同社の思いを反映した名称となっている。

＜所在地＞
【大阪本社】大阪府大阪市北区梅田3-3-10 梅田ダイビル12F
【東京本社】東京都港区三田3-11-36 三田日東ダイビル2F
【名古屋営業所】愛知県名古屋市中区栄1-3-3 AMMNATビル7F