

3/13
セミナー
レポート

診療所・クリニックの
サイバーリスクへの対応
を考える

3月13日、県保険医協会では診療所等におけるサイバーリスク対応セミナーを開催。

2021年からサイバー被害が急増

講師の松山氏は、まず近年のサイバーセキュリティ関連事案の傾向について解説。2020年まではホームページ等への攻撃やデータUSBの紛失等によるトラブルが主だったが、2021年に入ってからエモテットとランサムウェアによる被害件数が急増、かつ攻撃手法が高度化していると説明した。公表された被害件数だけでも2018～2020年の3年間で16件だったのに対し、2021～現在の1年2カ月間ですでに18件発生している。

エモテットとは？対策は

エモテットとは、攻撃者からのなりすましメールに添付されたファイル等を実行操作してしまった場合にウイルス感染するという攻撃手法。最近では迷惑メールフィルターが発達し、悪質なリンク添付のあるメールが弾かれるなどの対応がされるようになったが、そこに付け込んでメールフィルターをすり抜けるZipファイル形式でウイルス付きのWordやExcelファイルを送ってくるという事例が増えている。

2021年7月には岡山県の大学病院でもなりすましメールを受け取った従業員が添付リンクを踏んでしまったことにより、患者情報等を保管していたクラウドサービスの認証情報(ID、パスワード)が不正入手された。認証情報が一度入手されてしまうと、攻撃者は従業員の振りをしてログインし、データの閲覧やメールの送信先等を容易に入手でき、更なるなりすましメール送信のための踏み台に利用する。

このケースの問題は、①複数施設で勤務する非常勤医師などが、病院の指定しないクラウドサービスへの患者情報の保存や、指定しないメールサービスの個人的な利用が常態化していたこと、②病院のクラウドサービスの認証項目がIDとパスワードのみで強度が足りなかったことがあげられる。

2020年には日本医師会でもエモテット被害に合い、医師会を名乗ったメールが会員等に送られ拡散した。さらにその際のメール送信先リストが再利用されるとみられる二次被害も2021年末に発生している。

エモテット対策では、指定外の個人的なクラウド、メールサービスの利用を禁止することや、メール送受信時の

ファイル添付を禁止すること、疑わしいファイルが届いた場合は安易に開かず、ウイルスチェッカーに通すことなど共通認識を持つておくことが有効だ。また、指定サービスへのログイン時にもワンタイムパスワードの設定など認証強度を高める対策も必要だ。

ランサムウェアとは？対策は

ランサム(身代金)ウェアとは、何らかの方法で攻撃対象の端末をウイルス感染させ、システム障害やデータの暗号化などを実行した後、復旧のための身代金を要求する攻撃手法を指す。インターネット接続のある電子カルテ利用端末や検査機器の画像共有システムなどのネットワーク接続元から主に侵入される。

販売業者が「インターネットに繋がらないので安心」と謳って導入した電子カルテのVPN(通信事業者の独自ネットワーク上に作る仮想専用線を指す)が実際にはインターネット接続タイプだったことが攻撃点となったケースや、CTやMRI、遠隔読影システムなどの院内ネットワークとして導入した機器が実は遠隔保守サービスとセットになっていて、知らずに外部に繋がっていたケースが多くみられる。また、それらの機器のウイルス対策プログラムの定期更新を販売業者側が行うものと勘違いし、導入初期のままセキュリティが脆弱になっていたり、トラブル発生時にはサポートサービスが終了していた事例は業界では「あるある」だ。

主なランサムウェア対策としては、①インターネット接続タイプであ

れば、VPN機器の定期的なシステムアップデートをしたり、インターネット通信の送受信時にウイルス検知を行うハードウェアを導入する、②インターネット非接続のタイプであれば、内部サーバや端末のOSの脆弱性を感知・修正する市販のUSB型ウイルス検索・駆除ツールを使用する、③クラウドサービス等のバックアップシステムに保存するデータを後から変更できない状態で保存することなどが有効だ。




日々警戒心を持ってデータ管理を

医療機関でサイバー攻撃を受けた場合のリスクは情報漏洩だけではない。ひとたび事故が起きると、入院患者の管理や、手術の延期、救急受け入れ困難、外来停止等になり、患者対応も複雑になるほか、対応する従業員の疲労やストレスによる医療安全上のリスクも発生しやすくなる。営業機会損失による収入減や、システム復旧や被害調査にかかる費用、外来停止中の紙カルテ作成や会計の後日請求など、費用面でも負担が重くのしかかる。

ほとんどのサイバー被害に共通する攻撃者背景として、医療機関を専門的に狙った活動ではなく、あくまでもセキュリティ対策不足の施設がリストアップされた中で、偶発的に攻撃対象に選ばれたと推測する。自分の医療機関は小規模だから大丈夫だろうと思いつまらずに、オンラインによる診療が活発になっていく今こそ正しく警戒心を持って日頃のセキュリティ強化に繋がっていかなくてはどうか。

新型コロナ関連の支援制度 (2022.3月時点)

新型コロナの影響を受けて減収した場合や休業の際の助成制度について、2022年3月時点で利用できる制度を下表にまとめた。

制度名(事業者)	対象	給付額	申請締切	詳細
事業復活支援金 (中小企業庁)	①②いずれも満たす中小法人・個人事業者 ①新型コロナの影響を受けた事業者 ②2021.11月～2022.3月のいずれかの月の売上高が、2018.11月～2021.3月の同月の売上高と比べて30%以上減少した医療機関	50%以上減： 個人50万円、法人100～250万円 30～50%未満減： 個人30万円、法人60～150万円	2022.5.31 必着	
雇用調整助成金 (厚労省)	売上高が前年同月比5%以上減少し、雇用維持のために従業員に休業手当などを支払う事業者	休業手当などの費用のうち、1人あたり日額上限9,000円(1～2月分は11,000円)	対象となる期間の最終日から2カ月以内	
小学校休業等対応助成金 (厚労省・都道府県労働局)	雇用する労働者の申出により、2021.8.1～2022.3.31間に、①新型コロナに関する休校等、または②子どもが新型コロナに感染、疑似症状などにより親に有給休暇を取得させた事業者	(いずれも日額上限額) 2022.1月～2月取得分：11,000円 2022.3月取得分：9,000円 ※まん防実施期間中は15,000円	2022.5.31 必着	

春の共済募集キャンペーン実施中



保険医年金

老後の蓄え、資金運用に!

申込期間：4月1日～6月15日
加入日：9月1日

グループ保険

万一の死亡・高度障害に備える

申込期間：随時受付

お問合せは ☎ 026-226-0086 まで

休業保障

病気・ケガでの休業に備える
新型コロナ感染にも対応!

2種類の取扱いがごございます。
詳細はお問合せ下さい。

