今月の視点

医療機関のサイバーセキュリティ

常任理事　中村　　洋

徳島県つるぎ町立半田病院は2021年10月31日、電子カルテシステムが、盗んだデータを暗号化して利用不能にし、元に戻す代わりに金を要求するウイルス「ランサムウェア､Ransom（身代金）＋Software」に感染したと発表した。

感染したのはシステムのメインサーバで、患者約８万５千人分の個人記録が保存されていた。サーバへのアクセスができないため、11月１日から新規診療などの受け入れが停止された。31日午前０時半ごろ、英語で「あなたのデータは盗んで暗号化している。ランサムにお金を払わないと特別なウェブサイトにデータを公開する」と書かれた文書がプリンタから大量に出力され、感染が発覚した。システム担当の職員や電子カルテシステムのメーカーなどに連絡したが、対応できなかったため、午前８時55分ごろ、美馬署と県警本部に被害届を提出した。11月７日現在、電子カルテシステムは復旧せず、約100人の看護師が紙カルテを新たに作成して対処している。また新たな電子カルテシステムの導入について検討を始めた。

2021年５月31日には東大阪医療センターの遠隔読影システムが、サイバー攻撃を受け、大量の診断画像が暗号化され、犯人の要求に応じなかったため、数万枚が見られなくなった。

2018年10月には奈良県の宇陀市立病院の電子カルテシステムがウイルス感染し、電子カルテシステムの利用が不可能となり、さらにシステムデータが暗号化され、バックアップも正しく取得されていなかったため、長時間、患者1,000人以上のカルテが閲覧できなくなった。

本年６月には東京都新宿区のクリニックがサイバー攻撃を受けカルテの一部が閲覧できない状態になった。約４か月かけてやっと復旧することができた。その他ランサムウェア感染に対して密かに身代金を払った医療機関もかなりあるという。

攻撃者はどのようにして医療機関のシステムに被害を与えるのか？まず病院の医療情報システムへの侵入口を見つける。そのためにメールによるフィッシング（なりすまし）攻撃や、ソフトウェアの脆弱性を利用するのが一般的だ。システムに侵入すると、バックドア（コンピューターへ不正に侵入するための入り口）を仕掛け、ユーザーのPCにマルウェア（悪意のあるソフトウェア）をインストールする。遠隔画像診断システムで脆弱なVPN（インターネット上の仮想の専用線）を用いたり、セキュリティ保護が十分でない自宅のPC等から病院のシステムに接続したり、業務用PCで個人的なメールを閲覧したりすることはリスク要因になる。セキュリティが弱くなりがちな個人向けメールシステムを狙うフィッシング攻撃もある。

次に、攻撃者はシステム内を動き回り、バックアップやドメイン管理、OSそのものなど、止まると病院運営に重大な影響を与えるシステムにアクセスする管理者権限を奪取する。

最後に、攻撃者はシステム管理スタッフが手薄になりがちな週末のうちに、アクセスできる全てのファイルを暗号化する。

攻撃者は情報やシステムを使用不能にし、業務継続を人質に取って、暗号解除鍵の代金、すなわち身代金を要求するだけではない。身代金が期限内に支払われなければ、盗んだ情報を漏洩させると被害者を脅す。盗んだ情報の一部をマスコミにながしたり、ネット上に晒すこともある。

厚生労働省が令和３年６月28日付で発出した「医療機関を標的としたランサムウェアによるサイバー攻撃について（注意喚起）」の中でランサムウェア攻撃への対策として必要なことは
（1）組織のネットワークへの侵入対策
（2）インシデント対応体制の構築
（3）データ・システムのバックアップ
（4）情報窃取とリークへの対策
（5）医療情報システム等のセキュリティ対策
（6）その他医療機器のサイバーセキュリティ対応に係る留意点
と簡潔にまとめられている。

（1）組織のネットワークへの侵入対策、は重要だ。実際にどのようにすれば攻撃者の侵入が防げるのか？

電子カルテ、医事会計システムなどの医療情報システムをVPNも含めてインターネットに繋がないのが一番良い。インターネットに繋いでも、メール受信やWeb閲覧をしなければリスクはかなり低くなる。インターネットを通じて、医薬品などのマスターをダウンロードする仕様の医事会計システムや電子カルテもあるが、医療情報システム上では通常のメールの送受信やWeb閲覧を行うべきでない。どうしてもマスターなどのダウンロードのために医療情報システム内でメールの受信やWeb閲覧等が必要なら、業務専用のメールアドレスを作るべきである。もし知らないところからメールがきても、すべて開封せずに削除する。業務に必要なメールでも、メール内のWebのリンクをすぐには開かない。リンクの部分にマウスカーソルを当てれば（クリックはしない）、直下やステータスバーなどにリンク先アドレスが表示される。このアドレスと、メール中に表記されたアドレスが異なる場合には、偽メールであると考えてよいだろう。複数のリンクがある場合、一つのリンクだけがフィッシング用の偽リンクということもあるので注意が必要である。外部事業者から添付ファイル付きのメールが送られてきても、開く前に事業者に電話等でファイルを送ったかどうかを確認するぐらいの慎重さが求められる。業務に必要なサイト以外のWeb閲覧は行わない。

最新のセキュリティパッチを当てる、ウイルス対策を行う等、使用者の責任において医療情報システム内のパソコンの管理を行う必要があるが、なれないうちは外部事業者に相談する方が良い。ただ、外部事業者に任せきりにすることはリスクであり、外部事業者を管理することが重要である。外部事業者が持ち込んだパソコンからウイルスが拡散した例もある。保守事業者等との接続回線から攻撃を受けた例もある。前述の半田病院も「サーバーの遠隔保守用の通信回線などが、侵入経路の可能性がある」と発表している。同等かそれ以上のセキュリティ対策を委託先の外部事業者に求めることが必要だ。

USBメモリなどの外部媒体は情報持出のリスクだけでなく、外部媒体を介したウイルス感染も起こりうる。新品のものも含めてUSBメモリは一切用いないことが望まれる。市販のUSBには中にアプリが入っていることもあり、実際ウイルス入りのUSBメモリが販売されたこともある。物理的にUSBポートを塞ぐ（例えばテープで塞ぐ）のがよい。電子カルテからデータを書き出したいときには、新しいまっさらなCD-RやDVD-Rディスクを用いる。

また医療情報ネットワークでは無線LANの使用は極力避けることが望まれる。やむを得ず使用する際は現時点ではWPA2による暗号化を行い、電波の届く範囲を必要最小限にする。

（3）データ・システムのバックアップも、万が一の時の事業継続のために重要である。被害は感染端末のみならず、医療情報ネットワーク上の別の端末、サーバやクラウド上のデータにも及ぶ可能性がある。データをバックアップする際には、定期的に複数のメディアにバックアップを行い、バックアップ後は医療情報ネットワークから切り離しておくことが重要である。

医療機関におけるサイバーセキュリティ対策に資するために、2021年１月29日に厚生労働省により策定された「医療情報システムの安全管理に関するガイドライン 第5.1版」の別添資料として「医療機関のサイバーセキュリティ対策チェックリスト」及び「医療情報システム等の障害発生時の対応フローチャート」が2021年10月22日に公表された。

チェックリストは、医療機関のサイバーセキュリティ対策の現状を把握することを目的に、そのチェック項目を整理したものであり、(1) 経営層向けチェックリスト、(2) システム管理者向けチェックリスト、(3) 医療従事者・一般のシステム利用者向けチェックリストーの３種類から構成されており、医療機関のどの部分に弱みがあるのか把握し、優先的に必要な対策を検討する一助となるものだ。

フローチャートは医療機関がサイバーセキュリティの体制整備を行うにあたり、平時の備えや障害発生時に各担当者が行う対応について、まとめられており、体制整備や障害発生時の対応の確認を検討する一助となるものである。

まずは、(3) 医療従事者・一般のシステム利用者向けチェックリスト（**図**）をみて、回答してみて欲しい。次に、必要に応じて（1）経営層向けチェックリストや（2）システム管理者向けチェックリストも確認して欲しい。

また厚生労働省は、(経営者向け)、(システム管理者・セキュリティ管理者向け)、(医療従事者向け）の「医療機関等向けサイバーセキュリティ研修用動画」や「医療機関等向け情報セキュリティ研修教材」をホームページで公開している。是非ご覧になっていただければと思う。

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

ランサムウェアによる攻撃はこれからますます広がっていくことが予想される。特に長い休暇が続く年末年始は要注意だ。あとで後悔しないためにも早急に対策を取ることが求められる。

医療従事者・一般のシステム利用者向け　サイバーセキュリティ対策チェックリスト

記入者	日付

NO	チェック項目	チェック欄（○or×）
1	業務に不要なWEBサイトへのアクセスをしていないか	
2	システムの異常があった場合、院内のどこに連絡し、相談すればいいのか知っているか	
3	利用者が個人情報を入力・参照できる端末から長時間離席する際に、正当な利用者以外の者による入力のおそれがある場合には、クリアスクリーン（画面が他人から見えないようにするために、操作しないまま一定の時間が経つと自動的にパスワード付きスクリーンセーバーが起動するようにしたり、または自動的にログオフするように設定すること）等の対策を実施しているか	
4	従業員個人のUSBメモリ等の外部媒体を使用していないか又は業務上、外部媒体の使用が必要な場合は事前に申請し、医療機関が管理している外部媒体を使用しているか	
5	ソーシャルエンジニアリング（人の心理的・社会的な弱点や盲点をついて入手する手法）について理解し、安易にID・パスワードや個人情報等を外部提供しないようにしているか（本人確認やリンク先やメールアドレスの再確認等をした上で回答する等）	
6	見知らぬ相手先等からの添付ファイル付きの電子メールやリンク先のクリックは注意しているか（受信メールの信頼性を確認する、添付ファイルを開かない、安易にクリックしない等）	
7	メール送信前にメール送信確認画面を再度表示し確認したり、メールの遅延送信機能（送信ボタンを押しても、すぐに送信されず、任意の時間の経過後メール送信される機能。メール送信の取消等が可能となり、誤送信の防止に有用となる）等を活用し、メールの誤送信を防止しているか	
8	重要情報は電子メール本文に書くのではなく、添付ファイルに書いてパスワードなどで保護しているか なおパスワードは別手段で知らせる、あるいは事前に取り決めておく等の手法とセットで行うこと	
9	アップデート（ソフトウェアを最新の状態に更新すること）の通知が届いたときは、医療機関内の情報システム部門または担当者に確認したり、事前に情報システム部門より、対応方法の連絡がある場合は指示に従って処理をしているか	
10	患者の情報について目的外使用をしていないか	

図（厚生労働省ホームページより）