医療界の現在進行形を読む／ MMPG 医業経営ジャーナル

MMPG 医業経営 Journal

2023 8 Vol.265

発 行　メディカル・マネジメント・プランニング・グループ　TEL03-6721-9763（代）FAX03-6721-9764　https://www.mmpg.gr.jp

【キーワード】サイバー攻撃対策

医療機関に求められるサイバーセキュリティ対策

医療機関を狙ったサイバー攻撃が相次いでいます。なかには、数カ月も診療停止に追い込まれたケースもあります。そこで今回は、「医療情報システムの安全管理に関するガイドライン第6.0版」の概要を含めて、医療機関のとるべきセキュリティ対策について考えます。

規模の大小を問わず サイバー攻撃対策は必要

サイバー攻撃とは、パソコンやサーバーにつながっているネットワークを介した、システムの破壊やデータの窃盗などを指します。

その目的は多岐にわたりますが、医療機関に対しては「ランサムウェア」というウイルスによる攻撃が増えています。このウイルスに感染すると、端末に保存されているデータが暗号化され使えなくなります。そのうえで、攻撃してきた側は、データを復活させる対価として金銭を要求してくるのです。実際、ランサムウェアに感染し、通常診療の再開まで約２カ月間も要した病院もありました。また、直接的にサイバー攻撃を受けた医療機関の地域連携システムなどを介して、他の医療機関にも被害が拡大するようなリスクもあります。

つまり、規模の大小を問わず、医療機関にとってサイバー攻撃は対岸の火事とは言えず、その対策は喫緊の課題となっているのです。

サイバー攻撃の巧妙化受け ガイドラインを更新

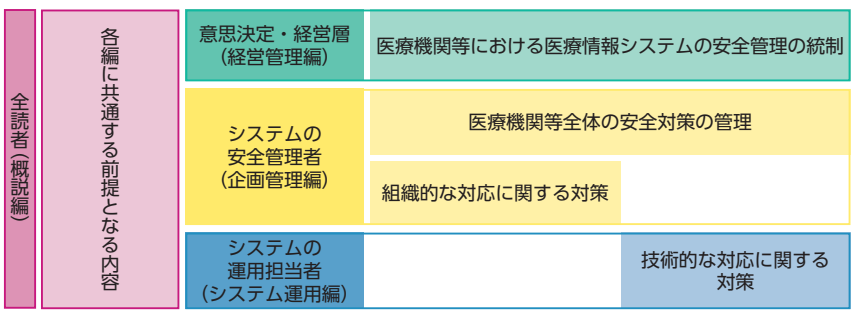
サイバー攻撃の多様化や巧妙化で診療業務等に大きな影響が生じていることを受けて、2023年４月、医療法施行規則改正により医療機関や助産所の管理者にサイバーセキュリティ対策が義務化されました。それに対応して2023年５月31日、「医療情報システムの安全管理に関するガイドライン」も更新されました。最新版となる第6.0版では、ガイドラインの理解を促し、医療情報システムの安全管理の実効性を高めるために、全体の構成や内容が大きく見直されています。

経営層と実務層に分けて 行うべき対策を提示

第6.0版の主なポイントの１つは、実効性を高めるために想定読者ごとにガイドラインを分けていることです。具体的には、ガイドラインの目的や全体構成などをまとめた「概説編」に加えて、経営管理層向けの「経営管理編」、セキュリティ安全管理担当のための「企画管理編」、そしてシステム運用担当者を対象とした「システム運用編」となっています（**図表**）。

なお、経営管理編では、安全管理に対する責任・責務をはじめ、医療情報システムに対するリスク評価を踏まえた安全管理やセキュ

図表　ガイドライン 第6.0版を構成する各編



出典：医療情報システムの安全管理に関するガイドライン 第6.0版（厚生労働省）

リティマネジメントシステムの確立、セキュリティインシデントへの対応、委託先の選定や責任分解――などについて、安全管理や運営担当者に指示、管理すべき項目がまとめられています。

外部委託や考え方のアップデートも必要

第6.0版では、外部委託や外部サービスの利用に関する整理も行われています。ここでは、医療情報システム事業者へ業務委託する場合の医療機関側の責任のあり方などが示されています。

なお、委託する事業者選定についても、「JIS Q 15001 個人情報保護マネジメントシステム」は「JIS Q 27001 情報セキュリティマネジメントシステム」の認証取得などの基準が明示されています。

情報セキュリティに対する新たな考え方も打ち出されています。従前、医療機関における情報セキュリティ対策としては、ファイアウォールを設置して閉域網のなかで「医療情報システムを構築するネットワーク型境界防御型思考」をベースにした取り組みが一般的でした。しかし、これでは境界防御をすり抜けてウイルスが侵入してくるリスクに対応するのは困難になります。そこで第6.0版では、すべてのトラフィックについて安全性を検証する“ゼロトラスト思考”を取り入れた対策が追加されています。

もちろん、境界防御思考が不要となるわけではなく、ゼロトラスト思考とうまく組み合わせて対応することが重要です。

そのほか、災害やサイバー攻撃、システム障害などの発生を想定し、BCPの整備を含めた必要な対応や対策、オンライン本人確認の活用、ローカル５Gなど新しいネットワーク技術の可能性など、新技術や規格についても記載されています。

セキュリティ対策は現状把握から始めよ

今後、医療機関では第6.0版を踏まえたサイバーセキュリティ対策が求められますが、その前に行っておきたいことがあります。それは、自院におけるサイバーセキュリティ対策の現状把握です。

これに関しては６月９日に、厚生労働省が医療関連団体などに通知した「医療機関のサイバーセキュリティ対策チェックリスト」に回答してみることをおすすめします。

▽医療情報システム安全管理責任者の設置、▽サーバー、端末PC、ネットワーク機器の台帳管理、▽リモートメンテナンスを利用している機器の有無の確認、▽アクセス利用権限の設定、▽インシデント発生時の組織内と外部関係機関への連絡体制の作成――など、質問に答えていけば、おのずと足りないものや優先的に取り組まなければいけないものが見えてくるはずです。

また、現状把握に関しては、電子カルテベンダーやセキュリティベンダーなどの専門家に、自院のネットワークに潜むリスクを抽出してもらう方法もあります。もちろん予算はかかりますが、将来的なリスクを回避しておくためにも一考すべきでしょう。

セキュリティ意識を高める教育研修も不可欠である

院内ネットワークのユーザー管理も重要です。これに関しては、職員のID管理や権限設定が十分に行われていないと、退職者のIDとパスワードを使った情報漏洩や不正アクセスなどを許すことになりかねません。医療機関の場合、医局派遣や非常勤などを含めて人材の流動性が高いため、権限設定やID管理に細心の注意が必要です。

不正アクセスを防ぐには、最新のセキュリティソフトへのアップデートなど、ネットワークセキュリティの強化も大切です。セキュリティソフトの導入によってパソコンの動作が遅くなるようなことがあれば、ただちにパソコン自体のアップデートも検討すべきです。

基本的なことですが、職員のセキュリティ意識を高めるための教育・研修も不可欠です。

病院として私物のUSBの使用を禁止したり、フィッシング詐欺やソーシャルエンジニアリング、SNSを通じた情報流出への注意喚起を行っていても、守られていないケースは少なくありません。たとえば先述のID管理にしても、パスワードを書き写した付箋をPCに貼りつけているような人もいます。

職員全員がサイバーセキュリティ対策の重要性を理解し、決められたルールを遵守してもらうには、定期的に研修を実施し、常にセキュリティ意識を持って仕事をしてもらえるような継続的な意識づけも重要です。

MMPG 医業経営 Journal
株式会社ユアーズブレーン
〒730-0042広島県広島市中区国泰寺町1丁目3－29　MRRデルタビル3階
TEL：082-243-7331　FAX：082-249-7070