

サービス推進室では、医療安全に関する情報を収集し、看護業務で役立つポイント等を付加して提供しています。点検ツールとしてお役立てください。

No.1

医療機関でのサイバー攻撃の被害のニュースを散見します。「ランサムウェア」による被害を防止できるように取り組みましょう。

身代金要求型のコンピューターウイルス「ランサムウェア」による医療機関へのサイバー攻撃が相次いでおり、厚生労働省への報告が求められるようになった 2018 年 10 月以降では、7 病院から被害報告を受けているとのことでした¹⁾。

不審なメールを開かないようにすることはもちろん
サイバー攻撃を受けた時の、発見者になる

アクセス権限の設定・管理等)の強化に加えて、職
被害を受けると、個人情報漏洩の問題だけでなく、
診療が継続できない状況で医療を提供することによる医療安全上のリスクも
生じます。継続的な職員教育を行いましょう。また、新入職員等へのオリエンテーションのプログラムには必ず取り入れましょう。

厚生労働省からは「医療機関等向けサイバーセキュリティ研修用動画」³⁾「医療機関等向け情報セキュリティ研修教材」⁴⁾も提供されていますので、医療安全管理と同様に重要な情報セキュリティ対策について職員が取り組めるよう、必要に応じて活用しましょう。

★ランサムウェアとは

ランサムウェアとは、金銭を脅し取ることを目的とした不正プログラムで、感染すると、『パソコン内のファイルが暗号化されて開けなくなったり、画面がロックされて使用不能になる。』『スマートフォンの画面がロックされて使用不能になる』『暗号化の復号や画面ロックの解除と引き換えに「身代金」を要求される』という特徴があります。仮に、犯人の要求に応じ、身代金を支払ったとしても、データが復旧できる保証はありません。

(注記) ランサムウェアとは、「Ransom (人質)」と「Software (ソフトウェア)」を組み合わせた造語です。

★警視庁 ランサムウェアに要注意！より

<https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/ransomware.html>