

Polar

医療の今と未来を描く「ポラール」

Vol. 8
2022



すべての革新は患者さんのために

中外製薬

Roche ロシュグループ

● VOICE

鈴木 龍太

日本介護医療院協会会長



● ZOOM UP!

高山 智子

国立がん研究センター
がん対策研究所がん情報提供部部長



● SPECIAL REPORT

尼崎市

がん患者アピアランスサポート事業

● 困ったことは先駆者に聞くべし
経営者のための相談支援センター

高橋 肇

社会医療法人高橋病院理事長

サイバー攻撃やウイルス感染への対策

第7回

高橋 肇

社会医療法人高橋病院理事長



Q サイバー攻撃やウイルス感染の対応策はどこから着手すべきですか。

A 電子カルテベンダーら他者任せにせず、自院に情報セキュリティ担当者を置き、スタッフの情報セキュリティに対するリテラシー教育にも力を入れる。

サイバー攻撃やウイルス感染から病院を守ることは、今や経営者にとって最優先事項と言え、BCPを考慮することが必要です。仮に電子カルテシステムが攻撃されてしまったら、診療の継続という点からも病院経営に大きな影響を与えかねません。

私は、情報セキュリティ責任者の配置から始めることをお勧めしています。当法人でも配置していますが、他業界で活躍する専門スタッフを新たに雇用する、それが難しければ外部委託でもよいと思います。

最も避けなければならないのは、自院で導入している医

療系システムのベンダーへ、全てを一任してしまうことです。ベンダーは、自社のシステムに精通していても、インフラやネットワークシステムにも明るいとは限りません。電子カルテベンダーはあくまで電子カルテシステムの専門家であって、ネットワークシステムは別なのです。

近年、サイバー攻撃を受けた際に補償してもらえる「サイバー保険」が注目されていますが、これも専門の担当者が確認して自院に最適なものを選ぶ必要があります。たとえば、保険金が支払われる条件に最新の基本ソフトを導入していることが契約書に盛り込まれているケースがあります。古いバージョンを使用する病院の場合、保険に入っても保険金の支払い対象とならない場合もあるのです。

また、日頃よりスタッフ1人1人の情報セキュリティに対するリテラシーを高めておくことも重要です。サイバー攻撃やウイルス感染から身を守るためには、きちんと教育を実施し事前に準備する必要があります。そうすることで被害を未然に防ぐことができるのです。こういった側面からも専門の担当者の活躍の場は多いと考えています。