

# エディトリアル

---

地域医療振興協会 常務理事／

セキュリティオペレーション室(SOC) 室長／システム調達戦略室(SPART) 室長 木下順二

PCに付箋でIDとパスワードが貼られている、外部者の目に触れる場所に業務用Wi-FiのSSIDとパスワードが貼られている、業務連絡にLINEやGmailなどの個人用サービスを使っている、zipファイルを添付したメールに続いてパスワードを記載したメールを送っている、個人契約のクラウドに業務ファイルや臨床写真が保管されている、個人のGoogleフォームを臨床研究に利用している……。その何が問題なの？という人に向けての本特集である。

地域医療の現場では、医療・介護・行政を横断した情報共有が不可欠となり、電子カルテや介護連携システム、クラウドサービスの活用が急速に進んでいる。情報の適切な共有は、多職種連携を支え、医療の質と継続性を高める基盤であるが、その利便性の裏側には情報漏えいやサイバー攻撃といったリスクが潜んでいる。

ランサムウェア攻撃の標的は地方の中小病院や診療所にも広がっている。業務委託先などを経由したサプライチェーン攻撃、クラウドサービスの設定不備を突いた犯罪、操作ミスによる情報漏えいも後を絶たない。厚生労働省が示す「医療情報システムの安全管理に関するガイドライン」では、ゼロトラスト、暗号化、認証強化などが提唱されているが、現場からは、何から手を付けたらよいか分からない、対応できる人がいない、時間が足りないという声も多く聞かれる。

生成AIの活用が医療にも広がり、文書作成支援などの可能性が期待される一方で、個人情報の学習、ハルシネーションといった新たなリスクも顕在化した。情報セキュリティはIT部門だけの問題から、全職員が関わる医療安全の一部になったのである。

本特集は地域医療振興協会のセキュリティオペレーション室およびシステム調達戦略室に関わる本部・各施設SEの共同執筆による。規模や立場の異なる現場の視点を持ち寄り、現場で働く全ての医療従事者に役立つ特集を目指した。電子カルテ・介護情報システム、オフィスアプリやメール、通信・ネットワーク対策、職員教育、そして生成AI活用まで、具体的なテーマを取り上げ、限られた人材と予算の中で、どのように安全性を確保し、運用に落とし込むかという実践知を共有することを目指した。

情報セキュリティはDXを妨げる足かせではない。安全な設計と運用があってこそデータは安心して共有され、DXの価値が最大化される。本特集が地域医療に携わる読者にとって自施設の取り組みを見直し、次の一步を考えるきっかけとなれば幸いである。

本特集とエディトリアルの構成検討に生成AI(M365 Copilot)を利用した。