

No.488

# 医療現場のサイバーセキュリティ確保に向けて： 専門家インタビュー調査から

坂口一樹、堤 信之

- ◆本稿の目的は、医療 DX が進展する将来を念頭に、医療経営の実情を踏まえた現実的なサイバーセキュリティ確保策の提言である。情報通信技術（ICT）やデジタル技術、情報セキュリティの専門家・実務家・学識経験者を対象に実施したインタビュー調査で得た知見を基に具体策を検討し、医療現場を取り巻く各ステークホルダー向けに、提言を取りまとめた。
- ◆医療機関には、システム管理の徹底、すなわち ICT 資産管理、院内システムのネットワーク構成図の作成と更新、ネットワークの出入り口対策、情報端末・通信機器のセキュリティ対策と脆弱性対応、ネットワーク内部の監視、有事の被害最小化策といった具体策が求められる。また、経営者と従業員の意識改革とあわせて、ベンダー（情報システムの販売業者）の活用や希少な ICT 専門人材を地域ごとにシェアする仕組みの構築を提言したい。
- ◆（1）医療界には、DX やサイバーリスクに関する情報の現場への伝達、集団交渉による対策費用の低減、経営者向けの啓発活動に加え、支援人材の受け皿や有事の現場支援を担う役割が期待される。また、（2）情報システム業界には一部ベンダーの質の改善を、（3）保険業界には、適正なリスク計算のための事例蓄積とサイバーリスク低減につながる付帯サービスの充実を、それぞれ期待したい。
- ◆国には、①司令塔組織（NISC）の見直しと強化、②脆弱性情報の確実な伝達と現場の対策実装支援、③システム仕様書を点検する第三者機関の創設、④サイバー空間のセキュリティ監視組織（SOC）の制度化と医療機関向け地域別 SOC の構築、⑤有事の相談窓口の一本化に加え、⑥財源の確保と DX 進展に伴うリスクに関する国民・患者向けの説明責任遂行を提言した。また、⑦社会全体の DX が進む将来に向けて、健康・医療に関するデータの廃棄ルールや真正性の担保手続き、フェイク情報拡散への対処法についての政策議論を始めておくべきである。

## ▼ダウンロード

<https://www.jmari.med.or.jp/wp-content/uploads/2025/01/wp488.pdf>