第Ⅷ章

日医総研ワーキングペーパー

No.453

病院・診療所のサイバーセキュリティ：
医療機関の情報システムの管理体制に関する実態調査から

坂口一樹、堤　信之

概要

・医療機関における情報システムの管理体制の実態把握を目的として、全国調査を実施した（病院約 5,000 施設と診療所 約 5,000 施設を対象とし調査、回収数 2,989、回収率 30.4％）。主な結果は、以下の通り。

・医療現場の組織体制は問題含みである。院内システムのネットワーク構成図を保有し、計画的に見直しをしているのは 5.7％に過ぎず、約半数は構成図を持っていなかった。専任の担当部門があるのは２割強で、３分の２弱は兼務の担当者あるいは院長自ら管理という体制である。計画的に対策費用を準備しているのは１割強であり、半数近くは費用を準備していなかった。

・行政の取り組みの認知度・活用度にも課題がある。情報システムの安全管理に関する厚労省ガイドラインを認知・活用している割合は 27.9％、サイバー攻撃を受けた際の届出先の認知割合は 29.2％、不正アクセス等に関する相談窓口の認知割合は 23.1％と、いずれも３割に満たなかった。

・サイバーセキュリティに関するリスクマネジメント体制にも、次の通り課題がある。【事前対策の状況】患者・受診者情報が保管されている情報端末の管理ルールや USB メモリ等の外部媒体の管理ルールについて、３割前後～４割強が「ルールなし」であった。４分の３超の施設は、サイバーセキュリティに関する従業員教育を実施していなかった。【発生時対策の状況】３分の２弱から８割強が、インシデント発生時の明文化された手順やルールがないとの回答であった。【事後対策の状況】サイバーセキュリティ保険への加入割合は１割に満たなかった。また、過去３年間にインシデントを経験した回答者のうち、４割超は再発防止に向けた対応にまで至っていなかった。

・以上の組織体制、行政の取り組みの認知度、リスクマネジメント体制については、総じて病床規模の大きさに応じて状況が良くなる傾向にあった。別の言い方をすれば、診療所や中小規模の病院ほど、情報セキュリティやサイバーセキュリティに関わる対策全般に問題を抱えているということである。

・直近３年間における実際のインシデント・アクシデントの経験に関しては、最も危惧される「サイバー攻撃により患者に直接の危害があった」との事象は確認されなかった。一方で、ウイルス感染や外部からの不正アクセス等のサイバーセキュリティに関わるインシデントの発生が確認できた。

・現場からの要望では、「サイバーセキュリティ対策の費用面での公的支援」と「自施設のサイバーセキュリティ対策のレベルがチェックできる仕組み」の２つが、ともに５割を超える施設が挙げた２大要望であった。

・以上の結果を踏まえて考察を加え、組織体制の充実、リスクマネジメント体制の強化、現場の要望への対応に向けた具体的な提言を行った。

▼本文
https://www.jmari.med.or.jp/download/WP453.pdf
▼別添資料１．単純集計表および病床規模別クロス集計表
https://www.jmari.med.or.jp/download/WP453_appendix1.pdf
▼別添資料２．「医療機関の情報システムの管理体制に関する実態調査」調査票
https://www.jmari.med.or.jp/download/WP453_appendix2.pdf

目次に戻る