

2023 年 4 月の医療法施行規則改正でセキュリティ確保が医療機関の責務として明文化され、経営管理層の責任のもとでの組織的対応が求められるようになった。医療 DX の実現にはサイバーセキュリティの確保が欠かせず、予防的な取り組み、BCP の策定、被害時に経営層と専門家を橋渡しする役割を担う人材が必要である。その役割には診療業務と病院情報システムの把握が前提となり、病院で実務経験を持つ人材がセキュリティの知識・技術を身につけることが期待されると筆者は述べている。

私はこれまでに二度の病院情報システム更新に携わった。そのたびに痛感するのは、筆者が前提とする構成の把握が、更新作業のなかで一時的に達成されるだけで、日常の業務として維持されていないことである。稼働後は構成図も台帳も更新されず、部門システムは各部署の判断で増えていく。次の更新時には再びゼロから調べ直すことになり、把握は担当者の記憶に頼る属人的なものにとどまる。これが私の考える課題である。

対策の第一は、構成情報の維持を定常業務として制度化することである。更新プロジェクトで作成したネットワーク構成図、機器台帳、システム間連携の一覧を、プロジェクトの成果物ではなく運用文書として位置づけ、更新の責任者と頻度を規程に定める。あわせて、部門システムや医療機器を院内ネットワークへ接続する際の届出を必須とし、機種、OS、サポート期限、保守接続の有無を登録しなければ接続できない運用とする。年一回の棚卸しで期限切れの機器を抽出し、次期の機器更新計画へ反映させる。把握が個人の記憶から組織の資産へ変わる。

第二に、システム更新の調達を人材育成と権限付与の機会として活用することである。私の経験では、仕様書に盛り込んだセキュリティ要件は予算の都合で削られやすい。そこで対策費を機能要件と別枠で計上し、削減する場合は残るリスクを文書化して経営会議に諮る手順とする。その説明を担当者自身が、想定される診療停止期間として示す。数年に一度の大きな判断の場に立つ経験は、経営層と専門家をつなぐ力を育て、担当者の役割を院内に認識させる。

日々の運用の積み重ねと、更新という節目の双方を使うことで、診療現場を理解した人材は育つと考える。

(929文字)

この小論文の作成には生成 AI を使用しています。
本解答例は優秀な論文の例として示しています。