医療経営士のための
職域の研究Ⅰ

医療DX・AI編 ④

DX時代にも重要なセキュリティ
～経営層が主体的に関与すべき理由～

コンピュータを活用するうえで欠かせないのがセキュリティです。DX時代は特にコンピュータの見えない（一般的には理解していない）部分に依存しているため、技術者の説明を鵜呑みにするしかないという状況が多いですが、経営者として何をポイントに考えれば病院を守れるのか、何を基準に投資の判断ができるのか、いまだに暗中模索ではないでしょうか。本稿では、セキュリティ対策を経営判断としてとらえるための視点について考えてみます。

セキュリティは常に更新が必要

コンピュータは、その処理が見えにくいことと成果が高度であることから、攻撃者にとっても都合が良いものになっています。技術が進化すればするほど、われわれも攻撃者もそれを学び、活用することで相手に勝とうとする、いわゆる〝いたちごっこ〟を繰り返しています。

他の分野での身近な例としては感染症があげられます。人類が抗生物質をつくれば細菌が耐性を獲得し、ワクチンをつくればウイルスが変異し、新薬を開発すれば再び耐性を得て……ということを繰り返しています。金融犯罪（詐欺など）も対策が進化するほど攻撃も進化します。対策が一度整えば終わりではなく、常に更新が必要という「本業とは異なるところに継続して時間やお金を使わなければいけない状況」には辟易としますが、それでもわれわれはそれらのリスクと向き合いながら、便利な道具を上手に使っていくという選択をしています。

どのようにリスクを把握するか

リスクコントロールといえば「スイスチーズモデル」が参考になります。情報セキュリティでは情報資産、脆弱性、脅威（攻撃者）の3つがすべて揃わないとリスクは顕在化しません（**図**）。どれか1つを否定すれば良いのですが、現実には情報資産を持たないわけにはいかないですし、脅威もなくなりませんから、結果的には脆弱性を抑えていくことになります。

リスクへの対策パターンは保有、回避、低減、移転の4つがあります。現実的には移転と低減をして保有することが多いと思いますが、ここで穴となりやすいのが、教育研修とIT-BCP（システム障害時の業務継続計画）です。

教育研修は、内容の陳腐化を防

金城悠貴（きんじょう・ゆうき）

済生会神奈川県病院経営戦略課長／帝京科学大学、関東学院大学大学院非常勤講師／神奈川研究会事務局／医療経営士2級