別紙3

厚生労働行政推進調査事業費補助金（地域医療基盤開発推進研究事業）
分担研究報告書

テーマ：医療機関におけるサイバーセキュリティ対策向上に向けた実態調査に関する研究

研究分担者　研究分担者　猪飼　宏　京都府立医科大学 附属病院医療情報部 部長

研究要旨

本分担研究では、医療機関におけるサイバーセキュリティ対策チェックリスト対応の実態を明らかにすることを目的として、公立の特定機能病院であるL病院に対しヒアリング調査を行った。 医療情報部門の体制、電子カルテ・ネットワーク・セキュリティ関連ベンダとの役割分担、資産管理や外部接続点管理、ログ・パッチ・バックアップ運用、IT-BCP 策定状況等を整理し、チェックリスト項目との対応状況と課題を抽出した。 その結果、L 病院では長年の運用経験とベンダとの協働により多くの項目が概ねカバーされている一方、移動端末や部門システムの統合管理、ゼロトラストを見据えたネットワーク再設計、セキュリティ人材の育成・評価など、組織的・構造的な課題が残されていることが明らかとなった。

A. 研究目的

医療のデジタル化に伴い、電子カルテ、オーダリング、部門システム、ネットワーク、外部保守接続、医療機器など多様なシステムが統合的に運用され、院内外のシステム連携が診療機能の基盤となっている。 サイバー攻撃やシステム障害により医療情報システムが利用困難となった場合、患者情報の閲覧、指示伝達、検査・処方・会計等が制約され、医療安全および診療継続に重大な影響を及ぼす恐れがある。

厚生労働省「医療機関におけるサイバーセキュリティ対策チェックリスト」は、医療機関が優先的に取り組むべき対策項目を提示しているが、その実装可能性や運用の成熟度は、病院規模、既存システム構成、人材配置、ベンダとの責任分界、予算制約等に左右される。

本分担研究では、チェックリストへの対応が比較的進んでいる公立大学病院である L 病院を対象に、医療情報部門の体制やベンダとの分担、資産管理・外部接続管理・ログ管理・バックアップ・IT-BCP といった実務運用の実態を把握し、その強みと課題を明らかにすることを目的とした。 併せて、長年蓄積された病院情報システム運用の経験知をどのように継承し、組織としてセキュリティ人材を育成・評価しうるかを検討し、チェックリスト対応の実効性評価に資する知見を得ることを目指した。

B. 研究方法

本分担研究では、2026 年 1 月から 3 月にかけて、L 病院の医療情報部門職員および電子カルテ・ネットワーク・セキュリティ関連ベンダ担当者を対象にヒアリング調査を実施した。 調査では、医療情報部門の体制、電子カルテおよびネットワーク・セキュリティ関連ベンダの役割、資産管理、外部接続点、MDS/SDS、利用者管理、ログ管理、パッチ管理、二要素認証、外部記憶媒体、バックアップ、IT-BCP に関する運用状況や課題について聞き取りを行った。

ヒアリングは厚生労働省「医療機関におけるサイバーセキュリティ対策チェックリスト」に沿って実施し、各項目に対する対応状況、運用上の工夫、実装上の制約やリスク認識などを半構造化インタビュー形式で収集した。 倫理面への配慮として、報告書では個別患者情報および機微な設定情報は記載せず、医療機関の実

務改善に資する範囲で結果を整理することとした。

C. 研究結果

L 病院では、端末・サーバを IP アドレスおよび所在と一体的に資産台帳で管理しており、電子カルテ端末を含む多くの機器について網羅的な把握がなされていた。 一方で、ノート PC や検査機器など移動して利用される機器については、必要に応じて通信ログを用いて所在確認を行う場面もあり、動的な資産の管理には一定の負荷を要していた。 電子カルテ以外の部門端末におけるウイルス対策やソフトウェアアップデートは、原則として各部門ベンダの管理に委ねられており、病院側で一元的に端末管理を行うソリューションの導入も検討されていたが、費用面から導入には至っていなかった。

リモート接続については、病院として共通の仕組みを整備し、ベンダごとに接続元 IP アドレスを極力限定したうえで ID とパスワードを発行していた。 ただし、一部の医療機器では仕様上、ベンダ固有の保守用外部回線を必要とするものが存在し、その場合は商用回線の設置を届け出制により許可することで、全ての外部接続を把握する運用が取られていた。 遠隔診療やクラウドサービス利用に伴い、専用の商用回線や専用線上の VPN 接続も増加しており、サービスおよび連携先拠点数の拡大に伴う費用増大が新たな課題となっていた。 ゼロトラストを前提としたネットワーク設計への移行も検討されていたが、電子カルテベンダ・ネットワークベンダともに十分な経験を有しておらず、中長期的な検討課題として位置付けられていた。

MDS/SDS については、適時調査や特定共同指導、立入検査の機会に整備状況が確認されており、概ね全項目で遵守状況が維持されていたため、個別の課題抽出に活用した実績は乏しかった。 利用者管理に関しては、特権管理者のパスワード桁数を増やすなどの強化が行われていたが、更新はシステム更改時などに限られ、日常的な頻繁更新は実施されていなかった。 一般ユーザのアカウントは人事情報と連動して発行・凍結・権限変更が行われているものの、大学病院特有の事情として、学生や研修医の頻繁な所属変更や、出向後も診療協力医として継続勤務するケースが多く、厳密なアカウント管理には一定の困難が認識されていた。

ログ管理では、サーバおよびネットワーク機器からログ収集が行われていたものの、ログ解析の経験を有する職員は限られており、日常的・体系的なログ分析は十分には実施されていなかった。 セキュリティパッチについては、EPP（エンドポイント保護ソフト）の定義ファイル等は院内の配信サーバから定期的に配布されていた一方で、Windows Update は電子カルテおよび部門システムベンダによる動作検証に多大な労力とコストを要することから、重要度の高いものに限って不定期に適用される運用であった。

バックアップについては、いわゆる 3-2-1 ルールに沿って、LTO ドライブによる外部保管に加え、遠隔地へのオンラインミラーリングを実施し、参照系システムとしても活用していた。 システム障害時には参照系から本系への切り替えにより診療継続を図る想定であったが、データ破損や改ざん発生時におけるバックアップデータからの本格的なシステム復旧については、ベンダ側の経験も十分とは言えず、今後の課題として認識されていた。

IT-BCP については策定済みであり、年 1 回の机上訓練が実施されていたが、全てのハザードを網羅した病院全体の BCP、ならびに教

育・研究を含む大学全体の BCP との連携や整合性については、引き続き検討が必要とされていた。 組織的課題としては、公的病院として行政との間で人事異動が頻繁に生じることから、病院採用職員と行政職員とで求められるキャリアパスが異なり、情報セキュリティに関する資格取得や専門性の維持が困難になりやすいことが指摘された。

D. 考察

公立大学病院である L 病院では、約 35 年にわたり病院情報システムを整備・運用してきた実績を背景に、電子カルテおよびネットワークそれぞれのベンダと密接な連携を取りながら、サイバーセキュリティチェックリストの大部分をカバーする運用が構築されていた。 一方で、部門システムを担当するベンダ間では技術力や対応能力にばらつきがあり、そのギャップを病院職員の経験やスキルによって補完せざるを得ない場面も多く、責任の分界が曖昧になりうることが課題として示された。

また、システムの開発・構築・運用に長年携わってきた担当者であっても、情報セキュリティやネットワークに関する最新の知識を継続的にアップデートするには多大な労力を要する。現行の人事制度や評価体系では、こうした学習・研鑽が十分に評価されにくく、個人の自己研鑽に大きく依存している実態が明らかになった。

特定機能病院など高度急性期医療を担う医療機関において、組織としてセキュリティ人材育成に取り組むためには、診療報酬上の施設基準や加算要件としてセキュリティ関連資格や専任配置を位置付けることや、公的病院における人事評価の中で資格取得・維持や継続教育を評価する仕組みを整備することが有用と考えられた。

E. 結論

L 病院でのヒアリングから、大規模医療機関における医療情報システムの安全な設計・構築・運用には、病院長の理解の下での明確な組織的位置付け、専任を含む情報システム人材の確保、ベンダとの調整スキルおよび信頼関係の構築が重要な役割を果たすことが確認された。

今後、遠隔医療や地域医療連携の拡大に伴い、中核医療機関が周辺医療機関に対して情報セキュリティ面でも支援を行う役割を担うことが想定される。 そのためには、組織マネジメント（人事評価を含む）を通じたセキュリティ人材育成、資格取得・維持の体系的支援、部門システム等を担うベンダ側でのスキル向上といった課題に計画的に取り組む必要があると考えられた。

F. 健康危険情報

なし

G. 研究発表

1. 論文発表

なし

2. 学会発表

なし

H. 知的財産権の出願・登録状況

（予定を含む。）

1. 特許取得

なし

2. 実用新案登録

なし

3.その他

なし