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　鳥飼　幸太　群馬大学医学部附属病院システム統合センター　准教授

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チェックリスト対応の実効性を検討するため、E 病院および F 病院に対して、情報システム管理体制、マンパワー、チェック方法、ベンダー対応、IT-BCP 等に関するヒアリングを行った。E 病院では、専任職員と委託・派遣職員を組み合わせた体制のもと、資産管理、外部接続点管理、SDS 確認、特権アカウント管理、外部記憶媒体制御、イミュータブルバックアップ等の対策が進められていた。一方、長期にわたり病院情報システムの監修・保守・更新を担ってきた職員の経験知を、後進にどのように移転するかが課題として認識された。F 病院では、臨床検査技師としての現場経験を起点に病院情報システム管理へ職域を拡張した人材が中心となり、組織的な医療情報部体制の整備、人材確保、ベンダーへの具体的指示、費用制約下での重点的対策が進められていた。両施設の結果から、チェックリスト対応は単なる項目充足ではなく、医療情報システムの運用知識、ベンダー調整能力、後継者育成、診療報酬・補助制度を含む資源配分の設計と一体で評価する必要があることが示された。

A. 研究目的

医療機関では、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、医療機器接続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・会計等の業務が制約され、医療安全と診療継続に影響する。厚生労働省の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、各医療機関が優先的に取り組むべき項目を示す一方、実装可能性は病院規模、既存システム構成、人材配置、ベンダーとの責任分界、予算制約に左右される。本分担研究の目的は、チェックリストへの対応が進む医療機関へのヒアリングを通じて、項目充足を支える組織能力、運用上の制約、後継者育成と知識移転に関する課題を整理し、持続可能な医療サイバーセキュリティ対策の実装条件を明確化することである。

B. 研究方法

令和 8 年 2 月 19 日に E 病院、令和 8 年 2 月 20 日に F 病院を対象として、現地または Web 会議を併用した半構造化ヒアリングを実施した。E 病院では、病院情報システム部門の担当者から、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ー、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 に関する回答を得た。F 病院では、医療情報部門の形成過程、人材確保、資格取得、インターン受入、ベンダー調整、費用制約と診療報酬制度に関する課題について聞き取りを行った。調査では患者個人を識別

する情報を収集せず、施設の組織体制、運用方法、情報システム管理上の課題を対象とした。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を記載せず、医療機関の実務改善に資する範囲で結果を整理した。

（倫理面への配慮）

本研究の施設へのインタビュー調査結果は具体的な施設が特定できないよう仮名化したうえで報告する。

C. 研究結果

E 病院は 950 床の特定機能病院であり、医療情報部門は専任 7 名、兼務 7 名、嘱託 3 名、委託・派遣 3 名から構成されていた。電子カルテは HOPE EGMAIN-GX で、構築ベンダーは富士通 Japan、ネットワーク機器は Cisco、ネットワーク構築は住友電設、セキュリティ対策ではセイコーソリューションズとのやり取りが多いとの回答であった。

1. E 病院における体制と運用

同院では、資産管理について Excel と SS1 を併用し、今後は ARMIS による収集を予定していた。ネットワークに接続していない機器や旧機器の網羅性には課題があり、部門管理機器を含めた資産把握が継続的な検討対象であった。外部接続点についてはルータおよびファイアウォールを管理し、リモートメンテナンス事業者を Excel で把握していた。リモート接続は申請制とし、SDS を用いてセキュリティ対応状況を確認していたが、ポケット Wi-Fi 等による把握外接続の可能性が課題として認識されていた。MDS/SDS は立入検査対応として収集が進められており、リモートメンテナンス事業者には SDS 提出と内容確認を求めていた。

利用者管理では、委託先ベンダーのアカウント情報漏えいを契機に特権管理者のパスワードをランダム生成の 13 桁へ変更し、台帳管理を行っていた。人事情報と連動したアカウント発行・停止、出向時の職種変更、申請書に基づく権限付与が実施されていた。OS のパスワード管理はシステム部で行う場合が多い一方、ミドルウェアやネットワーク機器の利用者設定は各ベンダーに依存する部分が残っていた。ログ管理ではサーバの eventlog/syslog、ネットワーク機器の syslog 集約、踏み台サーバにおける操作動画記録が実施または導入途中であったが、ログ相関分析は困難であり、通常時の解析は限定的であった。

セキュリティパッチについては、WSUS を用いて適用可能なサーバ群に半年に一度を基本として対応し、緊急度の高い脆弱性では IPA の情報等を参照しながら随時対応していた。アプリケーションやミドルウェアについてはベンダー側の製品サポートや運用設計が制約となり、閉域網前提の運用感覚からの移行が課題であった。二要素認証は一部部門でアプリケーションを利用し、令和 9 年 1 月に電子カルテ端末での適用を予定していた。外部記憶媒体は SS1 によるシリアル番号制御と物理的な USB ストッパーにより制限されていた。バックアップは Rubrik によりイミュータブルなバックアップを取得し、IT-BCP はシステム部で約 3 か月をかけて作成し、年 1 回の机上訓練を開始していた。

ヒアリングでは、30 年にわたり病院情報システムの監修、保守、更新を担ってきた職員の経験知が、迅速な障害対応、調達段階からの介入、資源配分の判断を可能にしてきた点が確認された。一方で、その経験知が個人に蓄積されているため、定年退職後に知識と技能が現

場に適用されにくくなることが課題として示された。若手職員は後進として情報システム課に配属され、引継ぎと OJT を受けているが、情報システム立ち上げ時の段階的成長を経験していない。着任時点で高度化、複雑化、大規模化した病院情報システムと向き合う必要があり、技術的課題と心理的負担が同時に生じることが明らかとなった。

2. F 病院における体制形成と人材確保

F 病院では、K 氏にヒアリングを行った。K 氏は入職時に検体検査技師として勤務し、検体検査領域の電子化に関与する中で、電子カルテやオーダリングシステムを含む病院全体の情報システム管理へ業務範囲を拡張してきた。組織への働きかけにより医療情報部が組織され、職員が加わることで現在の体制に至った。K 氏は上級医療情報技師の資格を取得し、T 大学医療情報学科からのインターン生を受け入れるなど、専門知識を有する人材の確保に取り組んでいた。

同院では、公的・準公的な病院組織に共通する人事枠の制約の中で、急速に拡大するサイバーセキュリティ要求に対応する人材登用が容易ではないとの認識が示された。電子カルテを担当する富士通 JAPAN 株式会社をはじめ、IT ベンダーの対応品質は担当者のスキルにより差が生じるとのコメントがあり、医療機関側が十分な知識を持ち、ベンダーに対して具体的な指示を出せる能力が重要であることが確認された。保険収載の枠組みの中で医療を提供する医療機関にとって、近年新たに求められるサイバーセキュリティ対策は、診療録管理体制加算等の制度的支援の拡充とともに、人材拡充を必要とする領域であった。

3. G 病院における体制形成と人材確保

G 病院では K 氏にヒアリングを行った。事務部門である医事課医療情報係によって資産管理が行われている。サイバーセキュリティ強度確保のため、固定 IP アドレスと MAC アドレスの紐づけを行い、任意の端末/サーバを院内 LAN に接続しても動作しない運用となっている。2025 年までは中央放射線部で検査機器のローカルアドレス運用を行っており、2026 年度の PACS 更新によってアドレスの一意化を行う予定であることが確認された。各診療科や診療支援部門からの端末要求は文書により行われ、週次定例の場にて払い出し/修理持ち込みの件数が把握されている。G 病院では 2011 年 3 月に東日本大震災で計画停電に見舞われたこと、夏季に落雷が多く停電が頻発する地域であることから、2013 年に非常用発電機を 200kW 追加し、停電時にはうち 1000kW を電子カルテが設置されている外来棟に給電する運用規定を定めている。

利用者管理として、8 桁 ID 化とパスワード有効期限 60 日の運用を行っている。最短パスワード長の制限、シンクライアント端末における IC カード認証ドライバの適用に課題が生じている。セキュリティパッチについては、適用可能なサーバ群に対応し、緊急度の高い脆弱性では IPA の情報等を参照しながら随時対応していた。EDR/XDR(Trend Micro 社)のアップデートにはオンライン接続によるパターンファイルのダウンロードを随時行うことで対応している。EDR には機械学習型挙動監視が有効化されており、端末の操作ログ確認の代わりに、不審な操作（許可されていないソフトウエアのインストールなど）を行うと検知されネットワーク隔離が自動で行われる。EDR/XDR のスキャン範囲は攻撃されやすい temp ファイルを含めていることが確認され、

動作障害を起こしやすい SQL を多用するプログラムに対しては EDR から証明書を発行し、検知除外を行いつつプログラムの真正性を担保するようにしていた。外部記憶媒体は管理側ソフトウエアにより、許可された USB のみを運用可能な方法としていた。バックアップは電子カルテ本体(PureStorage)によるイミュータブルなバックアップ、NEC 製 IStorage によるイミュータブル相当機能のバックアップ、参照系システムによるバックアップ、大学病院情報システムバックアップ(Gemini)により取得していた。IT-BCP はシステム部で 2024 年 11 月に作成され、内閣府が主催する分野横断型演習、全分野演習に対し、病院長、情報基盤センター長、CSIRT、電子カルテベンダー、PACS ベンダー、ネットワークベンダー、サーバベンダーのサプライチェーンが合わせて参加し、年 1 回の机上訓練を継続していた。人材確保については、大学教員側 3 名、事務職員側 7 名の 11 名体制で行われている。大学教員と電子カルテベンダー、ネットワーク/セキュリティベンダー、サーバベンダーが月 1 回保守会議を行い、1 か月内でのトラブル対応、アップデート対応などの報告受け、ならびにシステム全体に関係する調整事項の検討とアクション化を行っている。この方法では、運用年数の増加によりベンダー側にも保守スキルが蓄積することから、大学職員側が入れ替わった場合においても、ベンダー側からのスキル情報提供を継続できる。事務職員側で異動が生じるが、部署で専門職員として登用された職員が技術の維持やスキル伝達を行っている。またローテーションが医事課で行われることが多く、10 年程度で再び同じ部課に戻ることもあることから、現状では大きなスキル損失に至っていない。併せて、常駐ベンダーによる保守の中にセキュリティ監視を契約として含めることでマンパワーの充足をはかっている。今後の課題として、災害発生時における院内 BCP とのより整合の取れたアクションマニュアルの整備、急増する検査システム等の外部ネットワーク接続状況の把握、継続的な資産管理の維持が挙げられる。

D. 考察

3 施設の結果から、医療機関におけるサイバーセキュリティ対策は、チェックリスト項目の実施有無だけで評価するよりも、医療情報システムの構成理解、運用手順、ベンダー調整、権限管理、ログ確認、バックアップ、BCP 訓練を継続的に実行できる組織能力として評価する必要がある。E 病院の事例は、高度な実務経験を持つ職員が病院全体の情報システムを長期に把握することで、複雑なシステム変更や障害対応を統合的に判断できることを示す。同時に、その能力が個人依存となる場合、退職、異動、体調不良により組織としての対応能力が低下するリスクが生じる。F 病院の事例は、医療専門職が現場業務の電子化を契機に医療情報システム管理へ発展し、資格取得、教育、インターン受入を通じて人材基盤を形成する実装経路を示す。

後継者育成では、完成した巨大な病院情報システムを一度に理解させる方法ではなく、資産、ネットワーク、認証、外部接続、バックアップ、BCP、部門システム連携といった単位に分解し、変更管理、障害対応、リスク評価を小さな実務単位として経験させる教育設計が有効と考えられる。Group A、Group B、Group C のような人材層別化は、大学病院・特定機能病院等が地域の指導的役割を担い、中規模病院が自施設の防御力を高め、小規模医療機関が外部支援を受けながら最低限の対策を実施する構造を設

計するうえで有用である。ベンダー対応のばらつきに対しては、医療機関側の要件定義力、SDS/MDS の読み取り、保守契約条件へのセキュリティ要件明記、パッチ適用と検証の責任分界の明確化が実務上の要件となる。

E. 結論

E 病院、F 病院、G 病院へのヒアリングから、医療機関のサイバーセキュリティ対策は、情報システム部門の人数、専門性、長期経験、後継者育成、ベンダー調整能力、財政制度と密接に関連することが確認された。チェックリスト対応を持続的に実行するためには、項目ごとの技術対策に加え、医療情報システムの構成を継続的に理解する人材の配置、経験知の文書化、OJT の段階設計、地域内での実地研修、診療報酬・補助金・資格評価を含む人材確保策が必要となる。今後は、ヒアリングで得られた知見を、チェックリスト項目の実装難度、必要人材、ベンダー責任分界、医療安全上の優先度に対応づけ、医療機関が実行可能な対策パッケージとして整理することが課題である。

F. 健康危険情報

分担研究報告書に該当する健康危険情報は認められない。

G. 研究発表

1. 論文発表

該当なし

2. 学会発表

該当なし

H. 知的財産権の出願・登録状況

（予定を含む。）

1. 特許取得

該当なし

2. 実用新案登録

該当なし

3.その他

該当なし