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課題調査と解決策の検討

研究分担者　橋本　智広　　大津赤十字病院　事務部　医療情報課

研究要旨

本研究は、医療機関におけるサイバーセキュリティ対策の実効性を明らかにすることを目的に、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（厚生労働省）に基づき、全国の病院を対象としたアンケート調査および訪問インタビュー調査、電子カルテベンダー調査を実施したものである。その結果、ウイルス対策やアクセス制御、バックアップ等の基本的対策は一定程度普及している一方、専門人材の不足やベンダー依存により、運用面の実効性に課題が認められた。特に、ログの活用不足、セキュリティパッチ未適用、リカバリ訓練の未実施などが顕著であった。先進的な医療機関では、経営層の関与や現場職員の参画、復旧検証の実施等を通じてレジリエンスの向上が図られていた。今後は、好事例の共有とチェックリストの実装性向上を通じ、現場実態に即した持続的な対策推進が求められる。

A. 研究目的

近年、医療機関に対するサイバー攻撃の増加を受け、診療停止や患者の個人情報漏えいといった深刻な被害事案が確認されている。こうした状況を踏まえ、令和 5 年 4 月 1 日に医療法施行規則が改正され、病院、診療所及び助産所の管理者は、「医療の提供に著しい支障を及ぼすおそれがないよう、サイバーセキュリティを確保するために必要な措置を講じること」が法令上求められることとなった。同改正においては、管理者が講ずべき「必要な措置」の具体的内容について、最新の「医療情報システムの安全管理に関するガイドライン（厚生労働省）」を参照することが示されており、あわせて、医療機関が優先的に取り組むべき事項を整理した「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（厚生労働省）」（以下、チェックリストと略す）が策定され、毎年その内容が改版され周知されている。　この状況下で、医療機関におけるサイバーセキュリティ対策は、法令により管理者責務として明確に位置付けられたものの、その具体的な実装については、ガイドラインおよびチェックリストを参考としつつ、各医療機関の実情に応じた対応が求められている。

一方、医療法に基づく立入検査では、このチェックリストを基に医療機関の対応状況を確認されるものの、医療機関の実態は多様であり、その違いによりチェックリストに含まれる項目への対応が十分でないケースもあると想定される。同時に、当該項目はチェックリストの改版に伴い見直しが行われることから、医療機関はその対応に向けて速やかな検討に着手する必要となる。

本研究は、チェックリスト（令和 6 年版、令和 7 年版）に着目し、チェックリストに含まれる各項目について、医療現場においてその趣旨や考え方が正しく理解された上で実践されているかを把握・分析することを目的とする。これにより、単なるセキュリティ対策の実施有無にとどまらず、チェックリストが現場において実効的なツールとして機能しているかを検証し、今後の制度運用や見直しに資する知見を提供することにつなげ

る。

B. 研究方法

本研究は、6名の研究者（研究代表者 1 名、研究分担者 5 名）により構成される。次に示す 2 種類の調査を段階的に実施し、実態把握と参考事案の抽出、さらには課題抽出から対応策の検討を行った。

1. アンケート調査の実施

厚生労働省が提示するチェックリスト（令和 6 年版、令和 7 年版）の項目ごとに質問項目を設定し、当該項目への対応状況について調査した。調査の詳細は次のとおりである。回答結果については、項目ごとの実施状況や傾向を整理し、チェックリストの趣旨と現場実態との乖離の有無を分析した。

・調査期間：2025 年 10 月 15 日～11 月 30 日
・調査対象：国内の医療機関（病院を対象）
・調査方法：オンライン形式（Microsoft Forms を使用）
・調査項目：チェックリストに含まれる各項目に対して①から④について調査する。
①各項目の理解度　②実施状況　③運用面での工夫や課題　④その他

2. 訪問インタビュー調査の実施

アンケート調査の結果を踏まえ、チェックリストに基づく対応が積極的に実施されている医療機関を抽出し、当該医療機関を訪問してインタビュー調査を実施した。対象施設は〇施設であり、うち筆者が担当した対象施設は 4 施設であった。当該調査は、別添 2 に示すインタビューシートを作成し、これに含まれる項目について調査した。具体的には、チェックリストの全項目から、アンケート調査の結果から医療機関の対策が十分でないと判断した 12 項目を選出した。当該項目に対してインタビューする観点を事前に設定し、インタビュー調査の精度向上を目指した。

・筆者が担当した対象施設および調査日：
A 病院：800 床クラス、独立行政法人
（調査日：令和 8 年 2 月 10 日）
B 病院：600 床クラス、自治体
（調査日：令和 8 年 2 月 20 日）
C 病院：500 床クラス、企業
（調査日：令和 8 年 2 月 24 日）
D 病院：600 床クラス、公的
（調査日：令和 8 年 3 月 10 日）
・インタビュー時間：各施設 4 時間
・調査シートに含まれる調査内容：
A. 基本情報
A-1　病院情報
A-2　電子カルテﾍﾞﾝﾀﾞｰと構築ﾍﾞﾝﾀﾞｰ
A-3　ネットワーク機器ﾍﾞﾝﾀﾞｰと構築ﾍﾞﾝﾀﾞｰ
A-4　セキュリティベンダー
A-5　主要ベンダー
B. 調査項目
表1に示す 12 項目(B1-B12)について調査。

3. システムベンダーに対するインタビュー調査

医療機関に対して実施した訪問インタビュー調査内容を踏まえて、電子カルテベンダーに対してオンライン形式でインタビュー調査を実施した。対象ベンダーは、大規模医療機関に対する導入実績がある3社とした。

・調査期間：2026 年 3 月 17 日～3 月 25 日
・調査対象：電子カルテベンダー（日本 IBM、日本電気株式会社、富士通 Japan 株式会社）
・調査方法：オンライン形式
・調査項目：訪問インタビュー調査シートに基づく。

表 1：訪問インタビュー調査項目

No	大分類	チェックリスト 該当項目
B-1	セキュリティ人材	【 1-①】医療情報システム安全管理責任者を設置している。
B-2	資産管理	【 2-①】サーバ、端末PC、ネットワーク機器の台帳管理を行っている。
B-3	外部接続点管理	【 2-②】リモートメンテナンス（ 保守）を利用している機器の有無を事業者等に確認した。
B-4	MDS／SDSへの対応	【 2-③】事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（ MDS/SDS）を提出してもらう。
B-5	ユーザー管理	【 2-④】利用者の職種・ 担当業務別の情報区分毎のアクセス利用権限を設定している。※管理者権限対象者の明確化を行っている。
B-6	各種ログ管理	【 2-⑪】アクセスログを管理している。
B-7	セキュリティパッチ管理	【 2-⑥】セキュリティパッチ（ 最新ファームウェアや更新プログラム）を適用している。
B-8	二要素認証への対応	【 2-⑩】二要素認証を実装している。または令和9 年度までに実装予定である。
B-9	外部記憶媒体管理	【 2-⑨】USBストレージ等の外部記録媒体や情報機器に対して接続を制限している。
B-10	システムバックアップ運用管理	【 3-②】インシデント 発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。
B-11	IT-BCPの策定と訓練	【 3-③】サイバー攻撃を想定した事業継続計画（ BCP）を策定している。
B-12	その他	なし

※項目番号は令和7年版に準ずる

（倫理面への配慮）

本研究においては、アンケートおよびインタビューはいずれも任意参加とし、研究目的および取り扱い方針を事前に説明した上で同意を得た。また、収集した情報は本研究目的以外には使用せず、適切に管理した。

C. 研究結果

1. アンケート調査結果

1−1. 回答施設に関する情報

アンケートは医療機関の 550 施設からの回答が得られた。回答施設の傾向としては、経営形態としては私立の医療機関が 296 施設（53.8%）と過半数を占めており、次いで公的な医療機関（大学病院を除く）が 216 施設（39.3%）であった。医療機関の機能別では、二次救急医療機関が 259 施設（47.1%）と最も多く、地域医療支援病院が 154 施設（28.0%）、災害拠点病院（基幹・地域）が 173 施設（31.5%）と、地域医療の基幹を担う施設が多く含まれていた。病床規模に関しては、100 床以上 200 床未満の施設が 170 施設（30.9%）と多く、次いで 200 床以上 300 床未満が 87 施設（15.8%）、400 床以上 600 床未満が 84 施設（15.3%）、100 床未満が 77 施設（14.0%）と続いている。診療報酬における診療録管理体制加算の算定状況は、加算 3 が 199 施設（36.2%）、加算 1 が 185 施設（33.6%）、加算 2 が 127 施設（23.1%）となっている。

また、回答施設の 502 施設（91.3%）が電子カルテ等の「診療録の電子的保管」を導入済みであった。さらに、440 施設（80.0%）が医療情報部門を設置しており、電子カルテを含む情報システムの医療現場への展開とともに、その運用管理の必要性が組織として理解されていると想像される。以上のことから、本アンケート調査は電子カルテを導入している小中規模から大規模までの幅広い基幹的病院の現状を反映したものといえる。

1−2. 情報セキュリティ人材の現状

医療機関における情報セキュリティ人材の配置状況は極めて厳しい実態にある。具体的には、セキュリティに関する専門知識を有する人材を「配置していない」と回答した施設は 312 施設（56.7%）にのぼり、半数以上の医療機関で専門人材が不

在となっている。IPA の IT スキル標準レベル 4 以上相当の「高度専門人材」を配置できている施設は、わずか 29 施設（5.3%）という極めて限定的な状況にある。また、情報セキュリティ責任者（CISO）や医療情報システム安全管理責任者は、組織によっては、同一法人内で統一的な運用ルールが策定されており、その中に当該責任者をどの職に設定するか定めているケースもあるため、必ずしも専門知識を有することが当該責任者の条件になっていない。一方、専門人材を配置できない理由としては、「適任な人材がいない」ことが最大の要因として挙げられており、病床数に関係なく同様の回答が見受けられる。セキュリティ対策の方針決定にあたっては、医療情報システム安全管理責任者（404 施設）や CISO（248 施設）のほか、「保守契約を結ぶ医療情報システムベンダー」に依存している施設が合計で280施設（知識確認済み 186、未確認 94）に達しており、外部の知見に頼らざるを得ないという体制面の課題が浮き彫りとなった。

1−3．チェックシートにおけるカテゴリ別の現状と分析

1−3−1．組織体制と人材の現状

医療機関における CISO（情報セキュリティ責任者）や医療情報システム安全管理責任者の設置は形式上進んでいるが、実働を担う専門人材の不足が顕著であることが明らかとなった。高度な専門知識（IPA レベル 4 相当以上）を持つ人材を配置できているのはわずか 5.3%に留まり、56.7%の施設が専門人材を配置できていないため、多くが「適任者がいない」ことを理由に外部ベンダーへ依存せざるを得ない状況になっている。

1−3−2．資産・回線・リモート管理

サーバの台帳管理は 389 施設（70.7%）の施設で「全ての機器を把握している」と回答されているが、端末 PC の把握率は 341 施設（62.0%）、ネットワーク機器の把握率は 265 施設（48.2%）に留まっている。管理手法はエクセル等の汎用ソフトが448施設（83.7%）であり、資産管理ソフトを導入施設はまだ少ないと判断できる。外部回線の把握は、全て把握できているとされる施設は 388 施設（70.5%）で進んでいるものの、リモートメンテナンスにおいては自施設の仕組みを持ちつつも、ベンダー側の都合による例外接続を認めているケースが多く、管理の主導権を完全には握りきれていない実態がある。

1−3−3. MDS/SDS の活用とアカウント管理

MDS/SDS の提出を受けている施設は514施設（93.5%）と非常に高いものの、その内容を確認して具体的な対策（パスワード変更や設定変更）に繋げているのは 140 施設（25.5%）に過ぎない。アカウント管理では退職者の削除は 404 施設（73.5%）と進んでいるものの、端末ログイン時の ID 使い回しや自動ログインが約 40%あり、個人が特定できる管理の徹底に課題がある。

1−3−4．ログ管理・セキュリティパッチ適用・ソフトウェア管理

サーバのアクセスログの取得は、全ての機器のログを残している施設は 308 施設（56.0%）で実施されており、病院職員が定期的な確認を行っているのは、何らかのログを残していると回答された施設において 57 施設（11.6%）に留まっている。端末 PC のアクセスログの取得は、全ての機器のログを残している施設は 285 施設（51.8%）で実施されており、病院職員が定期的な確認を行っているのは、何らかのログを残していると回答された施設において 63 施設（14.0%）に留まっている。

セキュリティパッチの適用については、サーバ

への未適用が 263 施設（47.8%）、端末 PC への未適用が 296 施設（53.8%）、ネットワーク機器への未適用が 190 施設（34.5%）に達しており、「システムの動作保証がない」「診療停止を伴う」といった可用性とセキュリティのトレードオフが最大の障壁となっている。ソフトウェア管理では、端末へのインストール制限は対応されることが広がっている一方、不要なバックグラウンドサービスの停止は「知識不足」や「ベンダー任せ」により困難な状況にあると考える。

1−3−5. サーバー・端末・ネットワーク機器の認証

サーバー室の物理的な入退室管理は、用紙記録等で広く行われている。一方、サーバ・端末 PC・ネットワーク機器に対する認証方法として、二要素認証の実装は、いずれも 10%程度と極めて少数であった。当該認証の実装には導入コストや業務の煩雑化が理由とされ、現時点でも一要素認証（パスワードのみ）で運用されている施設が多い。その中で、パスワードの定期変更すら行えていない施設が 228 施設（41.4%）存在した。

1−3−6. 外部ストレージ・バックアップ

外部ストレージの制限は端末 PC で先行しているが、サーバー側では十分に対応できていない傾向が見受けられる。バックアップについて、本項目には 541 施設が回答を得ており、394 施設（72.8%）がオフラインバックアップを実現しているが、復旧の実証訓練を行っているのはわずか 34 施設（6.2%）に留まっている。中でも、手順の確認方法についてもベンダーに一任している施設が過半数となっている。

1−3−7. IT-BCP

IT-BCP の策定においては厚生労働省が作成した医療情報システム部門事業継続計画（BCP）を参考にした施設は 326 施設（59.2%）であった。IT-BCP は策定済みであるが、訓練による実効性の確認が今後の課題と考える。

1−4. アンケート調査結果のまとめ

本アンケート調査結果から、ウイルス対策ソフトの導入、アクセス制御の実施、バックアップの取得等、比較的基本的な技術的対策については、多くの医療機関で一定水準の対応がなされていることが確認されたが、「形式的な体制整備」に留まるケースもあり、「実効的な運用を想定した体制整備」が必要になると考える。例えば、厚生労働省のガイドラインや BCP ひな形の浸透により、責任者の設置や規定の策定、バックアップの取得といった基本的な枠組みは多くの施設で整備に向けて取り組まれている状況にある。一方、組織全体における責任体制の明確化や定期的な教育・訓練の実施、さらにインシデント発生時を想定した具体的な対応手順の整備と訓練が行われるべきである。ただし、医療機関に所属する人材として、これらの牽引役となる専門人材は不足していることが明らかとなった。高度専門人材の配置は 5.3%に留まり、その結果として、取得した MDS/SDS をリスク評価に活用できない、膨大なログを放置せざるを得ない、あるいは可用性への懸念からパッチ適用を断念するといった「受動的な対策」に留まっている実態が浮き彫りとなった。特に、「備え（バックアップや規定）」はあるが「検証（復旧訓練や見直し）」が進んでいないと考える。復旧訓練の実施率の低さは、有事の際の実効性に大きく影響を与えるものである。今後は、「今あるリソース」を活かしつつ、現場の医療職を巻き込んだ訓練やベンダーとの具体的な対策協議を通じて、組織全体の「対応力」を底上げしていくことが求められる。

２．訪問インタビュー調査結果

訪問インタビュー調査結果の要約を別添資料 6 に示す。

２−１．施設別結果

各病院のインタビュー調査結果に基づき、他施設の参考となる具体的な取り組みを 5 項目ずつ抽出した。

２−１−１．病院 A

①「セキュリティなき導入」を許さない厳格な統制

インシデントの経験から、独自チェックリストでセキュリティレベルを事前審査し、基準を満たさない機器は現場のニーズがあっても導入を許可しない強いガバナンスを確立している。

②クラウドを活用した 24 時間以内の復旧検証

電子カルテデータを Azure クラウドへバックアップし、実際に参照系サーバを 22 時間 16 分で構築できることを実証実験によって確認している。

③診療停止を伴う計画的なセキュリティパッチ適用作業の実施

端末 PC は月 1 回、サーバは 3 ヶ月に 1 回、あらかじめ設定した「平日 20 時〜23 時」のシステム停止時間枠で計画的にセキュリティパッチを適用している。

④Microsoft Teams を活用したデータ出力の申請フロー

二次利用等のためのデータ持ち出しが必要な際、Microsoft Teams を用いたデジタル申請・承認フローを構築し、証跡管理と効率化を図っている。

⑤コストを抑えた二要素認証の工夫

高価な IC カードの代わりに安価な IC タグと顔認証を組み合わせることで、委託業者を含む全利用者への展開し、全体のコストを抑制している。

２−１−２．病院 B

①現場と医療情報室を繋ぐ「コメディカル兼務」体制

診療放射線技師等の医療職 7 名を医療情報室兼務とし、「医療情報室と現場とのパイプ役」として午前は臨床、午後はシステム保守を担うことで現場感覚を運用に反映している。

②CAD 図面を用いた IT 資産の視覚的配置管理

端末 PC の設置場所をエクセル台帳だけでなく CAD（図面）上でマッピングし、物理的な所在を直感的に把握できるように整えている。

③独自規約による複数ベンダーのリモート管理

医療情報室が作成した「リモート規約」の遵守を全 22 ベンダーに義務付け、接続の主導権を病院側で保持している。

④脆弱性情報の能動的な収集体制

特定のベンダーからの連絡を待つだけでなく、IPA、JPCERT/CC 等のサイトから自ら情報を入手し、脆弱性への対策を検討する習慣が定着している。

⑤課題抽出のための机上訓練

IT-BCP の訓練を通じ、「現場と医療情報室を仲介する人員の不足」といった具体的なリソースの限界を事前に洗い出し、対策に活かす取り組みを実施している。

2−1−3．病院 C

①経営層が主導する病院内 CSIRT

医師でもある副院長を CSIRT 委員長に据え、グループ企業本社の CISO 体制と密に連携することで、経営と医療の両面からセキュリティを統制している。

②MDS/SDS における「曖昧回答」の徹底追及

ベンダーからの回答で「×」や「空欄」がある場合、必ずその理由を確認し、回答の曖昧性を排除した上でリスク評価を行っている。

③グループ企業本社基準による月次の脆弱性監査

グループ企業本社の基準に基づき、毎月のサーバセキュリティ監査を実施し、リスクの高さに応じて対策期限を厳格に管理している。

④全職種参加型「紙カルテ訓練」の実施

医療情報システムが停止したことを想定し、実際に医師や看護師ら 100 名が参加して紙カルテによる診療継続をシミュレートする訓練を実施した。

⑤カルテ不適切閲覧監査

「職員が入院した際の診療外閲覧」など、具体的なシナリオに基づいてカルテ監査を 6 ヶ月ごとに実施し、抑止力を高めている。

2−1−4．病院 D

①高度有資格者による組織的統治

情報処理安全確保支援士（登録セキスペ）かつ上級医療情報技師の資格を持つ責任者が実務を主導し、専門性の高い判断を院内で行える体制を構築している。セキュリティ対策に関する経営層への働きかけも積極的に行なっている。

②OS レベルからの実機リストア訓練の完遂

バックアップを取得するだけでなく、2025 年に OS レベルからの復元訓練（リストア）を実施し、実際にシステムを戻せることを技術的に確認した。具体的には、2 種類の仮想化基盤（VMWare、Nutanix AHV）において、稼働する VM（OS レベル）を Veeam Backup & Reprication にてバックアップし、そのバックアップデータを用いて同一基盤への復旧と異なる基盤への復旧が実現できるかを訓練した。

③セキュリティパッチ適用不能機器への「EDR」による補完

動作保証等の理由でセキュリティパッチが適用できないレガシー機器に対し、EDR を導入して常時監視を行うことで、リスクを許容範囲内に収める現実的な解決策を講じている。

④現場スタッフとの IT-BCP マニュアル共同策定

医療情報課員だけでなく各現場のスタッフを含めた複数名で IT-BCP マニュアルを作成することで、臨床現場で機能する実効性の高いマニュアルを整備している。

⑤本社報告フローと連動した資産の全数棚卸の定例化

毎年にグループ本社への IT 資産報告を行うタイミングに合わせ、資産管理ソフトを用いた全数棚卸を業務ルーチンとして完全に定着させている。

3．訪問インタビュー調査対象の 4 病院の取り組みに関する相互チェックと分析

各病院の対策を比較・検証すると、「100%の防御」という考え方から、「いかに早期に検知し、いかに迅速に復旧するか」というレジリエンスを意識した取り組みとなっていることが確認された。具体的には次の 5 点について示す。

（1）体制と人材の多様性

病院 C はグループ全体としての組織力を背景に、本社の CISO 体制と連携した非常に強固

なガバナンスが構築されていた。一方で、病院Bのような自治体病院では、行政職の人事サイクルという制約の中で、現場を熟知したコメディカル職員を兼務させることで「知識の橋渡し」を行っている点は組織を設計する上で参考になると考える。病院 D は、上級医療情報技師や情報処理安全確保支援士（登録セキスペ）といった高度な資格を持つ職員を核として、限られた体制の中でも専門性を担保している。

（2）「水際」でのガバナンス強化

病院 A は、過去のインシデント経験から「セキュリティレベルが低い機器は導入を許可しない」という非常に強い拒否権を医療情報部門が持っている。病院 B も同様に、物品管理担当部署と連携して「医療情報部門の許可なしには機器を購入できない」という仕組みを構築しており、組織的な管理体制整備が共通の有効手段となっている。

（3）バックアップと復旧の実効性

病院 A がクラウド環境上で参照系サーバを 24 時間以内に復旧させる検証を行っている点と、病院 D が OS レベルからのリストア訓練を実際に行っている点は、他施設においても参考とされたい事例となる。多くの施設が「バックアップの取得」に取り組む中、この 2 施設は、バックアップからの復元検証が実現できている。

（4）「形」から「質」への移行

厚労省のガイドラインに沿った体制（CISO の設置や IT-BCP の策定）は整備されつつあるが、その体制が実際の有事発生時に実行できるかが重要となる。策定した組織体制やマニュアルは、定期的に自施設の環境に合わせて見直す必要がある。実際には、訓練を通してマニュアルを見直すきっかけとすることができる。

（5）専門人材不足への「現実的な解」の提示

高度な専門人材を即座に採用することは困難であるが、病院 B のように「現場の知恵（コメディカル）」と「管理の知恵（行政・情報職）」を融合させることで、自立した管理が可能になると考える。

4．具体的な対策事例とその効果

訪問インタビュー調査結果から、医療機関において参考になる具体的な対策事例について示す。特に、必ずしも多額の予算を必要とせず、「運用のルール化」や「既存の人的資源の再配置」などによって比較的実現可能なものをまとめた。自施設の規模や実態に合わせて、自施設の取り組みを振り返り、さらなるセキュリティ対策に向けて参考にされたい。

（1）【人的リソースの工夫】 コメディカル兼務制度（病院 B）

○具体策：放射線技師や臨床検査技師、ME などを情報部門の兼務とし、自部署のシステムメンテナンスやトラブル対応の「窓口」とする。

○効果：情報部門に現場のニーズが正確に届くようになり、同時に現場側へのセキュリティ意識の浸透（啓蒙）がスムーズになる。

（2）【ガバナンスの工夫】 購入前チェックリストの徹底（病院 A・B）

○具体策：医療機器の導入時、契約書に判を突く前に、情報部門が作成した「セキュリティ要求事項」にベンダーが回答し、それを満たさない限り導入させない運用にする。

○効果：把握不可能な外部接続ポイントの発生を防止し、管理可能なアタックサーフェスを維持することができる。

（3）【実効性の工夫】 OS レベルのリストア訓練（病院 D）

○具体策：データのバックアップだけでなく、バックアップ管理ツールを用いて、OS や設定

情報を含めて丸ごと復旧させる訓練を定期的（年１回程度）に行う。
○効果：有事の際、「手順書はあるが実行できない」という最悪の事態を防ぎ、復旧までに必要な作業や正確な時間を経営層に報告できるようになる。
（４）【訓練の工夫】 100 名規模の全職種参加訓練（病院 C）、異常検知連絡訓練（病院 D）
○具体策：紙カルテを用いた診療継続訓練を、医師・看護師だけでなく事務部門も含む大規模なものとして実施する。また、現場で異常を検知した際に、マニュアルに従い初動対応ができるかを訓練する。
○効果：システム停止が「情報部門の問題」ではなく「病院全体の診療継続の問題」であるという共通認識が生まれ、インシデント発生時にすべきことを確認できる。
（５）【資産配置場所の把握】 資産配置場所のマッピング（病院 B・C）
○具体策：エクセル台帳だけでなく、CAD 図面（フロア図）上に端末 PC の配置場所を視覚的にプロットする。
○効果：インシデント発生時（特定の端末が通信遮断の対象になった際など）、その端末が「物理的にどこにあるか」を即座に特定でき、初動対応を加速させることにつながる。
（６）【資産管理ツールの活用】 専用の資産管理ツールの導入（病院 B・C・D）
○具体策：資産管理ツールを導入することで、資産台帳の管理のみならず、サーバや端末 PC の操作ログ取得と管理、外部記録媒体の接続制御にも活用できる。また、昨今の医療機器に対するセキュリティ対策を意識して、情報資産危険性自動評価技術も選択のひとつとなる。
○効果：ひとつのツールで複数のセキュリティ対策に寄与できる。医療情報部門の管理工数削減にも期待できる。

５．医療情報セキュリティ対策の深化と「病院 D モデル」の意義

訪問インタビュー調査対象の 4 病院の調査結果を俯瞰すると、医療機関におけるセキュリティ対策は、単なるツールの導入フェーズから、組織的なレジリエンス（回復力）の検証というフェーズへ移行していると考える。その中でも特に病院 D の取り組みは、多くの医療機関が直面する課題に対する「標準的な対策事例」として示される。

まず、「専門性の内製化」が重要な成功要因となっている。病院 D では、情報処理安全確保支援士と上級医療情報技師を保持する責任者が指揮を執り、外部ベンダーに依存しすぎない自立した意思決定を行なっている。これは、病院 B がコメディカルを巻き込んで知識を共有している事例と同様に、「現場を理解した専門家」が院内にいることの強みを象徴している。次に特筆すべきは、病院 D と病院 A に共通してみられる「検証の文化」である。多くの施設がアンケート調査結果等で「バックアップは取っているが復旧訓練は未実施」という課題を抱える中、病院 D は実際に OS レベルからのリストア訓練を成功させている。さらに、セキュリティパッチの適用に向けて取り組む必要性は理解できるものの、実際には適用に至っていない医療機関が多い。全ての機器にセキュリティパッチを適用することは重要であるが、医療現場ではアプリケーションの動作保証がされない等、様々な要因により困難な場合が多い。これに対し病院 D は、セキュリティパッチ未適用の機器にも EDR で重点監視するというリスクベースのアプローチを採用している。これは病院 A の「ネットワーク隔離」や病院 C の

「MDS/SDS の徹底査読」と並び、リソースが限られた中で最大の効果を上げるため戦略のひとつといえる。セキュリティパッチを適用する場合は、パッチが提供された際に、その重要度を確認し、適用タイミングを調整することが重要である。パッチ適用においてシステム停止が伴うケースもあり、複数のパッチをまとめて適用するようなスケジュールも検討されたい。

最後に、「現場の巻き込み」が形骸化を防ぐことにつながると考える。病院 D が IT-BCP 策定に向けた作業を医療情報課員に加え、現場スタッフを参画させたことは、セキュリティを「医療情報部門だけの問題」から「病院全体の診療継続の問題」へと意識改革の一つになったと想像する。総じて、訪問インタビュー調査結果から、これらの先進事例から学べるのは、高度な専門知識に裏打ちされた「実効性の証明」と、現場・経営層を巻き込んだ「組織的な合意形成」を両立させることの重要性であると考える。これらの知見は、専門人材の確保に悩む多くの医療機関にとって、既存のリソースをいかに再配置し、実戦的な体制を築くべきかという具体的な参考事例になるといえる。

6.システムベンダーに対するインタビュー調査

医療機関に対して実施した訪問インタビュー調査内容を踏まえて、電子カルテベンダーに対してオンライン形式でインタビュー調査を実施した。本調査から認識したこと、また課題とされることについて次に列挙する。

・セキュリティ対策として、医療機関側の要求に応じて対応しているベンダーがあった。

・製造元ベンダー、導入ベンダーが異なる場合は、導入ベンダー側でセキュリティ対策に関する方針が提示されるケースもある。

・電子カルテベンダーからの積極的なセキュリティパッチ情報の提供がない。

・システム稼働後に OS やミドルウェア等のパスワード変更等が医療機関から要求された場合、作業を担当する人材が不足しているために対応が困難となるケースがある。技術的な問題よりも、工数（リソース、コスト）の捻出が問題となる。

・ベンダーによっては医療機関側からの働きかけがなければセキュリティ対策の提案が十分に及んでいないケースもある。

得に、電子カルテ導入においては、製品の製造元ベンダーと導入を担当するベンダーが異なる場合も多く、両者間でサイバーセキュリティ対策への意識が異なるケースがあることが明らかとなった。各医療機関においては、これらの乖離についても着目した上で、システム導入作業を行うべきである。両者に乖離が生じた場合は、チェックシートを基に取り組むべき対策について医療機関からも提示した上で、ベンダー関係者内でもその理解を深め、医療機関とベンダーの相互理解に取り組む必要がある。

D. 考察

本研究から、医療情報システムのサイバーセキュリティ対策においては、チェックリストが「対策の方向性を示す有効な指針」である一方、現場の実情に合わせた理解と運用のためには、具体的な取り組み案を提示することが不可欠であることが示唆された。

特に、形式的な対応にとどまらず、具体的にチェックリストの項目が求めていることを明示し、担当者によってその解釈が異なることがないように示すことが必要と認識した。なぜその対策が必要なのかという考え方の共有や医療業務の特性を踏まえた実践的な運用設計が、継

続的な対策実施において必要な要素になると考える。また、積極的に取り組みを行っている医療機関の事例は、他の医療機関にとって有用な参考情報となり得ることから、今後は事例共有の仕組みづくりも重要な課題である。その一つとして、地域の医療機関同士で日頃からセキュリティ対策に対して共有できる組織を構築することも検討されたい。滋賀県では「滋賀県病院医療情報システム担当者の集い」が 2024 年から年 3 回実施されている。事務局は大津赤十字病院が務め、企画運営の中心を担っている。日頃から医療機関の担当者同士が交流することで、共助できる関係性の構築が可能となり、万が一サイバーインシデントが県内の医療機関で発生した際にも支え合うことのできる関係性が構築できると考える。

また、医療機関の多くはセキュリティ対策の必要性は理解されており、調達仕様に含めるべきであるとの考えは今後も必要となる。一方、セキュリティ対策を行うことは、調達全体のコストが高くなるという懸念も生じる。その中で、ベンダー側も費用を明確にしたうえで、標準提案として、セキュリティ対策レベルを厚労省ガイドラインやチェックリストが求めるレベルにまで引き上げ、その上で対応することが必要と考える。また、現在製品として提案されるシステムの多くは、標準機能にセキュリティ対策が含まれていないケースもあり、対策を加えるたびにコストが増加し、セキュリティ対策を投資として捉えることができない状況になるのではないか。実際には、標準機能にセキュリティ対策があらかじめ含まれたかたちで調達範求められる。今後は、医療機関の実態を踏まえた取り組み事例の共有や、チェックリスト自体の継続的な見直しを通じて、現場に即した形で実効性のあるサイバーセキュリティ対策が実囲の検討を開始し、不要とされる対策をその範囲から除外する等の流れにすること必要と考える。ベンダー側が「提案できる」のであれば、できることを適切に提案し、そこから施設の実情によって対策を検討できるような提案方式が実現されることを期待したい。電子カルテパッケージにセキュリティパッケージとしての適用を標準として展開されることを提案したい。

E. 結論

本研究では、「医療情報システムのサイバーセキュリティチェックリスト」に基づく医療機関の取り組み状況を、アンケート調査およびインタビュー調査により把握・分析した。

その結果、チェックリストは一定の対策水準を担保するための有効な枠組みである一方、運用面においては医療現場の実態との間に課題が存在することが明らかとなった。医療機関における対策の方向性を示す上で有効な指針である一方、その趣旨や考え方が十分に共有されていない場合、形式的な対応にとどまる可能性があることが示唆された。特に、医療機関においては、診療業務の特性や人的資源の制約を踏まえた運用が不可欠であり、チェックリストの各項目について「求められる背景・目的」を理解した上で、各施設の実情に応じた実装が重要であると考えられる。

今後は、医療機関の実情を踏まえた好事例の共有や、現場に即した形で実践可能なチェックリストの改善を通じて、医療機関における実効性の高いサイバーセキュリティ対策の推進が施される環境づくりが求められる。

積極的に取り組みを実施している医療機関においては、経営層の関与のもとで体制整備が行われていること、また医療現場の負担を考慮

した現実的な運用ルールの工夫がなされていることが確認された。一方、人材・時間・予算の制約、チェックリストの解釈の難しさといった課題も見受けられたことから、各医療機関は、「人員と予算の制約」という課題を抱えながらも、チェックリストを最低限取り組むべきセキュリティ対策として捉えて、運用ルールの徹底や既存資産の有効活用によって、実効性のある対策を模索し続ける必要がある。今後も時代に応じたチェックリストへの改版と、それに対して具現化して取り組むことができるかを検証しながら取り組む必要がある。

また、積極的に取り組みを行っている医療機関の事例は、他の医療機関にとって有用な参考となることから、こうした事例を共有する仕組みの整備や、チェックリストの分かりやすさ・実装容易性を高める工夫も検討すべき課題である。

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

・橋本智広. マルチプラットフォームとデータ保護戦略による信頼性強化～医療情報システムにおける強靭化とレジリエンスの両立を考える～. 第45回医療情報学連合大会, 2025年11月.

・橋本智広. IT-BCP 実践アプローチとサイバーレジリエンス強化に向けて ～アクションカード整備の重要性とサーバー仮想化基盤の分散管理による可用性確保～. 第 45 回医療情報学連合大会, 2025年11月.

・橋本智広. 医療機関におけるIT-BCPに基づくインシデント発生時の初動対応. 第 45 回医療情報学連合大会, 2025年11月.

・橋本智広. 現場目線で考える、医療機関の今すべき情報セキュリティ対策. 第 12 回 メディカルジャパン大阪（医療・介護・薬局 Week 大阪）. 2026年3月.

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