政策科学総合研究事業（臨床研究等ICT基盤構築・人工知能実装研究事業）
（総括・分担）研究報告書

医療機関におけるサイバーセキュリティ監査に求められる項目に関する研究

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
本研究では、2023 年度厚労科研で示された指導的立場のセキュリティ人材を有する医療機関、すなわち集中管理機関同士の相互チェックに用いることを想定し、医療機関におけるサイバーセキュリティ監査項目の案を作成した。監査技法は質問、チェックリスト、査閲、観察、再実施、サンプリング、脆弱性診断、ペネトレーションテストの 8 項目とし、各項目について患者死亡リスク、医療ワークフロー停止リスク、NIST CSF・RMF および IT-BCP の観点から求められる対策能力、医療情報システムの安全管理に関するガイドライン第 6.0 版との関係を整理した。作成した一覧は、情報資産単位の点検を診療機能単位のリスク評価へ接続し、相互チェックおよび共同 IT-BCP 訓練における確認項目として利用可能な構成とした。

A．研究目的

医療機関のサイバーセキュリティ対策では、医療情報の機密性、完全性、可用性を確保するだけでなく、電子カルテ、部門システム、医療機器、ネットワーク、クラウドサービス、リモート保守が診療機能へ及ぼす影響を評価対象に含める必要がある。「厚生労働省の医療情報システムの安全管理に関するガイドライン第 6.0 版」（令和５年５月）は、概説編、経営管理編、企画管理編、システム運用編に分けて安全管理を整理し、医療機関等におけるサイバーセキュリティ対策チェックリストも優先的に取り組む事項として示している［1］。一方で、監査項目を医療現場の停止リスク、患者安全リスク、診療継続判断へ対応させるためには、一般的な情報セキュリティ監査技法を医療機関の業務構造へ翻訳する作業が必要となる。

本分担研究の目的は、「集中管理機関同士が互いにセキュリティチェックを行う相互チェック」の実施に向け、医療機関における監査項目案を策定することである。監査項目は、NISC の情報セキュリティ監査の実施手引書に示される監査計画、監査実施、監査報告等の考え方［2］を基盤に置き、NIST Cybersecurity Framework 2.0 の Govern、Identify、Protect、Detect、Respond、Recover［3］、および NIST SP 800-37 Rev.2 の Risk Management Framework［4］と整合するよう整理した。

医療機関におけるシステム脆弱性［5］を侵入手段とするランサムウェア等の攻撃は、電子システム停止、予約診療の中止、救急搬送受入停止などの診療提供障害と関連することが報告されている。隣接施設に対するサイバー攻撃が地域の救急患者数、待機時間、急性期脳卒中対応指標に影響しうることも示されており［6］、監査項目には単一施設の情報資産に限定されない診療機能・地域機能の観点を含める必要がある。本研究では、患者死亡リスクと医療ワークフロー停止リスクを二つの主要軸として設定し、監査技法ごとに確認すべき内容を整理した。

B．研究方法

研究方法として、第一に、研究計画書に示された相互チェック研究の担当範囲を確認し、監査項目リスト案の対象を、集中管理機関が被評価機関のセキュリティ対策を確認する場面、および集中管理機関同士が相互にチェックする場面に設定した。第二に、厚生労働省ガイドライン第 6.0 版、同チェックリスト、NISC の情報セキュリティ監査の実施手引書、NIST CSF 2.0、NIST RMF、政府情報システムにおける脆弱性診断導入ガイドラインを参照し、監査で確認する証拠、管理策、運用能力の分類を抽出した。

第三に、医療機関のリスクを「患者死亡リスク」と「医療ワークフロー停止リスク」に区分した。患者死亡リスクは、ICU、SCU、手術室、麻酔、救急、生命維持装置、院内 IoT など、障害が短時間で患者状態に影響し得る領域を中心に整理した。医療ワークフロー停止リスクは、外来受付、会計、オーダリング、検査、画像、調剤、入退院、地域連携、クラウドサービス、VPN、ゲートウェイなど、診療提供の流れと復旧順位に影響する領域を対象とした。

第四に、監査技法を、質問、チェックリスト、査閲、観察、再実施、サンプリング、脆弱性診断、ペネトレーションテストの 8 項目に整理した。

各技法について、二つの医療リスク軸、望ましい対策ならびに能力、関連するガイドライン項目を表形式で記述し、xlsx ファイルとして監査リスト案を作成した。

倫理面への配慮として、本作業は公開資料、研究計画書、研究者の専門的知見、および監査項目案の作成を対象とし、患者個人情報、診療録、ログ実データ、実システムに対する診断結果を用いていない。今後、実医療機関における適用検証、脆弱性診断、ペネトレーションテスト、ログレビューを行う場合には、対象範囲、実施権限、診療影響回避手順、秘密保持、個人情報保護、医療安全部門との事前合意を明確化する。

C．研究結果

作成した監査リスト案は、監査技法を縦軸に、医療における患者死亡リスク、医療ワークフロー停止リスク、望ましい対策ならびに能力、関連付く医療情報システム安全管理ガイドライン第 6.0 版の項目を横軸に配置した。監査技法ごとに、文書確認にとどまらず、ヒアリング、現場観察、再実施、ログ・障害記録のサンプリング、脆弱性診断、限定的なペネトレーションテストを組み合わせる構成とした。

成果物では、患者死亡リスクに関わる 1 系・4 系の診療機能を高優先度領域として扱い、医療ワークフロー停止リスクでは外来、検査、会計、入退院、調剤、地域連携を停止影響の単位として扱った。これにより、一般的な資産管理の棚卸から、診療機能単位の停止影響、縮小診療、転院判断、紙運用、ローカルモード、リストア、復旧順位へ監査観点を展開できる構成となった。

望ましい対策ならびに能力として、CSF の Identify、Protect、Detect、Respond、Recover に加え、Govern の責任分界、戦略、説明責任を明示した。RMF の観点では、重要業務と重要システムの定義、制御策の選択・実装・評価、継続的モニタリング、残存リスクの把握を監査項目の背後に置いた。IT-BCP の観点では、停止判断、代替運用、復旧順序、訓練、ログ記録、再発防止策を確認対象とした。

別表 1 に、xlsx ファイルとして作成した監査項目リスト案を転記した。本文では成果の要約を表 1 に示す。

D．考察

本研究で作成した監査リスト案の特徴は、情報資産単位の監査を診療機能単位のリスク評価へ接続した点にある。従来の情報セキュリティ監査では、規程、台帳、アクセス制御、ログ、脆弱性、委託契約などを証拠として確認する。一方、医療機関では、同じシステム停止であっても、救急、集中治療、手術、検査、調剤、外来会計のいずれに影響するかにより、必要な判断者、許容停止時間、代替手順、患者説明、転院判断が異なる。この差異を監査項目に組み込むことで、チェックリストの結果を医療安全上の対応計画に接続しやすくなる。

患者死亡リスクと医療ワークフロー停止リスクを分けたことにより、監査結果の解釈も明確となる。患者死亡リスクでは、短時間の障害でも治療中断や判断遅延につながる機器・部門を優先的に評価する必要がある。医療ワークフロー停止リスクでは、患者一人当たりの急性危険度が相対的に低い場合でも、多数患者に対する受付停止、検査遅延、処方遅延、会計停止、地域連携停止が発生しうる。病院全体のリスク管理では、死亡リスクを独立して評価しつつ、影響患者数、診療機能稼働率、復旧時間を併せて扱う設計が望ましい。

医療機関においては、監査技法ごとの証拠力にも差があると考えられる。質問とチェックリストは短時間で範囲を広く確認できるが、回答者の理解度や院内文書の整備状況に依存する。査閲は責任分界や運用記録の整合性を評価できる。観察と再実施は現場の実行可能性を評価する上で有用であり、代替運用の人員、物品、導線、再入力工程を明らかにする。サンプリングは過去事象に基づく改善循環を評価できる。脆弱性診断とペネトレーションテストは技術的弱点と検知・対応能力を実証的に評価できるが、診療影響を回避する安全条件、検証環境、本番環境への影響抑制、実施権限の明確化を要件とする。

本研究により作成した本リスト案は、相互チェックの標準項目として利用できるだけでなく、共同 IT-BCP 訓練の評価票、医療機関向けサイバーセキュリティ対策チェックリストの補助資料、情報資産危険性自動評価技術の出力結果を解釈する枠組みとしても利用可能である。自動評価技術がネットワーク上の機器、通信、脆弱性、外部接続点を抽出した場合でも、その結果を診療機能停止リスクに変換するには、医療機関固有の業務依存関係を重ねる必要がある。本研究の表形式は、その変換に必要な確認事項を明示する役割を持つ。

今後の課題として、実医療機関における相互チェックでの適用性、所要時間、回答困難項目、証拠取得可能性、診療影響評価の妥当性を検証することが挙げられる。特に、小規模医療機関やグループ A 人材を持たない被指導機関では、監

査項目の粒度、用語、証拠提出方法を調整する必要がある。次年度の相互チェックおよび合同 IT-BCP 訓練では、本リスト案を用いて、監査項目の優先順位、必須項目、任意項目、技術診断を伴う項目、安全上除外すべき項目を分類することが望ましい。

Ｅ．結論

医療機関におけるサイバーセキュリティ監査項目案として、8 種類の監査技法を、患者死亡リスク、医療ワークフロー停止リスク、NIST CSF・RMF、IT-BCP、医療情報システム安全管理ガイドライン第 6.0 版へ対応させた一覧を作成した。

本成果は、集中管理機関同士の相互チェック、被指導機関への支援、共同 IT-BCP 訓練、情報資産危険性自動評価技術の結果解釈に利用できる基礎資料である。今後は、実施手順書、評価票、重み付け、診療機能別の優先順位、技術診断の安全条件を追加し、実医療機関での検証により監査項目の実効性を評価することが考えられる。

Ｆ．健康危険情報

（総括研究報告書にまとめて記入）

Ｇ．研究発表

1.　論文発表

該当なし。

2.　学会発表

鳥飼幸太、他分野に学ぶサイバーセキュリティレベル向上 ～専門家の視点から～（オーガナイザー・座長・演者）、第 45 回医療情報学連合大会 大会企画 1、一般社団法人日本医療情報学会、A 会場（2 階 大ホール）、2025 年 11 月 13 日

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

1) 鳥飼幸太、RMF に基づいた医療機関におけるサイバーセキュリティの整備、埼玉県警察本部主催 医療サイバーセキュリティセミナー、埼玉県警察本部、埼玉県浦和市、2026 年 3 月 16 日

2) 鳥飼幸太、医療サイバーセキュリティシミュレーション実践、関西広域連合規格ワークショップ、関西広域連合、滋賀県草津市、2026 年 3 月 5 日

3) 鳥飼幸太、医療機関におけるサイバーセキュリティ対策の理解と実践（座長）、第 45 回医療情報学連合大会 学会企画 4、一般社団法人日本医療情報学会、B 会場（2 階 中ホール）、2025 年 11 月 15 日

参考文献

［1］厚生労働省．医療情報システムの安全管理に関するガイドライン 第 6.0 版（令和 5 年 5 月）および関連資料
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

［2］国家サイバー統括室．政府機関等のサイバーセキュリティ対策のための統一基準に基づく情報セキュリティ監査の実施手引書．
https://www.cyber.go.jp/pdf/policy/general/SecurityAuditManual.pdf

［3］National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

［4］National Institute of Standards and Technology. NIST SP 800-37 Rev.2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. 2018. https://csrc.nist.gov/pubs/sp/800/37/r2/final

［5］デジタル庁．政府情報システムにおける脆弱性診断導入ガイドライン 2024．
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7fefc9ee/20240206_resources_standard_guidelines_guidelines_01.pdf

［6］Neprash HT, McGlave CC, Cross DA, Virnig BA, Puskarich MA, Huling JD, et al. Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. JAMA Health Forum. 2022. PubMed: https://pubmed.ncbi.nlm.nih.gov/36580326/

［7］Dameff C, Tully J, Chan TC, et al. Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US. JAMA Network Open. 2023;6(5):e2312270. PubMed: https://pubmed.ncbi.nlm.nih.gov/37155166/

［8］Jalali MS, Kaiser JP. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. Journal of Medical Internet Research. 2018;20(5):e10059. PubMed: https://pubmed.ncbi.nlm.nih.gov/29807882/

表 1　監査技法別の成果概要

監査技法	医療リスクに対する確認内容	監査上の位置づけ
質問（ヒアリング）	救急、手術、集中治療、生命維持装置などの停止判断、代替運用、最終判断者を確認する。外来、検査、会計、入退院、地域連携の縮小診療や手動運用も聴取する。	経営層、医療安全、診療部門、情報部門、委託先が共通言語でリスクと指揮命令系統を説明できるかを評価する。
チェックリスト	ハイリスク診療機能、停止時代替運用、復旧順位、CSF 各機能の達成度を一覧で自己点検できる構成とする。	ガイドライン付属チェックリストと院内独自項目を接続し、施設間相互チェックに用いる基礎資料とする。
査閲（規程・ログ等）	IT-BCP、情報セキュリティポリシー、医療安全管理規程、ネットワーク構成図、バックアップ手順、障害記録の整合性を確認する。	文書化された方針と実際の運用記録の差異を把握し、統制、責任分界、ログ管理、復旧手順の実装状態を評価する。
観察（視察）	ICU、手術室、救急室、外来、検査部門、薬剤部、地域連携窓口で、障害時暫定フローが現場で実行可能かを確認する。	机上手順と実運用の差、復旧時の再入力・照合作業負荷、医療安全上の判断の可視性を評価する。
再実施	ネットワーク遮断、非常電源切替え、EHR・LIS 停止時の模擬診療、バックアップリストア、VPN・ゲートウェイ切替えを限定的に試行する。	RTO・RPO、フェイルセーフ、アクセス制御、EDR、セグメント間通信制御の実測値と手順書の整合性を評価する。
サンプリング	重大インシデント、ヒヤリハット、障害ログ、変更管理記録、運用日誌、ヘルプデスク記録を抽出して診療影響を分析する。	過去事象から IT-BCP の想定妥当性を検証し、ISMS・PDCA の見直しへ反映する能力を評価する。
脆弱性診断	電子カルテ、LIS、RIS、医療機器管理端末、外部接続点、VPN、地域連携システムの設定不備とパッチ管理状況を確認する。	診断対象を RMF 上の診療リスクに基づいて選定し、緊急度に応じた是正計画へ接続する。
ペネトレーションテスト	本番生命維持系への直接攻撃を避け、検証環境や合意済み範囲で侵入、権限昇格、横移動、封じ込め、復旧能力を評価する。	実攻撃に近いシナリオで Detect、Respond、Recover の有効性を確認し、テスト範囲、安全条件、責任分界を明確にする。