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）

地域における共通基盤・集中管理体制によるサイバーセキュリティの実証のための研究

令和７年度　総括研究報告書

研究代表者　黒田　知宏

令和８（２０２６）年　５月

目　　次

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）
総括研究報告書

地域における共通基盤・集中管理体制による サイバーセキュリティの実証のための研究

研究代表者　黒田 知宏　京都大学 医学部附属病院

研究要旨
本研究では、相互チェック・合同 IT-BCP 訓練を通じてセキュリティ向上と人材育成を同時に進める枠組みを作ろうとするものである。初年度は、共通基盤として病院ネットワークに繋がる機器を検出する仕組みの導入と、規範となるチェックリストの策定、及び、相互チェック手順書と IT-BCP 訓練実施体制の策定を実施した。これらの成果により、二年度に具体的なチェック・訓練を実施する基本的な準備が整った。

黒田知宏・京都大学・教授
武田理宏・大阪大学・教授
谷川琢海・北海道科学大学・教授
橋本智広・大津赤十字病院・課長
川眞田実・大阪国際がんセンター・副診療放射線技師長
肥田泰幸・東都大学・講師
鳥飼幸太・群馬大学・准教授
油谷曉・京都大学・講師
楠田佳緒・京都大学・特定講師
芦原貴司・滋賀医科大学・教授
高倉弘喜・国立情報学研究所・教授

A．研究目的

医療機関を取り巻くセキュリティ人材の不足は深刻化している。少ない人材で喫緊のセキュリティ対策を実施するためには、優秀なセキュリティ人材を集約した指導的な医療機関（集中管理機関）を設置し、関連医療機関のセキュリティ対策の支援を行わせることで、短期的な情報セキュリティ確保を図るとともに、医療と工学技術に伴に明るい臨床工学技士・診療放射線技師を主たる対象としたセキュリティ教育を実施させることで、長期的なセキュリティ人材の養成を図ることが適当である。

本研究では、2023年度厚労科研（201221069A）で示した指導的立場のセキュリティ人材（グループA人材）を有する医療機関（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取り組みを通じてセキュリティチェックの手順書と監査項目を策定するとともに、これを複数のグループA人材を有さない医療機関（被指導機関）に適用してその実効性について検証する活動を実施する。この際、セキュリティチェックの効率性と有効性を向上するため、情報資産危険性自動評価技術の共通利用の枠組みを確立する。この枠組みは、集中管理機関が被評価機関の指導を行う際にも活用する。

加えて、グループC人材を有する被指導機関がランサムウェア攻撃等のサイバー攻撃を受けたことを想定したIT-BCP対応訓練を、被指導機関と集中管理機関が共同して実施することで、集中管理機関と被指導機関の役割を明確にした共同IT-BCP手順書を確立するとともに、グループC人材の実践的教育としての合同IT-BCP訓練の実効性について検証する活動を実施する。

初年度は、相互チェックのための監査項目策定と手順書の策定を行うとともに、IT-BCP訓練の下敷きとなる、参加医療機関の病院ネットワークの状況調査を行った。

B．研究方法

本研究は、1）集中管理機関同士の相互チェックに必要文書（セキュリティチェック手順書、セキュリティ監査項目一覧）の策定とチェックの実施（相互チェック）、2）集中管理機関と被指導機関との共同 IT-BCP 手順書の策定と IT-BCP 訓練の実施（共同 IT-BCP 訓練）、の二つの研究からなる。

1）相互チェック研究は、（1A）監査項目リストの策定、（1B）相互チェック手順書の策定、（1C）相互チェックの実施、の三つの研究から構成される。本研究では初年度に（1A）を、二年度の前期までに（1B）を実施し、二年度中頃をメドに、グループ A 人材を有する二つの医療機関、京都大学医学部附属病院と、大津赤十字病院の間で、実際に（1C）を実施し、（1A）及

び（1B）研究の成果について、その実用性を評価する。

2）共同 IT-BCP 訓練研究は、(2A) IT-BCP 計画の策定、(2B) 訓練シナリオの策定、(2C) 訓練の実施、の三つの研究から構成される。本研究では、大津赤十字病院を中心に「びわ湖あさがおネット」等の活動を通じて地域全体の行政・医療機関が相互支援体制（医療機関ネットワーク）を有する滋賀県地域、特に、大津市地域において、大津赤十字病院と京都大学医学部附属病院を集中管理機関として実施する。初年度に（2A）を、二年度の前期までに(2B)を実施し、二年度後期に(2C)を実施し、(2A) 及び (2B) 研究の成果について、主にグループ C 人材の実践的教育手法としての実効性の観点から評価する。

C．研究結果

1）相互チェック研究においては、本年はまず(1A)監査項目リストの策定を実施するとともに、(1B)相互チェック手順書の策定準備に着手した。(1A）においては、八つの監査手法と、三つの観点から詳細に検討され、相互チェックのみならず、IT-BCP計画策定に適用出来る構成に纏められた。(1B）においては、先行する医療安全分野の相互チェック手順に関する調査に基づいて、毎年監査する基本項目と、最新の脅威や課題に応じた重点項目を組みあわせることが効果的であること、及び、相互チェック全体を企画・運営する事務局的組織が必要であることを見出した。結果の詳細については、（1A）担当した鳥飼の、（1B）は担当した武田の分担報告書のとおりである。

2）共同IT-BCP訓練研究においては、本年はまず(2A) IT-BCP計画の策定を行うとともに、(2B)訓練シナリオの策定の準備をすすめた。（2A）においては、公開されているIT-BCPや電子カルテシステム停止時マニュアル、及び、サイバー攻撃被害報告書を調査しGroup C人材がGroup A人材へ支援を要請すべき項目等を洗い出して、手順書に纏めた。（2B）においては、訓練対象医療機関を選定し、被災時に掌握が必要な自院のネットワーク医療機器一覧を調査する方法を確立し「共通基盤」のモデルを整えるとともに、訓練シナリオ案の策定を進めた。結果の詳細については、担当した楠田・油谷・橋本の分担報告書のとおりである。

D．考察

本研究の遂行を通して、医療サイバーセキュリティは、高度な技術導入の問題ではなく、極めて泥臭い状況掌握の活動の積み重ねによって実施できるものであることが再確認されたとともに、たとえ「指導的な医療機関」であっても、泥臭く膨大な作業である状況掌握の活動は、必ずしも十分実施できておらず、これを支える「共通基盤」たる技術導入が極めて大きな役割を果たしうることが確認出来た。

E．結論

本研究では、サイバーセキュリティ人材が不足する中で、相互チェック・合同IT-BCP訓練を通じてセキュリティ向上と人材育成を同時に進める枠組みを作ろうとするものである。

本年度の研究では、その前提となる現状を知るための仕組みを「共通基盤」として設定し、その適用を通じて現状を把握するとともに、論理的に求められるチェックリストを作ることを並行して進めた。これらの活動によって、二年度に実施する、相互チェックと合同IT-BCP訓練のシナリオを立てるための準備が整ったと考えられる。

F．健康危険情報

該当無し

G．研究発表

1. 論文発表

該当無し

2. 学会発表

該当無し

3. その他

1) T. Kuroda. Medical Cyber Security of KUHP and Japan. UPM-KU Mini Symposium on Computer-Assisted Systems in Healthcare, Memorial Auditorium of Kyoto University School of Medicine. 2025年6月17日.
2) 黒田. 医療機関が抑えておくべき医療情報セキュリティの基礎. 新社会システム総合研究所 医療･介護戦略特別セミナー. オンライン. 2025年9月19日.
3) 黒田, Greenhalgh. 現場と経営をつなぐサイバーセキュリティ戦略. Claroty Nexus Days. ザ・リッツ・カールトン 京都. 2025年10月10日.
4) 黒田. 医療サイバーセキュリティを地域で支える仕組みを作る試み. 関西健康･医療創生会議シンポジウム. オンライン. 2025年12月15日.
5) T. Kuroda. Medical Cyber Security Strategy of KUHP. Internal Seminar. Helsinki University Hospital. 2026年1月22日.
6) T. Kuroda. Medical Cyber Security Strategy of KUHP. Kyoto-Zurich Joint Symposi

um. University of Zurich. 2026年1月23日.

7) T. Kuroda. Medical Cyber Security Strategy of KUHP. Internal Seminar. University of Oulu. 2026年1月26日.

H．知的財産権の出願・登録状況
（予定を含む。）

該当無し

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。

監査技法（NISC）	医療における患者死亡リスク	医療におけるワークフロー停止リスク	望ましい対策ならびに能力 （NIST CSF・IT-BCP 観点）	関連付く項目 （医療情報システム安全管理 GL 第 6.0 版）
質問（ヒアリング）	リスクを「患者死亡リスク」「医療ワークフロー停止」の2つに大別する。「患者死亡リスク」においてこれらが影響する1系・4系（手術/ICU等における生命維持装置、麻酔・手術、救急）について、サイバー攻撃や長時間障害時に「どの時点で何を止める／続けるか」「誰が最終判断を行うか」を各職種から聴取する。代替ワークフロー（紙カルテ・スタンドアロン機器など）を具体的に説明できるかを確認する。	「医療ワークフロー停止」のリスク視点から、外来受付～検査～会計、入退院事務、検査・調剤・地域連携が停止した場合の縮小診療や手動運用の手順を、診療科長・看護部・医事部・情報部門・ベンダから聴取する。ネットワーク分断や院外連携停止時の運用（地域連携システムやクラウドサービス停止時）を説明できるか確認する。	RMFによって重点指定された箇所について、CSF Identify／Protect に基づき「重要業務・重要システムの定義」「RMF 1～4系の優先順位」を説明できること。CSF Respond／Recover の観点から、インシデント発生時の指揮命令系統、広報・説明責任、善後策の検討プロセスを、経営層・企画管理者・システム運用担当者が共通言語で明確に回答できること。	概説編：医療機関等の責務とサイバー攻撃を踏まえた IT-BCP の必要性全般。経営管理編：1章「責任（平常時・非常時）」「委託・第三者提供の責任」、2.1～2.2「リスク評価とリスク管理方針・説明責任」、3.1「統制の体系」。
チェックリスト	RMF 1系・4系のハイリスク機能（ICU／SCU、手術室、救急、生命維持 IoT）が、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や院内独自チェックリスト上で別立ての管理対象になっているかを確認する。停電・ネットワーク断・ランサムウェア時に患者が死亡し得るシナリオが網羅されているかを点検する。	受付・会計・オーダリング・LIS／RIS・調剤支援・地域連携など各系統について、停止時の代替運用（縮小外来、紙運用、ローカルモードなど）と復旧順位がチェックリストに組み込まれているかを確認する。NIST CSF 各機能に対する達成度を自己点検できる形式になっているかをみる。	CSF Identify に基づく資産・業務の棚卸と重要度区分、Protect／Detect に基づく技術的・組織的対策項目、Respond／Recover に基づく IT-BCP チェック項目を、ガイドライン付属のチェックリストとローカルチェックリストで一貫して管理する能力。	概説編・別添「サイバーセキュリティ対策チェックリスト」、経営管理編 2章「リスク評価を踏まえた管理」、企画管理編「リスク評価とリスク管理」「システム・サービス事業者からの情報収集とチェックリスト活用」（MDS／SDS 等）。
査閲（レビュー：規程・ログ等）	「患者の生命・身体への影響を最小化しつつ診療継続を図る」ことが、情報セキュリティポリシー、IT-BCP、医療安全管理規程、救急・集中治療関連マニュアルのいずれにも一貫して書かれているかを査閲する。生命維持装置や手術支援機器の運用手順にサイバーインシデント時の取扱い（院内 LAN 切断、リモート保守遮断など）が明記されているかを確認する。	電子カルテ・LIS／RIS・調剤支援・地域連携システムの障害対応手順書、ネットワーク構成図、バックアップ・リストア手順、手動運用マニュアルを突き合わせ、RMF 2～4系のワークフローが停止した場合にどこまで代替可能かを文書から検証する。重大障害ログ・インシデント記録から、復旧時間と診療影響の整合性もレビューする。	CSF Identify／Protect：資産台帳・ネットワークトポロジー・責任分界表が最新であり、ガイドラインに沿って文書化されていること。Detect／Respond／Recover：ログ管理規程・インシデント対応手順・BCP 訓練記録から、検知～分析～復旧までのプロセスが実際に運用されているかを評価する能力。	経営管理編：1.3「委託・責任分界」、2.1～2.2「リスク評価とリスク管理方針」「ISMS の実践」、2.2.3「リスク分析を踏まえた要求仕様適合性」、3.1「統制」。企画管理編：組織体制規程、ネットワーク・クラウド・リモートサービス・情報管理に関する規程。システム運用編：アクセス管理、ログ管理、バックアップ・障害対応・災害対策に関する章全般。
観察（視察）	ICU・手術室・救急室等で、運用担当者が手順書に従って機器を運用しているかを現場で確認する。ネットワーク遮断や院内システム停止を想定した訓練時に、患者安全を優先した縮小医療や転送判断が実際に行われているかを観察する。	外来受付・検査部門・病棟・薬剤部・地域連携窓口で、障害時の暫定フロー（紙受付、紙オーダ、手書きラベル、電話連絡など）が現実的に回るかをウォークスルーする。復旧時のデータ再入力・照合作業が過大な負荷や入力ミスにつながっていないかを確認する。	CSF Protect／Detect：物理・環境・アクセス管理が現場で実効性を持っているか、観察を通じて評価する能力。Respond／Recover：訓練時に HICS などの指揮系統が実際に動作しているか、代替運用の起動・停止の判断が明確かを確認すること。	概説編：医療現場での安全管理と情報セキュリティの関係。経営管理編：3.1「統制」、4章（医療安全管理体制等）。企画管理編：運用手順・教育訓練・物理・環境対策に関する章。システム運用編：日常運用・障害対応手順、運用監視。
再実施	生命維持装置のネットワーク遮断試験、非常電源切替え試験、EHR／LIS の停止を想定した模擬診療などを、監査人立会いの下で限定的に再実施し、「患者に危険を与えずフェイルセーフに移行できるか」「医療安全上の判断が適切か」を検証する。	電子カルテ・ネットワーク・VPN・ゲートウェイ等の切替え試験を再実施し、外来や入退院事務、検査・調剤・地域連携がどの程度の停止時間であれば許容できるか、RTO／RPO が実測値と整合しているかを確認する。	CSF Protect／Detect：アクセス制御・セグメント間通信制御・EDR 等が期待どおりに動作するかを実証する能力。Respond／Recover：システム切替え、バックアップからのリストア、業務復旧手順が手順書通りに実行できるかをテストする能力。	経営管理編：2.1「リスク評価の実施」および 2.2「リスク管理」「ISMS の PDCA」、3.1「統制」。企画管理編：BCP／DR 設計、ネットワーク・電源・クラウド構成。システム運用編：バックアップ・切替え手順、定期訓練・テスト。
サンプリング	重大インシデントやヒヤリハットの記録から、RMF 1系・4系に関わる事例をサンプリングし、「サイバー要因の有無」「診療継続の可否」「患者転帰」を追跡する。重点リスクに対する再発防止策が講じられているかを評価する。	障害ログ、変更管理記録、運用日誌、ヘルプデスク記録から、システム停止や性能劣化の事例をサンプリングし、受付～検査～会計、入退院、地域連携に与えた影響と復旧時間を分析する。サンプリング結果と IT-BCP の想定が整合しているかを確認する。	CSF Detect：ログ・監査証跡・インシデント記録を継続的に分析する能力。Respond／Recover：サンプリング結果をもとに、リスク管理方針・BCP の見直しに反映する ISMS／PDCA の運用能力。	経営管理編：2.1～2.2「リスク評価とリスク管理」「説明責任」、3章「安全管理全般」。企画管理編：ログ・監査証跡管理、変更管理、インシデント管理。システム運用編：運用記録・障害記録の保存とレビュー。
脆弱性診断	電子カルテ、LIS／RIS、手術・麻酔装置の管理端末、院内 IoT（1-1／1-2）など、停止が直接生命に影響するシステムについて、パッチ管理や設定不備などの脆弱性を洗い出し、「攻撃されれば致死的結果になり得る箇所」を特定する。医療機器ベンダとの責任分界も確認する。	外来・病棟端末、VPN、ゲートウェイ、地域連携システム、クラウドサービスなどについて、脆弱性スキャンや設定レビューを実施し、ランサムウェアや侵入拡大の起点となる弱点を特定する。診療ワークフロー全体に波及する経路を可視化する。	CSF Protect／Detect：構成管理・パッチ管理・脆弱性管理プロセスの整備と、定期的な診断結果の評価能力。Identify：診断対象の選定が RMF 1～4系のリスクに基づいていること。Respond：緊急度に応じた是正計画の立案・実施能力。	NISC 監査手引書 表 2.1-2「脆弱性診断の概要」と注意点。 ガイドライン：概説編・企画管理編におけるサイバー攻撃対策・技術的対策、経営管理編のリスク評価とリスク管理、システム運用編の脆弱性管理・パッチ管理等。
ペネトレーションテスト	生命維持系ネットワークに対しては、原則として本番環境への直接攻撃は避ける前提で、検証環境やシミュレーションを用いつつ「侵入された場合にどこまで安全機能が維持できるか」「医療機器のフェイルセーフ設計が有効か」を検証する。テスト範囲と安全条件の合意が必須である。	受付・会計・オーダリング・LIS／RIS・地域連携・VPN・ゲートウェイなどを対象に、院外からの侵入、権限昇格、横移動、データ暗号化・窃取を想定した疑似攻撃を実施し、診療ワークフローがどの段階で機能不全に陥るか、検知・封じ込め・復旧の実力を評価する。	CSF Detect／Respond：SOC／EDR／ログ分析・アラート対応が、実際の攻撃シナリオに対して有効に機能するかを検証する能力。Recover：テスト結果を踏まえたネットワーク再設計、ゼロトラスト化、IT-BCP 強化の計画立案能力。Governance：テスト方針・スコープ・安全基準を経営層が承認し、責任分界を契約で整理していること。	NISC 監査手引書 表 2.1-2「ペネトレーションテストの概要」。 ガイドライン：概説編におけるサイバー攻撃リスクの位置付け、経営管理編のリスク低減と説明責任、企画管理編のネットワーク・クラウド・リモートサービスに関する安全管理、システム運用編のインシデント対応・事業継続。

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）
分担研究報告書

サイバーセキュリティ対策の相互チェックの手順書の作成

研究分担者　武田　理宏　大阪大学大学院医学系研究科

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向上と均てん化を目的として、医療安全分野で実施されている「相互チェック」や「ピアレビュー」の仕組みを参考に、サイバーセキュリティ対策の相互チェック手順書を作成することを目的としたものである。近年、厚生労働省による「医療情報システムの安全管理に関するガイドライン」改定や「サイバーセキュリティ対策チェックリスト」の策定等により、医療機関における対策強化がはかられている。しかし、対策には投資や専門人材が必要であり、各医療機関において適切な対策レベルを判断することは容易ではない。このため、他施設との比較や優良事例の共有を可能とする相互チェック体制の必要性が高まっている。

本研究では、大阪大学医学部附属病院中央クオリティマネジメント部へのヒアリングを通じて、国立大学病院で実施されている医療安全・質向上のための相互チェックおよび特定機能病院間のピアレビューの運営実態を調査した。医療安全分野では、過去の重大医療事故を契機として全国統一のチェック体制が整備され、現在は重点項目に特化した相互訪問型のレビューへと発展している。重点項目は、最新の課題やガイドラインを踏まえて専門 WG が設定し、2 年 1 サイクルで相互訪問と改善確認を行う仕組みとなっている。また、特定機能病院間のピアレビューでは、医療法に基づき毎年の実施が義務化されており、医療安全体制や医薬品管理等について継続的な相互評価が行われている。

これらを踏まえ、本研究ではサイバーセキュリティ対策においても、毎年実施する基本項目と、最新の脅威や課題に応じた重点項目を組み合わせた相互チェック制度の導入が有効であると考察した。基本項目には厚労省チェックリストや本研究班によるセキュリティ監査項目を活用し、重点項目は専門 WG が設定して 2 年間で改善状況を確認する運用が望ましいと考えた。また、訪問ペアを毎年変更し、Group A～C 人材を含めた多層的な参加体制とすることで、人材育成や知見共有にも寄与すると考えられた。さらに、制度運営には取りまとめ医療機関と専任事務局の設置が不可欠であり、継続的な予算措置や人的支援が必要であると考えられた。

A．研究目的

医療機関におけるサイバーセキュリティ対策は、厚生労働省が中心となる「医療情報システムの安全管理に関するガイドライン」改定や「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」策定、「医療機関におけるサイバーセキュリティ確保事業」等により対策が進められている。サイバーセキュリティ対策を進めるためには医療機関による投資が必要となる。各医療機関で費用対効果を見極めながら投資を行うことになるが、どこまで対策を進めることが望ましいかの判断は簡単ではない。また、サイバーセキュリティ対策には、医療機関のサイバーセキュリティ人材だけでなく、病院執行部の意向や医療情報システムベンダーやネットワーク事業者との調整が関わるため、他医療機関がどの程度の対策を進めているか、他医療機関の良い取り組み事例の把握などが非常に参考になると考えられる。

本研究では、サイバーセキュリティ対策の相互チェックの手順書の作成を目的としている。

B．研究方法

医療安全領域では、国立大学病院間では「医療安全・質向上のための相互チェック」、特定機能病院間では「特定機能病院間相互のピアレビュー」が実施されている。これらの相互チェックは、各施設の医療安全対策の向上だけでなく、全ての施設の医療安全対策レベルの均てん化に貢献している。

そこでサイバーセキュリティ対策においても、先行する医療安全対策の取り組みを倣った相互チェック手順を構築するため、国立大学病院の相互チェックの取りまとめを行っている大阪大学医学部附属病院中央クオリティマネジメント部からヒアリング調査を実施した。

倫理的配慮

本研究はヒアリング調査であり、人を対象とする研究は含まれず、倫理的配慮は該当しない。

Ｃ．研究結果

１．「医療安全・質向上のための相互チェック」

１―１．歴史と概要

平成11年に横浜市立大学病院で患者取り違え事故等が起こり、国立大学附属病院で「医療事故防止のための安全管理体制の確立に向けて（提言）」を作成し、この提言を実施できているかを全国統一チェック項目で相互チェック（500項目）することになった。

平成19年から、国立大学病院長会議の常置委員会診療担当（医療安全管理）校である大阪大学が実施するようになり、以下のような変革が行われた。

- 「自己チェックシート（従来の500項目）」と「重点項目（最新の知見から、取り組むべき事項）」の2本立てとする
- 重点項目について詳しい専門家を全国から集めた「相互チェックWG」を設置して、重点項目に関するチェック項目を作成
- 平成24年度からは重点項目について相互訪問にて確認・意見交換する年と、その際に指摘された事項を含めて改善に取り組んだことを報告する年との2年1セットに（相互訪問は2年に1回へ）
- 令和元年頃に自己チェックシートは不要と判断し終了。重点項目のみのチェックへ。

１－２．重点項目に関する相互チェック

基本的には（国内外の）ガイドラインや提言、なすべきこととされることがある程度明確な事柄を重点項目のテーマとし、その導入を促進することを目的としている

≪これまで取り扱ってきたテーマ≫

- 手術安全チェックリストの導入
- 鎮静下処置の安全
- 入院時支援
- 画像レポート確認
- 働き方改革と医療の質・安全の担保

≪スケジュール≫

4月：

- 重点項目のテーマを決定（担当校医療安全部門が中心となって議論）
- 重点項目によりWGメンバー決定

5～6月：

- WGを対面またはオンラインで開催し、質問項目を作成
- 事務局（担当校医事課）で、確定した項目をエクセルシート化
- 訪問ペアの作成

※訪問大学と被訪問大学が異なるように、かつ直近10年以内は同じ相手にならないように、（担当校医事課）がペア表を作っている

※病院長や副病院長の日程を合わせる必要があると、日程調整に苦慮する。

※厚生労働省は、地区レベルでの訪問案や、国公立だけでなく私立大学も含めて相互訪問する案を提案（国公立だけでなく、多様な背景を有する私立大学病院まで含めると、事務局負担が過剰になることと、文化も違うことから、医療安全では国公グループと私立グループに分けている）。

7月末：

- 全国の国公立大学病院医療安全担当窓口へ送付

⇒訪問大学と被訪問大学は秋に訪問できるよう日程調整

※訪問側は医療安全担当副病院長、医療安全部門、重点項目に応じたメンバー

9～12月初旬まで：

- 相互訪問
- 訪問校は、評価結果を事務局（担当校医事課）に提出

12月末：

- 事務局（担当校医事課）が全51大学病院のシートを単純集計したシートを作成
- 担当校医療安全部門に集計結果を共有

～翌年度4月：

- 担当校医療安全部門が中心となりつつWGメンバーで報告書作成

翌年度5月頃：

- 改善状況調査の項目を作成
- （担当校医療安全部門が中心に作成し、WGはオンライン開催とすることが多い）

翌年6月：

- 国立大学病院長会議総会で報告、報告書配布

翌年7月末：

- 改善状況調査シートを全国へ送付

２．「特定機能病院間相互のピアレビュー」

群馬大学病院の腹腔鏡で死亡症例が相次いだ事案を受けて厚労省が医療法を改正し、「特定機能病院間相互のピアレビュー」を「毎年」行うことが義務化された。

- 医療法で医療安全体制（全死亡症例の把握、質モニタリング、重大事象への対応など）、医薬品安全管理、未承認新規医薬品、高難度新規医療技術、外部監査の5領域を中心に相互訪問で確認を行う規程がある。
- 調査項目は前回の調査項目を引き継ぎながら

少しずつ深掘りしている、という状況である。
- 訪問のペアは、医療安全・質向上のための相互チェックと同じペアで、訪問時に同時に調査を行う。
- 相互チェックWGでは相互チェック用と、ピアレビュー用と、2種類の質問項目と報告書を作成することとなり、相互訪問も隔年から毎年へと変更になった。
- 「相互チェック＋ピアレビュー」項目を実地調査する年と「ピアレビュー」項目を主に実地調査する年（相互チェックは書面調査）の交互
- ピアレビューが開始となり厚生労働省から予算が事務局につくようにはなったが年々減少傾向となっている。
- 年間を通じた業務負担は非常に大きい。

D．考察

1．医療機関におけるサイバーセキュリティ対策の相互チェック

毎年チェックを行う基本項目と、サイバーセキュリティインシデントの発生状況や新たなサイバーセキュリティ対策などを反映した重点項目を定め、相互チェックを行うことが好ましいと考える。

基本項目は、厚生労働省が定める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を網羅した上で、本研究班で定める「セキュリティ監査項目一覧」からリストを作る必要がある。基本項目の相互チェックを毎年行うことで集中管理機関間のサイバーセキュリティ対策状況の比較だけでなく、経年的なサイバーセキュリティ対策の向上を定量化することができる。

重点項目は、集中管理機関のGroup A人材からWGメンバーを選定し、WGで適切なテーマを決める必要がある。重点項目は医療安全と同様に2年で1つのテーマを取り扱い、1年目の相互チェックを受けた改善状況を2年目で確認することで、確実なサイバーセキュリティ対策の向上につながると考えられる。

2．医療機関におけるサイバーセキュリティ対策の相互チェックの訪問ペアと訪問者、応対者の構成

訪問ペアは訪問機関と被訪問機関を異なるように設定することで、2つの医療機関とディスカッションができることになる。また、毎年、訪問ペアを変更することで、様々な医療機関のサイバーセキュリティ対策を学ぶことができる。

訪問者は集中管理機関のGroup A人材を含んだメンバー構成とすることを想定する。応対者は情報セキュリティ責任者（CISO）と医療情報システム安全管理責任者、医療情報システム安全管理責任者と異なればGroup A人材を想定する。今後の人材育成を考えると、それぞれの施設はGroup B人材、Group C人材も訪問者、応対者に含める検討をするべきである。

3．医療機関におけるサイバーセキュリティ対策の相互チェックの取りまとめ医療機関

上記を実現するためには、取りまとめ医療機関を設置することが必須と考える。

取りまとめ医療機関の医療情報システム担当部門が中心となり、相互チェックの企画運営を行っていく必要がある。医療安全の相互チェックでは1年を通じ継続的に業務が発生しており、サイバーセキュリティ対策の相互チェックにおいても専任の教官ポストの検討などが必要と思われる。

その作業負担を考えると事務局は必須と考えられ、医療情報システム部門との連携を考えると、取りまとめ医療機関内に置くことが好ましい。

以上のように取りまとめ医療機関にはしかるべき予算配分が必要と考える。

取りまとめ医療機関以外においても、重点項目の決定やチェック項目の選定を行うWGメンバーを輩出することや、相互チェックでペア医療機関を訪問する必要があるため、取りまとめ医療機関以外においても相応の予算配分が必要と考える。

E．結論

本研究では、医療安全分野で成熟している「相互チェック」および「ピアレビュー」の仕組みを参考に、医療機関におけるサイバーセキュリティ対策の相互チェック制度構築の方向性を示した。サイバーセキュリティ対策は、各医療機関単独で進めるだけでは限界があり、他施設との比較や優良事例の共有を通じて対策レベルを向上・均てん化することが重要である。基本項目と重点項目を組み合わせた継続的な相互チェックにより、経年的な改善状況を可視化し、実効性の高い対策推進が可能になると考えられる。また、WGによる重点項目設定、人材育成を意識した訪問体制、取りまとめ医療機関と事務局の整備が制度運営の鍵となる。今後は、本調査結果を踏まえ、サイバーセキュリティ対策相互チェックの具体的手順を策定していく予定である。

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

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

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）
分担研究報告書

IT-BCP手順書作成と地域合同訓練計画に関する研究

研究分担者　楠田 佳緒　京都大学医学部附属病院
研究分担者　油谷 曉　京都大学医学部附属病院
研究分担者　橋本 智広　大津赤十字病院

研究要旨
本研究では、指導的立場のセキュリティ人材（Group A 人材）を有する集中管理機関と、医工系人材を中心とする Group C 人材を有する被指導機関とが共同してサイバー攻撃に対応するための共同 IT-BCP 手順書の確立と、これに基づく合同 IT-BCP 訓練の実効性検証を目的としている。2025 年度は、既存の IT-BCP や国内医療機関におけるサイバー攻撃被害報告書を調査し、被害時に病院がとるべき行動および Group C 人材が単独では対応困難となる項目を抽出した。抽出された項目は「人材（作業）」「物品」「情報」の 3 区分に分類し、集中管理機関への支援要請事項として共同 IT-BCP 手順書のプロトタイプに組み込んだ。併せて、次年度に実施する合同 IT-BCP 訓練に向け、滋賀県内の 2 医療機関との調整を開始し、地域医療連携を活かした訓練実施体制の素案を策定した。本年度の成果により、被指導機関が攻撃を受けた際の対応行動と集中管理機関への支援要請の枠組みが具体化され、次年度の合同訓練による実効性検証に向けた準備が整いつつある。

Ａ．研究目的

本研究では、Group C人材を有する被指導機関がランサムウェア等のサイバー攻撃を受けたことを想定したIT-BCP対応訓練を計画する。本訓練を、被指導機関（Group C病院）と集中管理機関（Group A病院）が共同して実施することで、集中管理機関と被指導機関の役割を明確にした共同IT-BCP手順書を確立するとともに、Group C人材の実践的教育としての合同IT-BCP訓練の実効性について検証する。

2025年度の目的として、共同IT-BCP手順書の作成と、合同訓練の実施計画の策定を行うこととした。

Ｂ．研究方法

B-1　共同IT-BCP手順書の作成

地域の医療機関が協力してIT-BCPを実施するための手順書を作成する。具体的には、医療機関の既存のIT-BCPおよび電子カルテシステム停止時マニュアル、ならびに過去のサイバー攻撃被害報告書を調査する。さらに、調査結果をもとに、集中管理機関（Group A病院）と被指導機関（Group C病院）が共同で運用することを想定した共同IT-BCP手順書のプロトタイプを作成する。

B-2　合同訓練の実施計画

Group C病院がサイバー攻撃を受けたことを想定して、地域の複数の医療機関による合同訓練を計画する。具体的には、合同訓練への協力機関との調整、および合同訓練シナリオ案を検討する。

B-3　倫理的配慮

本研究では、文献調査・資料作成を実施するため、人を対象とする研究は含まれず、倫理的配慮は該当しない。

Ｃ．研究結果

C-1　共同IT-BCP手順書の作成

既に公開されている各医療機関および厚生労働省のIT-BCP（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版に基づくBCPひな形等）、ならびに各医療機関で整備されている電子カルテシステム停止時マニュアルを調査した。現在の医療機関では、電子カルテや部門システムに異常が生じた場合、まず「電子カルテシステム停止時マニュアル」の手順が実施される。その後、ネットワーク障害やサイバー攻撃が疑われる事象が確認された場合に「IT-BCP」の手順が実施される運用となっている。本研究では、後者の「IT-BCP」に着目した。

さらに、大阪急性期・総合医療センター等、近年に公表されたサイバー攻撃被害報告書を調査し、サイバー攻撃被災時に病院がとるべき行動を抽出した。次に、これらの行動をとる際にGroup C人材のみでは判断・実施が困難となり混乱が生じうる項目、または、Group A人材へ支援を要請すべき項目を洗い出した。

以上の調査から、Group C人材がGroup A人材へ支援を要請すべき項目について、「人材（作業）」「物品」「情報」の3項目に分類し、それぞれの具

体例を共同IT-BCP手順書のプロトタイプに組み込んだ。「人材（作業）」には、被害調査の技術的支援や、紙運用における人材提供等が含まれ、「物品」には、FAXやクリーンPC等の貸与、「情報」には、フォレンジック調査・初動対応の判断支援等が含まれる。

C-2　合同訓練の実施計画

来年度に実施する合同訓練に向けて、滋賀県内の2医療機関との調整を開始した（担当：橋本、油谷、楠田）。さらに、大津赤十字病院に加え、2医療機関（大津市民病院、琵琶湖中央リハビリテーション病院）に対して、ネットワークに接続されている医療機器を検出するシステムを導入した。本システムの導入により、サイバー攻撃の被災時に攻撃対象となりうるネットワーク医療機器の一覧が作成できた。これにより、地域におけるセキュリティ共通基盤のモデルが構築できた。

また、合同訓練シナリオの作成では、システム停止の通報から始まり、サイバー攻撃の発覚、対応、収束の一連の流れを机上で体験するシナリオ案を作成した。今後、シナリオのブラッシュアップにあたっては、Group C人材が現場で直面する判断項目を含め、集中管理機関からの支援を要請する場面を盛り込むなどして精査する。

D．考察

本年度の調査により、サイバー攻撃被災時に医療機関がとるべき行動の多くが、現場のIT人材だけで完結できない性質であることが明らかとなった。特に、フォレンジック調査の初動判断、代替機器の確保、攻撃手口に関する最新情報の収集といった事項は、平時から関連知識や人的ネットワークを蓄積している集中管理機関の関与なしには適時に実施することが困難であり、被指導機関の現場では混乱が生じやすい領域である。

Group C人材から集中管理機関への支援要請項目を「人材」「物品」「情報」の3区分に整理したことは、被災時に何を、誰に、どのような形で要請すべきかを構造的に示す枠組みを与えるものであり、共同IT-BCP手順書を実用的なもの近づけることができると考えられる。

一方で、共同IT-BCP手順書を実際に運用するためには、平時からの両機関での関係構築、支援要請の経路と判断権限の明確化、ならびに支援提供側である集中管理機関の受け入れ準備の検討が求められる。次年度に予定する合同IT-BCP訓練では、本手順書プロトタイプを訓練シナリオに適用し、Group C人材の判断行動と集中管理機関の応答行動を具体的に観察・評価する予定である。

E．結論

2025年度は、既存のIT-BCPおよびサイバー攻撃被害報告書を調査した。調査結果から、被指導機関(Group C病院)が集中管理機関(Group A病院)に対して支援を要請すべき項目を「人材」「物品」「情報」の3区分で整理し、これらを反映した共同IT-BCP手順書のプロトタイプを作成した。併せて、滋賀県内の2医療機関と合同IT-BCP訓練に向けた調整を開始し、次年度の訓練実施体制の素案を策定した。次年度に実施する合同訓練を通じて、共同IT-BCP手順書の実効性およびGroup C人材に対する実践的教育へと研究を進める。

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

医療情報システム部門
事業継続計画（BCP）

（Group C 人材向け）

〇〇年〇〇月〇〇日　初版

〇〇病院

〇〇部門

目次

第 1 章 総則

1.1　策定目的

本事業継続計画（以下、本 BCP という）は、〇〇病院（以下、当院という）においてサイバーインシデント発生時における組織的対応の基本方針及び職員の取るべき行動の基本原則を示すことによって、医療安全、情報保全を担保しつつサイバー攻撃に対応するセキュリティ体制の構築、ならびに早期復旧までを視野に入れた活動の実現により、国民に信頼される医療機関として社会福祉に貢献することを目的とする。

1.2　基本方針

当院は、個人情報の保護と医療サービスの継続性を確保するために、以下の方針に基づき、サイバーセキュリティ対策の水準を高めていく。

I.　安全かつ持続的な医療サービス提供を実現する
II.　サイバーセキュリティに対する脅威からの被害から事業を保護する
III.　リスクマネジメントの対象としてサイバーセキュリティを確保する
IV.　平時、非常時を通じて事業継続に関する説明責任を果たす
V.　被害後、医療安全を担保しつつ、迅速かつ合理的な医療業務復旧を行う

1.3　対象範囲

1.3.1 対象とする医療情報システム

対象とする医療情報システムは以下の通り。

I.　電子カルテシステム
II.　医事会計システム（レセプト）
III.　医用画像システム
IV.　各種部門システム（検査、処方など）
V.　オーダリングシステム
VI.　〇〇〇〇

1.3.2 想定する事象

本 BCP で想定される事象において、診療業務に影響するものを以下に挙げる。なお、自然災害、大規模停電等による電源喪失などの計画は別に定めるものとする。

I. 診療情報・参照情報・指示情報の確認・参照不能
II. 診療情報・参照情報・指示情報の入力不能
III. スタッフ間の連絡不能
IV. 情報機器・医療機器の操作不能・誤動作
V. ○○○○○○

また、これらの被害を引き起こすサイバー攻撃の例として以下が挙げられる。

I. 不正アクセス等
II. 標的型メール攻撃
III. マルウェア感染（ランサムウェアを含む）
IV. 分散型サービス妨害（DDoS 攻撃）
V. ○○○○○○
VI. 上記の予兆と思われる現象

1.4 文書の管理および周知

本 BCP は○○部門にて、現状を適切に反映した原本および関連資料の整備ならびに管理を行い、経営層の承認を受けた上で、当院の全職員に開示周知する。

第 2 章 体制整備

2.1 情報機器等の把握と適切な管理

平時において、非常時に備えたサイバーセキュリティの体制整備を以下のとおり行う。

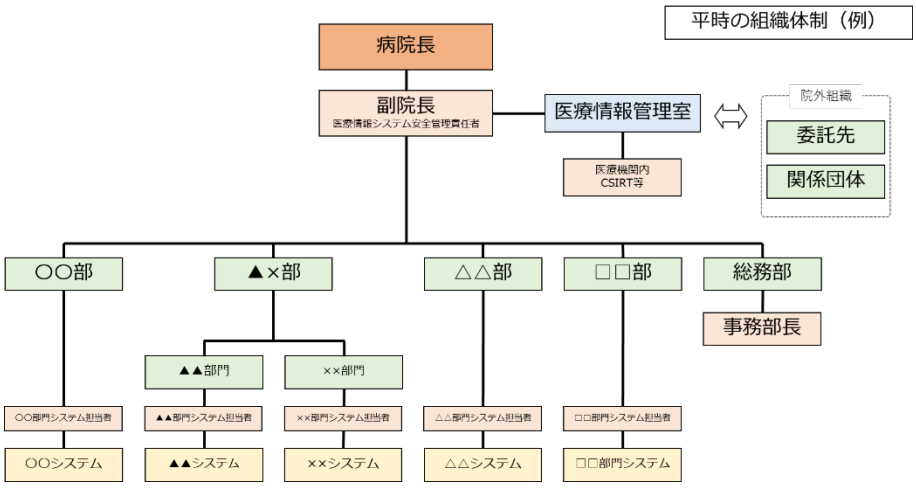
2.1.1 医療情報システム安全管理責任者

〇〇を、医療情報システム安全管理責任者として定める。△△（理事長、病院長）を当院におけるサイバーセキュリティに関する最高責任者とする。

（医療機関の規模・組織等によっては上記が兼務することも想定される。）

2.1.2 組織体制図

診療継続及び医療情報システムの復旧を目的としたサイバーセキュリティの組織体制を以下のとおり定める。担当部署、担当者、役割についても示す。



図〇：平時の組織体制図（例）

表〇：担当者の役割（例）

役割	担当部署・担当者	役割の概要
医療情報システム最高責任者	病院長	診療継続及び医療情報システムの復旧の計画策定を統括し、最終的な責任を負う。
医療情報システム安全管理責任者	〇〇	医療情報システム復旧の計画策定に関する各種検討作業を行う。
病院事務部	〇〇	診療継続の計画策定に関する各種検討作業を行う。
診療部門システム担当者	〇〇課	各診療部門システムの運用継続計画策定に関する各種検討作業を行う。
委託先	〇〇社	医療情報システムの運用保守及び緊急時の状況に関する情報提供・対策調整

2.1.3 情報機器台帳

医療情報システム安全管理責任者は、情報機器の現況を反映した管理台帳を以下（または別紙資料）のとおり整備する。併せて、定期的に棚卸しを行い、機器の所在と稼働状況の確認を行う。

表◯：情報機器台帳（例）

管理番号	メーカー	OS	ソフトウェア	ソフトウェアバージョン	IPアドレス	コンピュータ名	設置場所	利用者	登録日	状態	説明
001	A社	Win11	○○電子カルテ	2.0	192.168.○.○	Room1のPC１	Room1	a医師（○○科）	2020/12/1	稼働	
002	A社	Win11	○○電子カルテ	1.2	192.168.○.○	Room1のPC2	Room1	b医師（○○科）	2020/12/1	停止	メンテナンス
003	A社	Win8	○○電子カルテ	2.0	192.168.○.○	Room2のPC１	Room2	c医師（△△科）	2014/10/1	稼働	
004	B社	Win11	○○管理システム	5.0.1	192.168.○.○	Room3のPC１	Room3	a医師（○○科）、b医師（○○科）、c医師（△△科）	2021/8/1	稼働	

（出典：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マニュアル ～医療機関・事業者向け～ ）

2.1.4 ネットワーク・システム構成図

医療情報システム安全管理責任者は、医療機関等で導入している医療情報システムの全体構成図（ネットワーク図、システム構成図等）を整備する（ネットワークの全体像が分かりやすいものを作成）。併せて、構成、接続等に変更が生じた場合には構成図の更新を行い、常に最新の状態を保つ。

2.1.5 リスク評価・代替運用

各システムが利用できなくなった場合、その業務内容の代替手段を以下のとおり定める。また、代替運用方法については別途、システム停止時の代替運用マニュアル等にて定める。

表◯：業務内容に対する代替手段（例）

業務内容	システム	代替手段
診療録等	電子カルテシステム	紙運用
処方・検査	オーダリングシステム	紙運用（カーボンコピー）
放射線画像診断	PACS	撮影機器ワークステーションにて画像閲覧
会計	医事会計システム	未収扱いを検討
○○○○○○	○○○○○○	○○○○○○

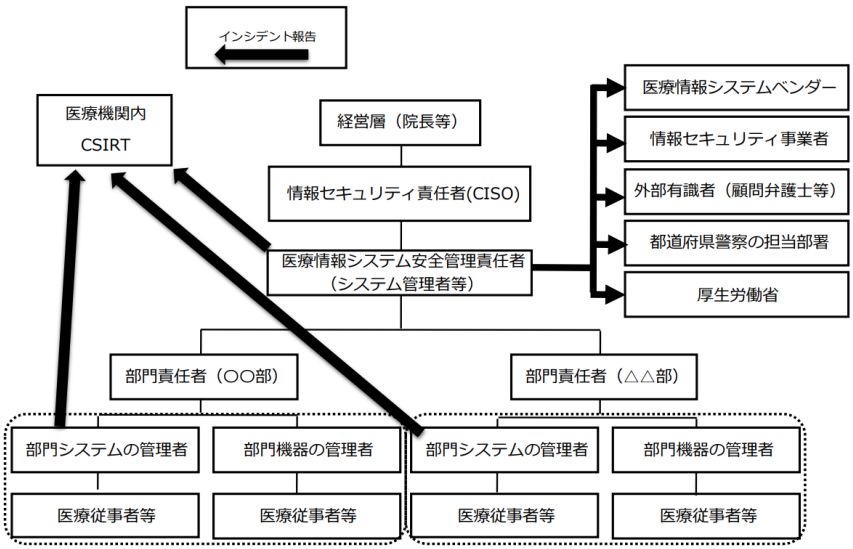
2.1.6 脆弱性に関する対策

医療情報システム安全管理責任者は、契約等で定められた責任分界をもとにサーバ、端末 PC、ネットワーク機器について脆弱性情報の収集を行う。脆弱性が発見された機器について、脆弱性対応プログラムの適応を行う。万が一、適応できない場合の代替手段（隔離運用、隔壁の追加、監視の強化、機器入れ替え等）について事業者等と合意した上で取り決め、実施する。

2.2　非常時に備えたサイバーセキュリティ体制

2.2.1 連絡体制図

診療継続及び医療情報システムの復旧に資するアクションを迅速に行う目的で、サイバーセキュリティの連絡体制（連絡先、担当、メールアドレス、電話番号、連絡目的等）及び外部関係機関の連絡先を以下のとおり定める。



（出典：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マニュアル ～医療機関・事業者向け～）

図〇：連絡体制図（例）

表〇：外部関係機関の連絡先一覧（例）

外部関係機関	連絡先
厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室	03-6812-7837 igishitsu@mhlw.go.jp
〇〇（都道府県警察の担当部署）	××-××××-××××
〇〇	××-××××-××××
〇〇	××-××××-××××

2.2.2 情報収集体制

当院における各システムの脆弱性情報について事業者等から情報提供を定期的に受け取ることができる体制を以下のとおり構築する。

表◯：事業者等の連絡先（例）

システム	担当	連絡先
電子カルテ	◯◯社	××-××××-×××× ◯◯@◯◯
保守委託先	◯◯社	××-××××-×××× ◯◯@◯◯
放射線撮影機器	◯◯社	××-××××-×××× ◯◯@◯◯
検査機器	◯◯社	××-××××-×××× ◯◯@◯◯
◯◯	◯◯社	××-××××-×××× ◯◯@◯◯

2.2.3 教育体制

本 BCP が迅速かつ適切に利用できるよう、年◯回以上の教育、訓練を実施する。情報セキュリティ責任者（CISO）、医療情報システム安全管理責任者は年間の教育計画に沿った訓練が適切に実施されるように監督する。訓練結果により、事前対策やサイバーインシデント発生時の対応計画等に解決すべき課題が発生した場合、課題の解決もしくは改善に向けた計画の立案をする。

2.2.4 バックアップ体制

サイバーインシデント発生時に備えた、データとシステムのバックアップの頻度、作成方法及び復旧方法について以下のとおり定める。

表◯：バックアップの作成と復旧方法（例）

システム	頻度	作成方法	復旧方法
電子カルテ	1 日	バックアップサーバにデータベースのバックアップを作成する	データベースを再構築した後に、バックアップサーバのデータを復元する
	7 日	磁気テープ・光学メディア・外付け HDD 等にデータベースとシステムファイルのバックアップを作成する	システムの OS を再構築した後に、磁気テープのシステムファイルとデータベースのデータを復元する
◯◯	◯◯	◯◯	◯◯
◯◯	◯◯	◯◯	◯◯

2.2.5 非常時の診療運用のための必要資料の準備

非常時には、電子カルテや部門システムをはじめ、電子機器端末やネットワークが使用できなくなる。したがって、本 BCP に加えて、システムトラブル時や自然災害時を想定した事業継続計画（システムダウン時マニュアル等）を作成し、診療行為を継続するための手順を定めることが求められる。

また、ランサムウェアなどのマルウェア感染が疑われる場合、感染拡大防止のために部分的なネットワーク遮断が求められる。ネットワーク構成図（物理・論理）を整備し、事前にネットワークの全体像を把握しておくことで、問題点の把握が迅速に行える。さらに、各ネットワークの接続先にある医療機器の一覧を整備することで、ネットワーク遮断時の影響の大きさを検討することができる。

事前準備

・システムダウン時マニュアル
・用紙：診療記録、注射指示簿、与薬指示薄、予約リスト、紹介状、処方箋、看護記録等
・物品：FAX の準備、通常ネットワーク以外の通信手段等
・ネットワーク構成図（物理・論理）
・医療機器リスト

第３章 サイバーインシデント発生時の対応

3.1　異常発見時の連絡先

異常発見時の連絡経路は 2.2.1 の表◯に示す通りとする。あわせて、各担当部門の連絡先は以下のとおり示す。なお、部門システムの管理者は連絡先が全職員に把握されるように明示して、常に最新版で管理し連絡経路が機能することを担保する。規模や期間に応じて、地域の支援病院へ助けを求める可能性も起こりうることから、被害を受けた病院に対して支援や指導が可能な支援病院との連携も事前に確認する。

表◯：部門連絡先一覧（例）

部署名	担当者	連絡先
○○部門	○○	××-××××-××××
システム管理室	○○	××-××××-××××
医療情報システム安全管理責任者	○○	××-××××-××××

システム	事業者	担当者	連絡先
電子カルテシステム	○○	○○	××-××××-××××
○○○システム	○○	○○	××-××××-××××
○○○システム	○○	○○	××-××××-××××
○○○システム	○○	○○	××-××××-××××

支援医療機関名	部署名	担当者	連絡先
○○○病院	○○	○○	××-××××-××××
○○○病院	○○	○○	××-××××-××××

3.2　システム異常の検知と経営層への情報伝達

システム異常を検知した場合、あらかじめ定めた項目（発生場所、発生箇所、発生日時、連絡者、異常の内容・範囲）について担当部門に報告できるように周知する。なお、口頭による連絡後、「報告様式」を用いて記録を残す。また、院内職員から発出された異常において、医療情報システム安全管理責任者によりサイバー攻撃の可能性が思慮された場合、2.2.1 で作成した連絡体制図を基に、速やかに経営層ならびに関係各所・外部関係機関に共有され、意思決定できるように努める。

3.3　初動対応

サイバーインシデント発生後は、以下のとおり対応する

3.3.1 原因調査

医療情報システム安全管理責任者はサイバーインシデントの原因や被害範囲の特定のために、医療情報システム・サービス事業者へ以下の調査依頼を指示または実施する。

I.　ネットワーク機器やケーブル等の調査
II.　電源系統、ブレーカー、ハードウェア、ソフトウェア等の調査
III.　情報漏えいの有無に関する調査
IV.　メンテナンスやデータ移行等の作業に関する調査
V.　○○○○○○

3.3.2 被害拡大防止

被害拡大防止のための対応を行う。まずは、バックアップに通ずるネットワークの遮断を行う。次に、外部の通信経路を遮断する。その上で、被害箇所から攻撃範囲および侵入経路の推定を行った上で、セグメンテーション境界において、通信を遮断して感染拡大防止を図る。

3.3.3 経営層への報告

医療情報システム安全管理責任者はサイバーインシデントについて経営層に対して、現在の被害状況を報告するとともにインシデント対応方法と患者安全を担保する運用方針案を提案する。この内容を踏まえて、経営層はシステム停止に伴う診療継続方針（診療体制の確保等）を検討し意思決定する。決定した内容は、速やかに 2.2.1 の連絡体制図で定める組織内ならびに外部関係機関へ周知を行う。

3.3.4 支援病院への協力要請

支援病院から協力を得る方法として、以下が挙げられる。なお、実際に支援病院が提供可能かどうかは事前に確認しておく必要がある。

（1）知識の提供

- 「今すぐ何をすべきか、絶対にしてはいけないことは何か」の助言
- 自分たちが行ったネットワーク遮断などの対応で十分か、被害拡大を防げているかの確認。
- 厚生労働省おたすけ隊、警察や行政（厚生労働省、文部科学省など）への通報
- ○○○○○○

（2）人材（作業）の提供

✧　各病棟や各診療科で発生している問題点を調査しまとめる作業
✧　システムの各ベンダーとの情報共有の支援
✧　〇〇〇〇〇

（3）物品の提供
✧　状況把握のためのホワイトボード
✧　〇〇〇〇〇〇〇

3.4　診療継続

サイバーインシデント対応と診療継続について報告を受けた経営層は以下のとおり対応する。

3.4.1 医療情報システムの縮退運転判断

経営層は医療情報システム安全管理責任者からの提案を受け、医療情報システム等の縮退運転または運転中止を判断する。また、インシデント対応中の診療継続においては、紙カルテの運用等、自然災害時を想定した事業継続計画（もしくはシステムダウン時マニュアル等）に則り運用する。

支援病院から協力を得る方法として、以下が挙げられる。なお、実際に支援病院が提供可能かどうかは事前に確認しておく必要がある。

（1）知識の提供
✧　停止時に実施するべき具体的手順の提供。
✧　〇〇〇〇

（2）人材（作業）の提供
✧　薬剤監査の人員、検査の目視確認の人員、紙伝票を伝送する人員
✧　〇〇〇〇

（3）物品の提供
✧　ネットワーク遮断に伴う物品の貸出・提供：
- 診療録：LAN 経由でないプリンターやコピー機、インク、用紙、診療録テンプレート、バインダーなど
- オーダー：紙伝票
- 検査：　デジカメ、CD-ROM、CD-ROM リーダー（USB メモリは感染拡大につながるため好ましくない）

- ○○○○：○○○○
- ✧ 電話機や FAX
- ✧ ○○○○

3.4.2 被害状況等調査（フォレンジック調査＋証拠保全）

医療情報システム安全管理責任者は、証拠保全の作業と診療継続に関する作業を調整しながら両立させる。具体的には、アクセスログの分析や情報の改ざん、暗号化の有無等からサイバー攻撃の範囲、個人情報漏えいの有無等の調査について医療安全を担保しつつ行う。必要に応じて医療情報システム・サービス事業者等へ協力依頼して調査を進める。なお、調査状況は随時経営層に報告する。

支援病院から協力を得る方法として、以下が挙げられる。なお、実際に支援病院が提供可能かどうかは事前に確認しておく必要がある。

（1）知識の提供

- ✧ 警察や厚生労働省チームが対応可能な遠隔サポート環境を提供するための手順
- ✧ 警察や後の調査のために、どのデータをどのように保存しておくべきかの具体的な手順
- ✧ ○○○○

（2）人材（作業）の提供

- ✧ 警察や厚生労働省チームと、セキュリティや病院の状況について、通訳できる人材
- ✧ ベンダーとの情報共有を支援
- ✧ ○○○○

（3）物品の提供

- ✧ 汚染されていない PC
- ✧ 独立した通信機器：モバイル Wi-Fi ルーター・予備のスマートフォンなど
- ✧ ○○○○

3.4.3 組織対応方針の確認と外部関係機関への報告

医療情報システム安全管理責任者の被害状況および調査結果に基づき、経営層は復旧対応方針（復旧に向けた対応、広報への対応）を決定し、その対応を関係者に指示する。

また、2.2.1 で定める外部関係機関へ報告を行う。外部関係機関へは被害拡大防止等の観点からできる限り早く連絡する。

支援病院から協力を得る方法として、以下が挙げられる。なお、実際に支援病院が提供可能かどうかは事前に確認しておく必要がある。

（1）知識の提供

✧　ホームページや行政へ技術面での報告書作成時における支援

✧　○○○○

（2）人材（作業）の提供

✧　緊急用グループメールの作成、メールアドレスの貸し出し

✧　支援病院の HP へ臨時に情報提供（患者へ情報提供する手段）

✧　○○○○

（3）物品の提供

✧　○○○○

3.5　復旧処理

復旧計画に基づいて、以下のとおり対応する。医療情報システム安全管理責任者は医療情報システムの事業者及びサービス事業者等と協力して復旧を行う。

3.5.1 復旧指示と復旧作業

医療情報システム安全管理責任者は、経営層からの復旧指示を起点とする復旧対応方針に基づき、システムの復旧作業(システムの再設定、再インストール、バックアップデータからの復元等)並びに検証作業を行う。必要に応じ医療情報システム・サービス事業者に対応を依頼する。あわせて、システム停止中に生じたアナログ情報についてシステムに反映させる選択肢を提示する。経営層は、アナログ情報の反映時期ならびに程度を医療安全の観点を踏まえて意思決定する。

支援病院から協力を得る方法として、以下が挙げられる。なお、実際に支援病院が提供可能かどうかは事前に確認しておく必要がある。

（1）知識の提供

✧　ホームページや行政へ技術面での報告書作成時における支援

✧　セキュリティ強化計画の提案
✧　○○○○

（2）人材（作業）の提供
✧　○○○○

（3）物品の提供
✧　○○○○

3.5.2 結果の確認

医療情報システム安全管理責任者は、復旧作業により復旧したシステムが安全な状態で正常に稼働したことを確認する。正常に稼働することが確認できた時点で、経営層に報告する。経営層は診療状況を総合的に勘案し、緊急時運用から通常運用への復旧を宣言する。

第 4 章 事後対応

4.1　報告

復旧後、復旧結果と情報漏えい事実の有無等について、経営層及び組織内に報告する。不足していたと考えられる事前対策、連絡先ならびに連絡内容について振り返りを行う。

4.2　再発防止

4.2.1 再発防止策検討・策定

4.1 の後、サイバー攻撃により発生した被害を抑止する手段について検討を行い、実施可能な選択肢を整備し、経営層に提案する。経営層は長期的視点と事業継続性の両立について検討し、安全性を維持するため再発防止策の選択を決定する。経営層は決定した再発防止策について、連絡経路を用いて全職員に周知する。

4.2.2 事業者への指示

経営層によって決定された再発防止策は、医療情報システム安全管理責任者等により、事業者が有するサービスや機器に対して対策を講じる必要があるかどうかを調査し、再発防止策の効果が出るよう対策実施を事業者へ打診する。事業者は、対策実施の時期や方法について、医療機関側と誠実に議論し、計画を立てて実施する。

4.3　情報公開

経営層は、類似のサイバー攻撃による被害拡大に対する警鐘を鳴らす目的、また当院を受診する患者への診療に関連する注意を喚起する目的で、速やかに情報公開を行う。情報公開内容は、知覚日時、現象、被害範囲、想定される攻撃経路、1 次対応、患者対応、復旧状況、事後対策などを含める。報告については、サイバー被害が発生した可能性が高い段階から迅速に行い、情報の更新を含めて複数回行う中で情報の確度を高めていく。

4.4　貸出物品の返却

地域の連携医療機関から物品や人材等の支援を受けた場合に、それぞれが適切な施設へ返却できるよう管理することが求められる。

研究成果の刊行に関する一覧表

書籍

著者氏名	論文タイトル名	書籍全体の編集者名	書　籍　名	出版社名	出版地	出版年	ページ
該当なし							

雑誌

発表者氏名	論文タイトル名	発表誌名	巻号	ページ	出版年
該当なし					

別紙５

令和８年　５　月　　８　日

厚生労働大臣
~~（国立医薬品食品衛生研究所長）~~ 殿
~~（国立保健医療科学院長）~~

機関名　京都大学

所属研究機関長　職　名　医学研究科長

氏　名　波多野　悦郎

次の職員の令和７年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　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）

２．研究課題名　地域における共通基盤・集中管理体制によるサイバーセキュリティの実証のための研究

３．研究者名　（所属部署・職名）医学研究科・教授

（氏名・フリガナ）黒田　知宏・クロダ　トモヒロ

４．倫理審査の状況

	該当性の有無 有　無	左記で該当がある場合のみ記入（※1）		
		審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること （指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査の場合は、その理由を記載すること。
（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：　　）
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：　　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：　　）
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■（有の場合はその内容：　　）

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。

令和8年2月25日

厚生労働大臣　　殿

機関名　国立大学法人大阪大学

所属研究機関長　職　名　大学院医学系研究科長

氏　名　石井　優

次の職員の令和７年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　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）

２．研究課題名　地域における共通基盤・集中管理体制によるサイバーセキュリティの実証のための研究

３．研究者名　（所属部署・職名）　大学院医学系研究科・教授

（氏名・フリガナ）　武田　理宏・タケダ　トシヒロ

４．倫理審査の状況

	該当性の有無	左記で該当がある場合のみ記入（※1）		
	有　無	審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること（指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査に場合は、その理由を記載すること。

（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：　　）
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：　　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■無 □（無の場合はその理由：　　）
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■有の場合はその内容：　　）

（留意事項）　・該当する□にチェックを入れること。

・分担研究者の所属する機関の長も作成すること。

別紙５

2026 年 3 月 31 日

厚生労働大臣
（~~国立医薬品食品衛生研究所長~~） 殿
（~~国立保健医療科学院長~~）

機関名　北海道科学大学

所属研究機関長　職　名　学長

氏　名　川上　敬

次の職員の令和７年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　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）

２．研究課題名　地域における共通基盤・集中管理体制によるサイバーセキュリティの実証のための研究

３．研究者名　（所属部署・職名）　北海道科学大学・教授

（氏名・フリガナ）　谷川　琢海（タニカワ　タクミ）

４．倫理審査の状況

	該当性の有無 有　無	左記で該当がある場合のみ記入（※1）		
		審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること （指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査の場合は、その理由を記載すること。

（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■（有の場合はその内容：

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。

別紙５

「厚生労働科学研究費における倫理審査及び利益相反の管理の状況に関する報告について
（平成26年4月14日科発0414第5号）」の別紙に定める様式（参考）

2026年 5月 11日

厚生労働大臣
(~~国立医薬品食品衛生研究所長~~)　殿
(~~国立保健医療科学院長~~)

機関名　　大津赤十字病院

所属研究機関長　職　名　　院長

氏　名　小川　修

次の職員の(元号)　　年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　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）

２．研究課題名　地域における共通基盤・集中管理体制によるサイバーセキュリティの実証のための研究

３．研究者名　（所属部署・職名）　　事務部　医療情報課　課長

（氏名・フリガナ）　　橋本　智広　（ハシモト　トモヒロ）

４．倫理審査の状況

	該当性の有無 有　無	左記で該当がある場合のみ記入（※1）		
		審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること （指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査の場合は、その理由を記載すること。
（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■（有の場合はその内容：

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。

2026年04月01日

厚生労働大臣　殿

機関名 地方独立行政法人大阪府立病院機構
大阪国際がんセンター

所属研究機関長　職　名 総長

氏　名 松浦　成昭

次の職員の（令和）７年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　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)

２．研究課題名　地域における共通基盤・集中管理体制によるサイバーセキュリティの実証のための研究

３．研究者名　（所属部署・職名）放射線診断・IVR 科／副技師長

（氏名・フリガナ）川眞田 実・カワマタ ミノル

４．倫理審査の状況

	該当性の有無	左記で該当がある場合のみ記入（※1）		
	有　無	審査済み	審査した機関	未審査（※2）
人を対象とする生命科学･医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること（指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査に場合は、その理由を記載すること。
（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：　　）
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：　　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：　　）
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■（有の場合はその内容：　　）

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。

別紙５

「厚生労働科学研究費における倫理審査及び利益相反の管理の状況に関する報告について
（平成26年4月14日科発0414第5号）」の別紙に定める様式（参考）

令和 8 年 5 月 14 日

厚生労働大臣
（国立医薬品食品衛生研究所長） 殿
（国立保健医療科学院長）

機関名　東都大学

所属研究機関長　職　名　学長

氏　名　吉岡　俊正

次の職員の 令和７ 年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　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）

２．研究課題名　地域における共通基盤・集中管理体制によるｻｲﾊﾞｰｾｷｭﾘﾃｨｰの実証のための研究

３．研究者名　（所属部署・職名）　幕張ヒューマンケア学部 臨床工学科　講師

（氏名・フリガナ）　肥田泰幸・ヒダヤスユキ

４．倫理審査の状況

	該当性の有無 有	無	左記で該当がある場合のみ記入（※1） 審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□	☑	□		□
遺伝子治療等臨床研究に関する指針	□	☑	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□	☑	□		□
その他、該当する倫理指針があれば記入すること（指針の名称：　　）	□	☑	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査の場合は、その理由を記載すること。
（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ☑　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ☑　無 □（無の場合はその理由：
当研究機関におけるＣＯＩ委員会設置の有無	有 □　無 ☑（無の場合は委託先機関：東都大学倫理審査委員会
当研究に係るＣＯＩについての報告・審査の有無	有 ☑　無 □（無の場合はその理由：
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ☑（有の場合はその内容：

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。

令和８年３月６日

厚生労働大臣
~~（国立医薬品食品衛生研究所長）~~ 殿
~~（国立保健医療科学院長）~~

機関名　国立大学法人群馬大学

所属研究機関長　職　名　学長

氏　名　石崎　泰樹

次の職員の令和７年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　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）

２．研究課題名　地域における共通基盤・集中管理体制によるサイバーセキュリティの実証のための研究

３．研究者名　（所属部署・職名）　医学部附属病院・准教授

（氏名・フリガナ）　鳥飼　幸太・トリカイ　コウタ

４．倫理審査の状況

	該当性の有無	左記で該当がある場合のみ記入（※1）		
	有　無	審査済み	審査した機関	未審査（※2）
人を対象とする生命科学･医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること（指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査に場合は、その理由を記載すること。
（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：　　）
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：　　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：　　）
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■（有の場合はその内容：　　）

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。

別紙５

令和８年　５　月　　８　日

厚生労働大臣
~~（国立医薬品食品衛生研究所長）~~ 殿
~~（国立保健医療科学院長）~~

機関名　京都大学

所属研究機関長　職　名　医学研究科長

氏　名　波多野　悦郎

次の職員の令和７年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　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）

２．研究課題名　地域における共通基盤・集中管理体制によるサイバーセキュリティの実証のための研究

３．研究者名　（所属部署・職名）大学院医学研究科・講師

（氏名・フリガナ）油谷　曉・ユタニ　アキラ

４．倫理審査の状況

	該当性の有無 有　無	左記で該当がある場合のみ記入（※1）		
		審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること （指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査の場合は、その理由を記載すること。
（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：　　）
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：　　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：　　）
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■（有の場合はその内容：　　）

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。

別紙５

令和８年　５　月　　８　日

厚生労働大臣
~~（国立医薬品食品衛生研究所長）~~ 殿
~~（国立保健医療科学院長）~~

機関名　京都大学

所属研究機関長　職　名　医学研究科長

氏　名　波多野　悦郎

次の職員の令和７年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　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）

２．研究課題名　地域における共通基盤・集中管理体制によるサイバーセキュリティの実証のための研究

３．研究者名　（所属部署・職名）医学研究科・特定講師

（氏名・フリガナ）楠田　佳緒　・クスダ　カオリ

４．倫理審査の状況

	該当性の有無 有　無	左記で該当がある場合のみ記入（※1）		
		審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること （指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査の場合は、その理由を記載すること。
（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：　　）
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：　　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：　　）
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■（有の場合はその内容：　　）

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。

別紙５

令和８年　５月　２５日

厚生労働大臣
（国立医薬品食品衛生研究所長）　殿
（国立保健医療科学院長）

機関名　国立大学法人滋賀医科大学

所属研究機関長　職　名　学長

氏　名　遠山　育夫

次の職員の(元号)　　年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　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）

２．研究課題名　地域における共通基盤・集中管理体制によるサイバーセキュリティの実証のための研究

３．研究者名　（所属部署・職名）　医学部・教授

（氏名・フリガナ）　芦原　貴司（アシハラ　タカシ）

４．倫理審査の状況

	該当性の有無 有　無	左記で該当がある場合のみ記入（※1）		
		審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること （指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査の場合は、その理由を記載すること。

（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■（有の場合はその内容：

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。