別紙１

厚生労働科学研究費補助金研究報告書表紙

厚生労働科学研究費補助金

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)

クラウド上の医療AI利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言

令和 7 年度 総括研究報告書

研究代表者　岡村 浩司

令和 8 (2026) 年 5 月

別紙２

厚生労働科学研究費補助金研究報告書目次

目　　次

別紙 3

厚生労働科学研究費補助金
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)

総合研究報告書
クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言

研究代表者　岡村 浩司　国立成育医療研究センター 室長

研究要旨

医療 AI との協調は、医療従事者の働き方改革と医療の均霑化を実現するための中核的な手段として位置づけられる。AI サービスが普及するためには、クラウドの活用と利用しやすい価格設定が不可欠である。本研究は医療機関のセキュリティ実態の把握、医療 AI サービスの開発と運用、ネットワークアーキテクチャの最適化、システム監査の標準化、および技術検証という 5 つの視点から横断的に検討を行った。設立母体などを踏まえ 26 医療機関にアンケートと対面ヒアリングの二段階調査を実施したところ、平均して 100 床あたり 1 名のシステム要員で ICT 全般を担い、リソース不足、知識習得時間の欠如、ベンダ依存が顕著であることが判明した。これらの知見を基に、アセスメント対策、監査、訓練、人材育成の各項目にわたる提言を策定し、PDCA サイクルの継続的実施に必要な制度的支援についても言及した。医療 AI サービスの開発では、実診療補助のためのモデルを複数開発し、コンテナ化、クラウド公開、サーバレスアーキテクチャへの移行により、安全性の確保とともに運用コストの最適化を実現した。生成 AI と AI エージェントの登場は専門家依存という従来の前提を覆し、未経験者による自律的な開発を可能にした。また、電子カルテ接続に過度な忌避感を持つ情報管理部門に対し、実証的根拠をもって安全性を説明できる環境が整いつつある。ネットワークアーキテクチャの面では、地域医療連携ネットワークを基盤に、内部侵入の早期検知、仮想ブラウザによる安全なクラウド接続、IT-BCP に基づく縮退運転設計を組み合わせた構成を提示した。情報共有基盤から地域の見張り番へ再定義し、共同監視、共同利用、共同訓練を実現することが、クラウド型医療 AI の安全な普及に資する現実的な方策であることを示した。システム監査においては、ガイドラインに準拠し 8 病院での監査を通じて、広く国内医療機関に適用可能な標準化へ向けた基盤を整えた。セキュリティの技術的基盤の観点では Claude Code Security の発表が画期的な転換点となり、専門人材の慢性的不足という医療機関の構造的問題に対し、人に依存しない形での対応が現実のものとなってきた。基本的脆弱性は AI ネイティブなセキュリティツールによって大幅に改善される可能性があり、対策を支える技術的基盤はこの一年間で質的に異なるものへと変貌を遂げた。医療、情報、セキュリティの三専門領域が新たな形で連携し、患者と市民の参画を促しながら医療 AI のさらなる発展へと繋げていくためには、新しい開発および運用体制の構築を前向きに捉える姿勢が求められる。本研究はその実現に向けた技術的、運用的、制度的指針を具体的な形で提示するものである。

研究代表者
岡村 浩司 (国立成育医療研究センター・室長)
研究分担者
宇賀神 敦 (医療 AI プラットフォーム技術研究組合・理事長)
藤井 進 (東北大学・教授)
金子 誠暁 (医療 AI プラットフォーム技術研究組合・システム WG リーダー)
尾﨑 勝彦 (徳洲会インフォメーションシステム株式会社・会長)
松井 俊大 (国立成育医療研究センター・医員)
中村 直毅 (東北大学・准教授)

A. 研究目的

ディープラーニング等 AI 技術の飛躍的な進歩により、医療 AI の有用性が広く認識され、医療の質向上や医療従事者の負担軽減などの実証が進められている。特に、2024 年 4 月からの医師の時間外労働の上限規制や、医療、介護の担い手不足の深刻化を背景に、医療 AI の活用は急務となっている。医療 AI は、医療従事者の業務効率化や医療レベルの高度化、患者サービスの向上に加え、専門医不在の離島や僻地における地域格差解消にも大きな可能性を持つ。しかし、その多くはインターネット上のクラウドに存在する一方、医療機関の電子カルテ等はインターネットから分離された閉じた環境にあり、特にカルテ端末からの利用の普及が進んでいるとは言い難い。さらに個人情報保護への配慮が求められる中、ランサムウェアをはじめとしたサイバー攻撃の危険性も高まっており、対策が求められている。

こうした状況に加え、大規模言語モデルおよび AI エージェントの急速な進展は、医療 AI 開発のあり方そのものを変えつつある。従来は専門家に依存していた開発プロセスが、AI 駆動型開発によって未経験者にも開放されつつあり、誰がどこまで開発できるのか、その品質やセキュリティは担保されるのかを実証的に検証することが新たな研究課題として浮上している。さらに、Claude Code Security や Claude Mythos に代表される AI ネイティブなセキュリティツールの登場は、従来の専門家集団による脆弱性探索という前提を根底から覆すものであり、セキュリティ専門人材の慢性的不足に悩む医療機関にとって、その影響と可能性を早急に見極める必要がある。AI が社会インフラと深く結びつく中で、医療情報セキュリティの構造そのものがどのように変容していくのか、その動向を継続的かつ注意深く調査・考察することが求められる。

これらの課題に対応するため、本研究では医療機関の類型化に基づいた最適なネットワークセキュリティ構成とシステム監査のルールを確立する。具体的には、国立成育医療研究センター(NCCHD)と医療 AI プラットフォーム技術研究組合(HAIP)の連携により、秘密分散、多要素認証、暗号化アルゴリズム、閉域網などの ITC およびセキュリティ技術検証を行い、医療 AI サービスの開発から評価、実装までを一気通貫で提供するプラットフォームの構築を目指す。さらに、東北大学が主導する地域医療ネットワークシステム MMWIN の活用や、徳洲会グループにおけるシステム監査の標準化など、具体的な実証を通じて、医療機関の電子カルテ端末から医療 AI をセキュアに、かつリーズナブルな費用で利用するための技術や方策を確立する。これにより、安全性を担保しながら医療 AI サービスの普及促進と医療技術のさらなる発展につなげることを目指す。

B. 研究方法

近年増加する医療機関へのランサムウェア被害について、特に最近発生した事例に注目し、被害内容、原因、経済的損失、復旧時間などを分析した。次に、医療機関のネットワークセキュリティ対応の実態を把握するため、設立母体、病床数、地域が分散されるよう配慮して選定した全国26医療機関(24病院、2診療所)に対して、2段階での調査を実施した。具体的には、事前アンケートによる基礎情報の収集と、その回答を踏まえた直接訪問によるヒアリングを行い、システム管理方法、セキュリティ人材の配置状況、厚労省セキュリティチェックリストの活用状況、システム監査の実施状況、IT-BCPへの対応などを詳細に調査した。この2段階のプロセスにより、対面ヒアリングを効率的かつ深く掘り下げることが可能となり、確認すべき内容を明確にすることができた。ヒアリングから明らかになった課題を分析して対策を提言に反映するとともに、医療機関のシステム構成を正確に把握することでネットワーク構成の類型化を行い、クラウドシフトを加速するための課題と具体的なネットワーク構成を示した。システム監査については、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」に基づき、標準化に向けた取り組みを継続した。徳洲会グループ内外の医療機関で実証的な監査を実施し、監査項目や提出資料の見直しを重ねることで、より実効性の高い監査手法の確立を目指した。

技術面では、東北大学病院において仮想ブラウザおよびランサムウェア対策用デコイを用いた実証実験を継続し、地域医療ネットワークシステムにおけるセキュリティサービスの展開可能性を検討した。医療AI開発の基盤としては、TensorFlowやPyTorchを活用した画像認識システムの構築、Dockerによるコンテナ化、クラウドサービス（AWS、Azure）を活用したデプロイ環境の整備を行い、サーバレスアーキテクチャへの移行とゼロトラスト[1]セキュリティモデルの実装に向けた検証を進めた。最終年度は特に、医療AI開発手法の変革という観点から、AI駆動型開発の実践的検証に取り組んだ。AIコーディングエージェントとして、VS Codeの拡張機能であるCline、Amazon Q DeveloperおよびKiroを試用し、LLMには主にAnthropic Claude Sonnetを活用した。未経験者がこれらのツールを用いてどこまで自律的に開発を完遂できるか、またその成果物の品質およびセキュリティは実用に耐えうるかを検証し、専門家依存を前提としない新たな開発・人材育成の可能性を探った。

また、AIネイティブなセキュリティツールの急速な台頭についても調査を行った。コードベース全体を横断的に解析し脆弱性検出から修正提案までを自動化するClaude Code Security、およびその能力をさらに引き上げるとされるClaude Mythosは、従来の専門家集団による脆弱性探索という前提を根底から変えうるものである。セキュリティ専門人材の慢性的不足という医療機関の構造的問題に対してこれらのツールがどのような解をもたらしうるか、また導入にあたっての課題や留意点は何かについて、技術的、組織的両面から検討を行った。AIが社会インフラと深く結びつく中で医療情報セキュリティの

[1] ゼロトラスト(zero trust)とは、「いかなるユーザ・デバイス・通信も、ネットワークの内外を問わず、デフォルトでは信頼しない」という原則に基づくセキュリティモデルである。従来の境界型セキュリティ(ファイアウォール等によりネットワーク内部を安全とみなす方式)とは異なり、すべてのアクセスに対して継続的な認証・検証・最小権限の付与を求める。米国国立標準技術研究所(NIST)のSP 800-207において標準的な概念として定義されている。

構造がどのように変容していくかは、継続的な調査が求められる重要な課題として位置づけた。

これらの調査、実証を通じて、医療機関の類型に応じた最適なネットワーク構成とセキュリティ対策の指針を示すとともに、クラウド上の医療 AI サービスの安全な利用環境の確立を目指した。

C. 研究結果

情報処理推進機構が発表した『情報セキュリティ 10 大脅威 2026』では、1 位がランサムウェアによる被害、2 位がサプライチェーンの弱点を悪用した攻撃と、2024 年版からの二大脅威に変わりはないが、特筆すべきは AI の利用をめぐるサイバーリスクが 3 位に初登場したことである。生成 AI を活用したサイバー攻撃の台頭により、境界防御型、ゼロトラスト型セキュリティによる防御という概念だけでは対応が困難になりつつあり、サイバー攻撃を受けても被害を最小化し医療継続を図るサイバーレジリエンスの考え方が一層重要となっている。医療機関へのランサムウェア被害の実態調査では、つるぎ町立半田病院（2021 年）、大阪急性期・総合医療センター（2022 年）、岡山県精神科医療センター（2024 年）などの事例分析を通じて、共通する脆弱性と被害パターンが明らかになった。特に、VPN 機器の既知の脆弱性を悪用した攻撃やバックアップ体制の不備が主な要因となっており、電子カルテシステムの停止や診療制限を余儀なくされ、復旧までに約 2 か月を要するケースが多く、経済的損失は復旧費用と診療停止による逸失利益を合わせると数十億円規模に及ぶことが判明した。

医療機関の実態調査では、宮城県内 330 施設へのアンケートと、全国 26 医療機関（24 病院、2 診療所）への詳細調査を実施した。医療機関では平均して 100 床あたり 1 名のシステム要員しか配置されておらず、セキュリティ監査の実施率は 46%、リスクアセスメントの実施率は 27%と低く、特に中小規模の医療機関での対策が不十分であることが明らかとなった。サイバーセキュリティチェックリストについては 87%の医療機関が記入を行っているものの、保健所からの具体的なフィードバックがないことへの課題も指摘された。また BCP については 55%の医療機関が対策を実施中または計画中であったが、自然災害対応の BCP とサイバー攻撃対応の IT-BCP は異なるものであり、経営層を含めた理解の促進が急務であることが示された。ヒアリング結果をもとにネットワーク構成をセキュリティ統制レベルに応じて類型化し、パスワード管理の徹底をレベル 0 として追加した 4 段階の類型化モデルを整備した(図 1)。さらに、病院 IT 部門向け（80 問）、病院経営層向け（15 問）、診療所向け（13 問）の 3 種類のアセスメントツールを β 版として 70 を超える医療機関や関係部門で試行した。

レベル	統制の主な内容	外部NW統制	記憶媒体利用統制	内部NW統制
0	● 基本的な実施事項	–	–	–
1	● 医療情報系ネットワークと、外部(別の組織やサービス）や院内の別ネットワークとの通信制御がある程度実施されているが、管理レベルが不十分である	一部出来ている	一部出来ている	出来ていない
2	● 医療情報系ネットワークと外部(別の組織やサービス）や院内の別ネットワークとの通信制御が実現され、構成やアクセス記録が維持管理されている ● マルウェア侵入や情報漏洩を防ぐため、USBメモリ等外部記憶媒体の利用制御・管理が行われている	出来ている	出来ている	出来ていない
3	● 医療情報系ネットワークと外部(別の組織やサービス）や院内の別ネットワークとの通信制御が実現され、構成やアクセス記録が維持管理されている ● マルウェア侵入や情報漏洩を防ぐため、USBメモリ等外部記憶媒体の利用制御・管理が行われている ● 医療情報系ネットワーク内部において、部門システム間の通信制御が実現され、維持管理されている	出来ている	出来ている	出来ている

図 1. 統制レベルに応じた類型化

システム監査については、厚生労働省ガイドライン第 6.0 版に準拠し、徳洲会グループ外の A 病院・B 病院を対象とした監査を実施

した。グループ外病院への適用にあたっては、ルールの有無の確認、帳票名や電子カルテアプリ名の汎用的な記載への書き換えなど監査チェックシートの大幅な見直しを行い、標準化に向けた整備を進めた(図 2)。A 病院では全 50 項目中 64%が指摘項目となり、課題の多さが浮き彫りとなった。B 病院では事前・事後のコミュニケーションを強化した結果、監査の実効性が向上し、また 3 段階評価では実態を十分に反映できないことが判明したため、充足率による 4 段階評価へと改訂した。これらの経験を通じて、広く国内医療機関に適用可能な監査の標準化に向けた基盤を着実に整えることができた。

	監査項目	チェック対象資料等	チェック対象資料等 提出方法	資料等 の確認	結果
管理体制					
1	医療情報システム安全管理責任者・企画管理者・情報システム運用担当者・情報セキュリティ責任者（厚労省ガイドライン上のこれらの役割を担う別名称の役職者でも良い）が任命され、それぞれの役割が明文化されている	①役職者名簿（氏名・所属・院内役職）が記載されたもの） ②役職者の役割が確認できる資料（規程の該当部分など）	①・②ともデータがPDFでご提出ください（①は最終更新日があるもの）	事前	△
2	院内の医療情報システムの安全管理やセキュリティ対策について協議・情報共有する情報システム委員会（別名称でも良い）が設置され、各部署から委員が選出されている		①・②ともデータがPDFでご提出ください（いずれも最終更新日があるもの）	事前	△
3	情報システム委員会は月１回程度開催されて機能しており、議事内容が幹部・各部署に共有されている	①情報システム委員会議事録 ②委員会の議事内容の幹部・各部署への共有が確認できる資料（回覧記録や幹部が出席する会議の議事録など）	①・②ともデータがPDFでご提出ください（①は直近の２回分）	事前	△
個人情報保護					
4	病院の個人情報保護方針が策定され、患者の見える場所に掲示されている	①病院の個人情報保護方針 ②個人情報保護方針の掲示状況（当日）	①はデータがPDFでご提出ください ②は当日掲示を確認します	事前および当日	○
5	医療情報システムから個人情報を含むデータを抜き出す際のルールが定め、適切に運用されている	①医療情報システムからのデータ抜き出しに関するルールが確認できる資料（規程の該当部分など） ②運用が確認できる資料（申請書類など）	①はデータがPDFでご提出ください（２部）	事前	○

図 2. 監査チェックシート抜粋

技術的な実証実験では、東北大学病院における仮想ブラウザとランサムウェア対策デコイの試験導入が成果を上げた。仮想ブラウザは電子カルテ端末内でのトラストゾーンとゼロトラストゾーンの両立を可能とし、既存システムへの影響を最小限に抑えながらクラウド上の AI サービスの安全な利用を実現した。デコイシステムについては攻撃の早期検知が可能であり、地域医療連携ネットワーク上での展開可能性も確認された。

クラウド型医療 AI の安全な利用環境を具体的に示すため、5 つのユースケースのヒアリングおよび実証を行った。既設ネットワークを活用した HAIP 上の医療 AI 利用（難易度：低）、地域医療連携ネットワーク経由でのクラウド AI 接続（難易度：高）、インターネット分離ソリューションを用いた音声 AI・Web 会議の利用（難易度：高）、リモートデスクトップによる院外からの電子カルテアクセス（難易度：低）、遠隔手術支援・オンライン診療（難易度：高または中）の 5 パターンである。既設のネットワークや地域医療連携システムを活用することで費用・運用変更の負担を抑えながら医療 AI を推進できる一方、医療機関ごとに異なるセキュリティレベルやネットワーク構成が導入の障壁となることが明確となった(図 3)。また、ベンダへのヒアリングでは、3 省 2 ガイドラインの医療機器への適用や解釈の難しさ、リスクベースの運用への見直しの必要性が指摘され、ディーラーにおいてはセキュリティへの意識が低く医療機関からも求められていない現状が浮き彫りとなった。さらに、IAM・PAM・EDR・SASE・XDR・SIEM など代表的なネットワークセキュリティソリューションの調査を継続し、ISMAP の登録状況等についても確認を行った。

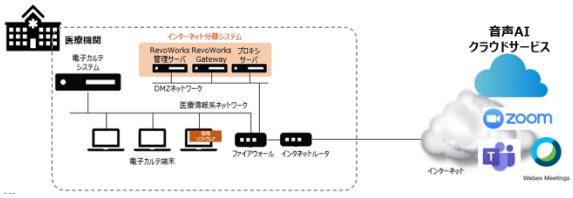


図 3. インターネット分離の概要

医療 AI 開発においては、グラム染色画像による感染症起因菌同定 AI およびファブリー病スクリーニング AI の開発を進め、サーバレスアーキテクチャへの移行によりコストを大幅に削減しながら耐障害性の高い運用環境を整備した。さらに、AI コーディング

エージェント（Cline、Amazon Q Developer、Kiro 等）と Anthropic Claude Sonnet を活用した AI 駆動型開発の実践的検証を行った。プログラミング未経験の小児科医大学院生がウェブアプリケーション開発を独力で完遂できたことは、専門家依存を前提とした従来の人材戦略からの脱却が現実のものとなったことを示している(図 4)。一方で、AI エージェント出力の確率的リスクへの対応や最終的な品質確認における人的レビューの必要性など固有の課題も明らかとなった。経験者においては、フォーム処理・コンテナ化・セキュリティ実装（XSS[2]対策、SQL[3]インジェクション対策等）の各面で大幅な効率向上が認められた。

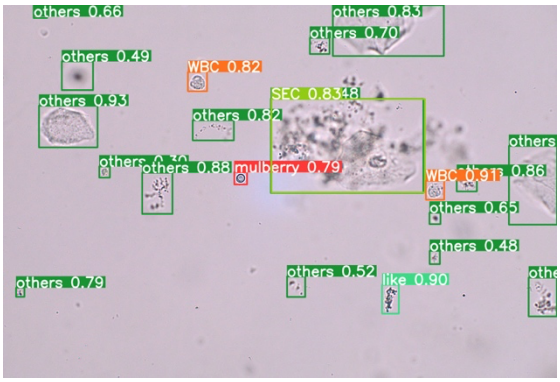


図 4. 尿沈渣顕微鏡写真の物体検出

AI ネイティブなセキュリティツールの動向調査としては、Anthropic が 2026 年に公開した Claude Mythos Preview を用いた OSS の脆弱性探索の報告にも注目した。一般に発表された調査では、nginx や Mozilla Firefox を含む主要プロジェクトから 2 万 3000 件超の脆弱性候補が特定され、中には Firefox の XSLT 処理エンジンに 20 年間潜伏していた Use-After-Free 脆弱性も発見された。しかし修正パッチが提供されたのはわずか 97 件にとどまり、AI による大規模な脆弱性発見に対して人間側の対応能力が新たなボトルネックとなっている現実が浮き彫りとなった。

D. 考察

医療機関のセキュリティ対策において、施設規模よりもセキュリティ意識と人材の充足状況が重要な要因であることが改めて確認された。セキュリティ人材が不足している施設ほどセキュリティ対策への満足度が低く、VPN 管理やランサムウェア対策といったリモート保守やデータ保護に関する支援を必要としていることが判明した。加えて、システム監査を通じて、病院幹部のセキュリティに対する関心と理解が現場全体のセキュリティレベルを左右する最大の要因であることが明確となった。幹部が積極的に関与する病院では院内 SE・システム委員会・一般職員を含む組織全体でセキュリティ対策に取り組む傾向が見られた一方、関心の低い病院では逆の状態にあり、結果として多くのリスクを抱えるケースが多かった。経営層の意識改革が、いかなる技術的対策にも先んじる根本的な課題であるといえる。

技術的な観点からは、仮想ブラウザとデコイシステムの組み合わせが、既存システムへの影響を最小限に抑えながら安全なクラウドサービス利用を実現する有効な解決策となることが示された。東北大学病院での実証実験では、1 台の電子カルテ端末上でゼロトラスト型のクラウドサービスと院内ネットワークのシステムを両立させることに成功し、地域医療ネットワークシステムを通じた展開可能性も確認された。クラウド型医療 AI

[2] クロスサイトスクリプティング、ウェブサイトの脆弱性を悪用した攻撃者によるコードをページ閲覧者に実行させる攻撃手法。

[3] SQL、リレーショナルデータベースのデータに対し、検索、更新等の処理をするための標準言語。

の促進には、AI サービスの性能向上だけでなく、医療機関が安心して接続し、利用し、止まっても診療を続け、地域で支え合うためのネットワークアーキテクチャが不可欠であり、MMWIN を活用した検討を通じ、地域医療連携ネットワークが地域の見張り番となりクラウド型医療 AI の安全な社会実装を支える基盤となり得ることが示された。

複数のユースケースの実証を通じて、既設のネットワークや地域医療連携システムを活用することで病院側の費用・運用変更の負担を抑えながら医療 AI を推進できることが確認された。遠隔医療ソリューションの活用は離島・僻地の医療格差縮小にも有効であり、院外からの電子カルテアクセスの普及は医師の働き方改革につながる可能性がある。一方で、医療機関ごとに異なるセキュリティレベルやネットワーク構成が導入の障壁となっており、セキュリティポリシーによっては HIS 系ネットワークのインターネット接続自体が許容されない場合もある。各医療機関が理想的なセキュリティ状態を維持するためには、セキュリティ有識者の支援とセキュリティ製品の導入コストの両面における解決策が引き続き求められる。

医療 AI サービスのアーキテクチャについては、従来の仮想マシン型からサーバレス環境への移行が有効であることが示唆された。クラウドプロバイダが提供するマイクロサービスアーキテクチャを活用したサーバレスへの移行は、攻撃範囲の限定、迅速な脆弱性対応、細粒度の最小権限付与によるリスク低減など、医療情報システムのセキュリティ要件と高い親和性を持つ。このような環境では ID ベースのアクセス制御が必要となるが、AWS IAM、Microsoft Entra ID 等がこれを担い、ゼロトラストセキュリティモデルの実現を効果的に支援する。サーバレスへの移行は従来、開発者に相応の学習コストと実装負担を求めるものであったが、AI コーディングエージェントの活用によりこれらの障壁が大幅に低減されることが今回の取り組みを通じて示された。AI エージェントは各クラウドサービスの詳細仕様を代替して実装するのみならず、XSS 対策・SQL インジェクション対策・認証認可の基本実装といったセキュリティ対策を標準的に組み込むことで、移行プロセスそのものをより安全に進める手段として有効である。AI コーディングエージェントの活用は、未経験者の開発参入障壁を大きく下げる一方、経験者がこれを活用することによる恩恵がより多岐にわたることも示唆された。しかしながら、一つの指示によってあらゆるセキュリティ対策が網羅されるわけではなく、医療・情報・セキュリティの各専門知識を連携させた具体的な指示と最終的な品質確認は引き続き不可欠である。患者情報保護をはじめとする医療固有の要件に対して生成 AI が初期段階から網羅的な対応を行うわけではなく、利用者側が明確な方向性を持って AI エージェントに臨む必要がある。AI エージェントを活用した標準化された開発手法への移行は従来型の人材戦略からの脱却を促し、医療機関における業務運営の一部として AI エージェントが機能する未来と、次世代が課題を独自に解決していく新たな道筋を拓くものと考えられる。

セキュリティ対策の構造的変容という観点では、AI ネイティブなセキュリティツールがもたらす恩恵とリスクの双方を医療情報セキュリティの文脈において継続的に注視していく必要性が示されている。Claude Mythos Preview による 2 万 3000 件超の脆弱性発見が示すように、AI による大規模探索能力の登場により、未知の脆弱性を発見すること自体が最大の障壁であるという従来の前

提は崩れ去り、今や人間側の対応能力の限界が新たなボトルネックとなっている。この知見は、セキュリティ専門人材の慢性的不足という医療機関の構造的問題と深く共鳴するものであり、AI エージェントによる常時監視・異常検知・インシデント分析・脆弱性評価の自動化は、医療機関が長年抱えてきたこの課題に対して現実的な補完手段となりうる。

これらの課題に対しては、医療機関のセキュリティレベルを正確に把握し、それに応じた適切な対策を講じることが重要である。アセスメント→セキュリティ対策→監査・訓練→人材育成・意識改革のサイクルを継続的かつ定期的に実行するために、本研究が開発したネットワーク類型化フローチャートおよびセキュリティアセスメントツール（IT 部門向け 80 問・経営層向け 15 問・診療所向け 13 問）は有効な基盤となる。システムセキュリティ監査については、200 床以上の医療機関では 3 年に 1 回の外部監査と毎年の内部監査の実施を推奨し、グループ外病院の監査を通じて開発した 4 段階評価体系と綿密なコミュニケーションプロセスを標準化することで、医療現場を知る病院職員によるシステムセキュリティ監査の有効性が明確に示された。IT-BCP については、計画の立案のみならず年 1 回の実際の訓練を通じて GAP を継続的に確認しブラッシュアップしていくことが、サイバーレジリエンスの実現に不可欠である。インセンティブ設計の観点では、診療報酬の施設基準における継続的な取り組みへの評価、金融機関からの借入金利のディスカウントやサイバー保険割引率アップといった民間インセンティブ、さらには優れた取り組みを行う医療機関の認定制度の整備が、セキュリティ投資と AI 活用への持続可能な動機づけとして重要である。

今後は、安全・安心なネットワーク環境の整備を医療 DX・データ利活用・医療従事者の働き方改革を支えるインフラと位置づけ、場所中心の医療から人間中心の医療への転換を見据えた取り組みを推進していくことが求められる。地域医療連携ネットワークを活用した共同利用モデルの確立と、医療・情報・セキュリティの専門家が連携しつつ AI エージェントを適切に指示・監督できる体制の整備が、その実現に向けた重要な鍵となる。

E. 結論

医療 AI の利活用は医療の質向上や効率化、地域格差の解消、医療従事者の負担軽減に大きな可能性を持つものの、セキュリティ面での課題が普及の障壁となっている。調査の結果、医療機関では平均して 100 床あたり 1 名のシステム要員しか配置されておらず、人材不足や知識不足、ベンダ依存体制という構造的な問題を抱えていることが改めて明らかとなった。医療機関・ベンダ・ディーラーそれぞれへの調査を通じて、保守メンテナンス用回線のセキュリティ不備、クラウドサービス利用の停滞、ガイドラインの解釈差による対応負担など、多層的な課題が浮き彫りとなった。これらに対しては、外部接続点のネットワーク集約、既存設備を活用したセキュアなネットワークインフラの構成、VPN＋α の新技術をガイドラインに反映する取り組み、省庁横断での解説整備が有効な対策として示された。

サイバー攻撃はもはや情報システムの障害ではなく、診療継続性の危機として捉えなければならない。電子カルテ停止、検査遅延、手術延期、救急受入制限、そして地域医療全体への波及は、医療機関が直面するサイバー攻撃の現実である。現在のランサムウェア攻撃は侵入後に内部偵察・権限奪取・横展開・

バックアップ侵害・情報窃取という一連のプロセスをたどるため、侵入を完全に防ぐだけでは不十分であり、侵入後の早期検知が重要となる。この観点から、デコイは医療機器や既存端末に大きな変更を加えることなく内部偵察段階での攻撃検知を可能にし、EDR や NDR と比較して医療機関の制約に適合しやすい手段として有効性が確認された。仮想ブラウザはトラストゾーンとゼロトラストゾーンを電子カルテ端末上で両立させることで、クラウド型医療 AI 利用に伴う外部接続リスクを低減する現実的な解決策となることが示された。

生成 AI を活用したサイバー攻撃が激増し攻撃が高度化している現在、境界防御型セキュリティとゼロトラスト型セキュリティを組み合わせた完全防御をめざす対策だけでは守り切れない時代となっている。サイバー攻撃のリスクは常に存在するという前提に立ち、万一攻撃を受けても医療の提供を止めないことが最重要の課題となる。組織全体でサイバーレジリエンスの考え方を実践し、IT-BCP により攻撃からの回復と医療提供継続の計画を立案した上で、日頃より実践訓練を重ねることが不可欠である。IT-BCP は復旧手順書ではなく縮退運転の設計図であり、紙運用だけでは長期障害に耐えられないため、復旧優先順位・代替診療・地域内連携・訓練・ナレッジ共有を包括的に整備する必要がある。

地域医療連携ネットワークは、情報共有の仕組みから地域医療を守る共通基盤へと発展し得る。人材不足・コスト不足・サイバーリスク・医療 DX・クラウド型 AI 利用という複数の課題に対し、地域での共同利用・共同監視・共同訓練を実現することは現実的かつ実効性の高い方策であり、MMWIN を活用した検討を通じてその可能性が具体的に示された。この課題に対し、仮想ブラウザによるトラストゾーンとゼロトラストゾーンの両立、ランサムウェア早期発見のためのデコイシステム、セキュリティアセスメントツールの活用など、具体的な技術的解決策の有効性が確認された。医療機関の特性に応じた体系的なシステム監査手法の確立においては、徳洲会グループ外を含む複数の病院での監査実施を通じて標準化が大きく前進した。監査を通じて明確となったのは、病院幹部のセキュリティへの理解と関与がセキュリティレベルを左右する最大の要因であるということである。幹部と院内 SE、現場の医療スタッフの共通理解と協力のもと、内部監査（年 1 回）と外部監査（2〜4 年に 1 回）を継続的に実施するサイクルを確立することで、セキュリティ対策が医療現場の日常運用に根付いていくことが期待される。経営層のセキュリティリテラシー向上、人材不足を補うための支援体制の構築、責任分界点の明確化、継続的なセキュリティ対策費用の確保など、組織的な取り組みは依然として不可欠である。

技術的基盤の観点では、この一年間で起きた変化は当初の想定をはるかに超えるものであった。AI コーディングエージェントの実用化により、ソフトウェア開発は AI 支援型から AI 駆動型へと本質的なシフトを遂げ、開発効率・コード品質・セキュリティ実装の各面において従来手法との明確な差異が生じている。国家サイバー統括室による ASM の継続的な調査において、AI 駆動型開発への移行後には脆弱性が一切検出されなくなったことは、その効果を客観的に示す具体的な成果である。さまざまなセキュリティ実装が AI エージェントによって開発プロセスに自律的に組み込まれるようになったことは、専門家の知識と経験に依存してきたセキュリティ対策の民主化という観点から本質的な

意義を持つ。また、マイクロサービスアーキテクチャを活用したサーバレス環境は、アイデンティティベースのアクセス制御を前提として設計されており、概念としては提唱されながらも具体性に乏しいと感じられてきたゼロトラストを自然な形で実装へと落とし込める基盤となりうる。生成 AI 登場以前に設計された SASE をはじめとする既存のセキュリティツールの多くはサーバレス運用を前提としておらず、現在の開発・運用環境の実態と乖離しつつあることも、本研究を通じて明らかとなった課題の一つである。

そして 2026 年、Anthropic による Claude Code Security の発表は、医療情報セキュリティの文脈においても見過ごすことのできない画期的な転換点となった。コードベース全体のデータフローを横断的にトレースし複雑な脆弱性パターンを検出する推論ベースの能力と、敵対的検証プロセスによる誤検知の大幅な削減、そして検出から修正パッチの提案・適用までをシームレスなワークフローで完結させるこの仕組みは、セキュリティ専門人材の慢性的な不足という医療機関が長年抱えてきた構造的問題に対して現実的な解を提示するものといえる。Claude Mythos はそのレベルをさらに引き上げており、2 万 3000 件超の OSS 脆弱性を特定し 20 年間潜伏していたバグをも発見したその能力は、未知の脆弱性発見が最大の障壁であるという従来の前提を根底から覆すものである。これまでランサムウェア被害の多くを招いてきたパスワード設定不備などの基本的な脆弱性は、こうした AI ネイティブなセキュリティツールによって大幅に改善される可能性があり、医療 AI サービス自体が攻撃の主要標的となった事例が確認されていないという現実と合わせて考えれば、電子カルテネットワークへの接続に過度な恐怖感を抱き新たな取り組みを忌避してきた医療機関の情報管理者に対し、実証的な根拠をもって安全性を説明できる環境が整いつつある。

人材育成の観点においても、状況は大きく変わった。AI エージェントを活用することで未経験の大学院生が物体検出 AI モデルとウェブアプリケーションの開発を独力で完遂できたことは、経験者や専門家への依存を前提とした従来の人材戦略からの脱却が現実のものとなったことを示している。AI エージェントは開発ツールであると同時に学習のツールでもあり、次世代の医療従事者や研究者が独自に課題を発見し解決していく可能性を、本研究の経験は具体的な形で示唆している。医療・情報・セキュリティという三つの専門領域がこれまでとは異なる形で連携しながら、患者および市民の参画を促しビッグデータに依存する医療 AI のさらなる発展へと繋げていくためには、こうした新しい開発・運用体制の構築を前向きに捉え、悲観的になりがちであった状況を積極的に転換していく姿勢が求められる。

F. 健康危険情報

本研究の対象は、医療機関やネットワーク、セキュリティ対策等であり、被験者の身体的健康に直接的な危険を及ぼすものではない。医療 AI サービスの利用促進が最大の目的で、個人情報漏洩のリスクに対しては、厳格な匿名化プロセス、暗号化技術の徹底的な適用、アクセス権限の厳密な管理、データ処理における最新のセキュリティガイドライン準拠等の対策を講じ、リスクを最小化し、より安全な情報管理システムの構築を実現することである。被験者の情報保護を最優先に、慎重かつ倫理的なアプローチを取る。

G. 研究発表

1. 論文発表

Yamanaka H, So T, Sakamoto N, Aoto S, Li XK, Wang Y, Shen Q, Migita O, Kosuga M, Okamura K. Automated detection of mulberry bodies in urinary sediment for non-invasive Fabry disease screening. *Clin. Chem. Lab. Med.* [doi: 10.1515/cclm-2026-0345] (2026)

Hayashi H, Kashizuka E, Sakata K, Motomiya N, Asakawa Y, Hayasaki M, Yokoi T, Yoshida T, Nishina S, Okamura K. Detection of pediatric cataracts through non-invasive facial photography using deep convolutional neural networks for early diagnosis. *BMC Ophthalmol.* **26**, 282 (2026)

Yamanaka H, Okamura K. Exploring deep learning and data requirements through image classification of *Erigeron annuus* and *Erigeron philadelphicus*. *BMC Res. Notes* **19**, 127 (2026)

Matsui T, Uchida Y, Tomizawa D, Yanagi K, Shoji K. Fatal group A streptococcal sepsis as initial presentation of acute lymphoblastic leukemia. *Pediatr. Int.* **68**, e70352 (2026)

Inoue R, Nakayama M, Ota H, Nakamura N, Fujii S, Ishii A, Saito A, Suzuki T, Nomura H, Goto N, Watanabe S, Maruyama H, Nozawa M, Uyama Y. Establishment of reliable identification algorithms for acute heart failure or acute exacerbation of chronic heart failure using clinical data from a medical information database network. *Front. Cardiovasc. Med.* **12**, 1642323 (2025)

Shibata M, Umezawa A, Aoto S, Okamura K, Nasu M, Mizuno R, Oya M, Yura K, Mikami S. Applicability of the regression approach for histological multi-class grading in clear cell renal cell carcinoma. *Regen. Ther.* **28**, 431–437 (2025)

2. 学会発表

藤井 進, 野中 小百合, 川本 章太, 中村 直毅. 医療機関の人材不足とセキュリティ課題への対応： 地域連携ネットワークを活用した実装可能な対策モデルの検討. *第 45 回医療情報学連合大会* **4-B-1-01**, 2025

岡村 浩司, 山中 宏勇. AI 駆動型開発がもたらす医療 AI サービス構築の革新と課題. *第 45 回医療情報学連合大会* **4-B-1-03**, 2025

中村 直毅, 金子 誠暁, 野中 小百合, 川本 章太, 藤井 進. 地域医療連携ネットワークにおけるサイバーセキュリティ対策：仮想ブラウザと集中管理型デコイシステムを統合した多層防御アーキテクチャの設計と実装. *第 45 回医療情報学連合大会* **4-B-1-04**, 2025

金子 誠暁. 医療機関の働き方改革を見据えた具体的ユースケースの事例紹介. *第 45 回医療情報学連合大会* **4-B-1-05**, 2025

福田 秀樹, 尾﨑 勝彦. 医療機関のサイバーセキュリティ対策 ―徳洲会グループシステム監査：標準化の試み―. *第 45 回医療情報学連合大会* **4-B-1-06**, 2025

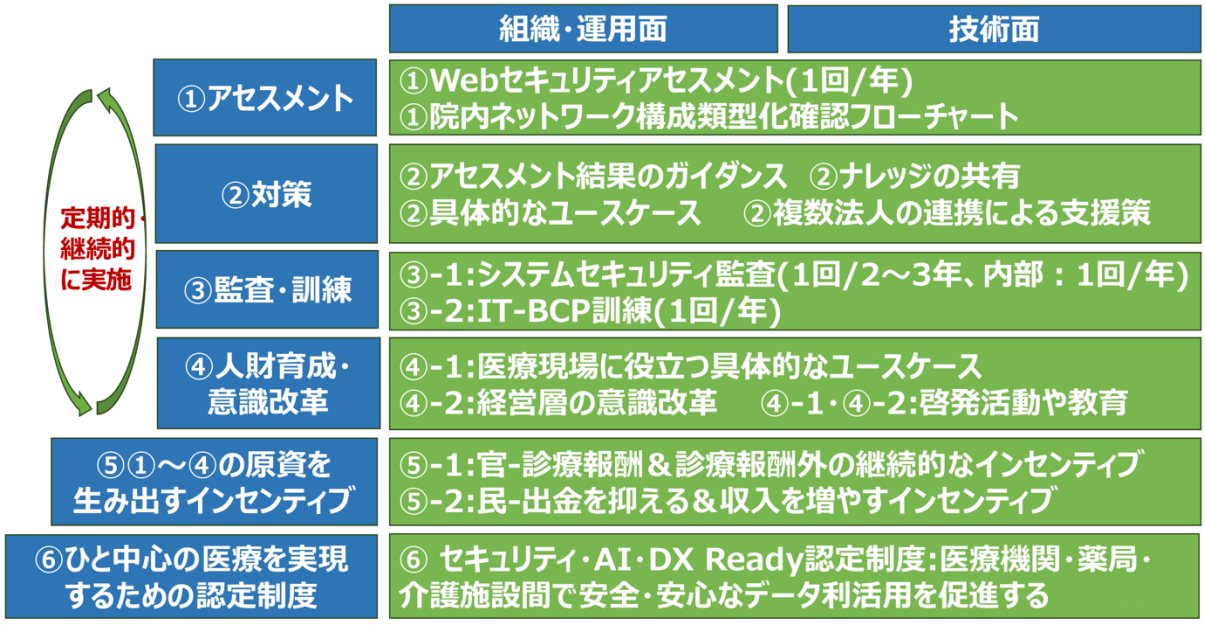
宇賀神 敦. 医療 AI の活用や医療 DX 推進に求められるセキュリティやガバナンス ―安心して医療 AI が利用できるデータ連携基盤やサイバーセキュリティの制度的支援の考察 ―. *第 45 回医療情報学連合大会* **4-B-1-08**, 2025

G. 知的財産権の出願

岡村 浩司, 仁科 幸子. 乳幼児の視覚異常スクリーニング方法、視覚異常スクリーニングシステム及び表示システム. 特願 2026-060427 (2026 年 4 月 1 日)

松井 俊大, 岡村 浩司. 菌種判別装置、菌種判別方法および菌種判別プログラム. 特願 2025-018598 (2025 年 2 月 6 日)

資料　クラウド医療 AI サービス利用のための提言



別紙 3

厚生労働科学研究費補助金
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
クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言

ネットワークアーキテクチャーグループ(東北大分担 SWG)
藤井進・中村直毅・野中小百合・川本章太

研究要旨

本研究は、医療機関の類型化に基づき、最適なネットワークセキュリティ構成とシステム監査ルールを提示することで、全国の医療機関が安全・安心かつリーズナブルな費用で医療 AI サービスを利用できる環境の整備を目的とする。

医療 AI の有用性が広く認識される一方で、個人情報保護やランサムウェアをはじめとするサイバー攻撃への対策が喫緊の課題となっている。近年、診療記録作成支援、診断補助、PHR 連携、画像・検査情報解析などの医療 AI は急速に普及し、その多くがクラウド型サービスとして提供されている。しかし、電子カルテ端末や診療系ネットワークから外部クラウドへ接続することは、情報漏えいやマルウェア感染のリスクを伴い、従来の境界型防御のみでは十分に対応できない。またランサムウェア被害は電子カルテ停止や診療機能の喪失を引き起こし、地域医療全体に影響を及ぼす「診療継続性の危機」として捉える必要がある。

本研究分担班では、東北大学が主導する地域医療ネットワークシステムである MMWIN を基盤として検討を行った。これまで宮城県内医療施設を対象としたアンケート調査（330 施設回答）を実施し、地域医療連携ネットワークに対して、従来の情報共有に加え、ランサムウェア対策、クラウドバックアップ、災害対応、セキュリティ人材不足への支援、AI 活用基盤としての役割が期待されていることを明らかにしてきた。

本年度はこれらの結果を踏まえ、サイバー攻撃を侵入後の内部偵察や横展開を含む一連のプロセスとして整理し、侵入を前提とした早期検知と被害抑止を重視したネットワークアーキテクチャーを検討した。具体的には、Decoy による内部侵入の早期検知、仮想ブラウザによる安全なクラウド接続環境の構築、IT-BCP に基づく縮退運転設計を組み合わせた対策を提示した。Decoy は既存環境への影響が少なく内部偵察段階での検知が可能であり、仮想ブラウザは電子カルテ端末上でトラストゾーンとゼロトラストゾーンを両立できる点で有効性を確認した。

さらに、これらの機能を地域医療連携ネットワーク上で共同利用することで、コスト負担の軽減と人材不足の解消を図る構成を提示した。すなわち、地域医療連携ネットワークを「情報共有基盤」から「地域の見張り番」へと再定義し、共同監視・共同利用・共同訓練を実現することが、クラウド型医療 AI の安全な普及に資する現実的な方策であることを示した。

以上より、本研究は、医療 AI の利活用促進とサイバーセキュリティ対策を統合的に捉え、地域単位での共通基盤整備の重要性を明らかにした。今後、医療 DX を持続的に推進するためには、地域医療連携ネットワークを活用した実装が重要であると提案する。

・藤井進：東北大学災害科学国際研究所 災害医療情報学分野　教授/東北大学病院　医療データ利活用センター長/東北大学病院メディカル IT センター副部長
・中村直毅：東北大学病院メディカル IT センター副部長　准教授
・野中小百合：東北大学災害科学国際研究所　上廣防災学寄附研究部門・災害医療情報学分野　助教/東北大学病院　医療データ利活用センター　助教
・川本章太：東北大学病院　医療データ利活用センター　助教

A. 研究目的

本研究の目的は、クラウド型医療 AI の利活用を安全かつ現実的に促進するため、医療機関のネットワークセキュリティ構成を類型化し、地域医療情報連携ネットワークを活用した実効性のあるセキュリティ対策、IT-BCP、共同運用モデルを提示することである。

医療 AI は、診療記録作成支援や問診支援、診断補助、PHR 連携、画像・検査情報の解析、医師業務支援など、医療現場の生産性向上に資する可能性を有する。特に医療従事者不足、地域偏在、診療業務の増大が進む中で、クラウド型 AI サービスは大学病院から中小病院、診療所まで広く利用される可能性がある。しかしクラウド型 AI を診療現場で活用するためには、電子カルテ端末や診療系ネットワークから外部クラウドへ安全に接続する必要があり、従来の境界型防御だけでは対応が困難となる。

一方で、医療機関に対するランサムウェア攻撃は単なる情報漏えいではなく、診療停止、救急受入制限、検査遅延、手術延期、地域医療への波及を引き起こす。大阪急性期・総合医療センターの事例では、給食事業者の VPN 機器を契機として侵入が生じ、認証情報の窃取、病院給食サーバへの侵入、電子カルテを含む基幹システムへの被害拡大が生じた（引用元名：大阪急性期・総合医療センター「情報セキュリティインシデント調査報告書 概要」：URL：https://www.gh.opho.jp/pdf/reportgaiyo_v01.pdf)。この事例は、病院本体だけでなく委託先、保守回線、VPN、認証情報管理を含めたネットワーク全体の設計が重要であることを示している。

また、英国 NHS の WannaCry 被害では、NHS England が 6,912 件の予約キャンセルを確認し、全体では 19,000 件超の予約がキャンセルされたと推計している（引用元名：National Audit Office「Investigation: WannaCry cyber attack and the NHS」：URL：https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/)。 これは、サイバー攻撃が医療安全および医療アクセスに直接影響することを示す象徴的事例である。

このような状況を踏まえ、本研究では、サイバーセキュリティを「情報システムを守る技術」ではなく、「診療を止めないための医療安全・地域医療継続の基盤」として位置づけた。特に大学病院や基幹病院は、サイバー攻撃時に自院を守るだけでなく、地域医療の需給バランスを支える役割を担う。したがって、クラウド型医療 AI の促進には一病院単独のセキュリティ強化ではなく、地域医療情報連携ネットワーク

を介して、監視、検知、AI 利用、IT-BCP 訓練、ナレッジ共有を共同化する仕組みが必要である。

最終年度である本年度は、これまでに得られたアンケート調査結果、仮想ブラウザと Decoy の試験導入、地域医療ネットワーク上での設計を発展させ、MMWIN を活用した実証的検討を行った。そして、地域医療情報連携ネットワークが、クラウド型医療 AI を安心して利用するための「地域の見張り番」となり得ることを、アーキテクチャー、コスト、医療機関の構造的課題、政策提言の観点から明らかにすることを目的とした。

B. 研究方法

本研究では、過去 2 年間の研究成果をもとに、クラウド型医療 AI 利用促進に必要なネットワークセキュリティ構成を、実際の医療機関の構造的課題と照合しながら再評価した。研究方法は、第一に被害事例の調査、第二に攻撃構造の整理、第三に医療機関のニーズ分析、第四に Decoy および仮想ブラウザの実証、第五に IT-BCP と地域共同運用モデルの検討の五段階で構成した。

まず、国内外のランサムウェア被害事例を調査し、攻撃経路や被害規模、復旧期間、診療・事業継続への影響を整理した。対象には、徳島県つるぎ町立半田病院、大阪急性期・総合医療センター、岡山県精神科医療センター、英国 NHS、米国 Change Healthcare、英国 Synnovis、さらに医療機関外ではあるが事業継続への影響が大きかったアサヒグループ事例を含めた。特にアサヒグループ事例は、対策を行っていた企業であっても境界機器や拠点ネットワーク機器を起点として侵害され、受注・出荷・物流等の基幹業務が停止することを示しており、医療機関における電子カルテ停止や診療停止のリスクを構造的に理解するための比較事例として扱った。

次に、ランサムウェア攻撃を侵入や内部偵察、権限奪取、横展開、暗号化・情報窃取、診療停止、説明・復旧対応という一連の過程として整理した。これにより、単に入口を守るだけでなく、侵入後の早期検知、横展開抑止、復旧優先順位、縮退運転、説明責任が必要であることを明確化した。警察庁の令和 7 年上半期資料では、ランサムウェア被害報告件数が 116 件であり、半期件数として令和 4 年下半期と並び最多であったことが示されている（引用元名：警察庁「令和 7 年上半期におけるサイバー空間をめぐる脅威の情勢等について」：URL：https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf）。

第三に、前年度に実施した宮城県内医療施設へのアンケート結果を再解釈した。対象は宮城県内の医療施設 1,753 施設であり、330 施設から回答を得た。有効回答施設数は 322 施設であった。調査項目は、地域医療連携システムに対する診療情報共有や紹介・逆紹介、リモート保守、クラウドバックアップ、ランサムウェア対策、AI 利用、安全な情報共有、セキュリティ人材不足に関するニーズを中心に構成した。前年度報告では、施設規模よりも、セキュリティ意識や人材不足の状況が、セキュリティ対策や新技術導入への関心に影響するこ

とが示された。

第四に、東北大学病院で試験導入した Decoy および仮想ブラウザを、MMWIN 上で共同利用する構成として再設計した。Decoy については、EDR や NDR と比較し、端末数に依存しにくい費用構造、医療機器や古い OS 端末への影響の少なさ、内部偵察段階での検知可能性を評価した。仮想ブラウザについては、電子カルテ端末からクラウド型 AI サービスへ接続する際に、端末側へ外部 Web コンテンツを直接実行させず、仮想環境で処理することにより、トラストゾーンとゼロトラストゾーンを両立できるかを検討した。

第五に、これらの技術を IT-BCP の中に位置づけた。すなわち、サイバー攻撃を完全に防ぐことだけを目的とするのではなく、攻撃が発生した場合に、どの診療機能を継続し、どのシステムを優先復旧し、どの時点でネットワークを切り離し、どのように地域内で患者受入や紹介を調整するかを検討した。PPT 資料では、IT-BCP を「防御や復旧対策の手順書」ではなく「縮退運転の設計図」と捉え、守るべきものはデータそのものではなく診療機能であると整理している。

以上の方法により、クラウド型医療 AI の促進に必要なサイバーセキュリティを、技術的対策、運用設計、地域共同化、政策提言の観点から総合的に検討した。

C. 研究結果

1. ネットワークアーキテクチャーの再検討

■サイバーセキュリティは「診療継続性」の問題

本年度の検討により、医療機関におけるサイバーセキュリティは、従来のように「情報システムを守る」「個人情報を守る」という範囲にとどまらず、「診療を止めない」ための医療安全上の課題として捉える必要があることが明らかとなった。PPT 資料では、サイバーセキュリティの焦点を「診療継続性」とし、IT-BCP を「縮退運転の設計図」と位置づけている。

医療機関の診療は、電子カルテやオーダリング、検査、画像、薬剤、会計、手術、救急、紹介・逆紹介、地域連携など、多数のシステムが連動して成立している。したがって、電子カルテが停止することは単なる記録手段の停止ではなく、検査依頼、薬剤確認、禁忌確認、手術準備、会計処理、地域連携の停止へ連鎖する。これは、医療機関におけるサイバー攻撃が、情報部門の問題ではなく、病院経営、医療安全、地域医療提供体制の問題であることを意味する。

本年度は、この認識を出発点として、被害事例や攻撃構造、早期検知、クラウド AI 利用、IT-BCP、地域医療連携ネットワークの付加価値化を一体的に検討した。

2. 最近の被害事例からみた課題

■アサヒグループ事例：対策していても突破され、事業が止まる

2025 年 9 月 29 日、アサヒグループホールディングスは、サイバー攻撃によるシステム障害の発生を公表した。同社の調査結

果によれば、攻撃者はグループ内拠点に設置されたネットワーク機器を経由してデータセンターネットワークへ不正アクセスし、ランサムウェアを一斉に実行した。被害拡大防止のため、同社はネットワーク遮断とデータセンター隔離を行った（引用元名：アサヒグループホールディングス「サイバー攻撃による情報漏えいに関する調査結果と今後の対応について」：URL：https://www.asahigroup-holdings.com/newsroom/detail/20251127-0104.html）。

この事例の重要性は、サイバー攻撃が「IT 障害」ではなく「事業停止」を引き起こした点にある。アサヒグループでは、受注、出荷、物流、コールセンターなどの業務に影響が生じ、国内工場の稼働や出荷にも制約が生じた。Reuters は、サイバー攻撃後に受注処理や出荷、コールセンター機能が停止し、国内 6 工場の生産にも影響があったと報じている（引用元名：Reuters「Japan's Asahi restarts beer production following cyberattack」：URL：https://www.reuters.com/world/asia-pacific/japans-asahi-restarts-beer-production-following-cyberattack-2025-10-06/）。

さらに、この事例ではアサヒグループが平時から NIST 準拠の管理体制や EDR 導入、SOC 監視、ペンテスト、脆弱性修正等を実施していたにもかかわらず、境界機器を起点とした侵害が発生したことが重要である。添付する IT-BCP の資料では、この点を「対策していても突破される」「重要なのは突破後に広げない設計である」と整理した。

医療機関に置き換えれば、これは電子カルテ障害が即座に診療影響へつながる構造と同じである。アサヒグループでは出荷や物流が止まったが、病院では検査、処方、手術、救急、入退院、紹介調整が止まる。つまり、サイバー攻撃は、産業では事業継続の問題であり、医療では診療継続の問題である。

この事例から得られる示唆は、第一に、十分な対策をしていても侵入され得ること、第二に、境界機器や拠点ネットワーク機器は常に入口になり得ること、第三に、侵入後の内部偵察と横展開を早期に検知できなければ被害が大きくなること、第四に、復旧とは「システムを起動すること」ではなく「安全に業務・診療を再開できる状態に戻すこと」である。

■医療機関の被害事例：病院規模に関係なく診療が止まる

医療機関におけるランサムウェア被害は、国内外で継続している。2017 年の英国 NHS に対する WannaCry 攻撃では、少なくとも 6,912 件の予約キャンセルが確認され、全体では 19,000 件超の予約がキャンセルされたと推計されている（引用元名：National Audit Office「Investigation: WannaCry cyber attack and the NHS」：URL：https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/）。

これは、サイバー攻撃が患者の受診機会や手術予定に直接影響することを示した象徴的事例である。

国内では、2021 年の徳島県つるぎ町立半田病院、2022 年の大阪急性期・総合医療センター、2024 年の岡山県精神科医療センターなどの事例がある。大阪急性期・総合医療センターでは、給食事業者側の VPN 機器の脆弱性を契機に侵入が発生し、給食事業者内の探索、認証情報の窃取、病院給食サーバへの侵入を経て、院内システムへ被害が拡大した（引用元名：大阪急性期・総合医療センター「情報セキュリティインシデント調査報告書 概要」：URL：https://www.gh.opho.jp/pdf/reportgaiyo_v01.pdf)。

同センターの調査報告書では、この事案により地域医療における病院の役割のかなりの部分を果たせない状況に陥り、患者や地域に大きな影響を及ぼしたと総括されている（引用元名：大阪急性期・総合医療センター「調査報告書」：URL：https://www.gh.opho.jp/pdf/report_v01.pdf)。

この記載は、サイバー攻撃が一病院内部の問題ではなく、地域医療提供体制全体に波及する問題であることを明確に示している。

また、2024 年の岡山県精神科医療センターの事例では、電子カルテを含む院内情報システムが暗号化され、紙カルテ運用への切替を余儀なくされた。さらに、患者情報流出の可能性が公表され、診療継続と個人情報対応の双方が課題となった。IT-BCP 資料では、この事例を通じて、攻撃が発覚する前から外部侵入や内部偵察が始まっていた可能性、認証基盤へのアクセス痕跡、紙運用の限界、VPN 脆弱性対応の遅れ、人材・コスト不足という構造的問題が整理した。

海外では、2024 年の Synnovis への攻撃により、英国 NHS の複数施設で病理検査サービスが停止し、外来や手術、輸血、救急診療に影響が生じた。英国政府の声明では、Synnovis 事案により 11,000 件超の外来および予定処置に遅延が生じたことが示されている（引用元名：UK Parliament Written Statement「Cyber Security and Resilience」：URL：https://questions-statements.parliament.uk/written-statements/detail/2025-11-12/hcws1046)。

これらの事例から、サイバー攻撃は病院規模に関係なく発生し得ること、また病院本体だけでなく、給食、検査、請求、物流、保守、委託先などの外部基盤が停止しても診療全体に影響することが明らかとなった。

3. 攻撃の見取り図

■ランサムウェアは「突然暗号化するウイルス」ではない

本年度の検討では、ランサムウェア攻撃を侵入や内部偵察、権限奪取、横展開、暗号化・情報窃取、診療停止、説明・復旧対応という一連のプロセスとして整理した。

従来、ランサムウェアは、端末に感染してファイルを暗号化し、身代金を要求するウイルスとして理解されることが多かった。しかし、現在の攻撃では、攻撃者はまず VPN、リモート保守、委託先接続、メール、認証情報、公開サーバ等から侵入す

る。その後、院内ネットワークを探索し、Active Directory 等の認証基盤、ファイルサーバ、バックアップ、電子カルテ関連サーバを把握する。最終的に、被害が最大化する時点で一斉に暗号化し、同時に情報窃取を行う。

このため、発覚時点では攻撃は既に最終段階にあることが多い。被害を小さくするには、暗号化が始まってから対応するのでは遅い。内部偵察や横展開の段階で異常を検知し、切り離し判断を行うことが重要である。

■攻撃経路の類型

医療機関において特に重要な攻撃経路は、VPN・リモート接続機器、メール、委託先・関連組織、認証情報、脆弱な公開サーバ・古い OS 端末である。

VPN やリモート接続機器は、医療機器や部門システムの保守に不可欠である一方、攻撃者にとっては正式な入口になり得る。特に、古い VPN 機器、脆弱性未修正、MFA 未導入、共有 ID、委託先用 ID の放置は重大なリスクである。

メールは、標的型攻撃やフィッシングの入口である。医師、看護師、事務職、委託先担当者は多忙であり、「注意する」だけでは対策にならない。教育は必要であるが、それだけでなく、MFA、Web 分離、添付ファイル対策、認証情報保護が必要である。

委託先・関連組織経由の侵入も重要である。大阪急性期・総合医療センターの事例が示すように、病院本体ではなく委託先の VPN やサーバが起点となることがある。医療機関は多くの外部事業者に依存しているため、契約、責任分界、接続管理、ログ監査、MFA、最小権限化が不可欠である。

認証情報の漏えい・使い回しも大きなリスクである。退職者アカウント、異動者アカウント、共有 ID、過剰な管理者権限、過去に漏えいしたパスワードの再利用は、攻撃者にとって有効な入口となる。特に認証基盤を奪われると、院内全体に横展開される。

脆弱な公開サーバや古い OS 端末も、医療機関特有の課題である。医療機器に接続された端末、検査装置付属 PC、更新できない OS、停止できないサーバは、EDR を導入できない場合がある。そのため、ネットワーク側での監視や Decoy による検知が重要となる。

4.　情報部門の優先順位の再定義

本年度の検討では、病院情報部門の役割を「情報システムを守る部門」から「診療継続を支える部門」へ再定義する必要があると考えた。

IT-BCP 資料では、サイバーセキュリティ対策を、止めない、戻す、説明する、の三つに整理した。止めないとは、入口を減らし、権限を守り、例外を減らし、検知し、地域医療への影響を抑えることである。戻すとは、隔離バックアップ、復元訓練、復旧優先順位、協力関係の構築により、診療を再開できる状態へ戻すことである。説明するとは、意思決定、報告・公表、証拠保全、再発防止を含むガバナンスである。

ここで重要なのは、サイバーセキュリティは情報部門だけで完結しないことである。切り離し判断、診療制限、救急受入停

止、患者説明、行政報告、報道対応、委託先対応は、病院長、CIO、医療安全、広報、法務、診療部門、地域連携部門が関わる経営判断である。

したがって、初動時には誰が判断し、誰に連絡し、どの時点でネットワークを切り離し、どの診療機能を残すかを事前に決める必要がある。

5. 早期発見手段としての Decoy

■EDR、NDR、Decoy の比較

本年度は、侵入後の早期発見手段として、EDR、NDR、Decoy の特性を比較した。

EDR は、端末やサーバにエージェントを導入し、不審な挙動を検知して封じ込めや調査を行う技術である。端末ごとの詳細な原因分析に有用であるが、医療機器、古い OS 端末、ベンダー管理端末にはエージェントを導入できない場合がある。また、端末数に応じて費用が増える。

NDR は、ネットワーク通信の振る舞いを監視する技術である。端末にエージェントを入れにくい環境でも利用できるが、通信量、監視範囲、ログ分析体制に応じた設計が必要である。

Decoy は、攻撃者を偽の資産に誘導し、通常業務では発生しないアクセスを検知するディセプション技術である。PPT 資料では、Decoy は「攻撃の入念な準備と事前調査段階でおとりに引っかける」技術であり、費用は端末数ではなく設置セグメント数に依存し、医療機器への対応も可能と整理されている。

Decoy は、ランサムウェアを完全に防ぐ技術ではない。しかし、攻撃者が内部偵察や横展開を行う段階で接触しやすい偽サーバ、偽フォルダ、偽認証情報を配置することで、暗号化が始まる前に異常を検知できる可能性がある。医療機関においては、この「早く気づく」ことが被害範囲を限定し、診療継続につながる。

■Decoy を地域で共同利用する合理性

Decoy を個別病院ごとに導入する場合、人材、費用、運用負担が課題となる。そこで本研究では、MMWIN のような地域医療連携ネットワーク上で Decoy を共同利用する構成を検討した。

IT-BCP 資料では、地域医療連携システムの新たな価値として、サイバーセキュリティ対策、人材不足・コスト問題、AI 利用の高まり、サイバー攻撃の高度化に対して、共通利用リソース化、コスト削減、人材共有化、AI の安心安全利用、共通基盤の創出、すなわち「見張り番」としての社会実装が示されている。

図 1　地域医療ネットワークシステムの見張り番を参照

図 2　decoy の配置図を参照

この構成では、地域連携ネットワーク側に Decoy 管理機能を集約し、参加医療機関に対して監視セグメントを設定する。検知ログは中央管理され、異常発生時には各施設へ通知される。これにより、個別施設が高度なセキュリティ人材や 24 時間監視体制を持たなくても、地域単位で早期検知を実現できる可能性がある。

特に中小病院や診療所では、EDR や SOC を単独で導入することは費用面・人材面で

困難である。Decoy を地域で共同利用すれば、1 施設あたりの負担を抑えつつ、攻撃の初期兆候を検知できる。これは、医療機関の構造的課題に整合した現実的な対策である。

6. 仮想ブラウザによるクラウド型 AI 利用環境

クラウド型医療 AI を診療現場で利用するためには、電子カルテ端末や診療端末から安全にクラウドサービスへ接続する必要がある。しかし、電子カルテ端末を直接インターネットへ接続することは、マルウェア感染、フィッシング、情報漏えい、認証情報窃取のリスクを増大させる。

従来の電子カルテ環境は、院内ネットワークを信頼領域とする境界型防御を前提としている。一方、クラウド型 AI は外部クラウド利用を前提とするため、ゼロトラストの考え方が必要となる。現場では、1 台の端末で電子カルテを操作しながら、同時に診療記録作成 AI、問診 AI、PHR 連携、画像解析 AI 等を使いたいという要請がある。したがって、同一端末上でトラストゾーンとゼロトラストゾーンを両立する設計が必要である。

本研究では、その手段として仮想ブラウザを検討した。仮想ブラウザは、Web コンテンツやクラウドサービスの処理を端末上で直接実行せず、仮想環境側で処理し、その表示結果のみを端末へ転送する技術である。これにより、外部 Web サイト由来のスクリプトやファイルが電子カルテ端末へ直接到達するリスクを低減できる。

前年度までに、東北大学病院では、仮想ブラウザを用いて、電子カルテ端末内でトラストゾーンとゼロトラストゾーンを両立させる試験を行った。その結果、クラウド上の AI サービスを利用しながら、端末の動作に大きな影響を与えず、データの受け渡しが可能であることを確認した。

本年度は、これを MMWIN 上で共同提供する構成として実証した。地域医療連携ネットワーク側に仮想ブラウザ基盤を設置すれば、参加医療機関は個別に複雑なゼロトラスト環境を構築しなくても、安全な外部接続経路を利用できる。これにより、クラウド型医療 AI を導入する際の技術的・心理的障壁を下げることができる。

7. IT-BCP の本質

本年度の検討では、IT-BCP を「復旧手順書」ではなく「縮退運転の設計図」として位置づけた。

ランサムウェア被害が発生した場合、多くの医療機関では紙カルテ運用に切り替える。しかし、紙運用は数日程度の応急対応としては有効であっても、数週間単位では医療安全上のリスクが増加する。検査結果、薬剤禁忌、アレルギー、重複投薬、手術予定、入退院調整、会計、紹介状など、多くの業務が電子システムを前提としているためである。

したがって、IT-BCP で検討すべきことは、「紙カルテを準備しているか」ではなく、「どの診療機能を残すか」「どのシステムを優先復旧するか」「どの患者を受け入れるか」「どの患者を他院へ紹介するか」「検査・薬剤・手術をどう優先するか」「地域内でどのように機能を補完するか」である。

IT-BCP 資料では、IT-BCP について、1 病院の停止が地域の需給バランスを崩し、救急受入制限、紹介・検査・画像連携の停滞、周辺病院への負荷集中を引き起こすと整理した。大学病院は地域医療の防波堤として、地域全体の縮退運転を考える責務がある。

また、IT-BCP は作成するだけでは機能しない。訓練を行い、振り返り、ナレッジを更新し、関係者間で共有する必要がある。本研究では、訓練や振り返りに AI を活用し、評価支援やナレッジ整理を行う可能性も検討した。これらを地域医療連携ネットワーク上で共有すれば、地域全体の対応力を底上げできる。

8. 前年度アンケート結果との接続

これまで宮城県内の医療施設 1,753 施設を対象に WEB アンケートを実施し、330 施設から回答を得た。有効回答施設数は 322 施設であった。回答施設の多くはクリニックであり、施設規模別にセキュリティ意識、地域医療連携システムへの期待、リモート保守、クラウドバックアップ、AI 利用、安全な情報共有に関する分析を行った。

その結果、地域医療連携システムには、従来の情報共有機能だけでなく、紹介・逆紹介、診療予約、クラウドバックアップ、ランサムウェア対策、災害時の情報共有、AI 診断支援、カルテ作成支援、安全な情報共有への期待があることが示された。

また、セキュリティ人材不足を感じる施設ほど、自施設のセキュリティ対策への満足度が低い傾向が認められた。施設規模そのものよりも、セキュリティ意識や人材不足の状況が、新技術導入への関心に影響していることが示唆された。

本年度の成果は、これまでの調査を実装面へ進めたものである。すなわち、これまでの調査・検討で明らかになった「ランサムウェア対策」「クラウドバックアップ」「AI 利用」「安全な情報共有」「セキュリティ人材不足への対応」というニーズに対し、本年度は Decoy、仮想ブラウザ、IT-BCP、ナレッジ共有、地域共同運用という具体的なアーキテクチャーを提示した。

9. 地域医療連携ネットワークの新たな価値

本年度の最も重要な結論は、地域医療連携ネットワークを、従来の「診療情報共有のための仕組み」から、「地域医療を守る共通基盤」へ再定義すべきであるという点である。

地域医療連携ネットワークは、既に多くの医療機関を接続している。これまでは、画像、検査結果、薬歴、病名、紹介・逆紹介などの情報共有が主な目的であった。しかし現在、医療機関は、医療 DX、クラウド型 AI、サイバー攻撃、人材不足、コスト制約、災害対応、地域医療逼迫という複数の課題に同時に直面している。

この状況では、一病院がすべてを自力で解決することは困難である。特に中小病院や診療所では、セキュリティ専門人材、24 時間監視、EDR/NDR、SOC、ゼロトラスト環境、復旧訓練、AI 利用基盤を単独で整備することは現実的ではない。

そこで、地域医療連携ネットワークを活用し、Decoy による侵入早期検知、仮想ブラウザによる安全なクラウド型 AI 利用、

IT-BCP 訓練とナレッジ共有、初動対応手順の標準化、監視ログの中央管理、地域内患者受入調整、AI サービスの安全な共同利用を行うことが有効である。

IT-BCP 資料では、地域医療連携ネットワークの新たな価値として、共通利用リソース化、コスト削減、人材共有化、AI の安心安全利用、共通基盤の創出、見張り番としての社会実装が整理した。

図 3　教育だけでは解決しないを参照

10. 政策提言としての位置づけ

本研究で示した地域医療連携ネットワークの活用は、日本医師会医療 IT 委員会における「医療 DX を適切に推進するための医師会の役割」に関する答申検討においても、地域医療情報連携ネットワーク活用の好事例として紹介すべきとの評価を受けた。これは本研究成果が単なる技術実証ではなく、政策的議論に接続したことを意味する。

クラウド型医療 AI を普及させるためには、AI サービスの性能向上だけでは不十分である。医療機関が安心して接続し、患者情報を安全に扱い、サイバー攻撃時にも診療を継続し、説明責任を果たせる基盤が必要である。

その意味で地域医療連携ネットワークを AI 利用やサイバーセキュリティ、IT-BCP、地域医療継続を支える共通基盤として再活性化することは、医療 DX を現実に進めるための政策的方向性の選択肢のひとつとなりうる。

11. まとめ

本年度の研究により、以下の点が明らかとなった。

第一に、サイバー攻撃は情報システムの障害ではなく、診療継続性の危機である。アサヒグループの事例が示すように、サイバー攻撃は事業の根幹を停止させる。医療機関では、それが電子カルテ停止、検査遅延、手術延期、救急受入制限、地域医療への波及として現れる。

第二に、現在のランサムウェア攻撃は、侵入後に内部偵察、権限奪取、横展開、バックアップ侵害、情報窃取を行う。そのため、侵入を完全に防ぐだけでは不十分であり、侵入後の早期検知が重要である。

第三に、Decoy は、医療機器や既存端末に大きな変更を加えずに、内部偵察段階で攻撃を検知できる可能性がある。EDR や NDR に比べて、医療機関の制約に適合しやすく、地域医療連携ネットワーク上で共同利用することで費用対効果を高められる。

第四に、仮想ブラウザは、電子カルテ端末からクラウド型 AI を安全に利用するための現実的な手段である。トラストゾーンとゼロトラストゾーンを両立させることで、クラウド型医療 AI 利用に伴う外部接続リスクを低減できる。

第五に、IT-BCP は復旧手順書ではなく、縮退運転の設計図である。紙運用だけでは長期障害に耐えられないため、復旧優先順位、代替診療、地域内連携、訓練、ナレッジ共有が必要である。

第六に、地域医療連携ネットワークは、情報共有の仕組みから、地域医療を守る共通基盤へ発展し得る。人材不足、コスト不足、サイバーリスク、医療 DX、クラウド型 AI 利用という複数の課題に対し、地域

で共同利用、共同監視、共同訓練を行うことは、現実的かつ実効性の高い方策である。

以上より、クラウド型医療 AI の促進には、AI サービスの性能向上だけでなく、医療機関が安心して接続し、利用し、止まっても診療を続け、地域で支え合うためのネットワークアーキテクチャーが不可欠である。本研究は、MMWIN を活用した検討を通じ、地域医療連携ネットワークが「地域の見張り番」となり、クラウド型医療 AI の安全な社会実装を支える基盤となり得ることを示した。

D. 健康危惧情報

代表者報告書で適時記載

E. 研究発表

- 報告書
  - ① 地域連携システムをベースにしたゼロトラストセキュリティの実現性の検討：ネットワークアーキテクチャーの検討(本報告書)

- **学会発表**
  - ① 藤井進;野中小百合;川本章太;中村直毅,医療機関の人材不足とセキュリティ課題への対応：地域連携ネットワークを活用した実装可能な対策モデルの検討,医療情報学連合大会論文集,45,,2025-11-15
  - ② 中村直毅;金子誠暁;野中小百合;川本章太;藤井進,地域医療連携ネットワークにおけるサイバーセキュリティ対策：仮想ブラウザと集中管理型デコイシステムを統合した多層防御アーキテクチャーの設計と実装,医療情報学連合大会論文集,45,,2025-11-15
  - ③ 藤井進,次世代医療基盤法の実装と展開：データ精度検証・地域連携・AI 活用による利活用の最前線,第 45 回医療情報学連合大会 日程表・プログラム,,,2025-11-15
  - ④ 中村直毅;藤井進;桜澤邦男;大田秀揮;張替秀郎,地域医療連携システムにおけるデータ利活用の取り組み～治験での活用を見据えて～,医療情報学連合大会論文集,45,,2025-11-15
  - ⑤ 藤井進,地域医療情報連携ネットワークの新しい使い方,令和 7 年度日本医師会医療情報システム協議会 抄録集,,13-14,2026-03-08

- **提言、その他**
  - ① 医療 IT 委員会の答申検討において、本研究分担者の発表が地域医療連携ネットワークの好事例として評価され、答申への反映が提案された。

F. 知的財産権の出願

- なし

資料　大学病院を核とした地域医療ネットワークの高度化と安全な運用

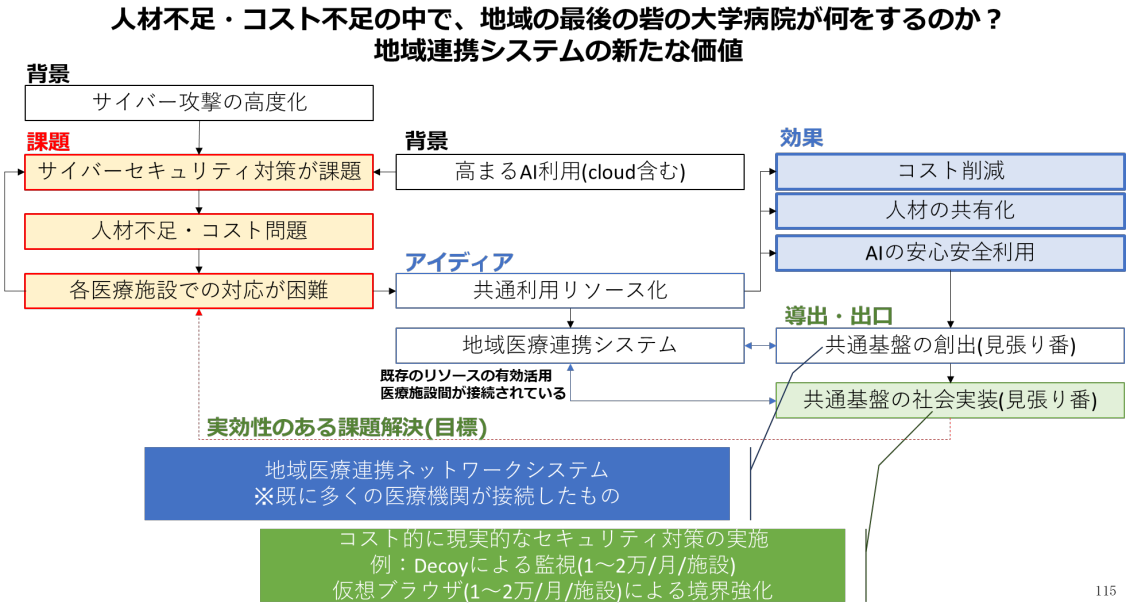


図１　地域医療ネットワークシステムの見張り番を参照

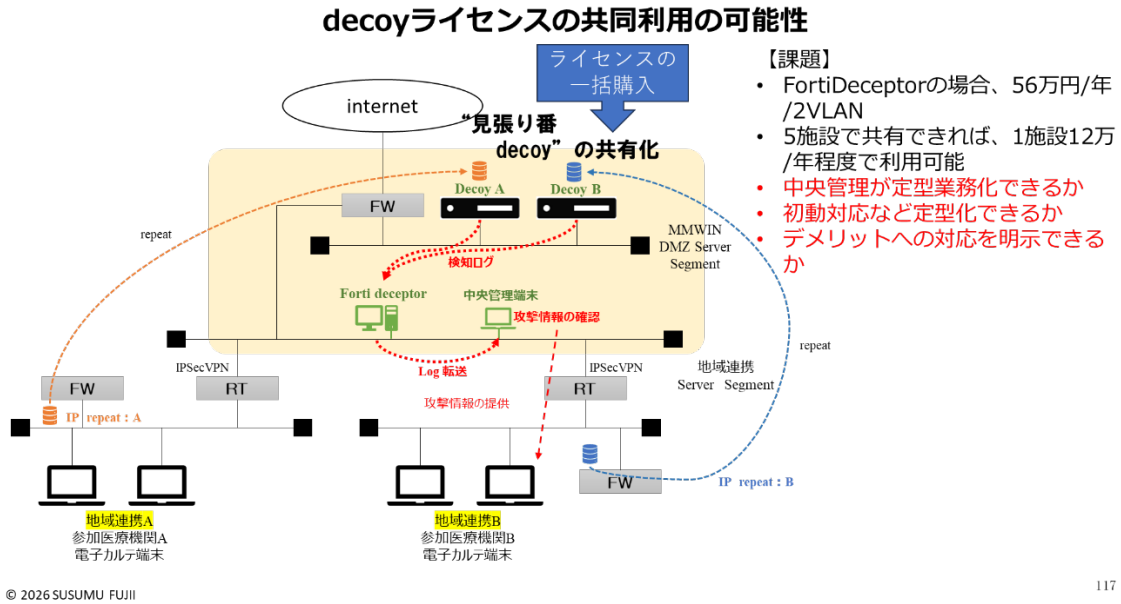


図２　decoy の配置図を参照

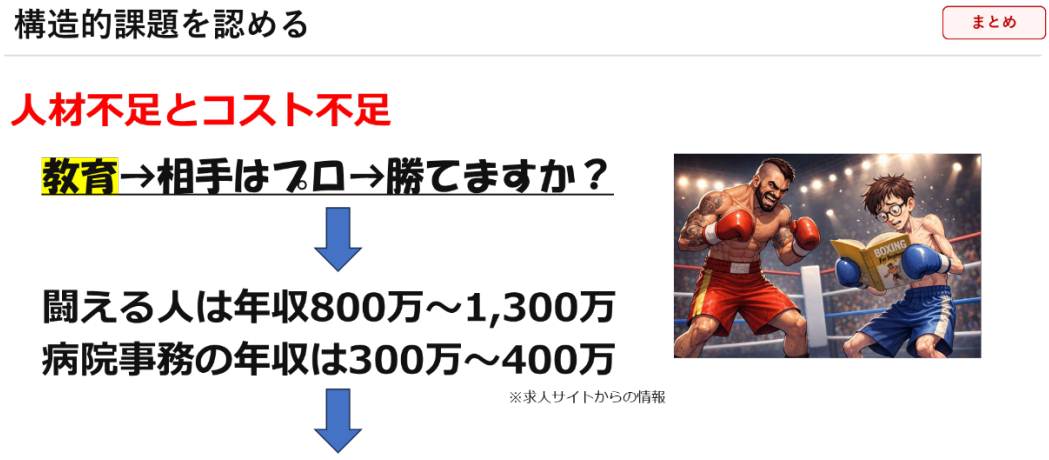


図３　教育だけでは解決しないを参照

別紙 3

厚生労働科学研究費補助金
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
クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言

研究分担者　金子 誠暁　医療 AI プラットフォーム技術研究組合及びシステム WG リーダ

研究要旨

医療従事者と医療AIとの協調は、医療従事者の働き方改革の実現や医療の均てん化には重要である。質の高い医療データに基づいて開発された医療AIサービスが次々に生まれ、幅広い医療機関で利用されるためには、利用しやすい価格とクラウドの利用が不可欠である。本研究では、医療機関の特性によって、費用対効果も意識した具体的なネットワーク構成やセキュリティ監査の方法を示すことにより、医療機関が安全・安心にクラウド環境上の医療AIサービスを利用できるためのルール策定を目的とした。

医療機関のセキュリティ対策の現状を理解するために、23医療機関に対面でヒアリングを実施した。ヒアリング内容をもとにネットワークの類型化をJASO TP-15002を活用し、脅威・リスクを整理した。

脅威・リスクをもとに、最新クラウドセキュリティに関する整理を行い、現状の医療機関のセキュリティをもとにクラウド利用に発展した際の対策を机上で整理した。
2024～2025 年度は医療機関から外部接続するユースケースを整理し、あわせてベンダ目線・ディラー目線のヒアリングも実施した。

A. 研究目的

2023年度は国内医療機関へのヒアリングを実行し医療機関の類型化案を策定し、類型化に基づいて、医療機関が外部ネットワークに出る際に、国内外の最先端セキュリティ技術を探索し、機能評価を行う。その結果、医療機関の特性によって、費用対効果も意識した具体的なネットワーク構成を示した。

2024年度は、2023年度の成果をもとに、医療機関から外部接続するユースケースを整理し、クラウド利用における課題点等を抽出した。

2025 年度は、2024 年度に残として残っていたユースケース 2 の評価の実施、ならびに医療機関に対してメンテンナンスを行っているベンダ及び医療機関に対して機器等を販売しているディラーを含めて幅広くヒアリングを実施した。

B. 研究方法

医療機関から外部接続するユースケースを選定し、該医療機関へ実態調査のためのヒアリングを実施した。

またベンダおよびディラーへヒアリングを実施した。

C. 研究結果

（1）ユースケースは以下の5パターンを選定した。

No1,4,5 は実際国内医療機関にて稼働させているベンダ様へヒアリングを実施した。

No2,3 はネットワークアーキテクチャグループの東北大藤井先生・中村先生にご協力いただき、PoC 環境を準備し評価を実施した。

① ユースケース1：医療機関側で新たなネットワークやシステムの新設工事負担なしに、既設のネットワーク・システムを利用して、医療AIプラットフォーム技術研究組合（Healthcare AI Platform Collaborative Innovation Partnership 、略称「HAIP」）に搭載されている医療AIを活用できるかを、株式会社ソフトウェア・サービス(略称SSI)と恵寿総合病院の協力を得て実証を行っている内容のヒアリングを行った。

医療機関にとってのメリットは以下である。

- 既設のネットワークを利用することでシステム利用のための機器購入等のコスト負荷がかからない。
- 電子カルテベンダーは、既設のネットワークを利用することで、医療機関側と導入調整がしやすい。
- 医師は、電子カルテ側の環境に機能を追加するため、医療従事者側の操作に影響がない。
- 医師は、AIサービスを利用することで、異変の見落とし防止や、業務の効率化できた。

② ユースケース 2：各医療機関が AI を活用する場合に課題となるシステムの導入コスト負荷を抑えるために、地域医療連携システムを経由し、HAIP の基盤に搭載されている AI に接続できるかを、東北大学病院の協力を得て実証を行った。

③ ユースケース3：AIの利用形態の1つとしてクラウド上にある音声AIの活用や電子カルテ端末によるWeb会議の利用を検討しており、端末側マイクデバイスで利用できる新しいインターネット分離ソリューションであるRevoWorks Browser(ジェイズ・コミュニケーション株式会社製品)を試験的に利用し、音声AIの活用やWeb会議が利用可能か東北大学病院様の協力を得て実証を行った。

医療機関にとってのメリットは以下である。

- 既電子カルテ端末がインターネットに接続できる為、別途インターネットに接続可能な端末を用意する必要がなくコストの削減が可能。
- 端末側のマイクデバイスを利用できるため、電子カルテ端末で音声 AI・Web 会議の利用もでき、医師の働き方改革に活用できる可能性がある。
- インターネット分離製品のため、セキュアにインターネットに接続できる。（ローカルコンテナ技術を利用しているため、万が一感染しても、端末のローカルデータに影響を及ぼさない）

但し、システムを導入するためのネットワーク変更・機器の導入コストが多くかかるデメリットもある。

④ ユースケース 4：医師の働き方改革制度に伴い、これまで院内利用のみが主体であった電子カルテシステムに、医師が院外からセキュアにアクセスできる仕組みが必要になることが想定される。院外からセキュアに電子カルテシステムへアクセスできる仕組みについて、既にリモートデスクトップサービス(略 RDP)を活用しているケースをヒアリングした。

医療機関のメリットとしては、併設のクリニックや外出先から電子カルテシステムにアクセスすることで、往診や緊急時のテレワーク等が可能になり、医師の働き方改革につながる可能性がある一方、サービス導入のコストとしてはネットワーク環境を用意するため割高になる。

- 常時 3Mbps の回線を保有可能なネットワークを用意する必要がある。
- クリニック⇔本院等医療機関を接続するための VPN または、閉域網を用意する必要がある。
- 外出先から医療機関のネットワークに接続するための、端末および VPN 装置、閉域網が必要となる。

⑤ ユースケース5：離島やへき地における医療の地域差を縮め、医療の質の向上や患者の利便性の

向上のため、徳洲会グループ採用しているボーダレス・ビジョン株式会社、天馬諮問株式会社の2社へヒアリングを行った。
医療機関にとってのメリットは以下である。

- 遠隔で医師と医師がつながることで、専門的な意識を持った医師の支援を受けながら、離島・へき地の医師が手術を行うことができる。
- ⇒患者も離島から本土に移動することなく、手術を受けられるため、移動等患者の負担も軽減できる。
- 教育ツールとして利用することで、離島・へき地の医師に対し、本土の医師が指導することができ、意思の技術力向上にもつながる。
- オンライン診療にも利用可能であり、遠方にいる患者の診察・診断ができる。
- 救急時に、専門外の患者に対して、専門医の支援をうけることができる。
- 既存でインターネットに接続可能な端末があれば、別途専用機器を用意することなくシステムの利用が可能(手術支援のための専用機器が必要な場合を除く)
- HIS系のネットワークに接続する必要がないため、重要ネットワークに影響なく導入が可能である。

但し、サービス導入のため、機材の購入が必要なことがある。

ユースケース導入難易度は以下と評価。
＜＜難易度：高＞＞
　実証システムを利用するためにネットワークの大幅な変更や新設・または機器の調達が必要となる。セキュリティポリシーにより実証システムを導入することが難しい
＜＜難易度：中＞＞
　既設ネットワークの軽微な変更、または機器の調達が必要となるが、実証システムの利用が可能
＜＜難易度：低＞＞
　既設ネットワークの変更が少ない、または設定変更なく実証システムの利用が可能
それら難易度をユースケースに当てはめると、

ユースケース	難易度
No1	低
No2	高
No3	高
No4	低
No5	高または中

であった。

（2） 医療機関への保守業務に関するベンダヒアリングの結果として、以下総括。
本ヒアリングの結果、ベンダ各社においては、医療機関向けリモート保守に関するセキュリティ対策や運用体制について、一定のルールや管理のもとで実施されていることが確認された。
一方で、セキュリティチェックリストや3省2ガイドラインの運用に関しては、医療機器と一般的な医療情報システムとの特性の違いにより、現場での対応や判断が難しい場面があるとの意見も挙げられた。また、医療機関ごとに異なる運用ルールやチェックリスト対応、ガイドラインの解釈差などにより、ベンダ側・医療機関側双方に一定の対応負担が生じているとの指摘もあった。
そのため、医療機器の特性を踏まえたリスクベースでの運用や、チェックリスト・ガイドラインの解釈の明確化、関係者間での共通理解の促進が今後の課題として示唆された。
3省2ガイドラインについて、ベンダ側の視点から、業務運用上で感じている課題や支障の有無について以下に整理する。
① 医療機器の特性を踏まえたガイドライン適用の必要性
医療機器は装置の種類や用途により扱う情報や業務内容が大きく異なるが、現行のガイドラインではその違いが十分に考慮されていないとの意見があった。また、電子カルテ等の情報システムと同一の基準で要求されることで、実運用との乖離が生じる場合があるとの指摘があった。
② リスクベースの運用への見直し
現在はチェックリスト形式での対応が中心となっているが、本来のリスクマネジメントの考え方に基づいた運用ができるよう、よりリスクベースの内容に見直すことが望ましいとの意見があった。
③ 医療機器運用とセキュリティ対策のバランス
医療機器では装置の安定稼働や正確な検査結果の提供が重要であり、過度なセキュリティ対策が装置の動作や検査精度に影響を与える可能性があるため、機器特性を考慮した対策が必要との意見があった。
④ ガイドラインの適用範囲や解釈の分かりにくさ
ガイドラインの適用対象や参照すべき資料が多く、医療機関や事業者間で解釈に差が生じる場合があるため、省庁横断での整理や分かりやすい解説の提供を望む声があった。
⑤ 医療機関との理解差による対応負担
ガイドラインに基づくリスク説明やチェックリスト対応において、医療機関側の理解度に差があり、説明

や調整に時間を要するケースがあるとの意見があった。
⑥ 運用管理に伴う負担
ガイドラインの要求事項が網羅的であるため、自社の規程や運用手順と紐づけて継続的に管理・更新していく作業に一定の工数を要するとの意見があった。

（3） ディラーへのヒアリング結果としては以下に示された。
3 省 2GL やサイバーセキュリティリストを知らない。セキュリティの商材を提案したことがない。サイバーセキュリティについて相談を受けることもほぼない。という結果が出た。つまり、ディラーはセキュリティへの意識は少なく、医療機関からも求められていない現状が見て取れた。

（4） ネットワークセキュリティ対策の代表的なソリューション調査を 2023 年度～2025 年度に実施した。
- アカウント層：ソリューション
  - IAM（権限のきめ細かな設定や、パスワードポリシー強制など含む認証基盤）
  - PAM（特権管理）
  - IGA（ID ライフサイクル管理）
- エンドポイント層：
  - EDR（PC やサーバにおけるウィルス等の不審な挙動を検知・対応）
  - UEM（デバイス設定、アプリケーション管理、セキュリティポリシー適用）
- ネットワーク層：
  - SASE（SSE、SD-WAN 含むネットワーク＆セキュリティ統合サービス）
- 監視・検知層：
  - EDR（PC やサーバにおけるウィルス等の不審な挙動を検知・対応）
  - XDR（エンドポイント、ネットワークなど広範囲に渡りウィルス等の不審な挙動を検知・対応）
  - SIEM（ネットワーク機器や各種ソフトウェアが生成するイベント情報の統合管理）、NDR（ネットワークトラフィックを分析し攻撃や不正の兆候を可視化・検知）

以上を選定し、クラウドセキュリティ技術の机上調査を行った。今年度は一部調査を追加し、また 2023 年度からのピックアップソリューションが ISMAP の登録状況等確認を行った。

D. 考察

複数のユースケースをヒアリング・実証した結果、医療機関が医療 AI やシステムを利用する場合、以下の効果が考えられる。
- 医療機関の既設のネットワーク・システム設備や地域医療連携システムを活用することで、病院側の費用・運用変更の負担を抑え医療 AI を推進できる
- 遠隔医療のための IT ソリューションを活用することで離島やへき地における医療の地域差を縮めることを可能とし、医療の質の向上や患者の利便性の向上に有効。
- クラウド上の医療 AI の利用による医療の質、業務の効率化が期待できる。
- 外出先や自宅など医療機関外から電子カルテ等の情報を閲覧可能とする事例が増えてきている。今後の需要次第では働き方改革につながることが期待できる

また、ユースケースを実施する中で医療機関が安全・安心にデジタル技術を活用するための課題も見えてきた。
- 医療機関によってことなるセキュリティレベル
  - 医療機関によっては、セキュリティ方針により電子カルテ端末など HIS 系の情報をインターネット側に接続できない。
  - クラウド上の医療 AI を利用するには、医療機関のネットワークをインターネットに接続する場合もある。そのため外部からの攻撃に備えたセキュリティ対策も必要である。
  - 各医療機関が理想的なセキュリティ状態を維持するためには、セキュリティ有識者の協力やセキュリティ製品の導入コストも必要となる。
  - 医療機関ごとに異なるネットワーク・システム構成
  - 既設のネットワークを利用して医療 AI を利用可能な医療機関も、ネットワーク帯域量によっては利用できない、または帯域量の変更が必要となる場合がある。
  - 医療機関のネットワーク構成によっては、医療 AI や IT ソリューションを導入するために、大幅なネットワーク構成の変更や機器の導入が必要な場合がある。
  - IT ソリューションによっては、端末に標準搭載されているサービスで利用可のであるが、製品によっては専用ソフトウェアを導入する必要があり、端末の他ソフトウェアとの互換性も考える必要がある。

E. 結論

医療機関・ベンダ・ディーラそれぞれの立場からアンケートを取得した結果、医療機関においては以下の課題があると考える。
・保守メンテナンス用の回線がベンダ各々あるため、セキュリティが不十分になりがちである。
・クラウドサービスの利用が停滞しており、情報の未活用の部分が多分にある。
・医療情報を扱うシステム担当者が不足しており、従事者の業務負担が増大している。
・医療にかかわるものがみなガイドラインを理解しているとは限らない。また、ガイドラインの適用対象や参照すべき資料が多く、医療機関や事業者間で解釈に差が生じている。
・既存の境界防御型のみでは、ランサムウェアからは守れない。
課題への対策として、
・医療機関からの外接点のネットワーク集約
・既存の設備や技術を活用しながら、セキュアなネットワークインフラを構成し医療 DX を支えること
・VPN＋αの新しい技術の活用をガイドラインとして導入可とする取り組み
・ガイドラインの解釈に差が出ないよう、省庁横断での整理や分かりやすい解説の提供
これらの取り組みを行うことでよりAI等のクラウド利用が促進するものと考える。

F. 研究発表

該当なし

G. 知的財産権の出願・登録状況

1. 特許取得　　特許取得予定なし
2. 実用新案登録　現時点で該当なし
3. その他　該当なし

資料　医療機関から外部接続するユースケースの整理

No	ユースケース名	ユースケースの目的や背景	本ステップにおける実証可否	実証協力病院	備考
1	医療機関の既設ネットワークを利用したAIサービスの活用	病院に新たな工事負担なしに、既設ネットワークを利用し、クラウド上の医療AIサービスを活用できるか実証が行われていたため、その内容をレポートとしてまとめ、他病院でも活用できるかを検討する。	未実証 既に実証が行われていたため、その内容をヒアリングしレポートに記載 実証期間 2024/5-2024/8	恵寿総合病院 病床数426床	利用技術・製品 • IP-VPN • インターネットVPN
2	地域医療連携システムを介したセキュアなインターネットの利用	各医療機関が医療AIの活用する場合に課題となるシステムの導入コスト負荷を抑えるため、地域医療連携システムを活用し、医療AIの利用が可能かを検証する。	実証済み 実証期間:2025/3	東北大病院 病床数1,160	利用技術・製品 • CATOクラウド • Azure
3	インターネット分離システムを利用したWeb会議および、音声AIサービスの活用	医療AIの利用形態の1つとしてクラウド上にある音声AIの活用を検討しており、端末側マイクデバイスで利用できる新しいインターネット分離ソリューションを試験的に利用し、音声AIの活用やWeb会議が利用可能かを検証する。	実証済み 実証期間: 2024/8~2025/3	東北大病院 病床数1,160	利用技術・製品 • RevoWorksBrowser 導入実績 • 複数病院に導入実績あり(総数非公開)
4	医師が院外からセキュアにアクセス可能なシステムを利用した電子カルテシステムの活用	医師の働き方改革制度に伴い、これまで院内利用のみが主体であった電子カルテシステムを、医師が院外からセキュアにアクセスできる仕組みも必要になることが想定され、 院外からセキュアに電子カルテシステムへアクセスできる仕組みについて検討する。	未実証 既に製品として実運用が行われているため、その内容をヒアリングしレポートに記載	-	利用技術・製品 • RDP • IP-VPN • インターネットVPN
5	遠隔医療システムを活用した手術支援実施	離島やへき地における医療の地域差を縮め、医療の質の向上や患者の利便性の向上のため、遠隔医療の実証を徳洲会が実証していたため、その内容をレポートとしてまとめ、他病院でも活用できるかを検討する。	未実証 既に実証が行われていたため、その内容をヒアリングしレポートに記載	-	5-1 利用技術・製品 • kizunaWeb • 導入実績：15病院以上 5-2 利用技術・製品 • TELEPRO • 導入実績：病院・大学含む15施設以上

図１　医療機関から外部接続するユースケース一覧

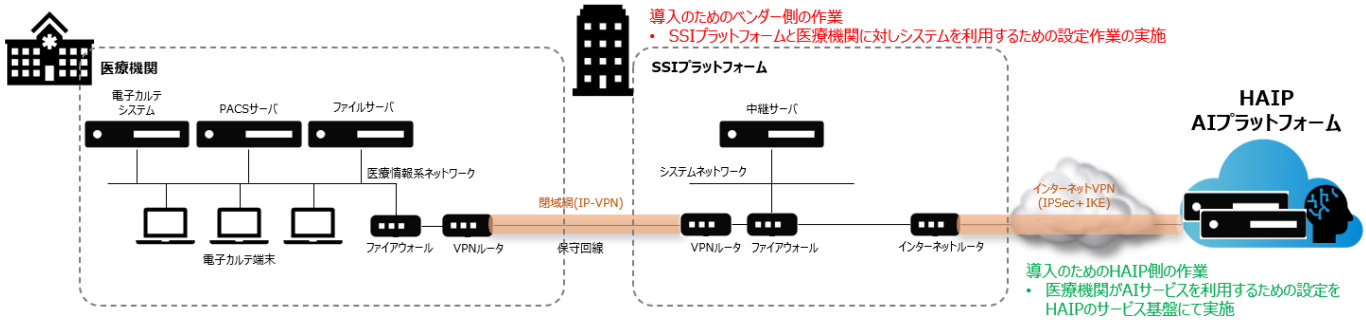


図２　ユースケース１の概要図

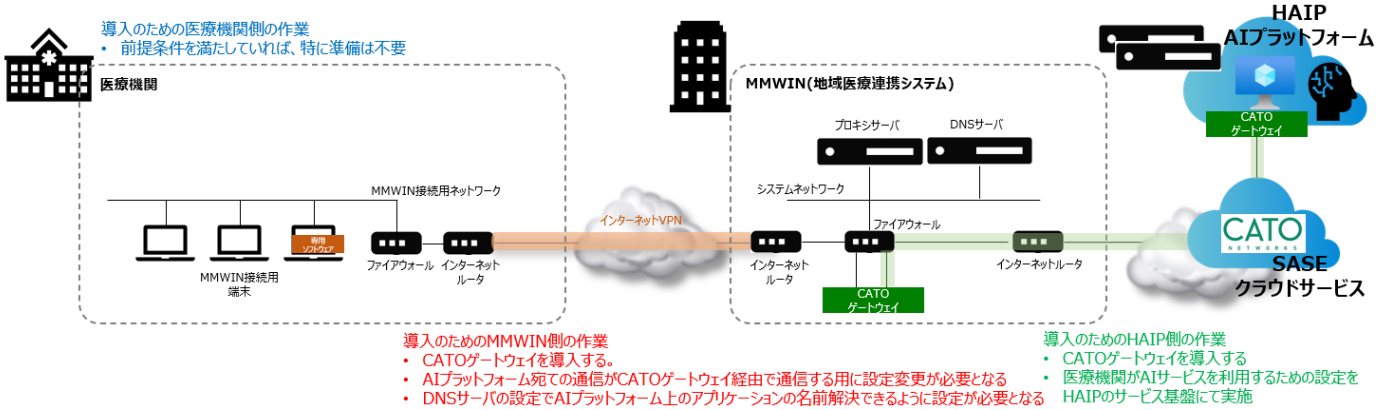


図３　ユースケース２の概要図

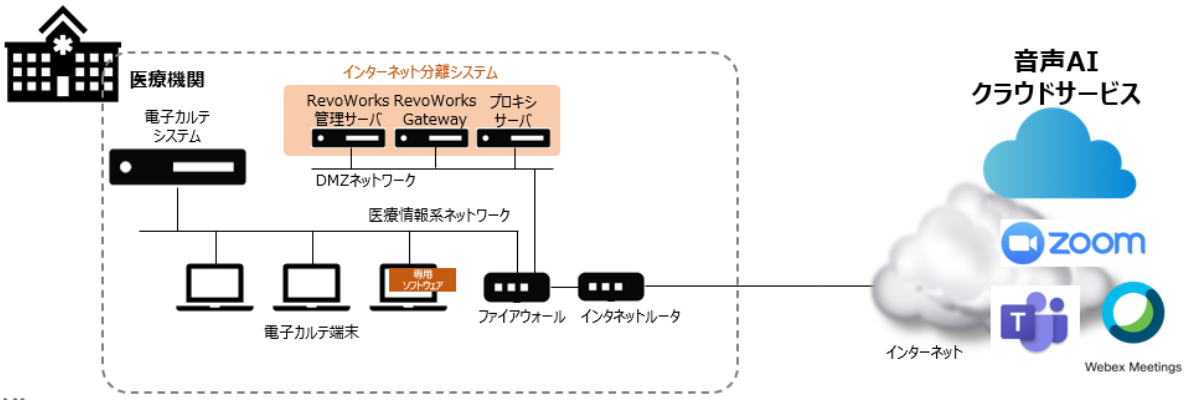


図４　ユースケース３の概要図

構成No	概要	接続元	接続先	接続方法
1	同じ電子カルテ情報を扱うクリニックから電子カルテシステムが存在する医療機関へRDP接続し電子カルテシステムを利用	クリニックの電子カルテ端末	電子カルテシステムが存在する医療機関	クリニックと医療機関を閉域網で接続、RDPを利用し、電子カルテシステムを利用
2				クリニックと医療機関をインターネットVPNで接続、RDPを利用し、電子カルテシステムを利用
3			電子カルテシステムが存在する医療機関の電子カルテ端末	クリニックと医療機関をインターネットVPNで接続、RDPを利用し、医療機関内の電子カルテ端末に接続し、電子カルテ端末経由で電子カルテシステムを利用
4	医師が外出先から医療機関の電子カルテを閲覧	外出用の持ち出し端末	電子カルテシステムが存在する医療機関	外出先の医師の利用端末から医療機関に閉域網を接続、RDPを利用し、電子カルテシステムを利用
5				外出先の医師の利用端末から医療機関にインターネットVPNを接続、RDPを利用し、電子カルテシステムを利用

図５　ユースケース４の構成パターン

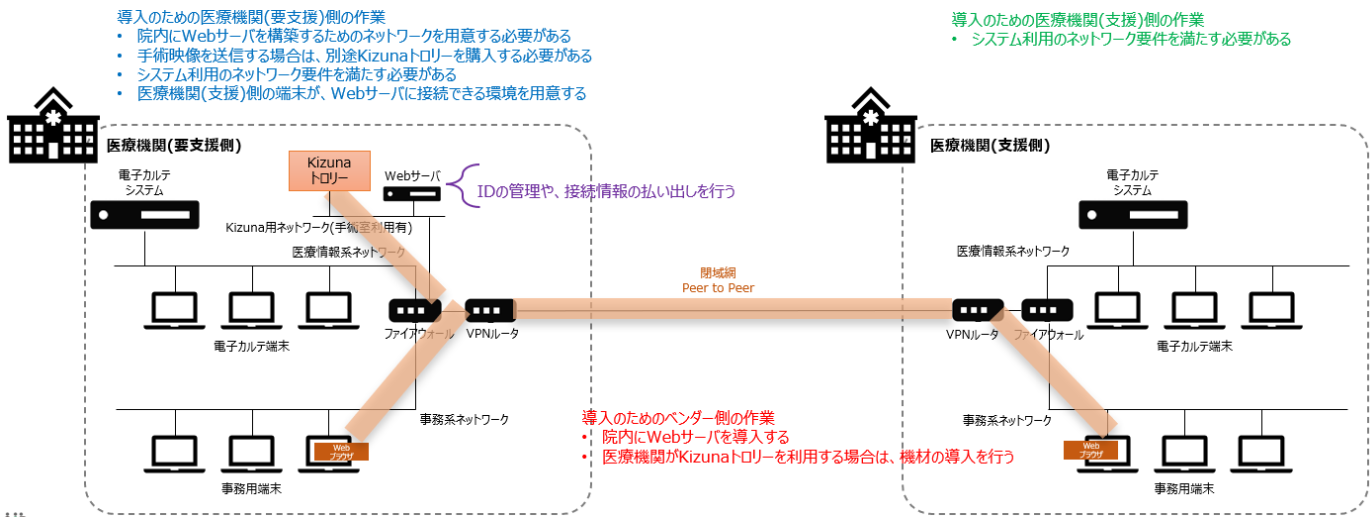


図６　KizunaWeb(ボーダレス・ビジョン社製品)

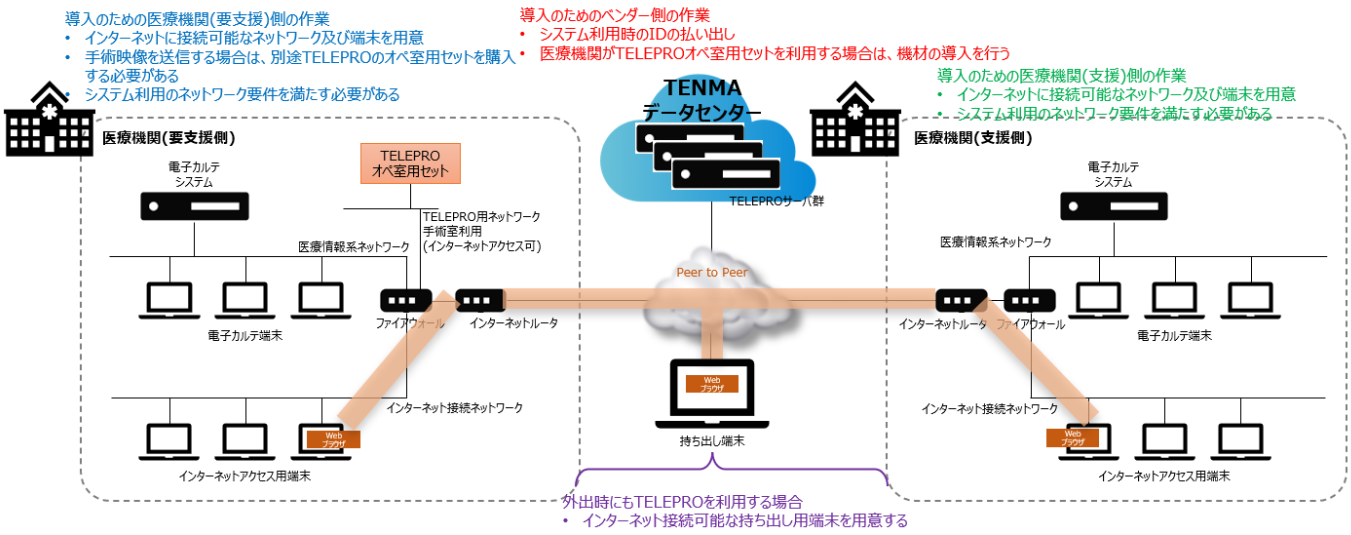


図 7　TELEPRO(天馬諮問株式会社製品)

別紙 3

厚生労働科学研究費補助金
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）

R7 年度　分担研究報告書（調査提言グループ・プロジェクトマネージャ）
クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言

分担研究者　宇賀神　敦　医療 AI プラットフォーム技術研究組合　理事長

研究要旨

医療従事者の働き方改革や医療の均てん化を実現するためには、医療従事者と医療 AI との協調が鍵となる。質の高い医療データに基づいて開発された医療 AI サービスが次々に生まれているものの、幅広い医療機関で利用されているとは言い難く、クラウドの利用に加えて利用しやすい価格設定が不可欠である。本研究では、医療機関のセキュリティの実態を把握するために、医療機関の設立母体、病床数、地域などの特性を踏まえて、24 病院、2 診療所の合計 26 医療機関に対して 2 段階で調査を行った。Step1 は、対面でのヒアリング実施前にアンケート調査票を対象の医療機関に送付して、訪問前に回答を入手し回答内容の確認を行った。Step2 は、アンケート調査の回答内容を正しく理解した上で、各医療機関に直接訪問してヒアリングを実施した。2 段階のプロセスを踏むことで、対面のヒアリングを効率的かつ深く掘り下げることが可能となり確認すべき内容を明確にすることができた。訪問に際しては、本研究班の技術検証グループに必ず同行してもらい、技術的な深掘りを行うと共に一部の医療機関のサーバ室を見学した。また一部のヒアリングには厚生労働省厚生科学課の担当官も同席し医療現場が抱える課題を直接聞いてもらった。今後の政策立案に少しでも役立つことを期待したい。この調査を通して、医療機関の ICT 導入状況、ネットワーク構成、人員体制、リスクアセスメント実施状況、システムセキュリティ監査状況、保健所によるセキュリティ立ち入り検査対応状況などの実態、医療現場が抱える課題等を把握することができた。さらに、医療機関のネットワーク構成をセキュリティガバナンスの点から 4 段階に類型化しそれぞれのセキュリティ対策を整理した。医療機関は平均して 100 床あたり 1 名のシステム要員で電子カルテシステムの導入、運用、トラブル対応やセキュリティ対策を実施しており、リソース不足が顕著である。また、新しい知識を吸収する時間が確保出来ない事やベンダーへの依存体制が顕著である事などが浮き彫りになった。さらに、医療機関に有益なユースケースのヒアリング調査のために追加で 2 医療機関の協力を得た。ユースケースについては、技術検証グループにてその成果をまとめた。

本成果を基に、以下に示す提言策定を行った。提言の構成は、アセスメント - 対策 - 監査 - 訓練 - 人材育成・意識改革のそれぞれの項目について、ツールの準備、具体的なユースケース、システムセキュリティ監査の具体的手法を示している。また、これらの PDCA サイクルを定期的かつ継続的に実施するために必要となる制度的支援についても言及した。

A. 研究目的

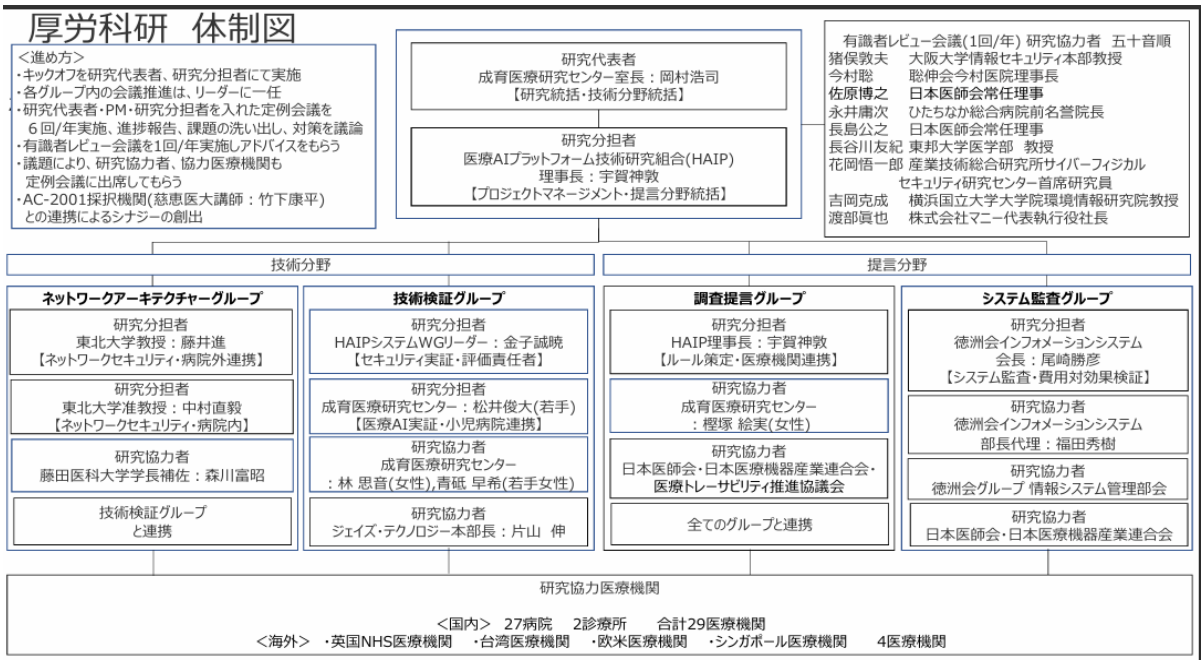
医療 AI は、深層学習による画像認識の飛躍的な精度向上により医療への有用性が示され、国内では内閣府による AI ホスピタル事業にて医療の質向上や医療従事者の負担軽減などの実証が進められた。一方で、医療機関における医療 AI サービスの利用は 10%程度との報告もあり、まだまだ導入が進んでいない。医療の提供環境にも変化が起こっている。ひとつは、2024 年 4 月から開始された医師の時間外労働の上限規制（年間９６０時間）による医療従事者の働き方改革であり、もうひとつは、2025 年に全人口の 18%（2180 万人）が後期高齢者となることに起因する医療・介護の担い手不足の深刻化である。今後医療機関に求められることは、サイバーセキュリティ対策と医療提供変化への対応の両立である。すなわち、サイバー攻撃の被害を防ぐために、医療機関の特性によって、最適なサイバーセキュリティ対策やシステム監査を継続的に実行することが重要であり、病院外からの電子カルテへのアクセスや SaMD(Software as a Medical Device）や SaMD 以外の AI サービスの利用による医療従事者の働き方改革の促進である。さらに、医療過疎地域などに対する専門医と非専門医のギャップを埋める遠隔医療やオンライン診療、在宅医療への対応、医療機関内外の多職種を含めたデータ連携が必要となる。

2021 年 4 月設立された医療 AI プラットフォーム技術研究組合(HAIP)は、医療機関が医療 AI サービスを安全、安心、リーズナブルな費用で利用できる実行環境の研究開発を進めている。医療 AI サービスの開発、評価から実装までを一気通貫に提供するプラットフォームを通じ、安全、安心で費用対効果の高いネットワーク環境及び安全性を担保するためのルール作りが、医療 AI サービス普及のために不可欠である。

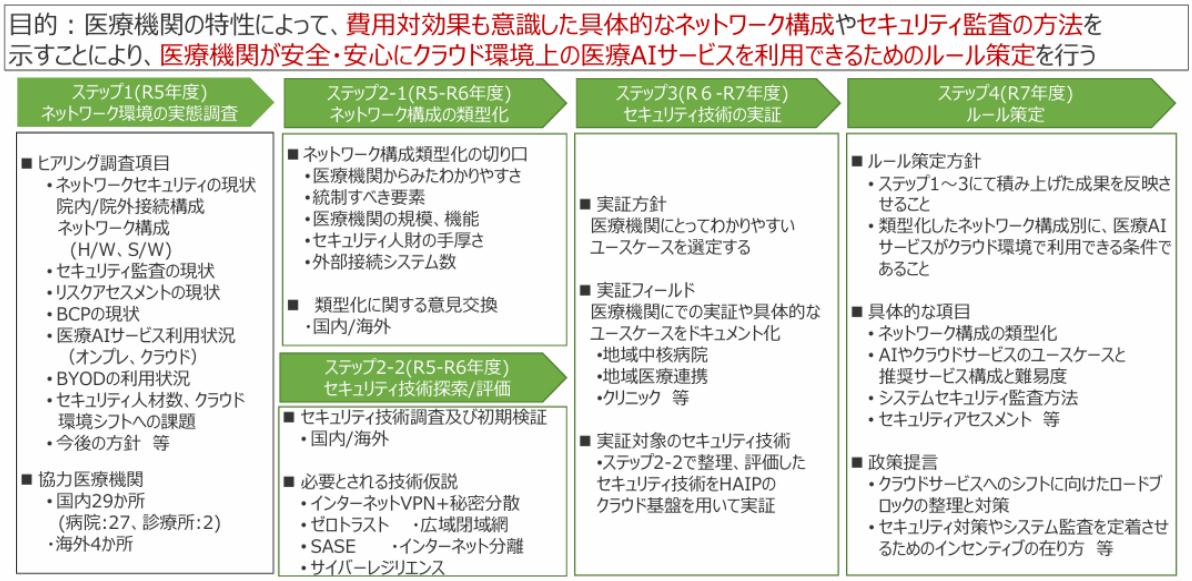
本研究は、医療機関が簡単に自己チェックを行えるアセスメントツールの検討、医療機関のネットワークガバナンスによる類型化と自己チェック、システムセキュリティ監査のルール策定、IT-BCP 訓練、医療 AI やクラウドサービスを医療機関が検討・導入しやすくするためのユースケースを示している。また、これらを定期的かつ継続的に行うためには、原資が必要となるため、そのための制度的支援案についても示している。全国の医療機関が安全、安心かつリーズナブルな費用で医療 AI サービスが利用できることにより、医療機関の経営改善や医療の質を高めることを目的とする。

B. 研究方法

医療機関の選定は、設立母体、病床数、地域が分散される様に配慮して選定を行った。国内 24 か所の病院、2 か所の診療所に対し、2 段階で調査を行った。Step1 は、対面での

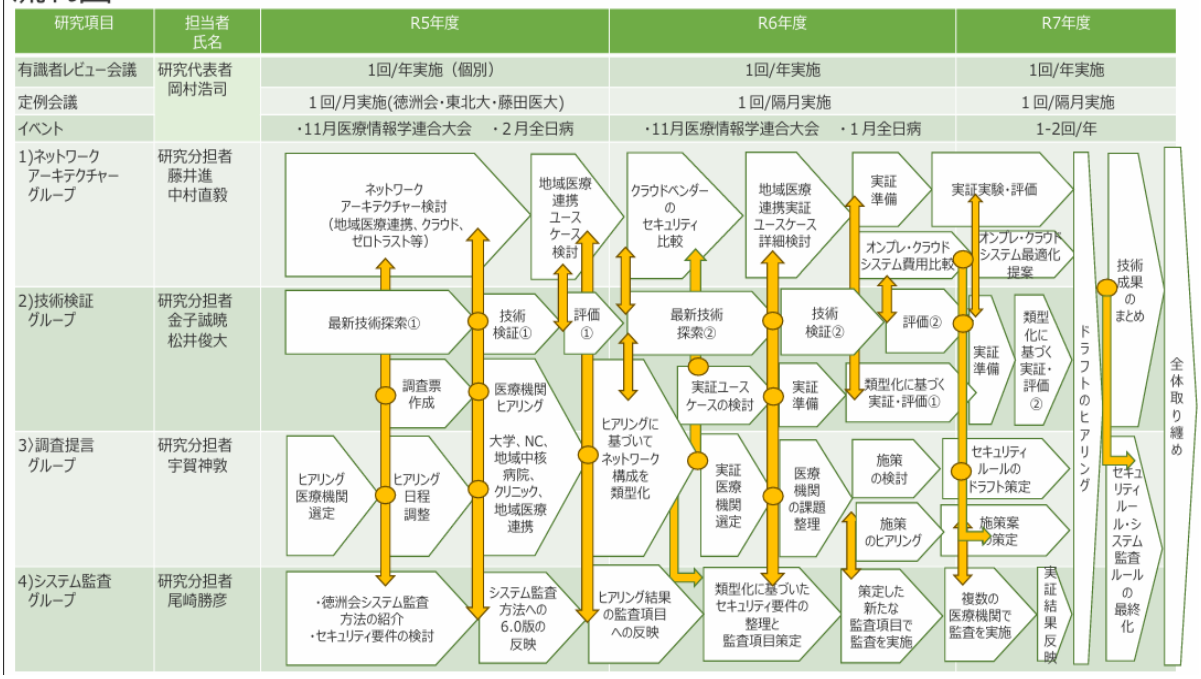


研究計画：各ステップにおける実施内容



ヒアリング実施前にアンケート調査票を対象の医療機関に送付して、訪問前に回答を入手し回答内容の確認を行った。Step2 は、アンケート調査の回答内容を正しく理解した上で、各医療機関に直接訪問してヒアリングを実施した。本 2 段階のプロセスを踏むことで、対面のヒアリングを効率的かつ深く掘り下げることが可能となり確認すべき内容を明確にすることができた。対面のヒアリングを通して、システム管理の方法、セキュリティ人材の数、厚労省セキュリティチェックリストの活用状況、システムセキュリティ監査の実施状況、IT-BCP に対する準備状況の実態を確認し、ここから明らかになった医療機関の課題を分析して、対策を提言に反映する。また、医療機関のシステム構成を正確に把握

流れ図



することで、ネットワーク構成の類型化を行い、クラウドシフトを加速するための課題を明らかにするとともに医療機関に求められる具体的なネットワーク構成を示す。

C. 研究結果

2024 年 1 月『情報セキュリティ１０大脅威 2024』が情報処理推進機構から発表された。1 位がランサムウエアによる被害、2 位がサプライチェーンの弱点を悪用した攻撃が挙げられており、つるぎ町立半田病院（2021）、大阪急性期・総合医療センター（2022）などが被害に遭ったのも上記のケースである。2023 年との順位変動で情報セキュリティ 10 大脅威をみてみると、3 位に内部不正による情報漏洩の被害、6 位に不注意による情報漏洩等の被害が順位を上げている。これらは、IT 技術だけでは防ぎきれないため、医療機関においては、定期的なセキュリティ監査の実施が非常に重要であり、定期的に従業員全員に対するセキュリティリテラシー向上の教育の実施が必要である。組織全体でトップダウンによるセキュリティの重要性を継続的に訴えていくことも重要である。2026 年 1 月『情報セキュリティ１０大脅威 2026』が情報処理推進機構から発表された。1 位がランサムウエアによる被害、2 位がサプライチェーンの弱点を悪用した攻撃であり、二大脅威であることに変わりはない。特筆すべきは、3 位に AI の利用をめぐるサイバーリスクが初登場したことである。生成 AI がサイバー攻撃を行う時代になっており、この進化が著しいため、もはや境界防御型セキュリティやゼロトラスト型セキュリティによる防御という概念だけでは防ぎき

れなくなっている。そこで、重要になるのが例えサイバー攻撃を受けても被害をできるだけ最小化して、医療の継続をおこなうサイバーレジリエンスの考え方を実践する事である。

（1）事前アンケート調査票の作成

事前アンケート調査票を研究班全体でレビューを実施し、23 項目の調査票を完成させた。調査項目の作成においては、今までに実施されていた厚労省、全日本病院協会、日本医師会総合政策研究機構の調査を参考にしつつ、今回の研究目的に必要な項目を策定した。

（2）医療機関の選定及び調整

従来実施されていたアンケート調査と本研究の大きな違いは、回答数とそのアプローチ方法である。本研究では、医療機関数は 26 である。医療機関の選定は、設立母体、病床数、地域ができるだけばらつく様に考慮した上で、２４病院、２診療所の計２６医療機関に協力いただいた（注：その後、ヒアリングについてさらに3医療機関の協力をいただき 27 医療機関、2 診療所の計 29 医療機関（付録 1)、海外ではシンガポール 2 病院、MoH に協力いただいた)。医療機関の実態を把握するために２段階のアプローチをとった。Ｓｔｅｐ１として事前アンケート調査票の送付及び事前回答の入手を行った（26 医療機関)。Ｓｔｅｐ２として、実際に医療機関へ訪問し、対面では事前回答結果に基づいた効率的かつ内容の濃いヒアリングが実施でき、医療機関の実態を把握できた（25 医療機関)。また、一部の医療機関では、サーバ室の見学も行った。なおＳｔｅｐ２所要時間は、1 医療機関当たり 1.5 時間程度であった。事前回答時間と合わせると、医療機関はかなりの時間を本件に費やしている。ご協力頂いた医療機関の皆様に感謝申し上げる。皆、セキュリティの専門家からの支援を求めている事が強く感じられた。

（3）事前アンケート及びヒアリング結果

① 導入システム

電子カルテ、医事会計システムは、全医療機関に導入されていた。オーダリリングシステムについても、1 医療機関を除き全ての医療機関に導入されていた。

これらのシステムについては、医療情報システム担当者がシステム構成の把握が出来ていた。しかしながら、PACS、臨床検査システム、調剤システムに代表される部門システムについては、システム構成の把握は各部門に任されていた。また、オンライン資格確認システムについては全医療機関で導入されていたが、電子処方箋については、どの医療機関でも導入していなかった。導入が進まない理由は、①システム導入費用がかかる割に医療機関のメリットが少ないこと②利用するには医師、薬剤師が HPKI カードを取得する

ことが必須であるが、HPKI カード発行までに時間がかかっている（半導体不足など）こと、及び、発行費用の課題があること③電子カルテなどのシステム改変が必要であるが、ベンダー側のシステム的な準備が整っていないこと、詳細仕様があいまいな部分があり、率先して導入する理由が見当たらないことが挙げられる。

② 医療情報システム担当者数

医療情報システム担当者は、各病院とも概ね 100 床当り 1 名の配置であった。配置人員が、前述のケースよりも多い医療機関が 2 医療機関あったが、この場合は電子カルテを内作、或いは IT ツール類を内作していたため、医療情報システム担当者というよりはシステム開発人員であった。医療情報システム担当者は、日々のシステム問い合わせやトラブル対応も業務に含まれている。その上に、医療機関内の電子カルテシステム、オーダリングシステム、医事会計システム以外のシステム構成の把握や外部ネットワーク構成の把握を行うことは甚だ困難である。さらに、セキュリティ対策は、非常に重要だと頭ではわかっていても、日常業務に追われ、最適なセキュリティ対策をタイムリーに実施することや最新のセキュリティ技術へのキャッチアップをすることも非常に困難であり、手が廻っていないのが現状である。

③ サイバーセキュリティチェックリストの活用状況

全体の 87%が記入済みまたは記入中であり、活用の意識は概ね醸成されていた。保健所の立入り検査時に、サイバーセキュリティチェックリストについての言及はあるものの、対策へのアドバイスやフィードバックは一切なかったとのことであった。医療機関としては、かなりの工数を捻出しているものの、双方向の会話にならず、一方通行の感が否めないため、改善を望む声が多かった。また、サイバーセキュリティチェックリストの表記が曖昧で、医療機関によって解釈のばらつきがあることも把握できた。

④ セキュリティ監査・リスクアセスメント

セキュリティ監査については 46%の医療機関が、リスクアセスメントについては 27%の医療機関が実施していた。セキュリティ対策は、継続が重要であり、定期的なセキュリティ監査の定着が肝要である。一方で、セキュリティ監査を実施できる人材は非常に限られているため、内部に人材がいないケースも多い。外部委託という選択肢はあるが、この場合は費用面の課題を解決する必要がある。

⑤ BCP

55%の医療機関が厚生労働省基準または医療機関内の独自ルールに沿った BCP 対策を実施中または計画中であった。また、電子カルテデータのバックアップや遠隔保管な

どは実施している医療機関が多かった。しかしながら、自然災害からの復旧に代表されるBCP とサイバー攻撃からの復旧に代表されるIT-BCP は異なるものであり、対策も異なることから、今後経営層を含めた教育によるIT-BCP のリテラシー向上や医療機関によるIT-BCP マニュアル策定のためのリファレンスドキュメントの提供などのアクションが必要であろう。

（4）ネットワーク構成の類型化

医療機関へのヒアリングに基づき、特にネットワークにおける通信制御の統制レベル（外部ネットワーク接続統制、記憶媒体利用統制、内部ネットワーク統制）に着目し、以下３段階に類型化を行った。

レベル１：外部ネットワーク接続統制、記憶媒体利用統制が一部実施されている

レベル２：外部ネットワーク接続統制、記憶媒体利用統制が十分実施されている

レベル３：外部ネットワーク接続統制、記憶媒体利用統制、内部ネットワーク統制が十分実施されている

また、最低限の統制レベルとして、大阪急性期・医療センターの報告書でもある様に、サーバや端末のパスワード管理が徹底され、定期的なパスワードの変更を行っていれば、サイバー攻撃によるシステムへ侵入を遅らせる事が可能となり、システムへの侵入を断念させられることができる。パスワード管理の徹底をレベル０として追加し、ネットワークセキュリティ構成類型化の最終化を行う予定である。今後は、医療機関から見て、選択しやすいフローチャート型の類型化モデルを作成し、協力参加機関に意見を頂いた。

レベル	統制の主な内容	外部NW統制	記憶媒体利用統制	内部NW統制
0	● 基本的な実施事項	–	–	–
1	● 医療情報系ネットワークと、外部(別の組織やサービス）や院内の別ネットワークとの通信制御がある程度実施されているが、管理レベルが不十分である	一部出来ている	一部出来ている	出来ていない
2	● 医療情報系ネットワークと外部(別の組織やサービス）や院内の別ネットワークとの通信制御が実現され、構成やアクセス記録が維持管理されている ● マルウェア侵入や情報漏洩を防ぐため、USBメモリ等外部記憶媒体の利用制御・管理が行われている	出来ている	出来ている	出来ていない
3	● 医療情報系ネットワークと外部(別の組織やサービス）や院内の別ネットワークとの通信制御が実現され、構成やアクセス記録が維持管理されている ● マルウェア侵入や情報漏洩を防ぐため、USBメモリ等外部記憶媒体の利用制御・管理が行われている ● 医療情報系ネットワーク内部において、部門システム間の通信制御が実現され、維持管理されている	出来ている	出来ている	出来ている

レベル	具体的な施策例
0	✓ PCやスマホのID管理、定期的なパスワード変更 ✓ 適切なユーザ管理（退職者ユーザーアカウントの削除など） ✓ サーバ、ストレージ、ネットワーク機器やアプリケーション、ネットワークアクセスに用いるID・パスワードの適切な維持管理、特権ユーザ管理の厳密化 ✓ 定期的な従業員へのセキュリティ教育、プライバシー教育の実施
1	レベル０に加えて下記を実施 ✓ 医療情報系NWがインターネットと直接接続しない構成とする ✓ 医療情報とそれ以外のネットワークとの間にルータやFWを配置し、必要な接続先・プロトコルのみ通信できる構成とする ✓ 医療情報系NWとインターネット接続系NWに接続する端末を分ける ✓ USBメモリ等外部記憶媒体の運用ルールを定める
2	レベル1に加えて、下記を実施 ✓ 外部との接続、および院内のネットワーク構成を把握し、構成図や各機器のコンフィグを維持管理する ✓ 特にインターネットにさらされるFWやルータ等の機器の継続的な脆弱性対応など、適切に維持管理する ✓ リモートメンテナンスなど外部からのアクセスが必要な場合は、ベンダ・利用者ごとにIDを払い出し、アクセス先を制御するとともに、多要素認証を導入するなどセキュリティに配慮する ✓ リモートメンテナンスなど、外部からのアクセス記録や作業ログと作業報告を定期的に突合し、意図しないアクセスを発見する ✓ 許可された端末で、また許可された記憶媒体のみ利用できるよう端末のデバイス制御を行い、外部記憶媒体の利用ログを定期的に確認する
3	レベル2に加えて、下記を実施 ✓ 部門システムとごとにネットワークセグメントを分割し、セグメント間はルータやFWで必要な接続先・プトロコルのみ通信できる構成とする

（5）ユースケース

医療機関にとって、有効な６つのユースケー

ス（①医療機関の既設ネットワークを利用した医療 AI サービス利用②地域医療連携ネットワークを活用したセキュアなインターネット利用③インターネット分離システムを利用した Web 会議や音声 AI サービスの利用④医師が院外からセキュアな環境で電子カルテのアクセス⑤遠隔医療システムを活用した手術支援、⑥ネットワーク結節点の集約によるセキュリティ安全性の担保）の選定を技術検証グループと共同で行った。上記の中で、医師が院外からセキュアな環境で電子カルテのアクセスのユースケースについて、3 つの医療機関のヒアリング先を選定し、技術検証グループと共にヒアリングを実施した。

（6）アセスメント

ヒアリングから医療機関が自組織のセキュリティ状況を容易かつ安価に実施できる方策が必要との考えに至った。その解決手段として汎用的な Web ベースのアセスメントツール（ISMS ベースで 175 問、5 段階評価）を参考にして、医療機関向けにできるだけ質問数を絞り込んでシンプルにした。また、用語解説を追加し 3 段階評価とした。かつ、医療情報システムの安全管理ガイドライン 6.0 版や R7 年度版セキュリティチェックリストの内容を質問に反映させて再構成を行った。用途別には、病院の IT 部門向け（80 問）、病院の経営層向け（15 問）、診療所向け（13 問）の 3 種類を準備した。病院の IT 部門向けは、病院のセキュリティについて、組織・運用面、技術面の 21 項目について数問ずつ設問を用意し、病院のセキュリティ全体を俯瞰できる内容とした。病院の経営層向けは、経営層（理事長、院長、事務長）がセキュリティに対する理解が不十分な病院は、システムセキュリティ監査の結果が低い結果がでており、経営層の意識改革が不可欠と判断して、作成した。診療所向けは、病院に比べ構成がシンプルな診療所に向けである。これら 3 種類を β 版として、70 を超える医療機関や関係部門にて試行を実施した。

D. 考察

今回の調査で多数の医療機関から多方面にわたる生の情報を取得し、多くの課題を抽出することができたとともに、ネットワークセキュリティ構成の類型化を行うことができた。研究開始時に策定した研究計画を進めるにあたって、とるべきアクションがより明確になった。

具体的には、セキュリティ人材が不足しており、かつ、経営が厳しい医療機関が多い中で、医療機関がセキュリティ強化のサイクルである、アセスメント（現状把握）→セキュリティ対策→監査・訓練（対策の確認）→人財育成・意識改革（組織の強化）→アセスメント（現状把握）のサイクルを継続的かつ定期的に実行するための助けとなるできるだけ

具体的かつ実効性の高い提言の策定が重要である。つまり、提言の中で示すべき方針は大きく２つあると考える。一つ目は、できるだけ少ない IT 投資で病院のセキュリティレベルをいかに向上するか。二つ目は、医療機関の IT 投資へのインセンティブをつけるための制度設計である。

① アセスメント（現状把握）

各医療機関が、自分自身のセキュリティレベルを正しく把握する。

医療機関ができるだけ少ない労力で現状を把握することが可能な 2 種類のツールを開発した。一つめは、ガバナンスにフォーカスしたネットワーク類型化モデルを活用しやすくするために、医療機関が自組織のセキュリティレベルを簡単に確認できる様なフローチャートを作成した。二つめは、Web ベースのセキュリティアセスメントツールを開発し、医療機関が比較的簡単に強み弱みを把握できるようにした。前述のとおり、本アセスメントツールは、用途別に病院の IT 部門向け、病院の経営者層向け、診療所向けを準備し、β版のトライアルをおこなった。結果としては、概ね好評であり、軽微な改善の要望については今後改善を行う。本アセスメントツールは、医療システムの安全管理に関するガイドライン(６.０版)や R7 年度版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準拠しており、自組織の強みや弱みを正確に現状把握するためだけではなく、ベンダーとの対話を具体的に進めるためのツールとしても利用が可能と考えている。本研究終了後は、医療システムの安全管理に関するガイドライン(６.1 版)の公開や R8 年度版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チェックリストの公開行われるため、本ツールへの反映を行う計画である。

② セキュリティ対策

前述のネットワーク類型化レベルを確認するフローチャートに則った対策案を示すこととしている。また、Web セキュリティアセスメント結果に則った対策案を具体的に示している。さらに、医療機関に役立つクラウド利用のためのユースケースを複数提示する。具体的には、安全・安心にクラウド上の AI サービスを利用する方法、自宅などのリモートから院内システムへのアクセスを行う方法、運用管理が不十分な外部ネットワーク結節点（モダリティ、サブシステム、電子カルテ等の保守回線や給食システムなどの外部サービス）を集約する方法、地域医療連携ネットワークにおいて、セキュリティ体制が脆弱な多くの医療機関をセキュリティ体制が整っている組織がまとめて面倒を見る方法などである。医療機関が使いたいと想定されるクラウドサービスのユースケースを実証し、具体的な事例としてドキュメントにま

とめ具体的なリファレンスモデルを作成することで、セキュリティ対策が以前に比して容易になると考える。Web セキュリティアセスメントの結果、点数が低い部分（3 点満点で 1.5 点以下）の対策案を提示する。また、さらに、医療機関が具体的なアクションを起こしやすい様に Health ISAC Japan、医療トレーサビリティ推進協議会、ソフトウエア ISAC、ＩＰＡなどと連携してマップを策定する計画である。

③ 対策の確認・訓練

定期的かつ継続的なシステムセキュリティ監査が重要である。システムセキュリティ監査の方法については、本研究班のシステム監査グループが研究を進めている。システムセキュリティ監査は、医療機関の規模や体制によって、受査することが困難な医療機関が多数存在すると考えている。また、監査する側の組織や体制整備も大きな課題であり、今後関係各所の知見を借りながら定着をめざすための具体化を進めていきたい。当面は、ある規模以上の医療機関（200 床以上）は 3 年に一度の外部監査の実施を、内部監査については、毎年一度の実施を推奨する。監査を補完する役割である、①で述べた Web セキュリティアセスメントツールを用い、人間ドックの様に 1 年に 1 回チェックを行うことにより、セキュリティ対策の現状把握だけではなく、1 年間の改善状況が見える化できると考えている。

訓練については、ネットワークアーキテクチャーグループが研究を進めている。

前述のとおり、生成 AI がサイバー攻撃を行う時代となり、攻撃の高度化が顕著であるため、サイバー攻撃を完全防御することは極めて困難になってきてる。従って、万一サイバー攻撃を受けた場合に、どうやって医療の継続的な提供を行うかが重要となっており、そのための包括的なアプローチであり上位概念がサイバーレジリエンスの考え方である。IT-BCP は、サイバーレジリエンスの考え方の内、障害からの復旧計画と実際の復旧を示すことが多い。IT-BCP は、計画の立案は重要であるが、災害時の避難訓練のように、実際の訓練をすることが極めて重要である。

1 年に 1 回は実際の訓練を行って、計画と現実の GAP を確認して IT-BCP の計画を継続的にブラッシュアップしていくことが重要である。日頃より、訓練をしていないと有事の際に間違いなく対処ができないと考えておいた方がよい。本提言でも IT-BCP について提言で言及している。

④ 人財育成・意識改革

人財育成については、組織として継続的な実施が必要である。医療機関に属する全員が必修として受講すべき基本的な研修と IT やセキュリティ業務として必要な専門的な研修を組み合わせて行う必要がある。本提言では、

研修の内容については深く掘り下げないが、提言のコンテンツは研修で使われる事を意識して、スライド形式で纏めている。是非、活用をしていただけるとありがたい。また、厚生労働省　ＮＩＳＴに掲載されているコンテンツを研修で活用することが大変有効と考える。さらに、生成ＡＩを医療機関で用いるケースが増えてきているため、生成 AI の利用者向けガイドラインも研修コンテンツとして有効である。

意識改革については、病院経営層の意識改革が極めて重要である。経営層のセキュリティに対する意識が低い医療機関はシステムセキュリティ監査の結果が悪く、意識が高い医療機関は結果が良いというデータがある。むしろ、ＩＴ人財の多い少ないよりも影響が大きい。

⑤ インセンティブ

官のインセンティブは、診療報酬の施設基準緩和が一番重要である。また、導入補助金の様な一過性のものではなく、継続した打ち手を高く評価してインセンティブにフィードバックする仕組みが必要であろう。

民のインセンティブは、出金を抑えるインセンティブとして、金融機関からの借入れ金利のディスカウントや損保会社のサイバー保険割引率アップなどが考えられる。収入を増やすインセンティブは、具体的なユースケースを共有したり、安全・安心なネットワーク経由で匿名化あるいは仮名化された医療データを提供することに対するインセンティブが考えられる。さらに、治験への参画を積極的に行うことによる収入アップも重要であろう。

⑥　認定制度

他の医療機関の見本となるセキュリティ対策を行っている医療機関、生成ＡＩなどのＡＩの活用を医療機関全体で行っており、業績改善や医療の質向上の定量的なアウトカムを示した医療機関を認定し、⑤に代表されるインセンティブを獲得できる仕組みの提案を行う。認定制度は、あくまで手段であり、目的はデジタル化、クラウド活用、AI 活用に向けた取組み、具体的なユースケースを他医療機関への共有と失敗事例の共有を行うことにより、同じ隘路に陥らない様にすること、及びセキュリティ投資や AI への投資へのインセンティブを一過性ではなく、社会システムとして継続できるようにすることである。認定するための項目整理と認定を行うプロセス、組織の検討を本研究が終了した後に検討を深めたい。

⑦ Human Centric Healthcare の実現

サイバーセキュリティ対策は、医療 DX、データ利活用、医療従事者の働き方改革を支える基盤と考えている。物流が劇的に発展した背景には、高速道路網などのインフラ整備によるものであり、医療 DX、データ利活用、

医療従事者の働き方改革の進展もそれをささえるインフラ整備が必須である。この場合のインフラの大きな要素は、安全・安心なネットワーク環境の整備であり、医療機関や自治体、介護施設、市民・患者に代表されるステークホールダーのセキュリティ対策である。これらが、インフラとして整備されると現在の医療機関を中心とした医療（場所中心の医療ともいえる。病院、診療所など特定の場所に市民・患者が出向く）からひと中心の医療（市民・患者が最適な医療を選択できて、医療過疎地域の方々へのリモートモニタリング、遠隔診療など）とのミックスが重要だと考える。また、ここでいうひとは、必ずしも市民・患者だけを指している訳ではなく、医師・看護師・薬剤師や医療従事者も含んでいる。これらの方々の過重労働、バーンアウト問題の解決や高度な専門スキルの継続（休職、退職後の再就職など、高度なスキルを活かす枠組み）問題を解決すべく、活動していきたい。

E. 結論

国内 26 医療機関に対して、事前アンケート調査を行った上で、対面による実態調査を行った。医療機関の ICT 導入状況、ネットワーク構成、人員体制、リスクアセスメント実施状況、システムセキュリティ監査状況、保健所によるセキュリティ立ち入り検査対応状況などの実態、医療現場が抱える課題等を把握することができた。また、医療機関のシステム構成を技術面から 4 種類に類型化し、それぞれのメリット、デメリットを整理した。さらに、医療機関に役立つ具体的な 6 種のユースケースの洗い出しとヒアリングを行った。

医療機関は平均して 100 床あたり 1 名のシステム要員で院内システムのトラブル対応やセキュリティ対策を実施しており、リソース不足や知識不足、またベンダー依存体制が浮き彫り、早急な対策が必要であると考えられる。サイバー攻撃の増加し、ランサムウェアによる被害が拡大している状況の中、境界防御型セキュリティに加えてゼロトラスト型セキュリティの導入が必要である。しかしながら、これまで境界型防御型セキュリティで守られてきた電子カルテのネットワーク構成を変更するためは、多くの課題がある事が確認できた。経営層のセキュリティリテラシー向上やモチベーション向上策の提言、セキュリティ人材不足を補うための施策、ベンダーと医療機関の間の責任分界点の明確化、定常的にかかるセキュリティ対策費用の手当などである。また、セキュリティ対策のサイクルを医療機関で定着させることが、医療 DX の実現や医療従事者の働き方改革を推し進める上で、必須となる。さらに、生成 AI によるサイバー攻撃が激増し攻撃が高度化

しているため、境界防御型セキュリティとゼロトラスト型セキュリティを組み合わせた完全防御をめざすセキュリティ対策では守り切れない時代になってきている。これからは、サイバー攻撃リスクは、常に存在し、万一サイバー攻撃にあっても医療の提供をとめないことが最重要の課題となる。組織全体でサイバーレジリエンス対応による予測・耐性・回復・適応能力を高め、IT-BCP により、サイバー攻撃からの回復及び医療提供の継続の計画を立案し、日ごろより実践訓練を行うことが唯一の解だと考える。これらを体系立てて提言としてまとめ、公開することにより、クラウド上の医療 AI 利用、医療 DX 及び医療機関やステークホールダー間のデータ利活用の促進や医療従事者の働き方改革の推進に少しでも貢献できれば幸いである。最終的には、医療機関中心の医療からひと中心の医療である Human Centric Healthcare へのシフトが進むことを期待してやまない。関係省庁や業界団体との連携をこれまで以上に深め、課題の解決に邁進していく所存である。

最後に、多忙の中、協力していただいた 29 の医療機関（付録２）に深謝します。

F. 研究発表

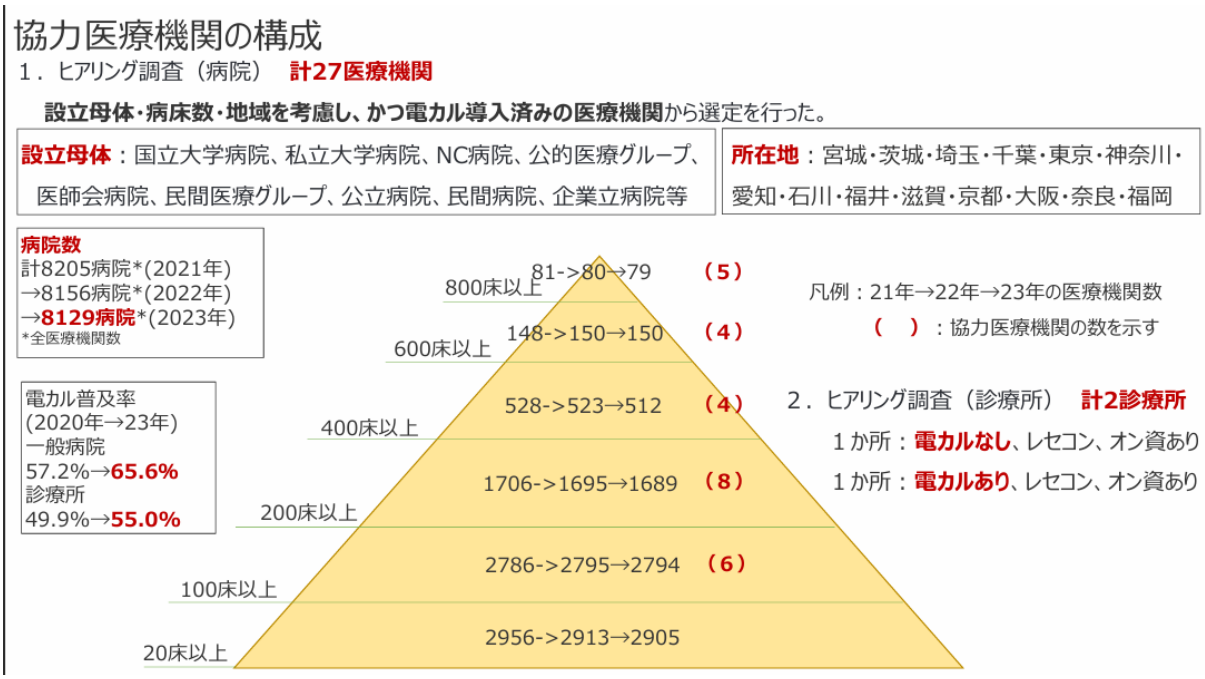
1. 宇賀神 敦, 医療機関に求められるサイバーセキュリティ対策とクラウド型AIサービスの活用, *週刊医学のあゆみ* 12月28日号, 2024, **Vol. 291 Nos12, 13**, 1123-1129
2. 宇賀神 敦, クラウド型AIサービス活用の課題と将来の展望について, *医療情報学*, 2024, **44(Suppl.)**, 371
3. 宇賀神 敦, AIサービス普及のための情報セキュリティのあり方, *INNERVISION*, 2024, **39**, 17-20
4. 宇賀神 敦, 医療機関の経営者は今こそ情報セキュリティに対する投資優先度を上げるべき, *月刊新医療*, 2023, **50**, 22－27
５. 宇賀神　敦、正しく恐れて、積極的に活用しよう！‐医療機関が押さえておくべき「医療・ヘルスケア分野における生成 AI 利用ガイドライン（第 2 版)」のポイント‐, ITvision, 2025, 55, 14－15
６. 宇賀神　敦, 医療 AI の活用や医療 DX 推進に求められるセキュリティやガバナンス‐安心して医療 AI が利用できるデータ連携基盤やサイバーセキュリティの制度的支援の考察 ‐, 第 45 回医療情報学連合大会, 2025, 45(4-B-1-08), 1－6
７. 宇賀神　敦, 中小医療機関が直面するサイバーセキュリティー課題と対策　論考②, 日本医療法人協会ニュース, 2026, 2026/5

G. 知的財産権の出願

該当なし

資料　ネットワークセキュリティ構成類型における協力医療機関

付録１：協力医療機関の構成



付録２：協力医療機関の一覧

協力医療機関一覧（１）

１．病院

#	医療機関名称	所在地	病床数	開設主体
1	藤田医科大学病院	愛知県豊明市	1376	私立学校法人
2	東北大学病院	宮城県仙台市青葉区	1160	国立大学法人
3	京都大学医学部附属病院	京都府京都市左京区	1131	国立大学法人
4	飯塚病院	福岡県飯塚市	1048	企業立病院
5	大阪赤十字病院	大阪府大阪市天王寺区	883	日本赤十字
6	横須賀共済病院	神奈川県横須賀市	740	共済組合
7	国立国際医療研究センター	東京都新宿区	719	国立研究開発法人
8	仙台医療センター	宮城県仙台市宮城野区	660	国立病院機構
9	福井大学医学部付属病院	福井県吉田郡永平寺町	600	国立大学法人
１０	国立成育医療研究センター	東京都世田谷区	490	国立研究開発法人
１１	越谷市立病院	埼玉県越谷市	481	公立
１２	恵寿総合病院 *1	石川県七尾市	426	民間
１３	淡海医療センター	滋賀県草津市	420	民間、地域医療連携推進法人

*1:24/1/1　23年度は能登半島地震のため、事前アンケート調査票の提出のみのご協力

協力医療機関一覧（２）
１．病院

#	医療機関名称	所在地	病床数	開設主体
１４	仙台病院	宮城県仙台市泉区	384	JCHO
１５	済衆館病院	愛知県北名古屋市	331	民間
１６	みやぎ県南中核病院	宮城県大河原町	310	公立
１７	日立製作所ひたちなか総合病院	茨城県ひたちなか市	302	企業立病院
１８	仙台徳洲会病院	宮城県仙台市泉区	250	民間
１９	練馬総合病院	東京都練馬区	224	公益財団法人
２０	生駒市立病院	奈良県生駒市	210	公立（医療法人徳洲会*2）
２１	柏市立柏病院	千葉県柏市	200	公立
２２	賛育会病院	東京都墨田区	199	社会福祉法人
２３	公立刈田綜合病院	宮城県白石市	199	公立（医療法人仁誠会*2）
２４	板橋区医師会病院	東京都板橋区	192	日本医師会
２５	JR仙台病院	宮城県仙台市青葉区	164	企業立病院
２６	博愛会病院	福岡県福岡市中央区	145	民間
２７	豊橋ハートセンター	愛知県豊橋市	130	民間

＊２：指定管理者として民間医療機関が公立病院の運営を行っている

協力医療機関一覧（３）
２．診療所

#	医療機関名称	所在地	病床数	開設主体
1	今村医院	東京都板橋区	0	民間（元日本医師会筆頭副会長）
2	斎藤医院	東京都板橋区	0	民間（板橋区医師会長）

１）診療所への更なる協力依頼、Webセキュリティアセスメントツール、地連への調査（日医総研）に関して、日本医師会長島常任理事、佐原常任理事に相談に伺った

別紙 3

厚生労働科学研究費補助金
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
クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言

研究分担者　尾﨑 勝彦　徳洲会インフォメーションシステム株式会社 取締役会長
研究協力者　福田 秀樹　徳洲会インフォメーションシステム株式会社導入管理部 部長代理

研究要旨

医療現場における医療 AI の利活用は働き方改革にも繋がる医療従事者の業務効率化と省力化、医療レベルの高度化、患者サービスの向上、さらに専門医不在など医療資源が不足している離島やへき地で提供される医療のレベルとカバーレンジを都市部に近づけるパワーを持つ。このように大きな可能性を持つ医療 AI であるが、その多くはインターネット上のクラウドに存在し、一方医療機関、特に病院で利用される電子カルテ等はインターネットから分離されたクローズドな環境の中にあるものが多い。本研究では医療機関の電子カルテ端末等から医療 AI をセキュアに利用するための技術や方策の検討と提言を行うが、そのためにはまず医療機関の院内情報システム、また医療機関そのものがセキュアな環境でなければならない。徳洲会グループでは、グループの IT 部門である「徳洲会インフォメーションシステム株式会社」とグループ病院の院内システムエンジニア約 180 名の集合体である「情報システム管理部会」が協力してグループ内の病院にシステムセキュリティ監査を行ってきた。この監査をより実効性のあるものにブラッシュアップし、さらにグループ外の医療機関にも適用しうる標準的な監査とすることで医療 AI の導入を進める医療機関のセキュリティレベル向上に繋げたいと考える。R 5 年度はまず 5 月にリリースされた厚生労働省「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」に準拠したシステム監査とすること、またこれまでの徳洲会グループ病院の監査結果をもとに改善を実施し、標準化に向けた土台作りを行った。続く R 6 年度・7 年度においては引き続き徳洲会グループ 6 病院で監査を実施して毎回フィードバックと改善を行うとともに、初のグループ外の 2 病院での監査を実施した。このグループ外病院の監査では監査項目や提出資料、評価方法についても大幅な見直しを行った。準備から実施、振り返りを通じて多くの気づきや課題を見出すことができ、目的である広く国内の医療機関に適用できる監査の標準化に向けて大きな一歩を踏み出すことができたと考える。また監査を通じてセキュリティレベルが高く維持されている病院、反対にハイリスクな病院それぞれにその要因は何か、さらには病院に対して真に効果的なシステムセキュリティ監査とはどんなものかについても考察し、提言とした。

A. 研究目的

医療現場における医療 AI の利活用は働き方改革に繋がる医療従事者の業務効率化と省力化、医療レベルの高度化、患者サービスの向上、さらに専門医不在など医療資源が不足している離島やへき地で提供される医療のレベルとカバーレンジを都市部に近づけうるパワーを持つ。このように大きな可能性を持つ医療 AI であるが、その多くはインターネット上のクラウドに存在し、一方医療機関、特に病院の電子カルテ等は現在もインターネットから分離されたクローズドな環境の中にあるものが多い。本研究では医療機関の電子カルテ端末等から医療 AI をセキュアに利用するための技術や方策の検討を行うが、そのためにはまず医療機関の院内情報システム、また医療機関そのものがセキュアな環境でなければならない。徳洲会グループでは、グループの IT 部門である「徳洲会インフォメーションシステム株式会社」とグループ病院の院内システムエンジニア（以下「院内 SE」）約 180 名の集合体である「情報システム管理部会」が協力してグループ内の病院にシステムセキュリティ監査を行ってきた。この監査をより実効性のあるものにブラッシュアップし、さらにグループ外の医療機関にも適用しうる標準的な監査とすることで医療 AI の導入を進める医療機関のセキュリティレベルの向上に繋げることが目的である。

B. 研究方法

Ｒ５年５月に公表された厚生労働省「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」（以下「厚労省ガイドライン」）にもとづき徳洲会グループの「情報システム運用管理規程」（以下「運用管理規程」）を改訂、９月に第 6.0 版をリリースした。この厚労省ガイドライン・運用管理規程それぞれの第 6.0 版に準拠した「システムセキュリティ監査チェックシート」にもとづきＲ５年度に３病院、Ｒ６年度・７年度には計８病院の監査を実施、毎回結果をフィードバックし監査項目や監査方法の見直しを行って次回の監査で検証、というサイクルにもとづく改善を継続的に行った。特にＲ７年３月のＡ病院、同８月のＢ病院は初の徳洲会グループ外の病院における監査であり、事前に監査チェックシートや提出資料の大幅な見直しを行うことで、またここでもフィードバックにより多くの気づきや課題を得ることができ、これらにもとづき国内の医療機関に広く適用するための標準化を試みた。

【システム監査実施病院】

Ｒ５年度

６月 30 日　古河総合病院（茨城県）

12 月 20 日　大垣徳洲会病院（岐阜県）

３月 15 日　湘南厚木病院（神奈川県）

Ｒ６年度

６月 25 日　東大阪徳洲会病院（大阪府）

12 月 19 日　宮古島徳洲会病院（沖縄県）

２月 28 日　山川病院（鹿児島県）

３月　７日　Ａ病院（愛知県）

Ｒ７年度

７月 30 日　野崎徳洲会病院（大阪府）

８月 29 日　Ｂ病院（千葉県）

１月 14 日　野田総合病院（千葉県）

３月 19 日　出雲徳洲会病院（島根県）

C. 研究結果

ここではＲ７年３月と８月に実施した徳洲会グループ外のＡ病院・Ｂ病院での監査について、その準備と実施および改善について記述する。

（1）A病院

1．監査チェックシートの見直し

監査チェックシートについては次の観点で見直しを行った。

表1　システムセキュリティ監査チェックシート

（抜粋）

	監査項目	チェック対象資料等	チェック対象資料等提出方法	資料等の確認	結果
管理体制					
1	医療情報システム安全管理責任者・企画管理者・情報システム運用担当者・情報セキュリティ責任者（厚労省ガイドライン上のこれらの役割を担う別名称の役職者でも良い）が任命され、それぞれの役割が明文化されている	①役職者名簿（氏名・所属・院内役職が記載されたもの） ②役職者の役割が確認できる資料（規程の該当部分など）	①・②ともデータかPDFでご提出ください（①は最終更新日があるもの）	事前	△
2	院内の医療情報システムの安全管理やセキュリティ対策について協議・情報共有する情報システム委員会（別名称でも良い）が設置され、各部署から委員が選出されている		①・②ともデータかPDFでご提出ください（いずれも最終更新日があるもの）	事前	△
3	情報システム委員会は月１回程度開催されて機能しており、議事内容が幹部・各部署に共有されている	①情報システム委員会議事録 ②委員会の議事内容の幹部・各部署への共有が確認できる資料（回覧記録や幹部が出席する会議の議事録など）	①・②ともデータかPDFでご提出ください（①は直近の２回分）	事前	△
個人情報保護					
4	病院の個人情報保護方針が策定され、患者の見える場所に掲示されている	①病院の個人情報保護方針 ②個人情報保護方針の掲示状況（当日）	①はデータかPDFでご提出ください ②は当日掲示を確認します	事前および当日	○
5	医療情報システムから個人情報を含むデータを抜き出す際のルールがあり、適切に運用されている	①医療情報システムからのデータ抜き出しに関するルールが確認できる資料（規程の該当部分など） ②運用が確認できる資料（申請書類など）	①はデータかPDFで ②は実際に使われた（記載のある）ものをデータかPDFでご提出ください（２部）	事前	○

① 運用管理規程等ルールの有無の確認

徳洲会グループには厚労省ガイドラインに準拠したルールブックである「情報システム運用管理規程 第 6.0 版」があり、グループ病院においてはこの規程にもとづく運用が適切に行われているかについて監査を行う。しかしグループ外の病院ではそもそもルールの有無が不明であるため、多くの項目で「①厚労省ガイドラインにもとづくルールがあり　②それにもとづく運用が行われているか」という観点でのチェック形式に変更した。

② 徳洲会グループ標準書式の書き換え

徳洲会グループ病院では運用管理規程の別紙として「ID・権限棚卸結果報告書」「外部記憶媒体貸与台帳」など計 27 種類の帳票を用いることでルールにもとづく運用を行うこととしており、監査チェックシートの「チェック対象資料等」にもこの帳票名を記載している。しかしグループ外の病院にはこの名称の帳票はないため、「電子カルテ ID の棚卸が行われたことが確認できる資料」「院外に情報機器を持ち出す際の運用が確認できる資料」といった記載に変更した。

③ 電子カルテのアプリ名等の書き換え

徳洲会グループ病院では同一メーカーの電子カルテを利用しており、監査チェックシートの「チェック対象資料等」にもそのアプリ名を記載しているものがある。これもグループ外病院の電子カルテメーカーが不明であるため、「電子カルテのアクセスログが表示された画面」「パスワードでの復帰が必要なスクリーンセーバ」などの記載に変更した。

④ 監査項目の見直し

グループ内外の病院を問わず、監査を通じて確認すべき事項としたものに加え、サイバーセキュリティに関する動向、厚労省の「病院における医療情報システムのサイバーセキュリティ対策に係る調査」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」等も参考に、監査項目の見直しを継続的に行った。

2．監査方法の見直し

① 事前提出資料の削減

病院側の準備の負担軽減のために事前提出資料が必要な項目数を従来の 46 から 42 へ減らし、その 4 項目については現地で確認することとした。

② 監査後の改善支援

徳洲会グループ病院においては監査報告書の提出後、その改善を 3～6 ヵ月かけてフォローアップする仕組みがあるが、今回の研究ではこの部分を行わないこととした。

上記①・②以外は監査の全体スケジュール（監査通知 → 資料の事前提出 → 文書監査と結果通知 → 現地監査 → 監査報告書提出）を含めグループ病院と同様に実施した。

3．監査の実施と結果

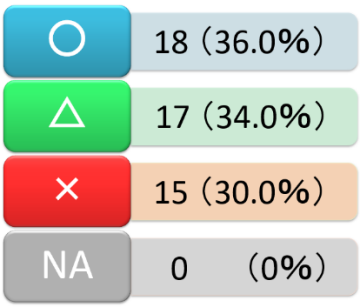
A病院での監査結果とそこにあらわれた課題について記述する。

① 監査結果：全体

×（未充足）と△（一部充足）を合わせると全 50 項目中 32 項目、全体の 64%が指摘項目と

なった。

表２　A病院の監査結果（全体）



○：充足　△：一部充足　×：未充足　NA：該当なし

② 監査結果：詳細

監査項目の内容を満たしていないものをカテゴリー別に、またその一部を具体的に次に示す。

表３　A病院の監査結果（詳細）

監査カテゴリ／項目数			監査結果			
カテゴリ	項目数	項目番号	○ 充足	△ 一部充足	× 未充足	NA 該当なし
管理体制	3	1～3	0	3	0	0
個人情報保護	2	4～5	2	0	0	0
文書類の整備	4	6～9	2	2	0	0
管理者権限の管理	3	10～12	1	0	2	0
ＩＤ・パスワード管理	8	13～20	4	1	3	0
サイバー攻撃・災害・BCP対策	9	21～29	3	3	3	0
サーバ管理	7	30～36	2	2	3	0
端末管理	8	37～44	4	2	2	0
ネットワーク管理	4	45～48	0	3	1	0
その他	2	49～50	0	1	1	0
合 計	50		18	17	15	0

×：未充足の項目（抜粋）

12　電子カルテのサーバ OS のアクセスログを取得し、いつでも調査可能な状態である

14　電子カルテIDのパスワードは次のいずれかである

A：１３桁以上の英数記号のパスワード（定期変更はなし）

B：８桁以上の英数記号のパスワードで最低２ヵ月に１度変更

C：二要素認証を採用

16　電子カルテIDの棚卸しが定期的に行われ、不要なIDの残存有無が確認されている

28　BCP 対策で定めた対応手順にもとづく訓練が定期的に実施され、手順の見直しが行われている

39　インターネットに繋がる情報系LAN上の端末やNASに診療情報を保管していない

△：一部充足の項目（抜粋）

6　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』に準拠した『情報システム運用管理規程』があり、各部署にペーパーで保管されている、あるいは各部署の端末から閲覧できる

24　USB メモリの利用に関するルールがあり、適切に運用されている

26　BCP 対策で定めた電子カルテ等院内システムがダウンした際の対応手順があり、各部署にペーパーで保管されている

34　サーバ室の空調機器は故障に備えて２基設置されており、サーバ室の室温異常をシステム運用担当者が把握できる

47　情報システム・医療機器の保守回線とこれに接続されたネットワーク機器（VPN ルータ・ファイアウォール）が一覧化され、適切に管理されている

（２）B病院

１．監査チェックシートの見直し

A病院での結果にもとづき、標準化として不十分と思われる部分を中心にブラッシュアップを行った。

２．監査方法の見直し

① 事前のコミュニケーションの強化

監査期間前に病院側のメンバーと監査メンバーでWebによる顔合わせおよび監査に関する説明と質疑応答の時間を設けた（約１時間）。これにより病院は比較的スムーズに監査準備に取りかかることができ、また資料準備期間のメールによる質疑応答もより活発に行われたと考える。

② 監査後のコミュニケーションの強化

監査報告書提出後に病院より報告書の内容についての詳細説明と意見交換の機会を設けることが提案された。これを受けて Web で実施し、病院は監査結果についてより深い理解を得られ、監査メンバーは病院からの率直な意見を聞くことで多くの気づきがあり、取り組むべき課題を知ることができた。非常に有意義な場となり、監査メンバーは監査後のコミュニケーションの重要性について認識した。

3．監査の実施と結果

A病院と比較すると院内のセキュリティルールや BCP 対策も整備されているなど、セキュリティレベルは高く感じられた。しかし総評で示した結果では指摘事項となる「△・×」の項目数はA病院とほとんど変わらなかった。個々の内容を確認すると「○にわずかに届かない△」が多いことが判明し、3段階評価が実態を表すには粗いものであることを実感した。そこで後日の監査報告書作成にあたり 4 段階評価（充足率で評価／A：80%以上　B：50～79%　C：20～49%　D：20%未満）を採用し、これにより監査メンバーが現地で感じたセキュリティレベルに近い結果を得ることができた。

表４　３段階 → ４段階評価への見直し

表５　B病院の監査結果（詳細）

監査カテゴリ／項目数			監査結果				
カテゴリ	項目数	項目番号	A	B	C	D	NA
管理体制	2	1～2	2	0	0	0	0
個人情報保護	1	3	1	0	0	0	0
文書類の整備	3	4～6	2	1	0	0	0
管理者権限の管理	4	7～10	1	1	0	2	0
ＩＤ･パスワード管理	8	11～18	2	0	4	2	0
サイバー攻撃･災害･BCP対策	10	19～28	5	3	1	1	0
サーバ管理	7	29～35	3	1	2	1	0
端末管理	8	36～43	3	1	3	0	1
ネットワーク管理	5	44～48	1	1	1	2	0
その他	2	49～50	0	1	0	1	0
合 計	50		20	9	11	9	1

D．考察

1．初のグループ外病院監査における考察

① 監査チェックシートの標準化

監査チェックシートは２度のグループ外病院の監査を通じてベースとなった徳洲会グループのものから様変わりし、なお改善の余地はあるもののより標準的な内容に書き換えることができた。

② コミュニケーションの重要性

システムセキュリティ監査の受審経験がない病院にとっては各フェーズでの綿密なコミュニケーションが想像以上に重要であることを実感した。期間前・資料準備期間中・現地監査中・総評時・監査報告書提出後、それぞれのフェーズで活発な質疑応答が行われることにより、病院は監査の意義や効果、取り組むべき課題などをより深く理解し、指摘された事項を改善するモチベーションを高めることができる。多く質問されたのはその項目について徳洲会グループでは具体的にどのような取り組みをしているかというものであったが、普段現場で対策に当たる現役の病院 SE が監査メンバーにいることで具体的な対策を示すことができ、これは病院にとって非常に有効なものであったと考える。

2．セキュリティレベルに差が生まれることに対する考察

徳洲会グループの内外を問わず、監査を行う

と病院によってセキュリティレベルに大きな差が生じていることがわかる。要因は様々考えられるが、過去の監査結果にもとづいて見ると病院の規模や病床区分、医療情報システムの規模、院内 SE の人数といったことにより明確な傾向は現れなかった。唯一要因として実感できるのは病院幹部のセキュリティに対する関心や重要性の認識の違いである。幹部がセキュリティ対策について理解のある病院（幹部が総評に出席し積極的に質問や相談を行う、指摘事項の改善の推進を院内に指示するなど）は現場の職員もセキュリティに関する意識が高く、院内 SE もセキュリティ関連業務に時間を割き、また各部門のメンバーで構成するシステム委員会が機能して病院全体でセキュリティ対策に取り組んでいるといった傾向が明らかになった。一方、病院幹部がセキュリティに対して関心を示さない病院は職員・院内 SE・システム委員会についても前述の逆の状態にあり、結果として多くのセキュリティリスクを抱えているケースが多い。

3.「求められるシステムセキュリティ監査」に関する考察

① 一般的なシステムセキュリティ監査の問題点

セキュリティベンダーやコンサル等の専門家によるシステムセキュリティ監査と改善支援は各業種で広く行われているが、これを現在の医療業界でそのまま行うには無理があると考える。現場への教育の不足も要因の一つだが、病院の SE ですら電子カルテや部門システムには強いがセキュリティは苦手とするケースが多い。ましてや病院幹部や一般職員にはセキュリティのハードルはまだまだ高い。

②「誰もが理解できるシステムセキュリティ監査」

監査を行って問題点を洗い出し、解決策を提示しても病院がその意義や内容を理解できなければ改善はできない。セキュリティ対策には少なくないコストが発生したり現場の職員に負担を強いるものもある。病院の幹部がその重要性を理解して費用を捻出し、院内 SE や現場の職員に強いメッセージを出す必要がある。「病院の誰もが理解できるシステムセキュリティ監査」が強く求められる。私たちがこの研究を通じて模索し実践してきた「医療現場を良く知る病院職員（SE）らによるシステムセキュリティ監査」の有効性を明確にできたと考える。

4．内部監査と外部監査に関する考察

徳洲会グループにおいても人的資源の制約により監査を行えるのは年 4 病院程度にとどまる。これでは監査を受けられない病院が多く、グループ全体のセキュリティレベルは思うように上がらない。そこで監査チェックシートから重要な項目を絞り、これに実施手順やチェック方法を記載した平易なマニュアルを作成、病院はこれにより定期的（年 1 回程度）に内部監査を実施する。さらに 2～4 年に 1 回程度の外部監査で専門的視点からの助言や支援を行い、病院幹部とも面談し理解を得る。このサイクルを確立することで病院のセキュリティレベルは確実に向上すると考える。

E. 結論

研究期間を通じて徳洲会グループで行ってきたシステムセキュリティ監査のブラッシュアップと標準化に、グループ内外の病院での監査を実施しながら継続的に取り組んだ。特に初の徳洲会グループ以外の 2 病院でのシステム監査が標準化に大きく寄与したと考える。また監査結果を考察することで病院のセキュリティレベルの差に病院幹部の理

解や認識が大きな影響を与えていることがわかり、病院幹部をはじめ中間管理職、現場の職員にも理解できるわかりやすいシステムセキュリティ監査が重要かつセキュリティレベルの向上に有効であることも考察できる。D.4.の内部監査と外部監査を継続的に実施することでセキュリティ対策が日常的なものとして医療スタッフの意識に、医療現場の運用に根付いていく。幹部と院内 SE、現場の医療スタッフの共通理解と協力のもと、病院のセキュリティレベルの向上が期待される。

F. 研究発表

福田 秀樹. 医療機関におけるサイバーセキュリティ対策～その現実と問題解決に向けて. *第 10 回日本医療安全学会学術総会,2024.4.13*

尾﨑 勝彦. 病院経営に大きなメリットをもたらす情報の一元化とデータの利活用. *医事業務 No.675, 2024.9.1*

福田 秀樹. 医療機関におけるサイバーセキュリティ対策～その現実と問題解決に向けて. *最新医療経営フェイズ3 Presents 医療経営セミナー<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>の有効な活用とは？, 2024.9.13*

福田 秀樹, 江苅 孝, 藤岡 和美, 尾﨑 勝彦. グループ病院でのセキュリティ対応とその課題～システム監査を中心に～. *医療情報学*, 2024, **44(Suppl.)**, 363-367

福田 秀樹. グループ病院でのセキュリティ対応とその課題～システム監査を中心に～. *第 11 回日本医療安全学会学術総会,2025.3.15*

福田 秀樹、尾﨑 勝彦. ～医療機関のサイバーセキュリティ対策～徳洲会グループシステム監査：標準化の試み. *医療情報学*, 2025

G. 知的財産権の出願

該当なし

資料：システムセキュリティ監査チェックシート① 項番 1～19

	項　目	監査対象資料等	監査対象資料：提出方法等	厚労省GL要求事項	資料等の確認時期	結果
	管理体制					
1	医療情報システム安全管理責任者・企画管理者・情報システム運用担当者・情報セキュリティ責任者（厚労省ガイドライン上のこれらの役割を担う別名称の役務者でも良い）が任命され、それぞれの役割が明文化されている	①役務者名簿（氏名・所属・院内役職が記載されたもの） ②役務者の役割が確認できる資料（規程の該当部分など）	①・②ともデータかPDFでご提出ください（①は最終更新日があるもの）	○	事前	
2	院内の医療情報システムの安全管理やセキュリティ対策について協議・情報共有する情報システム委員会（別名称でも良い）が設置され、議事内容が幹部・各部署に共有されている	①情報システム委員会名簿（氏名・所属が記載されたもの） ②情報システム委員会議事録 ③委員会の議事内容の幹部・各部署への共有が確認できる資料（回覧記録や幹部が出席する会議の議事録など）	①・②・③ともデータかPDFでご提出ください（①は最終更新日があるもの／②は2回分）		事前	
	個人情報保護対策					
3	病院の個人情報保護方針は個人情報保護法が求める内容を適切に反映（個人情報の利用目的や苦情相談窓口が明記されているなど）しており、患者の見える場所に掲示されている	①病院の個人情報保護方針 ②個人情報保護方針の掲示状況（当日）	①はデータかPDFでご提出ください ②は当日掲示を確認します	○	事前および当日	
	文書類の整備					
4	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』に準拠した『情報システム運用管理規程』があり、各部署にペーパーで保管されている、あるいは各部署の端末から閲覧できる	①ガイドライン第6.0版に準拠した運用管理規程 ②①が各部署でペーパー保管されている、あるいは各部署の端末で閲覧可能なこと（当日）	①はデータかPDFでをご提出ください ②は当日任意の部署で確認します	○	事前および当日	
5	『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』は医療機関確認用と事業者確認用（MDS／SDSを含む）が保管されている	①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（医療機関確認用） ②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（事業者確認用） ③MDS/SDS	①・②・③ともデータかPDFでご提出ください（②・③は2社分）	○	事前	
6	業務委託をしている外部業者とは秘密保持について明記した契約書を締結している	秘密保持契約書あるいは秘密保持条項が含まれる業務委託契約書等	データかPDFでご提出ください（2部）	○	事前	
	管理者権限の管理					
7	管理者ID（電子カルテのサーバOSや電子カルテの）は必要最低限のものが登録されている	管理者ID（サーバOSや電子カルテの）が記載された一覧表など	データかPDF（最終更新日があるもの）でご提出ください	○	事前	
8	サーバOSの管理者IDのパスワードは同一のもの、また容易に類推可能なものを使用していない	サーバOSの管理者IDのパスワード	当日確認します	○	当日	
9	管理者IDの棚卸しが定期的に行われ、不要なIDの残存有無が確認されている	管理者IDの棚卸しが行われたことが確認できる資料	データかPDF（棚卸し実施日があるもの）でご提出ください	○	事前	
10	電子カルテのサーバOSのアクセスログを取得し、いつでも調査可能な状態である	ログイン／ログアウトおよびログインの失敗ログが確認できる画面	画面のハードコピーをご提出ください	○	事前	
	ID・パスワード管理					
11	電子カルテIDの登録・変更・削除の申請と承認に関するルールがあり、適切に運用されている	①電子カルテIDの登録・変更・削除の申請・承認ルールが確認できる資料（規程の該当部分など） ②運用が確認できる資料（申請書類など）	①はデータかPDFで ②は実際に使われた（記載のある）ものをデータかPDFでご提出ください（2部）	○	事前	
12	電子カルテIDのパスワードは次のいずれかである A：13桁以上の英数記号のパスワード（定期変更はなし） B：8桁以上の英数記号のパスワードで最低2ヵ月に1度変更 C：二要素認証を採用	①電子カルテIDのパスワードの桁数・使用文字に関するルールが確認できる資料（規程の該当部分など） ②電子カルテIDのパスワード桁数・使用文字を制限する設定情報	①はデータかPDFで ②はデータかPDFあるいは設定情報画面のハードコピーをご提出ください	○	事前	
13	電子カルテのログイン試行回数は上限が設定されている	①電子カルテのログイン試行回数に関するルールが確認できる資料（規程の該当部分など） ②電子カルテのログイン試行回数を制限する設定情報	①はデータかPDFで ②はデータかPDFあるいは設定画面のハードコピーをご提出ください	○	事前	
14	電子カルテIDの棚卸しが定期的に行われ、不要なIDの残存有無が確認されている	電子カルテIDの棚卸しが行われたことが確認できる資料	データかPDF（棚卸実施日があるもの）でご提出ください	○	事前	
15	他の職員の電子カルテIDを利用するなどの不適切なID運用をしていない	①不適切なID運用の禁止を職員に周知する資料 ②その周知方法が確認できる資料（職員向け掲示、イントラサイト上にその情報が表示された画面、会議・研修会のレジュメや議事録など） ③職員の電子カルテID運用の認識（当日）	①はデータかPDFで ②はデータかPDFあるいは画面のハードコピーをご提出ください ③は当日任意の部署で職員の認識について確認します	○	事前および当日	
16	電子カルテの共用ID（複数の職員・実習生などが一定期間同じIDを利用するもの）に関するルールがあり、適切に運用されている	①共用IDのルールが確認できるもの（規程の該当部分など） ②共用IDの運用が確認できるもの（共用IDの管理簿など）	①はデータかPDFで ②は実際に使われた（記載のある）ものをデータかPDFでご提出ください		事前	
17	電子カルテIDごとのアクセスログを取得し、いつでも調査可能な状態にある	電子カルテのアクセスログデータあるいはアクセスログが表示された画面	データかPDFあるいは画面のハードコピーをご提出ください（1画面分程度）	○	事前	
18	電子カルテ利用者の職種・担当業務等による診療情報へのアクセス権限を設定している	電子カルテのデータアクセス権限の設定が確認できる資料（職種別権限一覧表など）	データかPDF（最終更新日があるもの）でご提出ください	○	事前	
	サイバー攻撃・災害・BCP対策					
19	すべてのサーバおよび端末にウイルス対策ソフトを導入し、最新のパターンファイルを適用している	①ウイルス対策ソフトのライセンスを購入していることが確認できる資料 ②端末管理台帳 ③ウイルス対策ソフトのパターンファイルの最終更新日時（当日）	①はデータかPDFで ②はデータかPDF（最終更新日があるもの）でご提出ください ③は当日電子カルテサーバと端末で定義ファイルの更新日時を確認します	○	事前および当日	

資料：システムセキュリティ監査チェックシート② 項番 20～37

	項　目	監査対象資料等	監査対象資料：提出方法等	厚労省GL要求事項	資料等の確認時期	結果
20	不審なメールの添付ファイルの開封、ウェブ利用でのウイルス感染警告アラート表示への対応方法など、インターネットに接続する端末のウイルス感染やサポート詐欺対策が周知されている	①ランサムウェアやサポート詐欺等のサイバー攻撃防止対策を職員へ周知する資料 ②その周知方法が確認できる資料（職員向け掲示、イントラサイト上にその情報が表示された画面、会議・研修会のレジュメや議事録など） ③職員のウイルス感染防止の認識（当日）	①はデータかPDFで ②はデータかPDFあるいは画面のハードコピーをご提出ください ③は当日任意の部署で職員の認識について確認します		事前および当日	
21	ランサムウェア等のウイルスの感染が発生した際の初動対応が周知されている	①ランサムウェア等ウイルス感染時の初動対応について記載された資料 ②その周知方法が確認できる資料（職員向け掲示、イントラサイト上にその情報が表示された画面、会議・研修会のレジュメや議事録など） ③職員のウイルス感染時初動対応の認識（当日）	①はデータかPDFで ②はデータかPDFあるいは画面のハードコピーをご提出ください ③は当日任意の部署で職員の認識について確認します	○	事前および当日	
22	USBメモリの利用に関するルールがあり、適切に運用されている	①USBメモリの利用に関するルールが確認できる資料（規程の該当部分など） ②USBメモリの制御設定情報（ActiveDirectory ・ウイルス対策ソフトなどの） ③USBメモリ利用許可端末の一覧（部署名・用途が記載されたもの） ④病院から部署・職員へ貸与しているUSBメモリの一覧 ⑤端末でのUSBメモリ制御状況（当日）	①・③・④はデータかPDFで ②はデータかPDFあるいは画面のハードコピーをご提出ください ⑤は当日任意の部署の端末で設定状況を確認します	○	事前および当日	
23	医療情報システムから個人情報を含むデータを抜き出す際のルールがあり、適切に運用されている	①医療情報システムからのデータ抜き出しに関するルールが確認できる資料（規程の該当部分など） ②運用が確認できる資料（申請書類など）	①はデータかPDFで ②は実際に使われた（記載のある）ものをデータかPDFでご提出ください（2部）	○	事前	
24	電子カルテサーバのデータバックアップは適切に取得・保管されている	電子カルテサーバのデータバックアップの仕組み（データの流れ、世代数、バックアップ間隔、オンライン／オフラインの別など）が確認できる資料	データかPDFでご提出ください	○	事前	
25	BCP対策で定めた電子カルテ等院内システムがダウンした際の対応手順があり、各部署にペーパーで保管されている	①BCP対策で定めた対応手順が確認できる資料（院内システムダウンマニュアル等） ②院内システムがダウンした際の職員の緊急連絡網 ③院内システムがダウンした際のシステム業者連絡先一覧 ④①・②・③の部署でのペーパー保管状況（当日）	①・②・③はデータかPDFでご提出ください ④は当日任意の部署でペーパーでの保管状況を確認します	○	事前および当日	
26	BCP対策で定めた対応手順には電子カルテ復旧後の事項についても記載されている	項目26の①と同じもの	データかPDFでご提出ください		事前	
27	BCP対策で定めた対応手順にもとづく訓練が定期的に実施され、手順の見直しが行われている	①電子カルテ等院内システムがダウンした際の訓練が実施されたことが確認できる資料（報告書・訓練記録など） ②訓練の手順見直しを行ったことが確認できる資料（議事録・検討資料・改定前と後のマニュアル等）	①・②ともデータかPDFでご提出ください	○	事前	
28	電子カルテサーバや主要なネットワーク機器は非常用電源に接続され、停電時にも電子カルテが限定された端末から利用できる	電子カルテサーバや主要なネットワーク機器の非常用電源への接続状況（当日）	当日接続状況を確認します		当日	
	サーバ管理					
29	サーバ管理台帳があり、随時最新の状態に更新されている	①サーバ管理台帳 ②①のシステム管理室での保管状況（当日）	①はデータかPDF（最終更新日のあるもの）でご提出ください ②は当日保管状況を確認します	○	事前および当日	
30	サーバの名称・機能がわかりやすく明示されている	サーバの名称・機能の明示（サーバに貼られたラベル・タグなど）状況（当日）	当日明示の状況を確認します		当日	
31	サーバの異常の有無を毎日確認している	サーバの異常の有無を記録している資料	データかPDFでご提出ください（直近1ヵ月分）		事前	
32	サーバ室は常時施錠されており、入退室管理が行われている	①サーバ室の入退室記録が確認できる資料 ②サーバ室の施錠管理状況（当日）	①はデータかPDFで提出ください（直近1ヵ月分） ②は当日施錠の状況を確認します	○	事前および当日	
33	サーバ室の空調機器は故障に備えて2基設置されており、サーバ室の室温異常をシステム運用担当者が把握できる	①サーバ室の空調設備（当日） ②室温異常時のシステム運用担当者等への通知方法（通知システムのマニュアルや送信されたメッセージなど）（当日）	①・②とも当日状況を確認します		当日	
34	サーバ室の天井部分からの水漏れ対策を行っている	サーバ室の天井からの水漏れ対策（当日）	当日対策の状況を確認します		当日	
35	サーバ室は災害時に被害を受けにくい場所にある	病院平面図（サーバ室のあるフロアのみ、階数が確認できるもの）	データかPDFでご提出ください	○	事前	
	端末管理					
36	電子カルテ端末の管理台帳があり、随時最新の状態に更新されている	①電子カルテ端末管理台帳 ②①のシステム管理室での保管状況（当日）	①はデータかPDF（最終更新日があるもの）でご提出ください ②は当日保管状況を確認します	○	事前および当日	
37	電子カルテ端末にパスワードでの復帰が必要なスクリーンセーバを設定している	電子カルテ端末のスクリーンセーバ設定状況（当日）	当日任意の部署で端末を確認します	○	当日	

資料：システムセキュリティ監査チェックシート③ 項番 38～50

	項　目	監査対象資料等	監査対象資料：提出方法等	厚労省GL要求事項	資料等の確認時期	結果
38	インターネットに繋がる情報系LAN上の端末やNASに診療情報を保管していない	情報系端末と共用NAS中の診療情報の有無（当日）	当日任意の部署の情報系端末と共用NASを確認します		当日	
39	院外に持ち出す情報機器（端末・記憶媒体等）の管理に関するルールがあり、適切に運用されている	①院外に情報機器を持ち出す際のルールが確認できる資料（規程の該当部分など） ②運用が確認できる資料（申請書類など）	①はデータかPDFで ②は実際に使われた（記載のある）ものをデータかPDFでご提出ください（2部）	○	事前	
40	個人所有パソコンの院内ネットワークへの接続ルールがあり、適切に運用されている	①個人所有のパソコンを院内ネットワークに接続する際のルールが確認できる資料（規程の該当部分など） ②運用が確認できる資料（申請書類など）	①はデータかPDFで ②は実際に使われた（記載のある）ものをデータかPDFでご提出ください（2部）	○	事前	
41	電子カルテ端末（ノート型）に盗難防止対策を施している	電子カルテ端末（ノート型）の盗難防止対策状況（当日）	当日任意の部署で端末を確認します	○	当日	
42	端末やサーバの廃棄に関するルールがあり、適切に運用されている	①端末やサーバの廃棄に関するルールが確認できる資料（規程の該当部分など） ②業者から提出された廃棄証明書・HDD破壊の写真等	①・②ともにデータかPDFでご提出ください	○	事前	
43	端末故障時に交換する予備機が常備されている	予備機の確保状況（当日）	当日予備機の確保状況を確認します		当日	
	ネットワーク管理					
44	院内のネットワーク機器管理台帳があり、随時最新の状態に更新されている	①ネットワーク機器管理台帳 ②①のシステム管理室での保管状況（当日）	①はデータかPDF（最終更新日があるもの）でご提出ください ②は当日保管状況を確認します	○	事前および当日	
45	院内LAN配線図があり、随時最新の状態に更新されている	①院内LAN配線図 ②①のシステム管理室での保管状況（当日）	①はデータかPDF（最終更新日があるもの）でご提出ください ②は当日保管状況を確認します	○	事前および当日	
46	情報システム・医療機器の保守回線とこれに接続されたリモート保守用のネットワーク機器（VPNルータ等）が一覧化されている	情報システム・医療機器保守回線およびネットワーク機器の一覧表など	データかPDFでご提出ください	○	事前	
47	リモート保守用のネットワーク機器のファームウェアは最新のものに更新されている	46の一覧表などでファームウェアの情報が記載されているもの	データかPDFでご提出ください	○	事前	
48	診療系の無線LANのSSIDは非表示（ステルス）かつ暗号化（WPA2以上）の設定をしている	①電子カルテ用の無線LANアクセスポイントの設定情報（SSID・ステルス情報・暗号化など） ②端末でSSIDが見られないこと（当日）	①はデータかPDFあるいは画面のハードコピーをご提出ください ②は当日任意の部署で端末を確認します	○	事前および当日	
	その他					
49	ソフトウェア管理台帳（電子カルテアプリケーション・その他）があり、随時最新の状態に更新されている	①ソフトウェア管理台帳 ②①のシステム管理室での保管状況（当日）	①はデータかPDF（最終更新日があるもの）でご提出ください ②は当日保管状況を確認します	○	事前	
50	サイバーセキュリティに関する職員への研修や教育、意識啓発の取組みが行われている	①職員研修が実施されたことが確認できる資料（レジュメ・議事録など） ②研修資料や院内に共有した厚労省・関係団体等による注意喚起文書等、	①・②ともデータかPDF（実施日等がわかるもの）でご提出ください	○	事前	

別紙 3

厚生労働科学研究費補助金

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

クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言

研究分担者　松井 俊大　国立成育医療研究センター 医員

研究要旨

画像認識を中心とする人工知能（AI）技術は、医療の質向上、業務効率化、地域格差の解消、医療従事者の負担軽減に資する可能性を有している。一方、医療 AI を実臨床で活用するためには、AI モデルの開発だけでなく、医療機関内外から安全に利用できるクラウド上での実装を想定した実装基盤の整備が不可欠である。本分担研究では、「クラウド上の医療 AI 利用促進」のうち医療 AI 開発を担当し、感染症診療支援を目的としてグラム染色画像 AI の開発とクラウド実装を想定したサービス構成の検討を行った。

菌血症や敗血症などの重症感染症では、起因菌を迅速に推定し、適切な抗微生物薬選択や医療デバイス管理につなげることが重要である。しかし、血液培養陽性時のグラム染色鏡検では、黄色ブドウ球菌とコアグラーゼ陰性ブドウ球菌のように、外観が類似していても臨床的意義が大きく異なる菌種の判別が困難な場合がある。本研究では、グラム染色顕微鏡画像から感染症起因菌を推定する医療 AI を開発した。特に、嫌気培養、好気培養などの培養条件により菌体形態に微細な差異が生じる可能性に着目し、培養条件ごとに複数の学習済みモデルを構築した。判別対象菌の培養条件に応じて対応するモデルを選択し、撮像画像を入力することで、外観が類似した菌種であっても高精度に判別することを目指した。

実施例として、コアグラーゼ陰性ブドウ球菌と黄色ブドウ球菌の判別モデルを作成した。嫌気培養画像 4,965 枚、好気培養画像 3,858 枚を用いて、物体検出モデルおよび画像分類モデルを構築した。画像分類モデルの 6 分割交差検証では、培養条件を考慮しないモデルの平均認識精度が 0.80 であったのに対し、嫌気培養データから作成したモデルでは 0.87、好気培養データから作成したモデルでは 0.91 であり、培養条件別モデルの有用性が示された。

さらに、本医療 AI をクラウド上で利用可能な感染症診療支援サービスとして展開することを想定し、画像入力、AI 推論、結果表示までをウェブアプリケーションとして実装可能な構成に整理した。コンテナ化による実行環境の再現性と移植性の確保、VDI 環境を介した医療機関内端末からの安全な利用、ならびにサーバレスアーキテクチャによる運用コスト最適化について検討した。本成果は、感染症起因菌同定支援 AI の開発に加え、医療 AI をクラウド上で安全かつ効率的に提供するための実装基盤を整理した点に意義がある。今後は、対象菌種の拡大、多施設外部検証、前向き臨床評価、画像取得条件の標準化に加え、電子カルテ端末等から安全に利用するための認証、アクセス制御、通信、ログ管理、データ保護を含むクラウド実装の実証を進める必要がある。

A. 研究目的

ディープラーニングによる画像認識技術は、医療 AI 開発の中核的技術の一つであり、画像診断支援、病理画像解析、顕微鏡画像解析など多様な領域で応用が進んでいる。本研究課題「クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言」では、医療 AI サービスをクラウド上で安全に利用できる環境の整備を目的としている。本分担研究では、そのうち医療 AI 開発を担当し、実際にクラウド利用を想定した医療 AI サービスとして、グラム染色画像から感染症起因菌の同定を支援する AI モデルの開発を行った。

感染症診療において、起因菌の迅速な推定は、早期の適切な抗微生物薬の選択による予後の改善、感染巣の推定、薬剤耐性菌対策における抗微生物薬適正使用の観点から重要である。特に、菌血症や敗血症などの重症感染症では、最適な抗菌薬治療の遅れが患者予後に影響する可能性が報告されており、その重要性は大きい。血液培養陽性時には、陽性検体のグラム染色標本を光学顕微鏡で観察し、染色性、形状、配列などからグラム染色分類を行うことで大まかな菌種の分類として 5 種類（連鎖状グラム陽性球菌、cluster 状グラム陽性球菌、グラム陽性桿菌、グラム陰性球菌、グラム陰性桿菌）に大別することが一般的である。しかし、実臨床では、外観が類似しているにもかかわらず、臨床的意義や治療方針が大きく異なる菌種が存在する。例えば、黄色ブドウ球菌とコアグラーゼ陰性ブドウ球菌はいずれも cluster 状グラム陽性球菌であり、ブドウの房状の集塊を形成するため、グラム染色像のみでの判別は容易ではない。一方、黄色ブドウ球菌菌血症は、抗菌薬選択、感染性心内膜炎や転移性病変の検索、デバイス関連感染の評価などが重要となり、コアグラーゼ陰性ブドウ球菌とは臨床対応が異なることがある。

訓練された観察者であれば、黄色ブドウ球菌とコアグラーゼ陰性ブドウ球菌を判別することは可能とされ、既報では SA の陽性的中率 95-97%と良好であるが（J Clin Pathol. 2004;57:199-201、感染症学. 2008;82:656-7）、小児感染症医・細菌検査技師を対象とした我々の研究では、SA の陽性的中率は中央値 62%と既報より認識精度が低く、ヒトの目による観察には観察者の熟練度や疲労度によって限界があることが明らかになった（第 54 回日本小児感染症学会　総会・学術集会　抄録集.2022: 181）。

そこで本研究では、グラム染色画像に対するディープラーニングを用いて、外観類似菌種を高精度に判別する医療 AI を開発することを目的とした。さらに、本研究課題の趣旨に沿って、将来的にクラウド上の医療 AI サービスとして安全に提供することを見据え、画像入力、判別、結果出力までをソフトウェアとして実装可能な構成とした。

B. 研究方法

1. 本研究での医療 AI 開発の位置づけ

本分担研究では、クラウド上で利用可能な医療 AI サービスの開発対象として、感染症起因菌同定支援 AI を開発した。開発対象は、血液培養陽性検体から作成したグラム染色標本の顕微鏡画像である。AI モデルは、顕微鏡画像中の菌体を検出する物体検出モデルと、検出された菌体画像を分類する画像分類モデルから構成した。本システムは、将来的にクラウド上のウェブサービスまたは医療 AI プラットフォーム上で利用することを想定し、ソフトウェアとして実装可能な構成とした。画像は、顕微鏡に接続されたカメラで撮像された画像、スライドスキャナで取得さ

れた画像などを想定した。

2. 菌種判別 AI の基本構成

本研究で開発した菌種判別 AI は、入力部、判別部、出力部から構成される。入力部は、判別対象菌の撮像画像を受け付ける。判別部は、培養条件に対応する複数の学習済みモデルを備え、判別対象菌の培養条件に応じて適切なモデルを選択する。出力部は、判別結果を利用者に提示する。学習済みモデルは、嫌気培養に対応するモデル、好気培養に対応するモデルなど、培養条件別に構築した。各モデルは、物体検出モデルと画像分類モデルから構成した。物体検出モデルは、画像中の菌体の位置および候補菌種を検出し、画像分類モデルは、物体検出結果に基づいて切り出された画像断片を分類する。

3. 培養条件別モデルの作成

菌体の形態は、嫌気培養、好気培養などの培養条件により微細に変化する可能性がある。そこで、本研究では、培養条件を区別せずに単一モデルを作成するのではなく、培養条件ごとに学習済みモデルを作成した。判別時には、判別対象菌の培養条件に対応するモデルを選択し、撮像画像を入力した。学習済みモデルの作成では、まず、血液培養陽性検体からグラム染色標本を作成し、光学顕微鏡で撮像した。菌種の正解ラベルは、生化学的検査、質量分析、またはその他の菌種同定結果に基づいた。顕微鏡画像上の菌体に対して、菌種の特徴を含む領域をバウンディングボックスとして手作業で指定し、菌種ラベルを付与した。アノテーションデータから、物体検出モデル用の教師データを作成した。また、バウンディングボックスの中心座標から一定サイズの画像断片をクロップとして切り出し、画像分類モデル用の教師データとした。

4. 実施例：コアグラーゼ陰性ブドウ球菌と黄色ブドウ球菌の判別

実施例では、外観上の判別が困難でありながら臨床的意義が大きく異なる菌種として、コアグラーゼ陰性ブドウ球菌（CNS）と黄色ブドウ球菌（SAU）を対象とした。両者はいずれもグラム陽性球菌であり、ブドウの房状に集塊を形成するが、病原性、組織侵襲性、人工物関連感染との関連、治療方針が異なるため、早期判別の臨床的意義が高い。

当センターで得られた血液培養陽性検体から、嫌気培養条件で得られた CNS 画像 2,498 枚、SAU 画像 2,046 枚、好気培養条件で得られた CNS 画像 2,467 枚、SAU 画像 1,812 枚を用いた。それぞれから無作為に 1,800 枚を抽出し、1,500 枚を訓練検証データ、300 枚をテストデータとして物体検出モデルを作成した。

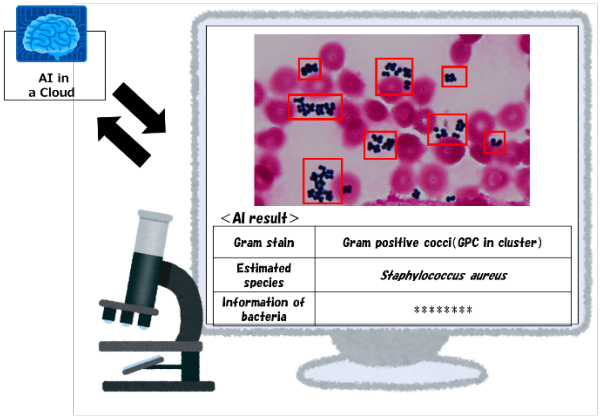
画像分類モデルでは、10 μm 四方に相当する 171 ピクセル四方の画像を細菌検査技師が手作業でアノテーションした。得られた画像クロップ数は、CNS は嫌気培養 11,480、好気培養 27,550、SAU は嫌気培養 12,473、好気培養 7,141 であった。各群から無作為に 6,000 クロップを抽出し、5,000 クロップを訓練検証データ、1,000 クロップをテストデータとして 6 分割交差検証を行った。

5. クラウド利用を想定した開発と検討

本医療 AI をクラウド上で利用可能な感染症診療支援サービスとして展開することを想定し、グラム染色画像の入力、AI 推論、結果表示までの一連の処理について、実装に必要な構成要素を整理した。医療機関側で取得した顕微鏡画像をウェブアプリケーション上で入力し、クラウド上または管理された実行環境上に配置した AI モデルにより菌体検出および菌種判別を行い、結果を利用者に返

す構成を想定した。クラウド実装にあたっては、医療データの安全な取り扱い、認証、アクセス制御、通信経路の保護、ログ管理、実行環境の分離、運用コスト管理を検討項目とした。実行環境については、ウェブアプリケーションのコンテナ化による再現性、移植性、運用管理性の向上を検討した。また、電子カルテ端末など医療機関内端末からの安全な利用を見据え、VDI 環境を介したアクセス方式を整理するとともに、利用頻度の変動に対応するため、サーバレスアーキテクチャの適用可能性についても検討した。以上により、グラム染色画像 AI をクラウド上で安全かつ効率的に提供するための基本的な実装構成を整理した。

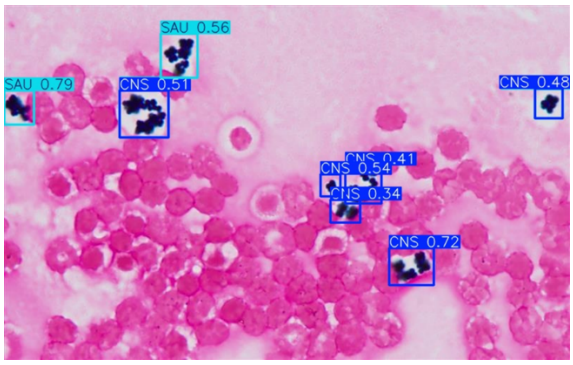
図 1　クラウド実装を想定した医療 AI サービス構成



C. 研究結果

物体検出モデルについて、培養条件別モデルと、培養条件を考慮しないモデルを比較した。テストデータとして、CNS 嫌気培養、CNS 好気培養、SAU 嫌気培養、SAU 好気培養の各 300 枚、合計 1,200 枚を使用した。物体検出モデルにおける誤検出数は、CNS では嫌気培養データから作成したモデルで 27/300、好気培養データから作成したモデルで 11/300、培養条件を考慮しないモデルで 59/600 であった。SAU では、嫌気培養データから作成したモデルで 7/300、好気培養データから作成したモデルで 29/300、培養条件を考慮しないモデルで 47/600 であった。培養条件別にモデルを作成することで、培養条件を考慮しないモデルより誤検出が少なくなる傾向が認められた。

図 2　グラム染色画像における菌体検出例



画像分類モデルについても、嫌気培養データから作成したモデル、好気培養データから作成したモデル、培養条件を考慮しないモデルを比較した。6 分割交差検証による平均認識精度は、嫌気培養データから作成したモデルで 0.87、好気培養データから作成したモデルで 0.91、培養条件を考慮しないモデルで 0.80 であった。

本医療 AI を、将来的にクラウド上で利用可能な感染症診療支援サービスとして展開することを想定し、画像入力、AI 推論、結果表示までの一連の処理をウェブアプリケーションとして実装可能な構成に整理した。具体的には、医療機関側で取得したグラム染色顕微鏡画像を入力し、クラウド上または安全な実行環境上に配置された AI モデルにより菌体検出および菌種判別を行い、その結果を利用者に返す構成とした。本構成では、医療 AI モデルを単独の研究用プログラムとして

ではなく、クラウド上で公開可能なサービスとして運用することを見据え、実行環境の分離、再現性、移植性を確保するため、コンテナ化を前提とした実装が可能であることを確認した。また、医療データを扱うサービスであることから、電子カルテ端末など医療機関内の端末から直接インターネット上のサービスへ接続するのではなく、VDI 環境を介してクラウド側のブラウザからサービスへアクセスする構成を検討した。これにより、利用者側端末へのデータ保存を最小化し、クラウド側の管理された環境内で AI 推論を実行する運用が可能となる。

さらに、医療 AI サービスは開発段階または限定利用段階では使用頻度が一定でないため、常時稼働する仮想マシンやコンテナ基盤のみで運用すると、利用頻度に比して運用コストが高くなる可能性がある。この課題に対応するため、API Gateway、オブジェクトストレージ、関数実行基盤、Web Application Firewall、Content Delivery Network 等を組み合わせたサーバレスアーキテクチャへの展開を想定し、必要時のみ推論処理を実行する構成を検討した。

このように、本研究では、グラム染色画像を用いた菌種判別 AI について、AI モデルの開発にとどまらず、クラウド上で安全かつ効率的に提供するための実装構成を整理した。これにより、今後、医療機関内端末、クラウド実行環境、AI 推論サービス、結果表示画面を連携させた実証へ進める基盤を構築した。

D. 考察

本分担研究では、クラウド上の医療 AI 利用促進を見据えた医療 AI 開発として、グラム染色画像から感染症起因菌同定を支援する AI モデルを開発した。特に、培養条件別に学習済みモデルを構築し、判別対象菌の培養条件に応じてモデルを選択する点が、本研究の重要な技術的特徴である。

グラム染色画像は、感染症診療において早期に得られる情報であり、安価かつ迅速である。一方で、外観が類似する菌種の判別には限界があり、熟練者でも判断が困難な場合がある。本研究では、ディープラーニングにより、ヒトの目では捉えにくい微細な画像特徴を学習させることで、CNS と SAU のような外観類似菌種の判別精度向上を目指した。6 分割交差検証において、培養条件別モデルが培養条件を考慮しないモデルより高い認識精度を示したことから、培養条件を考慮したモデル選択は有用である可能性がある。本技術は、菌血症や敗血症の初期診療において、抗微生物薬選択や追加検査、デバイス管理の判断を支援する可能性がある。特に小児専門病院では、免疫不全患者、移植後患者、集中治療を要する患者など、感染症の重症化リスクが高い患者が多く、迅速な診療支援の意義は大きい。

本研究で開発したグラム染色画像 AI は、画像を入力して推論結果を返すという処理構造を有するため、クラウド上の医療 AI サービスとして実装しやすい特徴を持つ。顕微鏡画像はデジタル画像として取得可能であり、医療機関側で撮像した画像を安全に送信し、クラウド側で AI 推論を行い、菌種判別結果を返す構成とすることで、専門家が常駐しない施設や医療資源の限られた地域でも、一定の診療支援を受けられる可能性がある。一方で、医療 AI をクラウド上で利用する場合、AI モデルの精度だけでなく、データの流れ、認証、アクセス制御、通信経路の保護、ログ管理、実行環境の分離、費用対効果を含めた運用設計が重要となる。特に、電子カルテ端末など医療機関内ネットワークに接続された端末からクラウドサービスを利用す

る場合には、従来の境界防御の考え方だけでは不十分であり、利用者、端末、サービス、データごとに権限を確認するアイデンティティベースのアクセス制御が必要となる。

本研究で検討した VDI 環境を介した利用形態は、医療機関側端末に画像データや解析結果を直接保存しない運用を可能にし、医療データを管理されたクラウド環境内で扱うための一つの現実的な方法と考えられる。また、コンテナ化は、開発環境と運用環境の差を小さくし、AI モデルやウェブアプリケーションの移植性を高める点で有用である。さらに、サーバレスアーキテクチャは、使用頻度が変動する医療 AI サービスにおいて、常時稼働リソースを減らし、利用量に応じたコスト管理を行ううえで有用である。ただし、サーバレス化や VDI 利用により直ちに十分な安全性が保証されるわけではない。実際の臨床利用では、画像データの匿名化、保存期間、監査ログ、障害時対応、推論結果の責任範囲、医療情報システムとの接続可否、院内セキュリティポリシーとの整合性を検討する必要がある。また、AI 推論結果は最終診断ではなく診療支援情報として扱い、培養同定、薬剤感受性検査、患者背景、臨床所見と統合して判断する運用が不可欠である。したがって、本分担研究における医療 AI 開発は、単に菌種判別モデルを作成するだけでなく、クラウド上で安全に利用できる医療 AI サービスへ発展させるための実装上の課題を明確にした点に意義がある。今後は、実際の医療機関端末からの利用を想定した接続実証、施設間で異なるネットワーク制約への対応、利用者認証およびログ管理の標準化、ならびに臨床現場で受け入れ可能な表示形式の検討が必要である。

E. 結論

クラウド上の医療 AI 利用促進を見据えた医療 AI 開発として、グラム染色画像を用いた感染症起因菌同定支援 AI を開発した。培養条件別に複数の学習済みモデルを構築し、判別対象菌の培養条件に応じてモデルを選択することで、CNS と SAU のような外観類似菌種の判別精度向上が示された。本技術は、菌血症・敗血症診療における早期の治療方針決定、抗微生物薬適正使用、薬剤耐性菌対策に資する可能性がある。

また、本分担研究では、グラム染色画像を用いた感染症起因菌同定支援 AI を開発するとともに、クラウド上での利用を想定した実装構成を整理した。画像入力、AI 推論、結果表示までをウェブアプリケーションとして提供可能な構成とし、コンテナ化、VDI 環境、サーバレスアーキテクチャを組み合わせることで、安全性、運用効率、コスト最適化を考慮した医療 AI サービスとして発展させ得ることを確認した。

今後は、AI モデルの外部検証と臨床評価に加えて、電子カルテ端末等から安全に利用するための認証、アクセス制御、通信、ログ管理、データ保護の実証を進める必要がある。本研究で整理した実装構成は、感染症起因菌同定支援 AI に限らず、クラウド上で医療 AI を安全に利用するための実証基盤として応用可能である。

F. 研究発表

該当なし

G. 知的財産権の出願

松井 俊大, 岡村 浩司. 菌種判別装置、菌種判別方法および菌種判別プログラム. 特願 2025-018598 (2025 年 2 月 6 日)

資料　クラウド利用を想定した感染症起因菌同定支援 AI の全体構成

別紙 3

厚生労働科学研究費補助金
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
クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言

研究代表者　岡村 浩司　国立成育医療研究センター 室長

研究要旨

人工知能技術の急速な進展は医療分野にも多大な可能性をもたらし、医療の質向上はもちろんのこと、効率化、地域格差の解消、医療従事者の負担軽減などを目指した取り組みが活発に展開されている。国立成育医療研究センターでは AI ホスピタル事業を契機として、職員を対象としたデータサイエンス教育、啓蒙活動を出発点に、グラム染色画像を入力とした感染症起因菌同定支援、尿沈渣顕微鏡写真からマルベリー小体を自動検出するファブリー病スクリーニングなど、実診療における補助手段としての医療 AI サービスの開発を進めてきた。これらのサービスは医療 AI プラットフォーム技術研究組合との連携のもとでコンテナ化され、クラウドからの公開と仮想デスクトップ基盤を介した安全な通信環境の構築が図られ、さらには運用コストの最適化を目的としたサーバレスアーキテクチャへの移行も行われた。一方、大規模言語モデルの技術革新、AI エージェントの登場によってアプリケーション開発は AI 支援型から駆動型へと移行しつつある。AI 駆動型開発による再構築を試み、開発効率、コード品質、セキュリティ実装の各面において従来手法との比較を行ったところ、定型的な作業における大幅な効率化の一方で、医療、情報、セキュリティの各専門知識を連携させた指示と最終的な品質確認の不可欠性を確認した。こうした変化と並行し、医療 AI サービスの普及を阻む要因として、情報管理部門が電子カルテネットワークへの接続に過度な恐怖感を抱き、新たな取り組みを忌避する事例が多いことも明らかとなった。医療 AI サービスは推論結果を返すのみで個人情報を保持しない構造であり、ランサムウェア攻撃の主要標的となった事例は確認されていない。責任回避を優先する組織的傾向がサービス普及の機会を逸失させている現状がある。さらに、生成 AI および AI エージェントの登場は、セキュリティ対策と人材育成の両面において従来の専門家依存型の体制からの脱却を可能にしつつあり、基本的な脆弱性への対応や未経験者による開発支援といった領域での有効性が示されている。加えて、クラウドプロバイダが提供するマイクロサービスアーキテクチャはゼロトラストの実装を容易にする特性を多く備えており、コスト削減とセキュリティ強化の同時実現という観点から、生成 AI 登場以前に設計された既存の SASE 等のセキュリティツールに代わる、新たなセキュリティ対策としての地位を固めつつある。本研究は、これら一連の技術的、組織的、制度的課題を横断的に検討し、電子カルテ端末から医療 AI サービスを安全かつ安心して利用できる環境の実現に向けた技術的、運用的指針を提示する。

A. 研究目的

人工知能技術は、ディープラーニングの登場から生成 AI さらには AI エージェントへと急速に進化を遂げ、医療分野におけるその影響はもはや研究開発の領域にとどまらず、サービスの開発、運用、セキュリティ対策のあり方そのものを根本から塗り替えつつある。こうした技術変革の潮流のなかで、皮膚がん診断をはじめとする数多くの有用性が実証されて以来、医療の質向上、効率化、地域格差の解消、医療従事者の負担軽減等を目指した研究開発が世界規模で活発に展開されてきた。我が国においても内閣府主導の戦略的イノベーション創造プログラムのもとで2018年よりAIホスピタルの取り組みが開始され、国立成育医療研究センター(NCCHD)は医療 AI プラットフォーム技術研究組合(HAIP)とともに採択を受け、感染症起因菌同定支援、腎細胞がん病理画像グレーディング支援、ファブリー病スクリーニングという三つの医療 AI サービスをコンテナとして実装し、限定的な公開ながら実運用可能な状態へと到達した。これらのサービスは Linux サーバ上のウェブアプリケーションとして開発され、コンテナ化と仮想デスクトップ基盤(VDI)を介したクラウド公開によって開発効率、運用コスト、セキュリティの各側面での改善が図られてきたが、電子カルテ端末からの安全なアクセスの実現、さらには患者および市民を含む一般ユーザへの開放という最終目標に向けては、依然として多くの技術的、組織的課題が残されていた。

こうした状況に対し、本研究が直面してきた課題の性質は、研究の進展とともに大きく変容してきた。当初はゼロトラストセキュリティモデルの実装とSASEアーキテクチャの試験的導入を中心とした技術的検討が主眼であったが、2024年末頃よりAIコーディングエージェントの実用化が急速に進み、開発のあり方そのものが根本から変わりつつある。大規模言語モデルと AI コーディングエージェントを組み合わせた AI 駆動型開発の実践において、ユーザが日本語の指示を与えるだけで、開発環境の整備からコーディング、テスト、デバッグ、ドキュメント作成に至るソフトウェア開発の全工程をエージェントが自律的に推進する状況が現実のものとなった。ファブリー病スクリーニングシステムの再構築を題材とした検討では、大学院生による未経験者開発においても物体検出 AI モデルおよびウェブアプリケーションの構築が実現され、AIエージェントが人材育成のツールとしても高い有効性を持つことが示された。また、仮想マシン上でのウェブサーバ運用からサーバレスアーキテクチャへの移行は、コスト効率の観点のみならず、サーバレスの各構成要素がアイデンティティベースのアクセス制御、すなわちゼロトラストの思想に沿って設計されているという特性から、セキュリティ強化の観点においても極めて合理的な選択であることが確認された。一方で、クラウドサービスへの依存度が高い設定管理の複雑さという課題も明らかとなったが、この領域こそ AI エージェントの活用が最も効果を発揮しうる領域でもある。

セキュリティ対策に関して、国家サイバー統括室によるアタックサーフェス管理(ASM)の継続的な調査対象となっている本研究環境では、従来の開発手法において OpenSSL やウェブサーバのバージョン問題、WordPress の残存ファイルといった指摘を受けてきた経緯がある。しかし AI 駆動型開発への移行後は、こうした指摘がなくなったことが確認されている。AIエージェントがSQLインジェクション対策や XSS への対処を含むセキュリティ実装を開発プロセスの中で

自律的に提案、適用する能力を持つことが、この変化の主要な要因と考えられる。従来、セキュリティ対策は専門家の知識と経験に依存する領域とされてきたが、AIエージェントの活用によってその民主化が現実のものとなりつつあることを、本研究の経験は具体的な形で示している。そして2026年になり、Anthropicが発表したClaude Code Securityの登場は、この状況をさらに決定的に変化させるものであった。コードベース全体のデータフローを横断的にトレースし、複数コンポーネントにまたがる複雑な脆弱性パターンを検出する能力、そして敵対的検証プロセスによる誤検知の大幅な削減は、従来の専門家集団による脆弱性探索という作業の前提を根底から覆すものであり、医療機関の情報管理者が抱いてきた過度な恐怖感や責任回避的な姿勢に対しても、客観的かつ実証的な安全性の根拠を提示できる可能性を秘めている。

本研究の目的は、以上の技術的および社会的変化を踏まえ、電子カルテ端末から医療AIサービスを安全かつ安心して利用できる環境の実現に向けた技術的、運用的指針を提示することにある。具体的には、AI駆動型開発がもたらす開発効率、コード品質、セキュリティ実装への影響を実証的に検討し、サーバレスアーキテクチャへの移行によるゼロトラスト実装の現実的な経路を示し、Claude Code Securityに代表される最新のAIネイティブなセキュリティツールの位置づけを医療情報セキュリティの文脈において整理する。また、これまで専門家依存、人材不足という構造的問題として語られてきたセキュリティ対策と開発体制の課題が、AIエージェントの積極的な活用によって解決可能な問題へと性質を変えつつあることを示し、医療、情報、セキュリティの各専門領域が従来とは異なる形で連携しながら、患者および市民の参画を促しつつ医療AI全体の発展へと繋げていくための新たな体制構築の方向性を論じることを、本研究の目的とする。

B. 研究方法

感染症起因菌同定支援およびファブリー病スクリーニングともに、顕微鏡画像のアノテーションにはMicrosoft VoTTを用いた。ラベルと位置情報をJSON形式で出力し、画像分類のための切り出しや、物体検出のためのYOLO形式への出力を独自Pythonスクリプトで行った。

感染症起因菌同定支援では、NCCHDの患者から得られた画像データを用い、腸内細菌科のバクテリア、エンテロコッカス属のバクテリア、バシラス属のバクテリア、レンサ球菌属のバクテリア、ヘモフィルス属のバクテリア、シュードモナス属のバクテリア、コアグラーゼ陰性ブドウ球菌、黄色ブドウ球菌、緑膿菌、肺炎レンサ球菌、化膿レンサ球菌、リステリア、コリネバクテリウム、淋菌などのグラム陰性球菌、さらに真菌であるカンジダを区別して検出するためのアノテーションを手作業で行なった。

まずTensorFlowを利用して画像の分類を試みた。データ拡張にはKerasを利用した。ImageNetで訓練されたInception V3の転移学習をHitachi SR24000/DL1を用いて実行した。物体検出については、Microsoft Azureコンピューティングインスタンスのサイズ Standard_NC12s_v3を利用して構築されたHAIPのAI開発基盤を利用した。アルゴリズムは、PyTorchを基盤とするYOLOv5を採用した。CentOS 7に設定したYOLOv5を用いて訓練を行い、物体検出モデルを作成した。

ファブリー病スクリーニングでは、NCCHDだけでなく、聖マリアンナ医科大学、上海の復旦大学の3機関から患者の尿検体を

収集した。各検体 10 mL を 3000 rpm で 10 分間遠心分離し、得られた沈渣を再懸濁させ顕微鏡化で観察、静止画及び動画の撮影を行なった。尿沈渣の構成成分は、マルベリー小体に加え、赤血球、白血球、結晶、細菌、精子、扁平上皮細胞、マルベリー小体様構造物、その他、合計 9 カテゴリに分類した。

Amazon EC2 のインスタンスタイプ g4dn.xlarge を利用し、Amazon Linux 2 に設定した YOLOv8 を用いて訓練を行い、物体検出モデルを作成した。

コンテナ作成は、CentOS 7 に設定した Docker にて行い、デプロイ確認は Minikube を利用した。ウェブアプリケーションとしての公開は Amazon ECS を利用し、また、HAIP サービス事業基盤からの公開は Azure Kubernetes Service を利用した。VDI クライアントは Microsoft Remote Desktop、サーバは Azure Virtual Desktop でクラウドの Windows にアクセスし、そのブラウザから HAIP ラボ基盤、およびサービス事業基盤にデプロイされているコンテナにアクセスさせた。ウェブカメラの制御は JavaScript のメディアストリーム API に含まれている getUserMedia を利用し、クラウドの Windows に接続されているデバイスを動作させた。

遺伝カウンセリング支援は、Amazon SageMaker から AWS SDK for Python を利用して Amazon Bedrock を利用する環境を構築し、オレゴンリージョンの Anthropic Claude 3 Sonnet および Claude 3.5 Sonnet を利用して比較を行った。サービス間のアクセス許可は AWS IAM のロール作成にて行った。RAG は最初は Amazon Kendra にて構築したが、後に Amazon Bedrock Knowledge Bases の利用に移行した。

サーバレスコンピューティングは、AWS Lambda に加え、Amazon API Gateway、Amazon S3、Amazon CloudFront、AWS WAF を用いて基本的なウェブサービスを構築し、必要に応じて Amazon Bedrock などを組み込んだ。サービス間のアクセス許可については AWS IAM を利用した。

AI コーディングエージェントについては、VS Code の拡張機能である Cline、また、Amazon Q Developer およびその後継である Kiro を試し、LLM としては主に Anthropic Claude Sonnet を用いた。

C. 研究結果

高度先進医療を提供する NCCHD は、免疫不全、臓器移植後に免疫抑制剤の投与を受けるなど、感染症に関してハイリスクな患者を多数抱えている。適切な抗生物質の選択など治療方針の決定は患者の予後に直結し、また不必要な抗生物質の使用は耐性菌の問題もあり、責任ある対応が求められている。そこで菌血症患者検体の顕微鏡写真から起因菌を迅速に同定する医療 AI の開発を行なった。

小児の菌血症患者の血液培養からグラム染色を行なって得られた顕微鏡写真に、生化学反応や質量分析によって決定された細菌や真菌の種類を正解ラベルとして教師データを作成した。まず、10 μm 四方のクロップに対してアノテーションを行い、グラム陽性

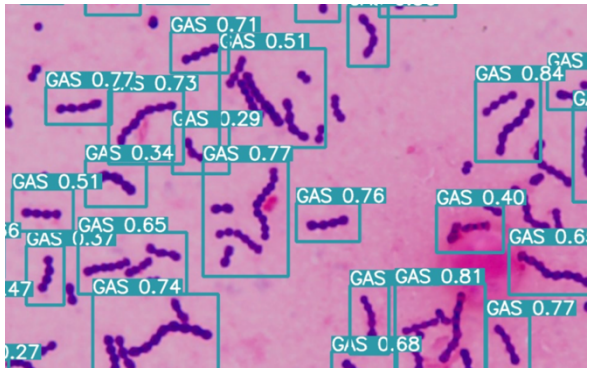


図 1 人食いバクテリア、化膿レンサ球菌の検出

桿菌、グラム陰性桿菌、グラム陽性球菌、グ

ラム陰性球菌、それから背景の 5 分類を試みた。Inception V3 の転移学習により訓練を行ったモデルに対し、ランダムに切り出した 10 μm 四方のクロップでテストを行った。多数のクロップに対する結果のうち、背景を除いた多数決を取ることで良好な結果が得られることを確認した。

感染症起因菌をより詳しく同定するため、15 細菌および 1 真菌を物体検出により区別するアノテーションを行なった。赤血球を加えた 17 ラベル、23,753 枚の写真から 347,234 クロップの切り出しで訓練を行なった。モデルは YOLOv5x を採用し、V100 を搭載する HAIP の AI 開発基盤で、150 エポック 34 時間をかけて独自モデルを完成させた(図 1)。

図 2 VDI でクラウドのウェブカメラを利用

本システムでは、互いに異なる培養条件に対応する複数の学習済みモデルを構築し、判別対象菌の培養条件に応じたモデルを選択して解析を行うことで、外観が類似した菌種であっても高精度な判別を可能としており、この点については特許を出願した。

扱う医療データを安全にやり取りする目的で、コンテナを VDI 環境で公開している。ユーザはリモートデスクトップクライアントを利用して、クラウドのブラウザにアクセスし、デスクトップ画像の通信で利用する形態である。顕微鏡写真はデータをアップロードすることもできるが、顕微鏡に接続されたコンピュータからの簡易的な利用を見据え、ディスプレイに表示された画像をウェブカメラで撮影して検出できるように設計されている(図 2)。その際には、ユーザが手元で操作するウェブカメラからのリアルタイム入力は、VDI によりクラウド側に存在するウェブカメラと直結している。

次にファブリー病であるが、この疾患は分解酵素の欠失や活性の低下により不必要な糖脂質が細胞内に蓄積し、年月を経て体全体に障害を与える先天性の代謝異常症である。10 歳頃になって手足の痛みなどの症状が現れるが、診断は難しく、原因が判明した頃には心臓や腎臓などの損傷が進み、40 歳頃に亡くなるケースが多々見られる。酵素補充療法などの治療が確立しており、早期に発見することがきわめて重要となる。

患者の尿には、糖脂質が蓄積した糸球体上皮細胞由来の特異的な形状の物体が観察されることが報告されていて、マルベリー小体と呼ばれている。NCCHD では独自にサンプルを収集し、また聖マリアンナ医科大学、上海の復旦大学小児医療センターの協力も得て、顕微鏡写真にマルベリー小体が写っているか否かを判別できる医療 AI モデルを開発し発表した。限られた数のサンプルから大量

の写真撮影を行い、尿に含まれるマルベリー小体、マルベリー小体様物質、赤血球、白血球、扁平上皮細胞、精子、細菌、結晶に加え、その他の計9種類を識別する物体検出モデルを作った (図 3)。

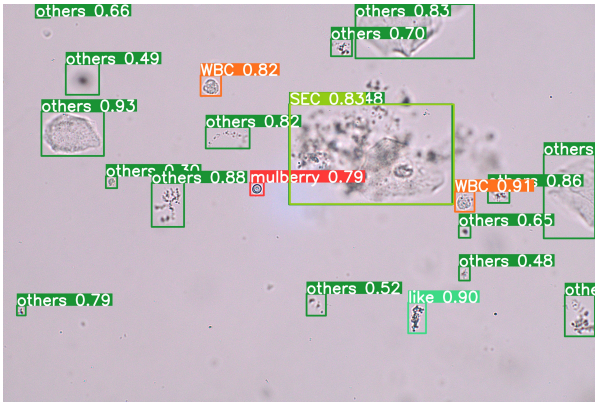


図 3 尿沈渣顕微鏡写真からのマルベリー小体検出

その後、AI コーディングエージェントが利用できるようになり、プログラミング未経験であった小児科医の大学院生にモデルの再構築とウェブアプリケーション作成に取り組ませ、課題等を調査した。通常、ウェブアプリケーション開発には複数のプログラミング言語やフレームワーク、インフラ知識の習得が前提とされるが、AI コーディングエージェントの活用により、そのような広範な事前学習なしにある程度機能するアプリケーションの構築が可能であることが示された。サーバレスアーキテクチャにおける個別サービスの詳細仕様についても、AI エージェントが代替して実装することで、未経験者の学習負担が大幅に軽減された。一方で、AI エージェントの出力が確率的であることに起因するリスクへの対応や、広範な権限を持つ AI への不安、そして最終的な品質確認における人的レビューの必要性など、未経験者が直面する固有の課題も明らかとなった。プログラミングスキルそのものの重要性は依然として認識されており、AI エージェントの活用が開発参入の障壁を下げる一方で、それを適切に活用、監督するための素養は引き続き求められることが示唆された。

経験者の立場からは、従来の開発手法と比較して大幅な効率向上が認められた。特にウェブサービスにおけるフォーム処理、ファイルのアップロード機能、および CRUD 操作においてコーディング負担の軽減が明らかであった。エラー対応が網羅的に実装され、一貫したコーディング規約が自動的に適用された。コンテナ化においては、環境構築の効

図 4 AI 駆動型開発によるウェブアプリケーション

率化とイメージサイズの軽量化が顕著であり、モニタリング等の設定も併せて構成された。サーバレスアーキテクチャの採用においては、個別サービスの詳細仕様を AI エージェントが代替して実装することによる学習負担の軽減が認められ、プログラミング未経験者にとって特筆すべき成果であった(図 4)。

AI エージェントによるセキュリティ実装として、コンテンツセキュリティの領域では XSS 対策、SQL インジェクション対策、ファイルアップロード制御が自動的に組み込まれた。セキュリティヘッダーの設定においては、他サイトからの不正アクセス制御、悪意あるコンテンツの読み込み防止、クリックジャッキング対策などの基本的防御機構が適用された。認証、認可の基本実装としては、安全なユーザー認証トークンの管理、セッション管理、およびアクセス制御が実装された。セキュリティパターンの統一、継続的な脆弱性評価、リアルタイムモニタリング、およびインシデントへの自動対応が標準的に組み込まれた。一方で、一つの指示によってあらゆるセキュリティ対策が網羅されるわけではなく、人的レビューの実施、定期的な更新、セキュリティポリシーの見直し、安全な MCP の利用、および固有要件への個別対応が別途必要であることが明らかとなった。また、今回のような医療 AI サービスの開発において利用可能な情報セキュリティチェックリストを Claude Sonnet 4.6 を用いて作成した(資料)。

大学院生からは、AI エージェントの活用により機能するアプリケーションの構築が可能であったとの評価が得られた。一方で、確率的な動作に起因するリスクへの対応、広範な権限を持つ AI への不安、プログラミングスキルの重要性の再認識、および人的な最終確認の必要性についての懸念も示された。AI エージェントを活用した標準化された開発手法への移行が効率的な人材育成につながる可能性が示唆されるとともに、従来型の人材戦略からの脱却という観点からも有効であるとの見解が述べられた。課題は残るものの、当初は悲観的に捉えていた状況に対して楽観的な展望を持って取り組んでいきたいとの感想が得られた。

日本人における頻度は欧米人と比べて高く、7000 人に 1 人と言われている。7000 検体に 1 検体、マルベリー小体が存在するか否かを医師や臨床検査技師が手作業で調べることはきわめて苦痛で困難であり、見落としも多くなると考えられる。マルベリー小体はあったとしても、多数確認されるわけでもない。この物体検出は動画にも対応しており、実際には、大量の写真あるいは動画を自動的に撮影し、自動的に検出するスクリーニングとしての開発を進めており、毎年各学年で行われる学校検尿と結びつけた社会実装を目指している。

最後に、遺伝カウンセリングを生成 AI で代替する試みであるが、まず、日本遺伝カウンセリング学会と日本人類遺伝学会が実施している認定遺伝カウンセラーの認定試験でどれほどの点数を取ることができるのか確認してみた。大規模言語モデルは Amazon Bedrock から API を介して Claude 3 Sonnet を利用し、2020 年度の基礎問題全 26 問の日本語原文をプロンプトとして入力したところ、正解率は 48%であった。選択肢を正解まで絞り切れていない回答が 11 問あり、これらには半分の点数を与えて計算しているが、合格レベルにはない状況である。その後、Claude 3.5 Sonnet が発表されたので改めて試したところ、正解率は 85%で合格レベルまで跳ね上がった。試験問題を解答するようシステムプロンプトとして指示を与えているだけでこ

のような結果が得られ、最近では基盤モデルとも呼ばれる大規模言語モデルは日進月歩の改良が進められていることがよく分かる。正解が得られなかった点については、関連情報を含むウェブページの HTML を集め、RAG(検索拡張生成)の構築により正解を出力できるよう改変することができた。

マルチモーダルであるため、家系図を理解することもでき、関連する論文を PDF のまま読み込んで患者向けに分かりやすい情報提供を行うこともできる。実際のカウンセリングにおいても、役に立つ情報を引き出せているが(図 5)、そもそも医師の指導のもとに行われなければならず、ハルシネーションやプライバシーの問題など解決しなければならない問題が多く残っている。

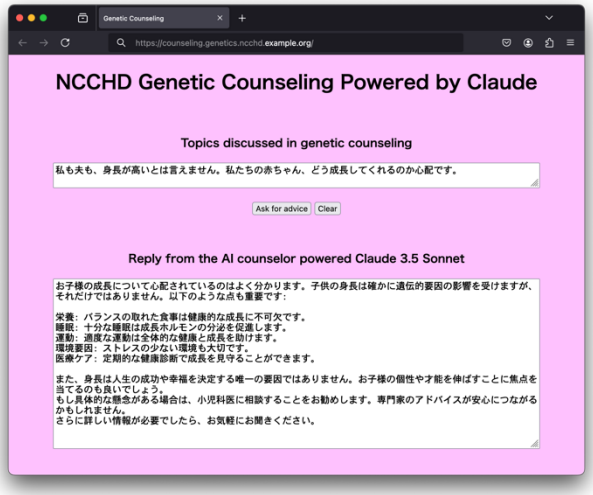


図 5 遺伝カウンセリングを生成 AI で代替

これら医療 AI サービスは開発段階ということもあるが、そうでなくとも使用頻度が高いとは言えず、クラウドの仮想マシンやコンテナとしての運用では、24 時間 365 日の連続稼働となり、ほとんど使われていないのに課金される状態が続くことになる。これに対し、サーバレスアーキテクチャを採用した場合は必要最小限のリソースで、API のコール数とデータ転送量に対してのみ課金が発生するため、コストを大幅に下げることが可能である。サーバーのセットアップ、メインテナンス、スケーリングといったインフラ管理からも解放される。各コンポーネントには自動的に復旧される仕組みも備わり、耐障害性の高い仕組みを作り上げることができ、作業を進めている(図 6)。

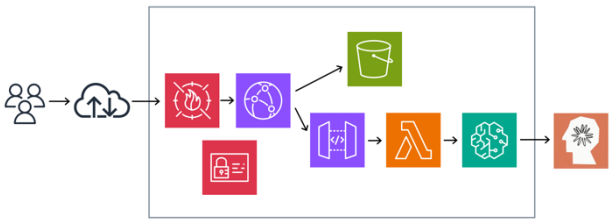


図 6 サーバレスのビルディングブロック例

D. 考察

従来のクラウドコンピューティングでは、1 つの仮想マシンに数多くのサービスや機能を載せ、運用を行っていたが、スケーラビリティ、独立性、柔軟性、コスト効率、開発速度などの点からクラウドプロバイダ自体がマイクロサービスアーキテクチャに移行し、クラウドユーザに対して各種多様なサービスを提供している。これらがサーバレスのビルディングブロックとなり、ユーザが用意する仮想マシンが不要となる。サーバレスを採用することは、セキュリティの観点においても多くの利点をもたらす。攻撃範囲の限定、迅速な脆弱性対応、動的な実行環境による攻撃対象からの回避、細粒度の最小権限付与によるリスク低減、監視ログの細分化による問題特定の容易化といった特性は、医療情報システムにおけるセキュリティ要件と親和性が高い。このような環境では、従来のネットワーク境界に依存したセキュリティ対策は成り立たず、ID ベースのアクセス制御が必要となるが、AWS IAM、Microsoft Entra ID、

Google Cloud IAM といったサービスがこれを担い、ゼロトラストセキュリティモデルの実現を見通し良く支援する。

サーバレスアーキテクチャへの移行は、その利点が明確である一方、各クラウドプロバイダが提供する個別サービスの詳細仕様の習得や、既存システムからの移行作業における複雑な設定変更など、開発者にとって相応の学習コストと実装負担を伴うものであった。しかしながら今回の取り組みを通じて、AI コーディングエージェントの活用によりこれらの障壁が大幅に低減されることが示された。AI エージェントは各クラウドサービスの詳細仕様を代替して実装するのみならず、コンテナ化における環境構築の効率化、イメージサイズの軽量化、モニタリング設定の自動構成といった移行作業全般を効率的かつ一貫した品質で遂行する。さらに、XSS 対策、SQL インジェクション対策、セキュリティヘッダーの設定、認証、認可の基本実装といったセキュリティ対策が標準的に組み込まれることから、サーバレスへの移行作業そのものをより安全に進められることが期待される。すなわち、AI コーディングエージェントの活用は、サーバレスアーキテクチャが本来持つセキュリティ上の利点を損なうことなく、その移行プロセスを加速させる手段として有効であると考えられる。

今回の結果は、AI コーディングエージェントが定型的な実装作業において顕著な効率化をもたらすことを示している。標準的な実装の自動化、一貫性のある対策の適用、セキュリティパターンの統一といった利点は、特に未経験者にとって開発への参入障壁を大きく下げるものである。しかしながら、本取り組みを通じて、むしろ経験者が AI エージェントを活用することによる恩恵がより多岐にわたることが示唆された。AI エージェントは定型的な作業を効率的に処理する一方、一つの指示によってあらゆるセキュリティ対策が網羅されるわけではなく、実運用に向けては医療、情報、セキュリティの各専門知識を連携させた立場からの具体的な指示と最終的な品質確認が不可欠である。

患者情報保護をはじめとする医療業界固有の要件やセキュリティ対策について、生成 AI が初期段階から網羅的な対応を行うわけではないことが明らかとなった。現状、電子カルテネットワークから医療 AI サービスへの直接アクセスは許容されておらず、インターネット側への接続は NTP サーバとの同期や MDM サーバの認証に限られているなど、医療情報システムには固有の制約が存在する。このような環境においては、利用者側が明確な方向性と具体的な指示を持って AI エージェントに臨む必要があり、医療分野と情報分野のこれまでとは異なる新しい形の連携が重要となる。セキュリティポリシーの継続的な更新、安全な MCP の利用、および固有要件への個別対応を組み合わせた、医療、情報、セキュリティの専門家による包括的な管理体制の構築が求められる。

医療機関の ICT セキュリティ分野では、専門家の慢性的な不足、人材確保の地域格差、不公平な処遇といった深刻な人材課題が存在する。AI エージェントの活用は、常時監視体制の実現、異常検知の高度化、即時対応、インシデント分析の効率化、最新セキュリティ情報の継続的更新、ベストプラクティスの自動適用、規制要件への適合性確認、脆弱性評価の自動実施、パッチ適用の自動評価とロールバック保証付き運用管理を通じて、これらの課題解決に寄与する可能性がある。さらに、教育の自動化、対応訓練の実施支援、マニュアル類の自動更新といった人材育成面での活用も期待される。AI エージェントを活

用した標準化された開発手法への移行は従来型の人材戦略からの脱却を促し、医療機関における一般的な業務運営の一部として AI エージェントが機能する未来、そして今後の若い世代がこれらの課題を独自に解決してゆく新たな道筋を拓くものと考えられる。今後の医療 AI 開発において AI エージェントの重要性は無視できないものとなっており、医療、情報、セキュリティの専門家が連携しつつ AI エージェントを適切に指示、監督できる体制の整備が急務である。

E. 結論

開発を行った医療 AI サービスに対し、運用コストの最適化を主な動機としてサーバレスアーキテクチャへの移行を進めた。その過程でマイクロサービスアーキテクチャがゼロトラスト実装を容易にする特性を多く備えていることを理解することができた。各構成要素がアイデンティティベースのアクセス制御を前提として設計されているサーバレス環境は、概念としては提唱されながらも具体性に乏しいと感じられてきたゼロトラストを、自然な形で実装へと落とし込める基盤となりうる。一方で、ゼロトラストを標榜する統合的な商用セキュリティサービスは依然として複雑で分かりにくく、必要性が不明瞭な高機能とそれに付随する高価格を前にすれば、医療機関が気安く導入できるものではない。また、生成 AI 登場以前に設計された SASE をはじめとする既存のセキュリティツールの多くは、サーバレス運用を前提としておらず、現在の開発、運用環境の実態と乖離しつつあることも、本研究を通じて明らかとなった課題の一つである。

こうした状況に対し、この一年間で起きた変化は、当初の想定をはるかに超えるものであった。AI コーディングエージェントの実用化により、ソフトウェア開発は AI 支援型から AI 駆動型へと本質的なシフトを遂げ、開発効率、コード品質、セキュリティ実装の各面において従来手法との明確な差異が生じている。国家サイバー統括室による ASM の継続的な調査において、従来の開発手法では指摘を受けていた OpenSSL のバージョン問題や WordPress の残存ファイルといった脆弱性が、AI 駆動型開発への移行後には一切検出されなくなったことは、その効果を客観的に示す具体的な成果である。SQL インジェクション対策や XSS 対策をはじめとするセキュリティ実装が AI エージェントによって開発プロセスに自律的に組み込まれるようになったことは、これまで専門家の知識と経験に依存してきたセキュリティ対策の民主化という観点から、本質的な意義を持つ。

そして 2026 年、Anthropic による Claude Code Security の発表は、医療情報セキュリティの文脈においても見過ごすことのできない画期的な転換点となった。コードベース全体のデータフローを横断的にトレースし、複数コンポーネントにまたがる複雑な脆弱性パターンを検出する推論ベースの能力と、AI が自らの検出結果に異議を唱える敵対的検証プロセスによる誤検知の大幅な削減は、従来の専門家集団による脆弱性探索という作業の前提を根底から変えるものである。重大度のみならず信頼度スコアを付与することで対処の優先順位付けを合理化し、検出から修正パッチの提案、適用までをシームレスなワークフローで完結させるこの仕組みは、セキュリティ専門人材の慢性的な不足という医療機関が長年抱えてきた構造的問題に対して、現実的な解を提示するものといえる。先日発表された Claude Mythos はそのレベルさらに引き上げていると報道されている。これまでランサムウェア被害の多くが引き起

こされてきたパスワード設定の不備などの基本的な脆弱性は、こうした AI ネイティブなセキュリティツールによって大幅に改善される可能性があり、医療 AI サービス自体が攻撃の主要標的となった事例が確認されていないという現実と合わせて考えれば、電子カルテネットワークへの接続に過度な恐怖感を抱き新たな取り組みを忌避してきた医療機関の情報管理者に対し、実証的な根拠をもって安全性を説明できる環境が整いつつある。

人材育成の観点においても、状況は大きく変わった。AI エージェントを活用することで、未経験の大学院生が物体検出 AI モデルとウェブアプリケーションの開発を独力で完遂できたことは、経験者や専門家への依存を前提とした従来の人材戦略からの脱却が現実のものとなったことを示している。AI エージェントは開発ツールであると同時に学習のツールでもあり、次世代の医療従事者や研究者が独自に課題を発見し解決していく可能性を、本研究の経験は具体的な形で示唆している。医療、情報、セキュリティという三つの専門領域がこれまでとは異なる形で連携しながら、患者および市民の参画を促しビッグデータに依存する医療 AI のさらなる発展へと繋げていくためには、こうした新しい開発、運用体制の構築を前向きに捉え、悲観的になりがちであった状況を積極的に転換していく姿勢が求められる。セキュリティ対策の実績を着実に積み重ねながら、管理者、患者、市民に対して分かりやすい説明を継続的に行うという地道な作業の重要性は変わらないが、その作業を支える技術的基盤は、この一年間で質的に異なるものへと変貌を遂げたといえる。

F. 研究発表

岡村 浩司, 山中 宏勇. AI 駆動型開発がもたらす医療 AI サービス構築の革新と課題. *第 45 回医療情報学連合大会*, **4-B-1-03** (2025)

Yamanaka H, So T, Sakamoto N, Aoto S, Li XK, Wang Y, Shen Q, Migita O, Kosuga M, Okamura K. Automated detection of mulberry bodies in urinary sediment for non-invasive Fabry disease screening. *Clin. Chem. Lab. Med.* [doi: 10.1515/cclm-2026-0345] (2026)

Hayashi H, Kashizuka E, Sakata K, Motomiya N, Asakawa Y, Hayasaki M, Yokoi T, Yoshida T, Nishina S, Okamura K. Detection of pediatric cataracts through non-invasive facial photography using deep convolutional neural networks for early diagnosis. *BMC Ophthalmol.* [doi: 10.1186/s12886-026-04795-9] (2026)

Yamanaka H, Okamura K. Exploring deep learning and data requirements through image classification of *Erigeron annuus* and *Erigeron philadelphicus*. *BMC Res. Notes* **19**, 127 (2026)

Fukami M, Okamura K, Sasaki S, Kagami M, Dateki S. Chromosomal and hormonal factors involved in human sexual dimorphism. *Endocr. J.* **73**, 175–181 (2026)

Miyai M, Tanaka-Yachi R, Aizawa K, Okamura K, Kusuhara H, Akutsu H, Nakamura K. Removing extracellular matrix from the cell surface prior to seeding enhances the adhesion of primary human hepatocytes to the culture vessel. *Genes Cells* **30**, e70059 (2025)

Taniguchi K, Hasegawa F, Okazaki Y, Hori A, Ogata-Kawata H, Aoto S, Migita O, Kawai T, Nakabayashi K, Okamura K, Fukui K, Wada S, Ozawa K, Ito Y, Sago H, Hata K. Approaches to evaluate whole exome sequencing data that incorporate genetic intolerance scores for congenital anomalies, including intronic regions adjacent to exons. *Mol. Genet. Genomic Med.* **13**, e70092 (2025)

Shibata M, Umezawa A, Aoto S, Okamura K, Nasu M, Mizuno R, Oya M, Yura K, Mikami

S. Applicability of the regression approach for histological multi-class grading in clear cell renal cell carcinoma. *Regen. Ther.* **28**, 431–437 (2025)

G. 知的財産権の出願

岡村 浩司, 仁科 幸子. 乳幼児の視覚異常スクリーニング方法、視覚異常スクリーニングシステム及び表示システム. 特願 2026-060427 (2026 年 4 月 1 日)

松井 俊大, 岡村 浩司. 菌種判別装置、菌種判別方法および菌種判別プログラム. 特願 2025-018598 (2025 年 2 月 6 日)

資料　医療 AI モデル開発とサービス公開における情報セキュリティチェックリスト

医療 AI モデル開発とサービス公開における情報セキュリティチェックリスト

対象： 医療 AI モデルの開発から公開・運用までの全フェーズ
目的： 安全な医療 AI サービスの構築と継続的な品質確保
注記： ☆印は LLM・AI エージェント活用時に特に注意が必要な項目

A. 開発環境・ツールのセキュリティ

A-1. AI エージェント・LLM ツールの選定と利用ポリシー

☐ 利用する LLM・AI エージェントのプライバシーポリシーを確認し、医療情報を含むプロンプトの入力禁止を徹底した ☆
☐ 組織としての利用ポリシーを策定し、開発チーム全員に周知した
☐ AI エージェントの出力が確率的であることを開発チーム全員が認識している ☆
☐ エンタープライズ向けプランまたはオンプレミス環境での利用を検討した

A-2. API キー・MCP 管理と権限付与

☐ API キーをソースコードに直接記述せず、秘密管理サービスを利用している（AI エージェント生成コードも含めて確認）☆
☐ MCP サーバの提供元が信頼できることを確認し、AI エージェントのアクセス範囲を最小限に制限した ☆
☐ AI エージェントによる自律的なコマンド実行に人的承認フローを設けた ☆

A-3. 開発・本番環境の分離

☐ 開発・ステージング・本番環境を明確に分離し、本番環境への自動デプロイに人的承認を組み込んだ
☐ 開発環境に実際の患者データ・個人情報を使用していない
☐ AI エージェントが生成した設定ファイルに本番環境の認証情報が含まれていないことを確認した ☆

B. AI モデル開発におけるデータセキュリティ

B-1. 学習データの管理

☐ 学習データの匿名化・非識別化が適切に行われている
☐ 学習データの取得・保存・転送時に暗号化が施されている
☐ 学習データへのアクセス制御が実装され、アクセスログが記録されている
☐ AI エージェントを用いたデータ処理スクリプトに患者情報が混入していないことを確認した ☆

B-2. モデルの管理

☐ 学習済みモデルのバージョン管理が行われている
☐ モデルの再学習・更新時にデータセキュリティの確認を再実施する手順が定められている
☐ モデルの出力に個人情報が含まれないことを確認した
☐ LLM を用いた特徴量生成・前処理において意図しないデータ漏洩がないことを確認した ☆

C. コード・アプリケーションセキュリティ

C-1. AI エージェント生成コードのレビュー

☐ AI エージェントが生成したコードを必ず人的レビューし、そのまま本番利用しない ☆
☐ 依存ライブラリの脆弱性を確認した（AI エージェントが古いバージョンを採用する場合がある）☆
☐ AI エージェントが一つの指示で全セキュリティ対策を網羅するわけではないことを認識し、個別に確認した ☆

C-2. 基本的なセキュリティ実装

☐ XSS 対策・SQL インジェクション対策が実装されている
☐ セキュリティヘッダーが適切に設定されている（他サイトからのアクセス制御、クリックジャッキング対策等）
☐ 安全なユーザー認証・セッション管理・アクセス制御が実装されている
☐ ファイルアップロードの検証・制御が実装されている

D. インフラ・クラウド・サーバレス構成

D-1. サーバレス移行とセキュリティ

☐ サーバレスアーキテクチャへの移行作業において AI エージェントを活用し、移行手順の一貫性と安全性を確保した ☆
☐ IAM による最小権限の原則が適用されている（AWS IAM・Microsoft Entra ID・Google Cloud IAM 等）
☐ サーバレス環境におけるデータの保存・転送時の暗号化が標準的に設定されている
☐ イベント駆動型サービス（AWS Lambda 等）における認証・リクエスト署名が適切に設定されている

D-2. コンテナ・監視設定

☐ コンテナイメージに不要なパッケージが含まれておらず、イメージサイズが最小化されている（AI エージェント生成の Dockerfile も確認）☆
☐ リアルタイムモニタリングとログ収集が設定されている
☐ 異常検知とインシデント自動対応の仕組みが構成されている
☐ パッチ適用の管理とロールバック手順が定められている

E. 医療固有の要件

E-1. 法的・倫理的要件

☐ 個人情報保護法・医療情報システムの安全管理に関するガイドラインへの適合を確認した
☐ 医療機器該当性の確認を行い、必要に応じて薬機法上の手続きを実施した
☐ 倫理審査・院内承認プロセスを経ている
☐ 患者情報保護に関する要件を AI エージェントへの指示に明示的に組み込んだ ☆

E-2. ネットワーク・アクセス制御

☐ 電子カルテネットワークと医療 AI サービス間の接続制限を確認・遵守している
☐ サービス側からの電子カルテネットワークへのアクセスが遮断されていることを確認した
☐ 許可された通信経路（NTP 同期・MDM 認証等）以外の外部接続が発生していないことを確認した
☐ AI エージェントが医療固有のネットワーク制約を認識した上で設定を生成していることを確認した ☆

F. AI サービス公開時のセキュリティ

F-1. 公開前確認

☐ 脆弱性評価・ペネトレーションテストを実施した（AI エージェントによる継続的な脆弱性評価も活用）☆
☐ 入力値の検証とサニタイズが全入力フォームに実装されている
☐ レート制限・DoS 対策が実装されている
☐ プロンプトインジェクション攻撃への対策を講じた（LLM を利用したサービスの場合）☆

F-2. 公開後の管理

☐ 利用者認証とアクセスログの記録・監視体制が整っている
☐ インシデント発生時の対応計画と連絡体制が整備されている
☐ 利用規約・プライバシーポリシーが整備・公開されている
☐ AI サービスの出力に関する免責事項と人的確認の必要性が明示されている ☆

G. 運用・保守・継続的管理

G-1. 定期的な評価と更新

☐ セキュリティポリシーの定期的な見直しと更新を実施している
☐ 利用する AI エージェント・LLM ツールのアップデートと変更内容を定期的に確認している ☆

☐ 依存ライブラリ・コンテナイメージの定期的な脆弱性スキャンを実施している
☐ AI モデルの再学習・更新時にセキュリティ確認を再実施する手順が定められている

G-2. 人的管理体制

☐ AI エージェントが生成・更新した設定・コード・ドキュメントの最終確認を人が行う体制が整っている ☆
☐ セキュリティに関する教育・訓練を定期的に実施している（AI エージェントによる支援も活用）☆
☐ インシデント対応訓練を定期的に実施している
☐ 担当者不在時のバックアップ体制が整っている

H. LLM・AI エージェント利用に関する固有リスク

H-1. AI エージェント利用時の固有リスク管理

☐ プロンプトに機密情報・患者情報・認証情報を含めていない ☆
☐ AI エージェントの自律的な判断に過度に依存せず、重要な意思決定には人的判断を介在させている ☆
☐ AI エージェントが生成したセキュリティ設定が、医療固有の要件を満たしているかを専門家が確認した ☆
☐ AI エージェントへの権限付与は必要最小限にとどめ、定期的に見直している ☆

H-2. AI エージェント活用の継続的改善

☐ AI エージェント活用による標準化された開発手法への移行が組織的に推進されている
☐ AI エージェントを活用した人材育成・教育の仕組みが整備されている
☐ AI エージェントの活用状況と成果を定期的に評価し、組織の開発プロセスに反映している
☐ 医療・情報・セキュリティの専門家が連携し、AI エージェントへの指示と最終確認を分担する体制が整っている ☆

改訂履歴 Ver. 1.0　Claude Sonnet 4.6 初版作成

別紙４

研究成果の刊行に関する一覧表

書籍

宇賀神 敦, Automation in Hospitals and Healthcare (Chapter56), *Springer Handbook of Automation (2nd Edition)*, 1209−1233, 2023

雑誌

岡村 浩司 (研究代表者)

Yamanaka H, So T, Sakamoto N, Aoto S, Li XK, Wang Y, Shen Q, Migita O, Kosuga M, Okamura K. Automated detection of mulberry bodies in urinary sediment for non-invasive Fabry disease screening. *Clin. Chem. Lab. Med.* [doi: 10.1515/cclm-2026-0345], 2026

Hayashi H, Kashizuka E, Sakata K, Motomiya N, Asakawa Y, Hayasaki M, Yokoi T, Yoshida T, Nishina S, Okamura K. Detection of pediatric cataracts through non-invasive facial photography using deep convolutional neural networks for early diagnosis. *BMC Ophthalmol.* **26**, 282, 2026

Yamanaka H, Okamura K. Exploring deep learning and data requirements through image classification of Erigeron annuus and Erigeron philadelphicus. *BMC Res. Notes* **19**, 127, 2026

Fukami M, Okamura K, Sasaki S, Kagami M, Dateki S. Chromosomal and hormonal factors involved in human sexual dimorphism. *Endocr. J.* **73**, 175–181, 2026

岡村 浩司. AI 駆動型開発がもたらす医療 AI サービス構築の革新と課題. *第 45 回医療情報学連合大会* 4-B-1-03, 2025

Miyai M, Tanaka-Yachi R, Aizawa K, Okamura K, Kusuhara H, Akutsu H, Nakamura K. Removing extracellular matrix from the cell surface prior to seeding enhances the adhesion of primary human hepatocytes to the culture vessel. *Genes Cells* **30**, e70059, 2025

Taniguchi K, Hasegawa F, Okazaki Y, Hori A, Ogata-Kawata H, Aoto S, Migita O, Kawai T, Nakabayashi K, Okamura K, Fukui K, Wada S, Ozawa K, Ito Y, Sago H, Hata K. Approaches to evaluate whole exome sequencing data that incorporate genetic intolerance scores for congenital anomalies, including intronic regions adjacent to exons. *Mol. Genet. Genomic Med.* **13**, e70092, 2025

Shibata M, Umezawa A, Aoto S, Okamura K, Nasu M, Mizuno R, Oya M, Yura K, Mikami S. Applicability of the regression approach for histological multi-class grading in clear cell renal cell carcinoma. *Regen. Ther.* **28**, 431–437, 2025

岡村 浩司, 松井 俊大. 電子カルテ端末からの利用を見据えた医療 AI サービスの開発. *医療情報学* **44**(Suppl.), 354-357, 2024

Morita-Nakagawa M, Okamura K, Nakabayashi K, Inanaga Y, Shimizu S, Guo WZ, Fujino M, Li XK. Supervised machine learning of outbred mouse genotypes to predict hepatic immunological tolerance of individuals. *Sci. Rep.* **14**, 1, 24399, 2024

岡村 浩司. 医療×AI: AWS の生成 AI サービスと切り拓く医療の新時代 —遺伝カウンセリングへの活用に向けて—. *ITvision* **52**, 19, 2024

Matsubara K, Ohgami Y, Okamura K, Aoto S, Fukami M, Shimada Y. Machine learning trial to detect sex differences in simple sticker arts of 1606 preschool children. *Minerva Pediatr.* **76**, 343-349, 2024

Hattori A, Seki A, Inaba N, Nakabayashi K, Takeda K, Tatsumi K, Naiki Y, Nakamura A, Ishiwata K, Matsumoto K, Nasu M, Okamura K, Michigami T, Katoh-Fukui Y, Umezawa A, Ogata T, Kagami M, Fukami M. Expression levels and DNA methylation profiles of the growth gene SHOX in cartilage tissues and chondrocytes. *Sci. Rep.* **14**, 8069, 2024

Kawano T, Okamura K, Shinchi H, Ueda K, Nomura T, Shiba K. Differentiation of large extracellular vesicles in oral fluid: combined protocol of small force centrifugation and sedimentation pattern analysis. *J. Extracell. Biol.* **3**, e1143, 2024

Amano N, Narumi S, Aizu K, Miyazawa M, Okamura K, Ohashi H, Katsumata N, Ishii T, Hasegawa T. Single-exon deletions of ZNRF3 exon 2 cause congenital adrenal hypoplasia. *J. Clin. Endocrinol. Metab.* **109**, 641–648, 2024

Uchiyama T, Kawai T, Nakabayashi K, Nakazawa Y, Goto F, Okamura K, Nishimura T, Kato K, Watanabe N, Miura A, Yasuda T, Ando Y, Minegishi T, Edasawa K, Shimura M, Akiba Y, Sato-Otsubo A, Mizukami T, Kato M, Akashi K, Nunoi H, Onodera M. Myelodysplasia after clonal hematopoiesis with APOBEC3-mediated CYBB inactivation in retroviral gene therapy for X-CGD. *Mol. Ther.* **6**, 3424−3440, 2023

岡村 浩司.ゲノム塩基配列を用いたディープラーニングから考察する未来の遺伝カウンセリング. *遺伝カウンセリング学会誌* **43**, 199–205, 2023

岡村 浩司. スプレッドシートに代わる関係データベースの活用. *遺伝子医学* **13**, 67−73, 2023

Yoshida M, Nakabayashi K, Yang W, Sato-Otsubo A, Tsujimoto S, Ogata-Kawata H, Kawai T, Ishiwata K, Sakamoto M, Okamura K, Yoshida K, Shirai R, Osumi T, Kiyotani C, Shioda Y, Terashima K, Ishimaru S, Yuza Y, Takagi M, Arakawa Y, Imamura T, Hasegawa D, Inoue A, Yoshioka T, Ito S, Tomizawa D, Koh K, Matsumoto K, Kiyokawa N, Ogawa S, Manabe A, Niwa A, Hata K, Yang JJ, Kato M. Prevalence of pathogenic variants in cancer-predisposing genes in second cancer after childhood solid cancers. *Cancer Med.* **12**, 11264−11273, 2023

Azuma N, Yokoi T, Tanaka T, Matsuzaka E, Saida Y, Nishina S, Terao M, Takada S, Fukami M, Okamura K, Maehara K, Yamasaki T, Hirayama J, Nishina H, Handa H, Yamaguchi Y. Integrator complex subunit 15 controls mRNA splicing and is critical for eye development. *Hum. Mol. Genet.* **5**, 2032−2045, 2023

Uryu H, Migita O, Ozawa M, Kamijo C, Aoto S, Okamura K, Hasegawa F, Okuyama T, Kosuga M, Hata K. Automated urinary sediment detection for Fabry disease using deep-learning algorithms. *Mol. Genet. Metab. Rep.* **33**, 100921, 2022

Aoto S, Hangai M, Ueno-Yokohata H, Ueda A, Igarashi M, Ito Y, Tsukamoto M, Jinno T, Sakamoto M, Okazaki Y, Hasegawa F, Ogata-Kawata H, Namura S, Kojima K, Kikuya M, Matsubara K, Taniguchi K, Okamura K. Collection of 2429 constrained headshots of 277 volunteers for deep learning. *Sci. Rep.* **12**, 3730, 2022

宇賀神 敦 (研究分担者)

宇賀神 敦. 中小医療機関が直面するサイバーセキュリティー課題と対策 論考②, *日本医療法人協会ニュース*, 2026/5, 2026

宇賀神 敦. 医療 AI の活用や医療 DX 推進に求められるセキュリティやガバナンス ―安心して医療 AI が利用できるデータ連携基盤やサイバーセキュリティの制度的支援の考察 ―. *第 45 回医療情報学連合大会* 4-B-1-08, 2025

宇賀神 敦. 正しく恐れて、積極的に活用しよう!-医療機関が押さえておくべき「医療・ヘルスケア分野における生成 AI 利用ガイドライン（第 2 版)」のポイント-, *ITVison* **55**, 14−15, 2025

宇賀神 敦. 医療機関に求められるサイバーセキュリティ対策とクラウド型 AI サービスの活用. *医学のあゆみ* **291**, 1123−1129, 2024

宇賀神 敦. クラウド型 AI サービス活用の課題と将来の展望について. *医療情報学* **44**(Suppl.), 371, 2024

宇賀神 敦. AI サービス普及のための情報セキュリティのあり方. *INNERVISION* **39**, 7, 17–20, 2024

宇賀神 敦. 全日本病院協会 病院情報セキュリティ対策 WEB セミナー～ 医療機関に求められる IT セキュリティと BCP ～, 医療機関における情報セキュリティ対策やセキュリティ監査について 2024 年 2 月 23 日

宇賀神　敦. 医療 AI プラットフォームの社会実装による医療従事者の働き方改革・医療 DX 実現への貢献 , 厚生労働省主催 保険医療分野 AI 社会実装推進シンポジウム, 2024 年 1 月 11 日

宇賀神　敦. 人とテクノロジーの協調による医療従事者の働き方改革と患者 QoL 向上に向けた取組み, 第 97 回日本薬理学会年会 共催シンポジウム AI ホスピタルが医療を変える『心とこころが通い合う先進的な医療現場』, 2023 年 12 月 15 日

宇賀神 敦. 安全・安心なネットワーク環境やクラウド基盤に支えられた AI サービスの利活用による医療・ヘルスケアのデジタルトランスフォーメーション, 第 43 回医療情報学連合大会 大会企画 2『境界型防御からゼロトラストへ』, 2023 年 11 月 24 日

宇賀神 敦. 医療機関の経営者は今こそ情報セキュリティに対する投資優先度を上げるべき. *月刊新医療* **50**, 22–27, 2023

宇賀神 敦. 人とテクノロジーの協調による医療現場の働き方改革-タブレット・ロボット・アバターを用いた実証事例. *別冊医学のあゆみ*, AI ホスピタルの社会実装, 24–32, 2023

宇賀神 敦. がん薬物療法で治療中の外来患者向け副作用 AI 問診システム, *癌と化学療法* **50**, 667–674, 2023

宇賀神 敦. 医療 AI プラットフォームの社会実装, 第 5 回日本メディカル AI 学会学術集会, 2023 年 6 月 17 日

宇賀神 敦. サイバーセキュリティの現状と対策について, 全日本病院協会 病院情報セキュリティ対策 Web セミナー, 2023 年 2 月 20 日

宇賀神 敦. AI を用いた医療現場向けスマートコミュニケーション技術の開発,SIP 第二期 AI ホスピタル成果発表シンポジウム 2022, 2022 年 12 月 17 日

https://www.nibiohn.go.jp/sip/publications/symposium/AIHospitalSymposium20221217_B01.pdf

宇賀神 敦. 人とテクノロジーの協調による医療現場の働き方改革, *医学のあゆみ* **282**, 882–890, 2022

宇賀神 敦. ヘルスケアデジタルトランスフォーメーションの現状と今後, *行政＆情報システム* **58**, 45–50, 2022

藤井 進 (研究分担者)

Inoue R, Nakayama M, Ota H, Nakamura N, Fujii S, Ishii A, Saito A, Suzuki T, Nomura H, Goto N, Watanabe S, Maruyama H, Nozawa M, Uyama Y. Establishment of reliable identification algorithms for acute heart failure or acute exacerbation of chronic heart failure using clinical data from a medical information database network. *Front. Cardiovasc. Med.* **12**, 1642323, 2025

藤井 進. 医療機関の人材不足とセキュリティ課題への対応： 地域連携ネットワークを活用した実装可

能な対策モデルの検討. *第 45 回医療情報学連合大会* 4-B-1-01, 2025

藤井 進, 野中 小百合, 中村 直毅. 地域医療連携ネットワークシステムを活用したゼロトラストのニーズ調査. *医療情報学* **44**(Suppl.), 368-370, 2024

藤井 進, 境界型防御からゼロトラストへ - 様々な視点からゼロトラストへの転換を考える –, 第 43 回医療情報学連合大会 43rd JCMI （Nov.2023）p141−143

藤井 進, 野中 小百合, 山下 貴範, 中村 直毅. 境界型防御からゼロトラストへ 医療機関からの視点, 第 43 回医療情報学連合大会 43rd JCMI （Nov. 2023）p144

藤井 進, 野中 小百合. 災害時の医療情報提供に関する意識調査, 第 29 回日本災害医学会学術集会, **Vol.28** Supplement, Japanese Journal of Disaster Medicine, p454, 2024/02.

Fujii S, Kunii Y, Nonaka S, Hamaie Y, Hino M, Egawa S, Kuriyama S, Tomita H. Real-time prediction of medical demand and mental health status in Ukraine under Russian invasion using tweet analysis. *The Tohoku Journal of Experimental Medicine* **259**, 177–188, 2022

佐々木 宏之, 古川 宗, 阿部 喜子, 藤井 進, 布田 美貴子, 藤田 基生, 丸谷 浩明, 亀井 尚, 江川新一. 東日本大震災を経験した東北大学病院の事業継続計画(BCP)策定ステップと事業継続管理(BCM). *精神神経学雑誌* **124**, 184–191, 2022

金子 誠暁 (研究分担者)

金子 誠暁. 医療機関の働き方改革を見据えた具体的ユースケースの事例紹介. *第 45 回医療情報学連合大会* 4-B-1-05, 2025

八田 泰秀, 友村 清, 堀田 稔, 小林 勇渡, 金子 誠暁. 医療 AI 普及に向けた共通基盤の研究開発. *INNERVISION* **37**, 7, 15−19, 2022

八田 泰秀, 金子 誠暁. AI ホスピタルの社会実装に向けて. *日経 XHealthEXPO2022* 発表 2022 年 10 月 19-21 日

尾﨑 勝彦 (研究分担者)

福田 秀樹, 尾﨑 勝彦. 医療機関のサイバーセキュリティ対策 —徳洲会グループシステム監査：標準化の試み—. *第 45 回医療情報学連合大会* 4-B-1-06, 2025

福田 秀樹, 江苅 孝, 藤岡 和美, 尾﨑 勝彦. グループ病院でのセキュリティ対応とその課題〜システム監査を中心に〜. *医療情報学* **44**(Suppl.), 363-367, 2024

植松 直哉, 真辺 篤, 福田 秀樹, 藤村 義明, 髙橋 則之, 尾﨑 勝彦, 大橋 壯樹, 福田 貢, 東上 震一. 徳洲会メディカルデータベース(TMD)の活用実績とデータカタログ作成、医療情報学会学術大会 2023 年 11 月

江村 葵, 植松 直哉, 赤松 直樹, 真辺 篤, 野口 幸洋, 福田 秀樹, 藤村 義明, 髙橋 則之, 尾﨑 勝彦. 徳洲会グループにおけるチャットアプリケーションを用いたコミュニケーションの活性化、医療情報学会学術大会 2023 年 11 月

尾﨑 勝彦. 病院運営をデータ利活用で最適化する. *医学のあゆみ* **283**, 747-753, 2022

松井 俊大 (研究分担者)

Ishikawa K, Masuda H, Matsui T, Anami Y, Shindo T, Kubota M, Ishiguro A. Inferior vena cava thrombosis secondary to pyomyositis and vertebral osteomyelitis in a 15-year-old boy. *Pediatr. Int.* **68**, e70396, 2026

Matsui T, Uchida Y, Tomizawa D, Yanagi K, Shoji K. Fatal group A streptococcal sepsis as initial presentation of acute lymphoblastic leukemia. *Pediatr. Int.* **68**, e70352, 2026

Nishi K, Fukui K, Matsui T, Okada S, Ikuse T, Miyata Y, Aiba H, Chiba H, Funaki T, Isayama T, Ito Y, Kamei K. Neonatal acute kidney disease in the National Center for Child Health and Development (NCCHD)-neoAKI Cohort: risk factors and prognostic outcomes. *Pediatr. Nephrol.* **41**, 845−852, 2026

Hisano H, Shoji K, Matsui T, Kato H, Fukui K, Kano M, Yamada Y, Gocho Y, Ishiguro A. Subsequent bacteremia associated with intravascular catheter colonization with Staphylococcus aureus, Gram-negative rods, and Candida species in children. *J. Infect. Chemother.* **31**, 102600, 2025

Hikino K, Shoji K, Saito J, Fukunaga K, Liu X, Matsui T, Utano T, Takebayashi A, Tomizawa D, Kato M, Matsumoto K, Ishikawa T, Kawai T, Nakamura H, Miyairi I, Terao C, Mushiroda T. Analysis of factors influencing the relationship between voriconazole plasma concentrations and adverse effects in a paediatric population. *Br. J. Clin. Pharmacol.* 91, 2020−2027 , 2025

Ikuse T, Yamada M, Kasai T, Aiba H, Matsui T, Funaki T, Shoji K, Kato I, Miura S, Sugahara Y, Ogimi C. Secondary Attack of Symptomatic SARS-CoV-2 Infections Among Roommates in a Children's Hospital. *Hosp. Pediatr.* **15**, e88−e92, 2025

Ikuse T, Matsui T, Shoji K, Kono N, Yamada M, Ogimi C, Takahashi C, Funaki T, Ide K, Matsumoto S, Ito R, Shimabukuro R, Gocho Y, Hayakawa I, Ishikawa T, Sakamoto S, Kasahara M, Igarashi T. Neonatal acute liver failure cases with echovirus 11 infections, Japan, August to November 2024. *Euro. Surveill.* **30**, 2400822, 2025

Hisano H, Shoji K, Matsui T, Kato H, Fukui K, Kano M, Yamada Y, Gocho Y, Ishiguro A. Subsequent bacteremia associated with intravascular catheter colonization with Staphylococcus aureus, Gram-negative rods, and Candida species in children. *J. Infect. Chemother.* **31**, 102600, 2025

Kim H, Ikuse T, Matsui T, Sakaguchi H, Ishiguro A, Shoji K. Factors distinguishing leukemoid reaction from hematological malignancy in children. *Pediatr. Int.* **66**, e15837, 2024

Kasai T, Yamada M, Funaki T, Tao C, Myojin S, Aiba H, Matsui T, Ogimi C, Miyake K, Ueno S, Miyairi I, Kato H, Shoji K. Antibody titer trends after SARS-CoV-2 vaccination in patients aged 12-25 years with underlying diseases. *J. Infect. Chemother.* **31**, 102579, 2025

Shoji K, Hikino K, Saito J, Matsui T, Utano T, Takebayashi A, Tomizawa D, Kato M, Matsumoto K, Ishikawa T, Kawai T, Nakamura H, Miyairi I, Terao C, Mushiroda T. Pharmacogenetic implementation for CYP2C19 and pharmacokinetics of voriconazole in children with malignancy or inborn errors of immunity. *J. Infect. Chemother.* **30**, 1280−1288, 2024

Funaki T, Yamada M, Miyake K, Ueno S, Myojin S, Aiba H, Matsui T, Ogimi C, Kato H, Miyairi I, Shoji K. Safety and antibody response of the BNT162b2 SARS-CoV-2 vaccine in children aged 5-11 years with underlying diseases: A prospective observational study. *J. Infect. Chemother.* **30**, 773−779, 2024

Aiba H, Funaki T, Yamada M, Miyake K, Ueno S, Tao C, Myojin S, Matsui T, Ogimi C, Kato H, Miyairi I, Shoji K. Association between use of antipyretics and antibody titers after two doses of the BNT162b2 SARS-CoV-2 vaccine in adolescents and young adults with underlying diseases. *J. Infect. Chemother*. 2024, **30**, 176−178

Matsui T, Ogimi C. Risk factors for severity in seasonal respiratory viral infections and how they guide management in hematopoietic cell transplant recipients. *Curr. Opin. Infect. Dis.* 2023, **36**, 529−536

Okai M, Ishikawa T, Tamura E, Matsui T, Kawai T. Granulicatella adiacens Bacteremia in Chronic Granulomatous Disease. *J. Clin. Immunol.* **43**, 85−87, 2023

Shoji K, Funaki T, Yamada M, Mikami M, Miyake K, Ueno S, Tao C, Myojin S, Aiba H, Matsui T, Ogimi C, Kato H, Miyairi I. Safety of and antibody response to the BNT162b2 COVID-19 vaccine in adolescents and young adults with underlying disease. *J. Infect. Chemother.* **29**, 61−66, 2023

Fujikawa H, Shimizu H, Nambu R, Takeuchi I, Matsui T, Sakamoto K, Gocho Y, Miyamoto T, Yasumi T, Yoshioka T, Arai K. Monogenic inflammatory bowel disease with STXBP2 mutations is not resolved by hematopoietic stem cell transplantation but can be alleviated via immunosuppressive drug therapy. *Clin. Immunol.* **246**, 109203, 2023

Tanita K, Kawamura Y, Miura H, Mitsuki N, Tomoda T, Inoue K, Iguchi A, Yamada M, Yoshida T, Muramatsu H, Tada N, Matsui T, Kato M, Eguchi K, Ohga S, Ishimura M, Imai K, Morio T, Yoshikawa T, Kanegane H. Rotavirus vaccination and severe combined immunodeficiency in Japan. *Front. Immunol.* **13**, 786375, 2022

中村 直毅 (研究分担者)

Li B, Kumada K, Shimada M, Shirota H, Tokunaga H, Yamaguchi-Tanaka M, Inoue C, Yamazaki Y, Yamamura A, Furukawa T, Komine K, Ogishima S, Tamahara T, Saito S, Shimizu R, Iikubo M, Yamauchi K, Saito T, Fujimaki SI, Abe Y, Nakamura N, Ota H, Nagami F, Kinoshita K, Nakazawa T, Motohashi H, Ishii N, Ishioka C, Harigae H, Tominaga T, Yaegashi N, Yamamoto M. Establishment and Operation of a New Style Clinical Biobank: The Tohoku University Clinical Biobank. *Tohoku J Exp Med.* [doi: 10.1620/tjem.2025.J152], 2026

中村 直毅. 地域医療連携ネットワークにおけるサイバーセキュリティ対策： 仮想ブラウザと集中管理型デコイシステムを統合した多層防御アーキテクチャの設計と実装. *第45回医療情報学連合大会* 4-B-1-04, 2025

Inoue R, Nakayama M, Ota H, Nakamura N, Fujii S, Ishii A, Saito A, Suzuki T, Nomura H, Goto N, Watanabe S, Maruyama H, Nozawa M, Uyama Y. Establishment of reliable identification algorithms for acute heart failure or acute exacerbation of chronic heart failure using clinical data from a medical information database network. *Front. Cardiovasc. Med.* **12**, 1642323, 2025

Obara T, Ishikuro M, Noda A, Murakami K, Orui M, Shinoda G, Ueno F, Matsuzaki F, Onuma T, Matsubara H, Metoki H, Kikuya M, Hatanaka R, Chiba I, Nakaya K, Kogure M, Nakaya N, Sugawara J, Kure S, Kobayashi M, Kobayashi T, Suzuki Y, Kawame H, Sakurai-Yageta M, Nagase S, Nakamura N, Nakamura T, Mizuno S, Nagaie S, Ogishima S, Narita A, Tamiya G, Koreeda S, Nagami F, Tamahara T, Goto M, Otsuki A, Taira M, Hidaka T, Kawashima J, Kodama EN, Uruno A, Hamanaka Y, Tomita H, Hashizume H, Noguchi K, Katsuoka F, Koshiba S, Kumada K, Nobukuni T, Ohneda K, Mugikura S, Shimizu R, Kambe M, Saito Y, Kobayashi T, Izumi Y, Kinoshita K, Fuse N, Yaegashi N, Hozawa A, Yamamoto M, Kuriyama S; Tohoku Medical Megabank Project Study Group. Cohort Profile Update: The Tohoku Medical Megabank Project Birth and Three-Generation Cohort Study (TMM BirThree Cohort Study) 2023 update. *Int. J. Epidemiol.* **54**, dyaf148, 2025

中村 直毅, 野中 小百合, 藤井 進. 医療機関および地域医療連携ネットワークシステムでのセキュリティの現状. *医療情報学* **44**(Suppl.), 358-359, 2024

中村 直毅. インターネット回線の冗長化の試み 簡易的かつ安価な仕組みで障害に備える. *医事業務* **30**, 22−26, 2023

菊地 徹矢, 田山 智幸, 中村 直毅. 入院患者向け無料 Wi-Fi サービスの展開 快適な入院環境の提供を目指して. *医事業務* **30**, 27−30, 2023

園部 真也, 藤井 進, 中村 直毅, 横田 崇, 志村浩 孝, 小林 智哉, 志賀 卓弥, 大田 英輝, 荻島 創一, 田宮 元, 植田 琢也, 冨永 悌二. 東北大学病院における匿名加工医療情報および仮名加工情報の利

活用と産学連携へ向けた取り組み. *日本医療情報学会春季学術大会抄録集*, 128–129, 2023

Chong Song, Yoichi Kakuta, Kenichi Negoro, Rintaro Moroi, Atsushi Masamune, Erina Sasaki, Naoki Nakamura, Masaharu Nakayama. Collection of patient-generated health data with a mobile application and transfer to hospital information system via QR codes, Computer Methods and Programs in Biomedicine Update 3 100099–100099, 2023

高山 真, 有田 龍太郎, 小野 理恵, 只野 恭教, 菊地 章子, 稲葉 洋平, 中村 直毅, 阿部 倫明, 石井 正. 新型コロナウイルス感染症軽症者等宿泊療養施設における 管理課題解決のための情報共有・往診システムの構築. *日本医療・病院管理学会誌* **59**, 157–167, 2022

佐々木 恵利奈, 中村 直毅, 角田 洋一. 電子カルテシステムとスマートフォンの問診アプリケーション間の双方向連携によるデータ入力の効率化. *月刊新医療* **49**, 20–23, 2022

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 3 月 12 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　国立研究開発法人
国立成育医療研究センター

所属研究機関長　職　名　理事長

氏　名　五十嵐　隆

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　クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言

３．研究者名　（所属部署・職名）システム発生研究部・組織工学研究室長

（氏名・フリガナ）岡村 浩司（オカムラ コウジ）

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）	■　□	■	国立成育医療研究センター 国立大学法人東北大学	□
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）

令和 8 年 5 月 20 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　医療AIプラットフォーム
技術研究組合

所属研究機関長　職　名　理事長

氏　名　宇賀神 敦

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　クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言

３．研究者名　（所属部署・職名）理事長

（氏名・フリガナ）宇賀神 敦（ウガジン アツシ）

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）	■　□	■	国立成育医療研究センター 国立大学法人東北大学	□
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６月３日

厚生労働大臣　殿

機関名　国立大学法人東北大学

所属研究機関長　職　名　総長

氏　名　冨永　悌二

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　クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言（23AC1001）

３．研究者名　（所属部署・職名）　災害科学国際研究所 災害医学部門 災害医療情報学分野・教授

（氏名・フリガナ）　藤井　進・フジイ　ススム

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：研究実施の際の留意点を示した。　）

（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 20 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　医療AIプラットフォーム
技術研究組合

所属研究機関長　職　名　理事長

氏　名　宇賀神 敦

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　クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言

３．研究者名　（所属部署・職名）システム WG・リーダー

（氏名・フリガナ）金子 誠暁（カネコ アキトシ）

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）	■	□	■	国立成育医療研究センター 国立大学法人東北大学	□
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）

令和 8 年 2 月 26 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　徳洲会インフォメーション
システム株式会社

所属研究機関長　職　名　代表取締役社長

氏　名　髙橋 則之

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　クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言

３．研究者名　（所属部署・職名）取締役会長

（氏名・フリガナ）尾﨑 勝彦（オザキ カツヒコ）

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）	■　□	■	国立成育医療研究センター 国立大学法人東北大学	□
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 1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　国立研究開発法人
国立成育医療研究センター

所属研究機関長　職　名　理事長

氏　名　五十嵐　隆

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　クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言

３．研究者名　（所属部署・職名）小児内科系専門診療部 感染症科 ・ 医員

（氏名・フリガナ）松井 俊大（マツイ トシヒロ）

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）	■　□	■	国立成育医療研究センター 国立大学法人東北大学	□
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。

令和８年３月２６日

厚生労働大臣　殿

機関名　国立大学法人東北大学

所属研究機関長　職　名　総長

氏　名　冨永 悌二

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　クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言

３．研究者名　（所属部署・職名）　大学病院・准教授

（氏名・フリガナ）　中村　直毅　ナカムラ　ナオキ

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：　研究実施の際の留意点を示した。　）

（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。