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。

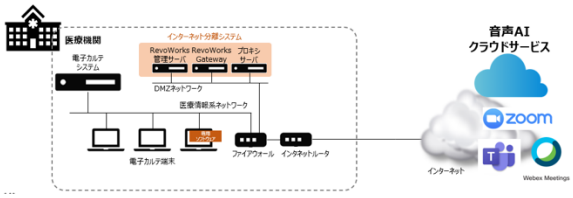

図 3. インターネット分離の概要

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。

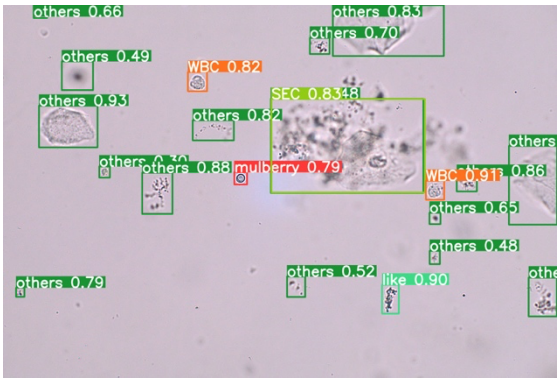

図 4. 尿沈渣顕微鏡写真の物体検出

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