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

医療従事者の持続可能な就労環境の構築と、地域を問わない質の高い医療の提供は、現代医療が解決すべき根本的な課題である。医療 AI との協調は、その双方に応えうる中核的な手段として位置づけられる。AI サービスの広範な普及には、クラウドの積極的活用と利便性が不可欠であり、本研究では、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な検討を行った。設立母体などを考慮して選定した 26 医療機関に対し、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、100 床あたり平均して 1 名のシステム要員が ICT 全般を担っており、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。これらの知見を踏まえ、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 サービスの開発においては、実診療補助を目的としたモデルを複数構築し、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を通じて、安全性の確保と運用コストの最適化を同時に達成した。生成 AI および 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根底から覆し、未経験者による自律的な開発を現実のものとした。あわせて、電子カルテ接続に過度な忌避感を抱く情報管理部門に対し、実証的根拠に基づい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として、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。同基盤を情報共有の枠組み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。システム監査の領域では、ガイドラインに準拠した 8 病院での実績を通じて、国内医療機関に広く適用可能な標準化への基盤を整えた。セキュリティ技術という観点では、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、人的依存によらない対応が現実的な選択肢として浮上してきた。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を持ち、対策を支える手法はこの一年間で質的に異なる次元へと変貌を遂げている。新たな開発および運用体制への移行を前向きに推し進めることが、医療、情報、セキュリティの三領域の連携を深め、患者と市民の参画のもとで医療 AI をさらなる高みへと導く鍵となる。

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

AI 技術の飛躍的な進歩は、医療の姿を根底から変えようとしている。ディープラーニングの臨床応用が現実のものとなるにつれ、医療 AI の有用性は広く認識され、医療の質向上や医療従事者の負担軽減に向けた実証が着実に積み重ねられている。とりわけ、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 の実装と活用は喫緊の課題となっている。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の解消にも大きな可能性を秘めている。しかし、医療 AI 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置かれており、特にカルテ端末からの利用が十分に普及しているとは言い難い状況にある。さらに、個人情報保護への配慮が一層強く求められるなか、ランサムウェアをはじめとするサイバー攻撃の脅威も増大しており、実効性ある対策の構築が急務となっている。

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根本から変えつつある。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。

上記の諸課題に正面から取り組むべく、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ことを目的とする。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と方策を確立する。こう

した取り組みの総体を通じて、安全性を堅固に担保しながら医療 AI サービスの普及を加速し、医療技術のさらなる発展と患者・市民への還元を実現することが、本研究の最終的な到達点である。

B. 研究方法

医療機関のネットワークセキュリティ対応の実態把握を目的として、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）を対象に、二段階構成による調査を実施した。第一段階として事前アンケートによる基礎情報の収集を行い、第二段階としてその回答内容を踏まえた直接訪問によるヒアリングを実施した。ヒアリングでは、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。この二段階のプロセスを採用することにより、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、確認すべき内容を予め明確化することができた。あわせて、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も、特に最近発生した事例に着目し、被害内容、原因、経済的損失、復旧時間などの観点から体系的な分析を行った。ヒアリングから浮かび上がった課題を分析して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提示した。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」に準拠し、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において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。

技術面においては、東北大学病院を実証フィールドとして仮想ブラウザおよびランサムウェア対策用デコイを活用し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 開発の基盤整備としては、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。最終年度には特に、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重点的に取り組んだ。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が実用に耐えうるかを検証することで、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多角的に探った。

加えて、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・考察を行った。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

[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。

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として注目した。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いかなる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・組織的の両面から検討を加えた。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構造がどのように変容していくかという問いは、継続的な追跡調査が不可欠な重要課題として本研究の射程に位置づけた。

以上の調査および実証の積み重ねを通じて、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 サービスを安全に利用できる環境の確立を目指した。

C. 研究結果

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%にとどまり、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得られていないことへの課題も指摘された。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 は本質的に異なるものであり、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 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た。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。これらの経験の積み重ねを通じて、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・③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	○

図 2. 監査チェックシート抜粋

技術的な実証実験においては、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ることが確認され、地域医療連携ネットワーク上への展開可能性も見出された。

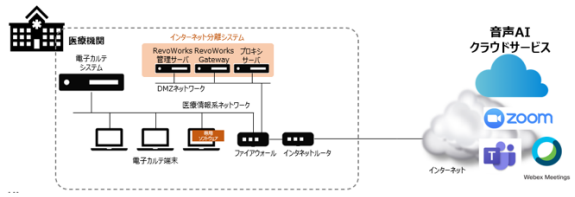


図 3. インターネット分離の概要

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)。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。

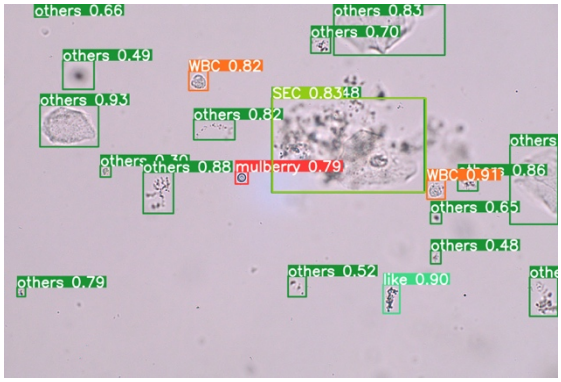


図 4. 尿沈渣顕微鏡写真の物体検出

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端的に示している(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。

AI ネイティブなセキュリティツールの動向調査として、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着目した。公開された調査では、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明確に示された。

D. 考察

ランサムウェア攻撃によって電子カルテが完全停止し、手書きの紙伝票で診療を続けた病院が復旧まで2か月以上を要した――こうした事例は、もはや他人事ではない。セキュリティ対策の充足度が、患者の命に直結する問題であるという現実を、本研究の調査結果は改めて突きつけている。医療機関のセキュリティ対策においては、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規定要因であることが確認された。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切実に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顕著に見られた一方、関心の薄い病院では逆の状態に陥っており、結果として多くのリスクを内包するケースが大半であった。いかなる技術的対策にも先んじて取り組むべき根本的な課題は、経営層の意識改革にほかならない。

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 の普及促進には、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、安全に利用し、障害発生時にも診療を継続し、地域

[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。

で互いに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る。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しての役割を担い、クラウド型医療 AI の安全な社会実装を下支えす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最大限に活用することで、病院側の費用・運用変更の負担を抑えながら医療 AI の導入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・僻地における医療格差の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直結する可能性を秘めている。他方で、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現実的な障壁となっており、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していくためには、セキュリティ有識者による継続的な支援と、セキュリティ製品の導入コスト低減という両面における解決策が引き続き強く求められる。

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求められるが、AWS IAM や 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課するものであったが、AI コーディングエージェントの活用によって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明確に示された。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も有効に機能する。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引き下げる一方、経験者がこれを活用した際の恩恵がより多岐にわたることもあわせて示唆された。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と問題意識を持って AI エージェントに臨む姿勢が求められる。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、次世代が課題を自ら発見し独自に解決していく新たな道筋を切り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一層鮮明となった。Claude Mythos Preview による 2 万 3000 件超の脆弱性発見が端的に示すように、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根底から崩れ去った。今や人間側の対応能力の限界こそが新たなボトルネックとなっており、この構造的転換は深刻に受け止める必要がある。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かつ即効性のある補完手段となりうる。

これらの課題に対応するうえで肝要なのは、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段階的に講じていくことである。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）は有効な実践的基盤となる。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する。グループ外病院の監査を通じて構築した 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、医療現場を熟知した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裏付けられた。IT-BCP については、計画の立案にとどまらず年 1 回の実地訓練を通じて GAP を継続的に確認し改善を重ねていくことが、サイバーレジリエンスの実現に向けた不可欠なプロセスである。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の向上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な位置を占める。

今後の展望として、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して明確に位置づけ、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着実に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有機的に連携しつつ 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

病院の 100 床あたりシステム要員わずか 1 名——この一つの数字が、日本の医療機関が抱えるセキュリティ問題の深刻さを余すところなく物語っている。人材不足、知識不足、ベンダ依存という構造的問題は今に始まったことではないが、生成 AI を駆使したサイバー攻撃の高度化と医療 DX の加速が重なる現在、その脆弱性はかつてないほど鮮明に露呈している。

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。侵入を完全に防ぐことに主眼を置く従来の発想から、侵入後の早期検知と継続的な医療提供を前提とするサイバーレジリエンスへと発想を転換することが急務である。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、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、クラウド型医療 AI の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。IT-BCP は復旧手順書ではなく縮退運転の設計図であり、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したうえで、日頃より実践訓練を重ねることが不可欠である。

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・コスト制約・サイバーリスク･医療 DX という複合的な課題に対し、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。システム監査については、徳洲会グループ外を含む複数の病院での実施を通じて標準化が大きく前進した。監査が一貫して示したのは、病院幹部のセキュリティへの理解と関与こそ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事実である。内部監査（年 1 回）と外部監査（2〜4 年に 1 回）を継続するサイクルを組織に根付かせることが、持続的なセキュリティ対策の礎となる。

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 駆動型へと本質的なシフトを遂げ、国家サイバー統括室による ASM の調査において AI 駆動型開発への移行後に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裏付ける成果である。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。そして 2026 年、Anthropic による Claude Code Security の発表は決定的な転換点となった。コードベース全体を横断的に解析し脆弱性の検出から修正パッチの提案・適用までをシームレスに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不足という医療機関の構造的問題に対して現実的な解を提示するものである。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いよいよ整いつつある。

未経験の大学院生が AI エージェントを活用して 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したという事実は、専門家依存を前提とした従来の人材戦略の終わりを告げるものである。医療・情報・セキュリティという三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歩みを進めるために必要なのは、変化を脅威としてではなく好機として前向きに受け止める姿勢である。対策を支える技術的基盤は質的に異なる次元へと変貌を遂げた。あとは、それを使いこなす意志と体制があるかどうかである。

F. 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.* [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)

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)

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)

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

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. *第 44 回医療情報学連合大会* **2-C-5-01**, 2024

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. *第 44 回医療情報学連合大会* **2-C-5-02**, 2024

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 44 回医療情報学連合大会* **2-C-5-04**, 2024

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. *第 44 回医療情報学連合大会* **2-C-5-05**, 2024

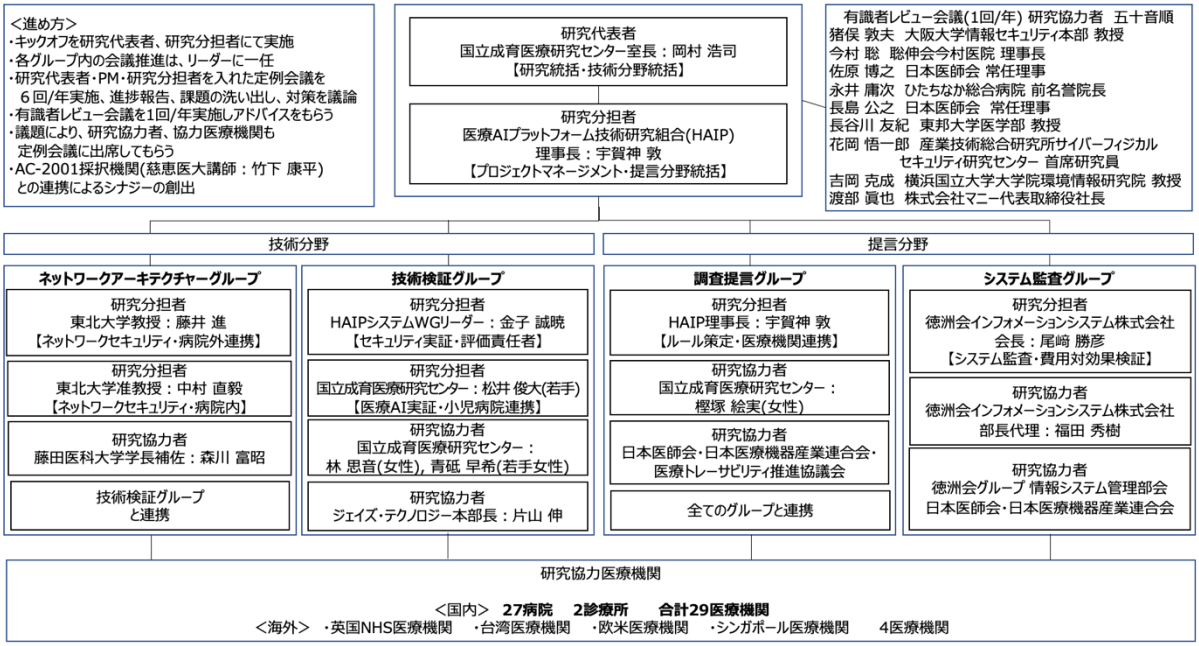
宇賀神 敦. クラウド型 AI サービス活用の課題と将来の展望について. *第 44 回医療情報学連合大会* **2-C-5-06**, 2024

G. 知的財産権の出願

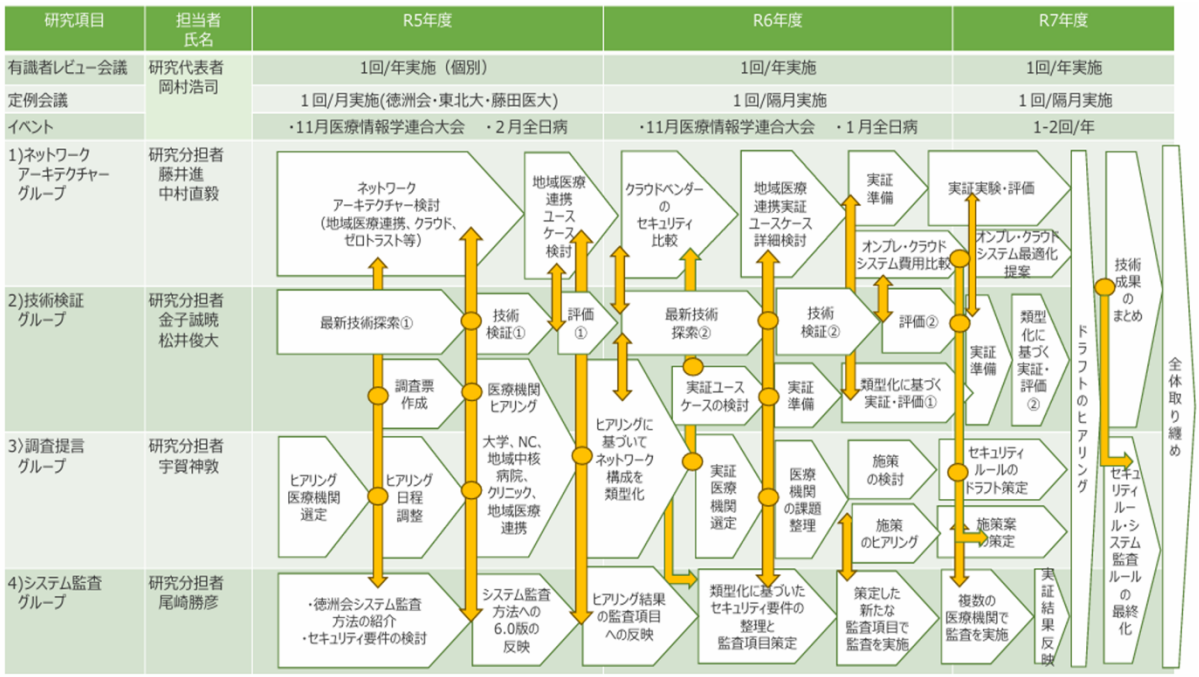
岡村 浩司, 仁科 幸子. 乳幼児の視覚異常スクリーニング方法、視覚異常スクリーニングシステム及び表示システム. 特願 2026-060427 (2026 年 4 月 1 日)

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 1. 研究体制図



資料 2. 期間全体に渡る調査研究項目



資料 3.　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