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）

総括研究報告書
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

研究要旨

クラウド上の医療 AI サービスの活用は、医療従事者の働き方改革や医療の均霑化に重要な役割を果たすことが期待されている。特に、専門医不在など医療資源が不足している離島や僻地における医療レベルを都市部に近づける可能性を持つ一方で、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対策が喫緊の課題となっている。本研究では、医療機関が安全かつ経済的にこれらのサービスを利用できる環境の整備を目指し、複数のアプローチによる包括的な調査・検証を実施した。まず、地域医療ネットワークシステムを活用し、大規模なアンケート調査を実施、さらに 26 医療機関への事前アンケートと対面ヒアリングによる 2 段階の詳細調査を行い、医療機関の実態把握に努めた。その結果、半数以上が AI 活用に前向きな姿勢を示す一方で、システム要員の深刻な不足や、ベンダーへの依存度の高さ、新しい知識習得のための時間確保が困難であるなどの課題が明らかになった。また、紹介などの業務の効率化や、ランサムウェア、災害を想定したバックアップ機能の必要性が強く求められていることも判明した。これらの課題に対応するため、仮想ブラウザとランサムウェア対策デコイの実証実験を実施し、端末の動作に影響を与えることなくクラウド上の AI サービスの安全な利用とデータの受け渡し、また、ランサムウェアの早期発見に有効であることが確認された。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、それぞれの段階に応じた適切なセキュリティ対策を整理した。システム監査に関しては、徳洲会グループの病院をモデルケースとして、厚生労働省の最新ガイドラインに準拠した監査手法の開発と実証を行った。特に、グループ外の病院への展開を視野に入れ、監査項目や提出資料の見直しを行い、標準化された監査手法の確立に向けた基盤を構築した。医療 AI 開発の面では、感染症起因菌同定支援システムやファブリー病スクリーニングシステム、生成 AI を利用した遺伝カウンセリングの開発を進めた。また、使用頻度の変動に対応したコスト最適化と運用効率化を目的として、サーバレスアーキテクチャへの移行を進めており、ゼロトラストセキュリティモデルの実装についても検討を行っている。今後は、これらの知見をもとに、標準化されたシステム監査手法の確立とセキュリティ対策の実装を進め、医療 AI の安全な利用環境整備と普及促進を目指していく。特に、医療機関のシステム要員不足やセキュリティ対策の課題に対する実践的な解決策の確立が重要となる。

研究代表者
岡村 浩司 ・ 国立成育医療研究センター
システム発生研究部 ・ 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 ・ 専務理事
藤井 進 ・ 東北大学 ・ 教授
金子 誠暁 ・ BIPROGY 株式会社 ・ 第
四室長
尾﨑 勝彦 ・ 徳洲会インフォメーション
システム株式会社 ・ 代表取締役社長
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

近年、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、2025 年に向けた医療、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医療の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

本研究では、医療機関におけるセキュリティ対策の現状把握と実効性の高い対策の確立に向けて、複数のアプローチによる調査・検証を実施した。

まず、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 2024 年度に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、地域性を考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（Step1）と、その回答を踏まえた直接訪問によるヒアリング（Step2）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。

また、2023 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」に基づき、システム監査の標準化に向けた取り組みを進めた。特に、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」や「ランサムウェア対策用デコイ」を用いた実証実験を行い、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。さらに、医療 AI 開発の基盤として、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セキュリティモデルの実装に向けた検証を進めた。

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

本研究の結果として、医療機関におけるセキュリティ対策の現状と課題、および具体的な技術的解決策の有効性について、多くの知見が得られた。詳細については、続く 5 件の分担研究報告書にまとめているので、以下ではその概要を記す。

医療機関へのランサムウェア被害の実態調査では、2021 年の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、被害を受けた医療機関では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 ヶ月を要するケースが多く見られた。経済的損失も、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。その結果、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、日常的なシステム運用やトラブル対応に追われ、セキュリティ対策への十分な注力が困難な状況が明らかとなった。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った。また、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。

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」の試験導入が大きな成果を上げた。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、地域医療ネットワークシステム上での展開可能性も確認された。

本研究における医療 AI の開発は、実際に動くサービスを作り、本研究のプラットフォームにてセキュリティ等の検証を行う意味でも重要な位置を持つ。グラム染色画像からの感染症起因菌同定支援システムでは、15 細菌および 1 真菌を高精度で識別可能なモデルを開発し、特許出願に至った。また、ファブリー病スクリーニングシステムでは、尿沈渣中のマルベリー小体を自動検出する技術を確立し、学校検尿との連携による効率的なスクリーニング実現への道筋を示した。ともに HAIP サービス事業基盤からユーザを限定しているが公開に至っている。生成 AI を利用した遺伝カウンセリングにおいても、医療機関で、あるいは患者のスマートフォンで利用可能であることは確認できたが、遺伝カウンセリングという行為は医師の指導の元に行われなければならず、社会実装を目指すにはまだまだ多くの障壁がある。これらのシステムは、コスト最適化と運用効率化を目的としてサーバレスアーキテクチャへの移行を進めており、使用頻度に応じた最適な課金体系の実現も視野に入れている。

システム監査の標準化に向けた取り組みでは、徳洲会グループの実績をもとに、より汎用的な監査手法を確立した。特に、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」に準拠した監査項目の整備により、グループ外の医療機関でも適用可能な実践的な監査体制を構築した。監査結果からは、パスワード管理の不備や BCP 対策の不足など、具体的な改善点も明確になった。

さらに、医療機関のクラウド移行を支援するため、主要クラウドプロバイダのセキュリティサービスについて包括的な比較調査を実施し、セキュリティ監視、アクセス制御、データ保護、リスク管理の各領域における実践的な選定指針を確立した。

これらの結果は、医療機関における安全な AI 利用の実現可能性を実証するとともに、セキュリティ対策の標準化に向けた具体的な指針を提供するものとなった。特に、限られた人的リソースの中でも実装可能な技術的解決策と、それを支える監査体制の確立は、今後の医療 AI サービスの普及促進に大きく貢献するものと期待される。

D. 考察

本研究の結果から、医療機関におけるクラウド上の医療 AI サービス利用に向けた課題と展望について、以下の考察が導かれる。

まず、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明らかになった。因子分析の結果、診療情報の共有とクラウド技術の活用が最も重視されており、特にランサムウェア対策や災害対策としてのバックアップ機能への関心が高いことが示された。また、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。

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。特に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。

さらに、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。サーバレスアーキテクチャは、コスト効率や運用管理の簡素化だけでなく、セキュリティ面でも攻撃範囲の限定や脆弱性対応の迅速化といった利点があり、ゼロトラストセキュリティモデルの実装にも適している。

一方で、医療機関ごとに異なるネットワーク・システム構成や、セキュリティポリシーの違いが、医療 AI サービス導入の障壁となっていることも明らかになった。特に、電子カルテネットワークからインターネットへの接続制限は依然として大きな課題であり、セキュリティと利便性のバランスを取る必要がある。

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。具体的には、セキュリティアセスメントツールの開発や、定期的なシステム監査の実施、そして医療機関の特性に応じたリファレンスモデルの整備が求められる。特に、人材不足が深刻な医療機関に対しては、外部委託やクラウドサービスの活用を含めた包括的な支援策の提供が必要である。

今後は、これらの知見をもとに、より具体的な導入ガイドラインの策定と、継続的なセキュリティ対策の実施を支援する体制の構築が求められる。特に、地域医療ネットワークシステムを活用した共同利用モデルの確立は、中小規模の医療機関における安全な医療 AI サービス利用の実現に大きく貢献すると考えられる(資料)。

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、ベンダー依存体制という構造的な問題を抱えていることが明らかとなった。この状況下で、増加するサイバー攻撃やランサムウェアの脅威に対応するため、ゼロトラストセキュリティの導入が必要とされているが、従来の境界型防御で守られてきた電子カルテネットワークの構成変更には多くの課題がある。

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や、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。また、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も進められている。しかし、これらの施策を実効性のあるものとするためには、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、組織的な取り組みが不可欠である。

今後は、これらの技術的・組織的対策の実証を重ねながら、医療機関および患者にとって費用対効果の高いソリューションを確立し、関係省庁や業界団体との連携を深めながら、医療 DX の実現と医療従事者の働き方改革の推進を図っていく必要がある。

F. 健康危惧情報

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 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*, 2024, **44(Suppl.)**, 354-357

2. 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*, 2024, **44(Suppl.)**, 358-359

3. 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

4. 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*, 2024, **44(Suppl.)**, 368-370

5. 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

H. 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 医療 AI サービスの利用に想定されるネットワーク構成