別紙１

研究年度終了報告書表紙

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 6 年度 総括・分担研究年度終了報告書

研究代表者　岡村 浩司

令和 7 (2025) 年 5 月

別紙２

研究年度終了報告書目次

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

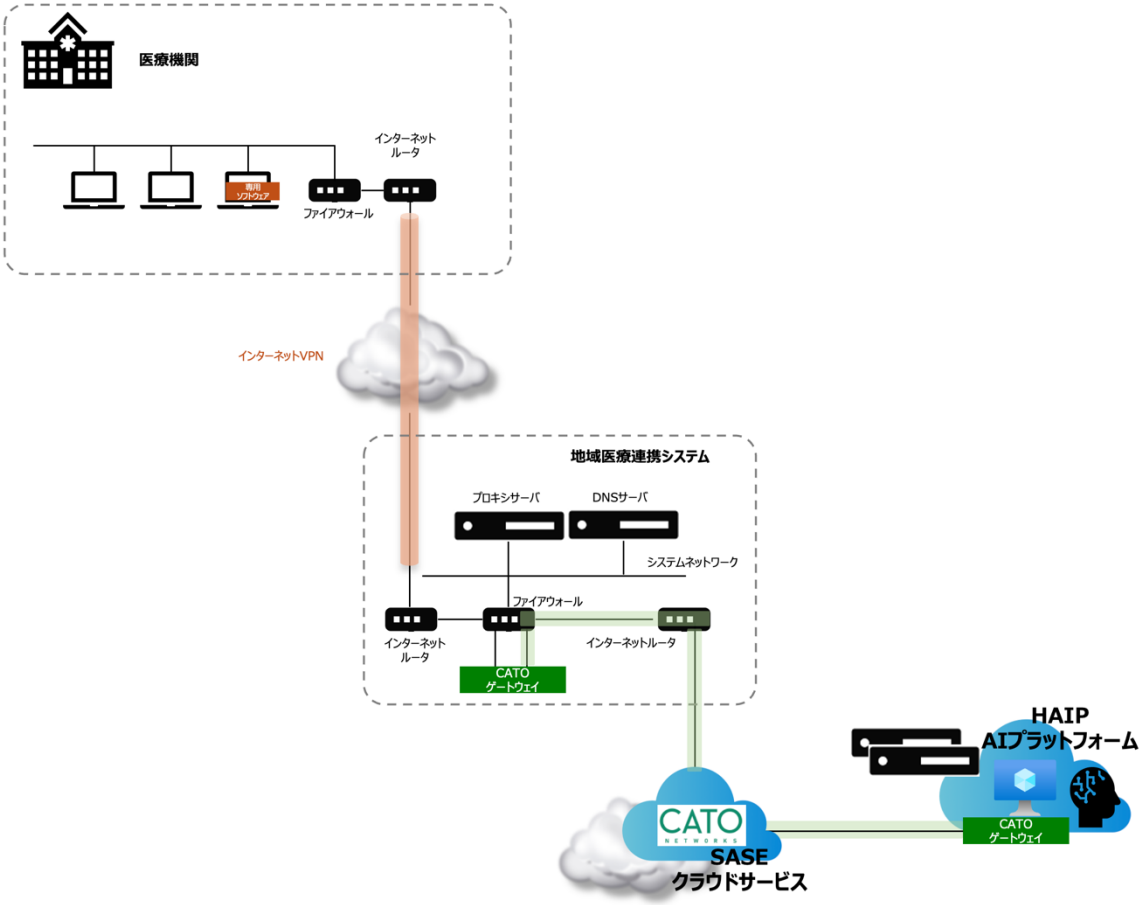
4. 藤井 進, 野中 小百合, 中村 直毅. 地域医療連携ネットワークシステムを活用したゼロトラストのニーズ調査. *医療情報学*, 2024, **44(Suppl.)**, 368-370

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



（公募番号：23AC1001）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　2024 年度の活動報告書

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

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。

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「MMWIN (Miyagi Medical and Welfare Information Network)」を活用し、これらの相反する課題を同時に解決する方策を検討した。宮城県内のすべての医療施設を対象にアンケートを実施し、330 施設から回答を得た。その結果、従来の地域医療ネットワークシステムを活用した情報共有だけでなく、紹介・逆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が明らかとなった。また、セキュリティ対策に関する人材不足を懸念する声も多く、現実的な対応はまだ十分に進んでいないことが示唆された。一方、AI を地域医療ネットワークシステムを介して活用することに対しては、半数以上の施設が賛同を示しており、今後 AI の有効性が認められていけば、そのサービスの需要がさらに高まる可能性があると考えられる。

これらの調査結果を踏まえ、東北大学病院では「仮想ブラウザ」と「ランサムウェア対策のデコイ」の試験導入を行い、さらに地域医療ネットワークシステム上で同様のサービスを提供できるようにネットワーク設計を実施した。仮想ブラウザは、電子カルテ端末内においてトラストゾーンとゼロトラストゾーンを両立させる仕組みであり、クラウド上の AI サービスを利用しながら、コピー&ペーストによるデータの受け渡しが可能であることを確認した。特に端末の動作に影響を与えないことも確認され、実用性の高さが示された。また、デコイについては、ランサムウェアの被害そのものを防ぐものではないものの、早期発見の可能性が高く、既存システムへの影響が少ないことが確認された。

理論的および設計の観点から、本研究で提案したランサムウェア対策は地域医療ネットワークシステム上での提供が可能であることが示された。今後、さらなる実証実験を通じて、より実用的なセキュリティ対策の確立を目指す。

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

A. 研究目的

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およびシステム監査ルールを提示することにより、全国の医療機関が安全・安心かつ合理的なコストで医療 AI サービスを活用できる環境の整備を目的とする。近年、医療 AI の有用性が広く認識される一方で、個人情報の保護やランサムウェア等のサイバー攻撃への対応が喫緊の課題となっている。

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「MMWIN（Miyagi Medical and Welfare Information Network)」を活用し、こうした課題の両立的解決の可能性を検討する。

本年度は地域医療連携システムに対する臨床機能、セキュリティ対策、AI サービスに関する需要を調査・分析し、得られた知見に基づいて実効性のある安全・安心な AI 利活用基盤のネットワークアーキテクチャーを構築・提示することを目的とする。

B. 研究方法

本研究では、近年本邦において増加するランサムウェア被害の実態を把握することを起点とし、被害の内容や原因、経済的損失、復旧に要した時間などを整理・分析する。特に 2024 年度に発生した医療機関への被害事例に注目し、過去の事例と比較しながら、同様の原因が繰り返されているのか、またなぜ十分な対策が講じられなかったのかについて検証することで、既存のセキュリティ対策の実効性を評価する。

次に、医療機関におけるネットワークセキュリティ対応の現状と課題を把握するため、宮城県内の医療施設を対象にアンケート調査を解析する。調査項目は、地域医療連携システムに対する臨床機能、セキュリティ対策、AI 活用に関するニーズを中心に構成する。

得られた調査結果をもとに、具体的なセキュリティ対応策を設計し、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」等を用いた実証実験を行う。その実施過程と評価結果を踏まえ、地域医療ネットワークシステム上における同様のセキュリティサービスの展開可能性について検討する。

C. 研究結果

1. ネットワークアーキテクチャーの検討

■ランサムウェア被害の与える影響

本邦の医療機関におけるランサムウェア被害は、深刻な影響を及ぼしている。以下に、主な事例の原因、復旧までに要した時間、被害総額などの詳細をまとめる。

① 徳島県つるぎ町立半田病院（2021 年 10 月）

原因: ランサムウェア「LockBit 2.0」に感染。VPN 機器の既知の脆弱性を悪用さ

れ、院内ネットワークに侵入されたと考えられている。

復旧までの期間：約 2 ヶ月。電子カルテや会計システムが使用不能となり、一部診療科で新規患者の受け入れを中止した。

被害総額：調査・復旧費用で数億円以上、診療制限などによる逸失利益は数十億円以上と報告されている。

参考：
https://www.iij.ad.jp/global/column/column141.html?utm_source=chatgpt.com

② 大阪急性期・総合医療センター（2022 年 10 月）

原因：給食委託事業者の VPN 装置の脆弱性を経由してランサムウェア攻撃を受け、電子カルテシステムが暗号化された。

復旧までの期間：約 2 ヶ月。外来診療や各種検査が停止した。

被害総額：具体的な金額は公表されていないが、復旧費用や診療停止による逸失利益を含めると、73 日間の停止による経済的損失は数十億円規模と推測される。

参考：
https://www.sbbit.jp/article/sp/150139?utm_source=chatgpt.com
https://www.gh.opho.jp/pdf/reportgaiyo_v01.pdf
https://www.gh.opho.jp/pdf/report_v01.pdf

③ 福島県立医科大学附属病院（2017 年 8 月）

原因：ランサムウェア「WannaCry」に感染。感染経路は特定されていないが、複数の医療機器が影響を受けた。

復旧までの期間：詳細な期間は不明だが、感染した機器の初期化やデータ復旧に時間を要したと推測される。

被害総額：具体的な金額は公表されていないが、一部の検査データが保存できず、患者への説明や再検査が必要となったと考えられる。

参考：
https://www.jfss.gr.jp/article/1674?utm_source=chatgpt.com

④ 宇陀市立病院（奈良県、2018 年 10 月）

原因：ランサムウェア「GandCrab」に感染。ウィルス対策ソフトが最新の状態ではなく、バックアップも不十分だったと報告されている。

復旧までの期間：詳細な期間は不明だが、紙カルテでの運用期間は 2 日との報告がある。ただし、データの復旧には時間を要し、システムログが消去されたため感染経路の特定が困難だった。

被害総額：具体的な金額は公表されていないが、患者 3,835 人の診療記録のうち 1,133 人分のデータが暗号化され、復旧作業に多額の費用がかかった。また、個人情報流出に対する対応コストも発生した。

参考：https://udacity-hospital.jp/activities/?utm_source=chatgpt.com

⑤ 市立東大阪医療センター（2021 年 5 月）

原因：ランサムウェア「REvil」に感染。病院内サーバへの不正アクセスが原因とされている。

復旧までの期間：詳細な期間は不明だが、医療用の撮影画像参照システムがダウンし、代替サーバの立ち上げまでに時間を要したとの報告がある。

被害総額：具体的な金額は公表されていない。

検討した事例から、医療機関におけるランサムウェア被害は、診療業務の停止、電子カルテの使用不能、医療データの喪失、経済的損失など、多方面に深刻な影響を及ぼすことが明らかとなった。特に、VPN 機器の脆弱性やバックアップ体制の不備が攻撃の主な要因となっているケースが多く、医療機関におけるセキュリティ対策の脆弱性が浮き彫りとなった。これらの結果は、技術的および運用上の観点から、早急な対策の強化と体制の見直しが求められることを示している。

■2024 年に発生した事案

大阪急性期・総合医療センターの事例は社会的に大きなインパクトを与えたが、残念ながら医療施設におけるランサムウェア被害は依然として続いている。

・最新の事例：岡山県精神科医療センターおよび東古松サンクト診療所（2024 年 5 月 19 日）

被害概要：

2024 年 5 月 19 日、岡山県精神科医療センターおよび東古松サンクト診療所がランサムウェアによるサイバー攻撃を受け、電子カルテを含む総合情報システムに障害が発生した。

参考：
https://www.popmc.jp/j6w25163/?utm_source=chatgpt.com

被害の詳細：

システム障害：攻撃により電子カルテシステムが暗号化され、システム内には脅迫メッセージと攻撃者の連絡先メールアドレスが確認された。

情報流出：総合情報システム内の共有フォルダに保存されていた患者情報（氏名、住所、生年月日、病名など）や病棟会議の議事録等が流出した可能性がある。影響を受けた患者情報は、過去 10 年分で最大約 4 万人分に及ぶと報告されている。

参考：
https://www.popmc.jp/j6w25163/?utm_source=chatgpt.com

原因と対策：

原因：これまでの報告事例と同様に、VPN 機器の脆弱性が攻撃の原因として指摘されている。

対応の遅れ：同センターは 2023 年 6 月に自治体病院の全国組織から VPN 機器の脆弱性に関する通知を受けていたが、機器の更新を検討しながらも進展がなく、対策が棚上げされていたと報道されている。

参考：
https://www.sanyonews.jp/article/1565381

対応状況：

診療体制：システム障害発生後、紙カルテを用いた診療体制に切り替え、医療サービスの提供を継続。6 月 1 日からは仮の電

カテゴリ名	クリニック		介護施設		病院（200～399床）		病院（200床未満）		病院（400床以上）		総数	
	n	%	n	%	n	%	n	%	n	%	n	%
クリニック	258	100	0	0	0	0	0	0	0	0	258	80.12
介護施設	0	0	4	100	0	0	0	0	0	0	4	1.24
病院（200～	0	0	0	0	15	100	0	0	0	0	15	4.66
病院（200床	0	0	0	0	0	0	39	100	0	0	39	12.11
病院（400床	0	0	0	0	0	0	0	0	6	100	6	1.86
欠測値	0	0	0	0	0	0	0	0	0	0	0	0
総和	258	100	4	100	15	100	39	100	6	100	322	100

表 1　回答施設数の内訳

子カルテシステムを導入し、診療を再開した。

情報流出の確認：6 月 7 日に岡山県警より、ダークウェブ上に患者情報が掲載されているとの連絡を受け、情報流出が正式に確認された。

■ランサムウェア被害対応での身代金

前述のつるぎ町立半田病院では、病院側は公式には身代金の支払いを拒否し、東京の事業者にデータ復旧を依頼している。ただし、一部の報道では病院側が身代金を支払った可能性が指摘されている。

参考：
https://www.topics.or.jp/articles/-/788524?utm_source=chatgpt.com

2.　【地域医療連携システムを介したセキュリティ対応の検討】

■意識・需要調査アンケートの実施

宮城県内の医療施設（介護施設内の診療室を含む）1,753 施設を対象に、2024 年 3 月に WEB アンケートを実施した。本調査の目的は、地域連携システムにおいてクラウドを活用し、ゼロトラスト型セキュリティ対応を実現する場合に、どの程度のニーズがあるかを把握することである。

アンケート項目については、文末に「A1. 地域連携システムにおけるセキュリティ対応のニーズ調査」を添付した。

■意識・需要調査アンケートの結果

回答数は 330 施設、有効回答施設数は 322 施設であった。最も多かったのはクリニックであり、全体の 80%を占めた。病院については、施設規模によってセキュリティ対応の要件が異なる可能性があるため、200 床未満、200～400 床未満、400 床以上の 3 つのカテゴリーに分類した。

施設規模が大きいほど、有意に MMWIN への加入率が高くなる傾向がみられたが、本調査の目的は地域医療ネットワークシステムへの期待を明らかにすることである。そのため、アンケート結果の分析においては、MMWIN への加入の有無を重視しないこととした。

施設規模ごとのセキュリティ意識の違いや、地域医療連携システムの各機能に対する魅力の感じ方、リモート保守やクラウドバックアップの必要性の認識、AI 活用への関心、情報共有の安全性に関する認識について、Dunn 検定を用いて施設規模が与える影響を調査した。

その結果、「自施設のセキュリティ人材不足を感じるか」という設問においてのみ、有意な差が認められた（表 2）。

特にクリニックでは、「セキュリティ人材が不足している」と感じる割合が低かった。これは、そもそも専任のセキュリティ担当者を置かず、クラウド型電子カルテの提供ベンダーなど外部委託に依存している可能性があるためと考えられる。また、診療規模の関係で外部接続の機会が少なく、セキュリティ人材の必要性自体が低いことも背景要因として挙げられる。

表 2　施設規模の与える影響

	クリニック	介護施設	病院（200～399 床）	病院（200 床未満）	病院（400 床以上）
クリニック		258,4	258,15	258,39	258,6
		-12.843	-59.893	-30.901	-21.510
		0.287	2.543	2.028	0.587
		1.0000	0.04400	0.17023	1.00000

<< 多重比較（独立多群） >>

・変数名：自施設のセキュリティ人材が不足していると感じますか？

・検定法：Dunn2：出力内容：

・1 段目=データ数;2 段目=順位和の差;3 段目=Q 値;4 段目=P 値

以降では、①セキュリティ人材の対応や意識、②地域医療ネットワークシステムに求める機能、③セキュリティ対応、④AI の利用について、それぞれ詳しく掘り下げる。各設問に対する回答については、「別紙アンケート結果」を参照されたい。

①　セキュリティ人材対応・意識

セキュリティ対応に関しての自己評価であるが、小規模施設（クリニック）では「セキュリティ人材が不足している」と感じる割合が低い。これは、そもそもセキュリティ担当者を置かず、外部委託に依存している可能性があることは述べた。それに加えて、大規模病院（400 床以上）では「セキュリティ対策が十分である」と感じる割合が低い。大きな施設ほどリスクを認識しやすく、課題を感じやすいのかもしれない。

その課題感を感じやすい中規模以上の病院（200 床以上）では、MMWIN への参加率が高い。病院同士の連携が求められるため、参加のメリットを感じやすい。

②　地域医療ネットワークシステムに求める機能

大規模病院では、検査結果や病歴の共有に対する関心が比較的高く、診療情報を連携することで患者の管理を効率化したいと考える傾向が見られた。一方、クリニックでは情報共有への関心が比較的低く、特に「紹介・逆紹介機能」に対する関心は大規模病院と比

べて低い傾向にあった。これらの結果を踏まえると、各医療機関の実態に即した機能の提供が求められると考えられる。ただしこれまでの情報共有以外にもニーズがあることは確認された。

③ セキュリティ対応

大規模病院では、「クラウドバックアップ」や「ランサムウェア対策」への関心が高く、システム運用の負担を軽減しつつ、セキュリティリスクを低減したいという意図がうかがえた。

一方、クリニックでは「リモート保守の向上」に対する関心が比較的低かった。これは、サーバ管理の必要性が少ないため、対策の優先度が低い可能性があると考えられる。

しかしながら、災害対応におけるバックアップの活用については、施設規模を問わず関心が高かった。このことから、こうした社会課題を適切に反映した対策の重要性が示唆された。

④ AI 利用について

大規模病院では、AI 活用に対して積極的な傾向が見られ、診療の効率化や医師の負担軽減を期待している可能性がある。

一方、クリニックでは「AI を使いたい」と考える割合が比較的低かった。これは、業務フローがシンプルであることや、専門的な診断支援の必要性が少ないことが影響している可能性があり、AI の必要性をあまり感じていないことが考えられる。

しかし、日常診療において AI の有用性がより明確になり、実際の業務に組み込まれることで、こうした課題が改善され、AI に対する需要が高まる可能性があると考えられる。

■類型

意識調査の結果をもとに、要因分析による類型化を実施した。結果を表 3(文末)に記す。

- **因子の解釈**

バリマックス回転後の因子負荷量をもとに、各因子の特徴を分析した。その結果、診療情報の共有に対する関心を示す因子、クラウド技術や災害対策に対する意識を示す因子、リモート保守や IT 管理の簡素化に関する因子、AI 活用と安全な情報共有に対する因子、セキュリティ人材の不足意識に関する因子、外部業者とのシステム管理に関する因子、そして施設規模が影響を与える因子の七つが抽出された。

第一の因子は、画像や検査結果、薬歴、病名の共有、さらには紹介・逆紹介や診療予約に関連しており、診療情報を円滑に共有することへの関心の強さが示された。

第二の因子は、クラウドバックアップ、ランサムウェア対策、災害対策バックアップへの関心と強く結びついており、医療機関におけるクラウド技術の活用やセキュリティ対策、特にバックアップに対する関心の高さがうかがえた。

第三の因子としては、VPN 回線の集約や VPN サーバの保守負担軽減、外部業者サーバの管理簡素化といった要素が含まれ、医療機関における IT 管理の負担軽減やリモート保守の効率化が求められていることが示唆された。

第四の因子は、AI 診断補助やカルテ作成、さらには安全な情報共有に関するものであり、AI 技術の活用に対する関心や、それを安全に運用するための仕組みが重要視されていることが明らかとなった。

第五の因子は、セキュリティ人材の不足と強く結びついており、医療機関におけるセキュリティ対策を担う人材の確保が大きな課題となっていることが分かった。

第六の因子は、外部業者との接続管理と関連しており、医療機関が外部業者とのシステム管理の簡素化を求めていることが示唆された。

最後に、第七の因子は施設規模と関連しているものの、他の因子と比較すると影響は限定的であり、施設の規模が直接的な要因として機能するよりも、個々の医療機関のニーズがより重要であることが示された。

- **全体の考察**

分析の結果、診療情報の共有とクラウド技術に対する関心が最も高く、これらの要素が医療機関の ICT 環境において特に重要視されていることが明らかとなった。診療情報の共有は、医療の質の向上や業務の効率化に直結する要素であり、特に大規模病院において強く求められている。一方で、ランサムウェア対策や災害対策としてのクラウド技術の活用に対する関心も高く、医療機関におけるデータ管理の安全性確保が重要視されていることが分かった。

また、IT 管理の負担軽減やリモート保守の効率化に関する関心も一定程度見られた。VPN の集約やサーバ保守の負担軽減、外部業者のサーバ管理の簡素化といった点が求められており、特に IT リソースの限られた医療機関にとっては重要な課題となっている。さらに、AI の活用についても関心が示されており、診断支援やカルテ作成を通じた業務効率の向上が期待されていることが分かった。ただし、AI の活用においては、安全な情報共有の仕組みの確立が必要とされており、AI 技術の発展とともに、そのセキュリティ対策の整備も求められる。

一方で、セキュリティ人材の不足が大きな課題として挙げられた。特に大規模病院では、専門のセキュリティ人材の確保が困難であり、外部委託や教育支援の強化が必要とされている。クリニックにおいては、セキュリティ対策の優先度が低い傾向にあるものの、シンプルで低コストなセキュリティ対策の導入が求められる可能性がある。

さらに、外部業者とのシステム管理についても課題として挙げられ、特に大規模病院ではこれまでのランサムウェア被害から、医療機器メーカーや給食業者など、複数の外部業者との連携が必要となることから、その管理負担の軽減が求められている可能性がある。

施設規模の影響については限定的であり、施設規模が大きいほど情報共有の必要性が高まるものの、それ以外の要素、特にセキュリティ対策やクラウド活用との関連性は低いことが分かった。これは、施設規模にかかわらず、個々の医療機関のニーズに応じた対応が重要であることを示唆している。

- **まとめと提案**

これらの結果から、医療機関では診療情報の共有とクラウド技術の活用が重要視されていることが明らかとなった。診療情報の共有については、大規模病院だけでなく

クリニックにおいても、簡易的な情報共有手段の導入が利便性向上につながる可能性がある。また、クラウド技術を活用した安全なデータ管理の推進が求められており、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の活用が重要な課題となっている。

さらに、IT 管理の負担軽減や AI の活用に関する施策も重要である。VPN の統合やリモート保守の仕組みを改善することで、医療機関の運用負担を軽減することが期待される。また、AI 診断支援やカルテ作成の導入を進めることで、業務効率の向上が見込まれる。

セキュリティ人材の不足については、大規模病院における専門人材の確保が困難であるため、外部委託の活用や教育支援を強化することが求められる。一方、クリニックでは、シンプルで低コストなセキュリティ対策を導入することで、対策の実効性を高めることができる。また外部業者とのシステム管理についても、特に医療機器メーカーや給食業者らとの連携を強化し、負担を軽減する施策が必要とされる。

一方で施設規模の影響は限定的であり、個別の医療機関のニーズに応じた対応が重要となる。診療情報共有やクラウド技術の活用を推進しながら、IT 管理の簡素化や AI の活用、セキュリティ対策の強化を図ることで、より安全で効率的な医療環境の構築が可能となると考えられる。今後は、これらの課題を踏まえた具体的な施策の立案や、施設規模別の詳細な分析を進めることが求められる。

■傾向

次に、自施設における人材不足の認識とセキュリティ対策の満足度との関係性について分析を行った。

まず、「自施設のセキュリティ人材が不足していると感じますか？」と「自施設ではセキュリティ対策がきちんとできていると思いますか？」という二つの設問の相関関係を示す（図 1）。両者には一定の相関が見られ、人材不足を感じている施設ほど、セキュリティ対策に対する満足度が低い傾向が明らかとなった。

この結果を踏まえ、施設規模、人材不足の認識、セキュリティ対策の評価という三つの要素を用いて、さらに詳細な傾向分析を行うこととした。

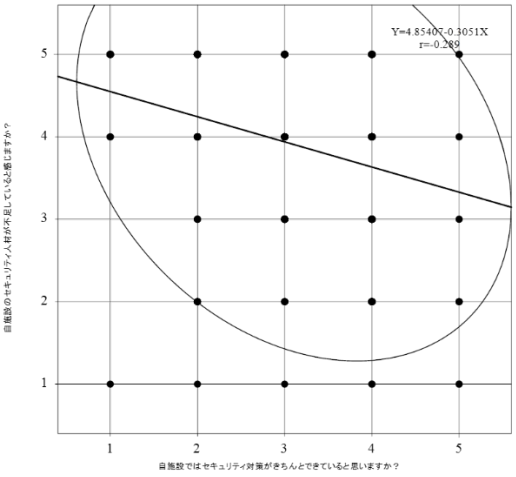


図１　セキュリティに関する相関

r = -0.2894　(-0.3868～-0.1857)（ ）は 95.0% 信頼区間。相関係数の有意性 P=0.00000[t=-5.392 n=318]。X を基準に Y を回帰：回帰直線 Y = a + bX = 4.85407 - 0.3051X

「施設規模」「セキュリティ人材の不足感」「セキュリティ対策の意識」の三つの要因

が、各アンケート項目の回答に与える影響を分析するため、3 レベル枝分かれ分散分析（Three-way ANOVA）を実施した。結果を表 4(文末)ならびに表 5 に示す。

施設規模はすべての質問項目において統計的に有意な影響を示さず、医療機関の規模による違いはほとんどないことが明らかとなった。一方で、セキュリティ人材の不足感は VPN 管理やランサムウェア対策の意識に影響を及ぼし、人材不足を感じる施設ほど、リモート保守やバックアップ管理の改善に対する関心が高い傾向が見られた。また、セキュリティ対策の意識は画像共有、災害対策、AI 情報共有の安全性に影響を与えており、セキュリティ対策を重視する施設ほど、新技術を利用した情報共有に積極的な姿勢を示していることが分かった。

特に、画像共有の魅力や災害対策のクラウドバックアップ、AI 情報共有の安全性といった項目においては、セキュリティ対策の意識が統計的に有意な影響を及ぼしていた。一方で、VPN サーバ管理の負担軽減やランサムウェア対策のクラウドバックアップについては、セキュリティ人材の不足感が影響を及ぼしており、セキュリティ人材が不足している施設ほど、これらの対策への関心が高いことが示された。

考察すると、施設規模の影響は限定的であり、むしろ施設の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の導入に対する関心を決定づける重要な要因であることが明らかとなった。特に、セキュリティ人材が不足している施設では、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施策への関心が高く、これらの分野に対する支援策が求められている。一方で、セキュリティ対策の意識が高い施設ほど、画像共有や AI 技術を活用した情報共有の安全性に対して前向きであり、これらの分野での技術導入が進む可能性が示唆された。

また本研究においては、医療機関の施設規模がセキュリティ対策の意識や新技術導入に及ぼす影響は認められなかった。従来、大規模病院では IT リソースが充実しており、小規模クリニックではその整備が不十分であると考えられてきたが、本研究の結果は、施設の規模よりも、各医療機関のセキュリティ意識や人材の充足状況がより重要な要因であることを示唆している。これは、医療機関における ICT 導入やセキュリティ対策の推進において、施設規模に応じた一律の施策よりも、各施設のニーズに基づいた柔軟なアプローチが求められることを示している。

■まとめ

ここまでの結果を踏まえ、今後の施策としては、以下の点が重要である。まず、施設規模ではなく、セキュリティ意識や人材不足に応じた施策を講じることが求められる。特に、セキュリティ人材が不足している施設に対しては、VPN 管理やランサムウェア対策の強化を目的としたリモート管理の支援策を提供することが有効である。具体的には、クラウドベースの管理システムの導入や、外部委託によるシステム監視の強化が挙げられる。

また、画像共有や AI 技術の活用を推進するため、セキュリティ対策に関する教育やトレーニングを強化することが重要である。

特に、セキュリティ意識の高い施設では、AIを活用した情報共有の安全性向上に関心があることから、これらの施設に対する技術支援を優先的に行うことで、効率的な導入を促進できると考えられる。

さらに、セキュリティ人材の不足に対応するためには、システム管理の外部委託やクラウドサービスの導入を推奨することが有効だろう。本研究において、特にVPNサーバ管理やランサムウェア対策に対する関心が高いことが確認されたため、これらの分野に特化した支援策を優先的に実施することで、医療機関のICT運用の負担軽減につながる可能性がある。

加えて、新技術の導入を進める際には、セキュリティ意識の高い施設へのアプローチを強化することが効果的である。本研究では、「災害対策のクラウドバックアップ」や「AI情報共有の安全性」といった項目に対して、セキュリティ意識が統計的に有意な影響を及ぼしていることが示された。したがって、これらの技術の導入を推進する際には、セキュリティ意識の高い施設を中心に施策を展開し、その成功事例をもとに他の施設へと普及を図ることが望ましい。

■実証実験

そこで地域医療ネットワークシステムを活用し、セキュリティ対策によって人員不足の解消を図る具体的な方策を検討し、東北大学病院で実証することとした。さらに、その技術(プロトコル)が地域医療ネットワークシステムで実際に提供可能かどうかについても、具体的に検討を進めることとした。

3. 【地域医療連携システムを介したセキュリティ対応の実証】

■ランサムウェア被害への対応

ランサムウェア被害を未然に防ぐには、VPNサーバ等の管理を徹底することであり、多くは未然に防げる可能性がある。一方で人の操作が介在することも避けられず、適切でない対応をすることで、被害を受ける可能性が否定できない。

そこで少ない人員で対応でき、既存システムの変更等がなく、安価に対応できる方法がないかを検討しこのような脅威に対抗するための防御策の一つとして デコイシステム（Decoy System） が注目した。デコイシステムの概要、ランサムウェア対策における有効性、および医療機関での応用について以下のようにまとめる。

● デコイシステムの概要

デコイシステムとは、サイバー攻撃の検知および分析を行う防御システムの一種である。このシステムでは、攻撃者が標的とする重要なシステムやデータとは別に、意図的に「罠」となるシステムやファイルを配置し、攻撃の監視および分析を行う。特にランサムウェア対策としては、攻撃の早期検知や被害の抑制に寄与する。

● ランサムウェア対策としてのデコイシステムの構成

デコイシステムは、以下の要素から構成されることがある。

1. ダミーファイルの配置

デコイシステムでは、重要なデータに見えるが、実際には価値のないダミーファイ

ルを作成する。これらのファイルが改ざんまたは暗号化された際に即座にアラートを発信し、管理者へ通知を行うことで、迅速な対応が可能となる。

2. デコイサーバー（Honeypot）の設置

本番環境とは分離されたネットワーク上に「仮想のシステム」を構築する。これにより、攻撃者をデコイ環境に誘導し、マルウェアの挙動をリアルタイムで監視し、攻撃手法を分析する。

- **異常検知および自動対策の組み込み**

デコイシステムは、攻撃を検知した際に以下のような対応を自動的に実施するようにしている。

1. ネットワークの遮断：感染の拡大を防ぐために、攻撃対象となったネットワークを隔離する。
2. 管理者への即時通知：攻撃の発生を即時に報告し、対応を促す。
3. AI・機械学習の活用：通常の業務プロセスと異なる不審な動作を識別し、より高精度な検知を行う。

- **攻撃者の行動ログの記録**

デコイシステムは、侵入経路や使用された攻撃ツールを特定し、今後のセキュリティ対策の強化に活用する。また、得られた攻撃ログをもとに、企業や医療機関の防御システムの改善に貢献する。

- **医療機関におけるデコイシステムの活用**

医療機関は、電子カルテシステムや患者データを扱うため、ランサムウェア攻撃の主要な標的となる。そのため、デコイシステムの導入は、以下のような形で医療機関のサイバーセキュリティ強化につながるであろう。

- **偽の電子カルテデータの配置による早期検知**

実際の患者情報とは異なる電子カルテサーバを設置し、攻撃が試みられた際に防御策を即座に発動できる体制を構築する。

- **ネットワークセグメントの分離によるリスク軽減**

デコイシステムを活用し、攻撃が本番環境に到達する前に隔離する仕組みを導入することで、リスクを低減する。

こうしたことから、デコイシステム導入することで、以下のメリットが得られる可能性がある。

1. 早期検知が可能：攻撃者がデコイに引っかかることで、迅速な対応が可能となる。
2. 被害の最小化：本番環境とは異なる環境で攻撃を検出し、感染の拡大を防ぐことができる。
3. セキュリティ強化に貢献：攻撃手法の分析を通じて、防御戦略の改善に活用できる。

これら調査の結果、デコイシステムはランサムウェア攻撃に対する高度な防御策の一つであり、攻撃者を欺くことで被害を最小限に抑えると同時に、セキュリティ対策

の強化にも寄与することが明らかとなった。特に、医療機関においては患者情報の保護に極めて有効な手段となり得ると考えられる。

この有効性を検証するため、東北大学病院において実証実験を実施することとした。そのシステム構成の詳細については図 2 および図 3（文末）に示す。今回の実証では、既存のシステム環境に変更を加えることなくデコイシステムを導入することが可能であり、この点からも現実性の高い防御手段であることが確認された。

しかしながら、デコイシステム自体が感染し、ネットワークからの切断等の対応が間に合わなかった場合、かえって感染リスクを高める可能性が指摘された。そのため、導入の費用対効果と感染リスクとのトレードオフをどのように設定するかが今後の課題として残る。

一方で、地域医療ネットワークシステム上のサーバセグメントまたは DMZ セグメントにデコイサーバを設置することで、ネットワークに参加する医療機関へ論理的に展開できる可能性が示された。このアプローチを採用すれば、各医療機関に専任の管理者が不在の場合でも、中央管理によりアラートの一元的な監視・管理が可能となる。特に、既存のシステム構成を変更する必要がないことから、導入の実効性が高いことが確認された。

先述の懸念点と同様に、今後は感染リスクと運用コストのトレードオフをどのように最適化するか が、実用化に向けた重要な課題となる。

■ゼロトラストとトラストゾーンの併用

電子カルテシステムは、従来のトラストゾーン（境界型防御）に基づいて構築されており、ゼロトラスト型の防御と併用されている事例は少ないのが現状である。しかし、近年では AI サービスがクラウド型で提供されるケースが増えており、電子カルテ端末からクラウドサービスを利用する際には、ゼロトラスト型の防御を適用する必要がある。実際には、1 台の電子カルテ端末が、境界型防御のもとで院内ネットワークに接続されながらも、ゼロトラストの原則に従ってクラウドサービスを利用するという環境が求められている。

そこで Web 分離技術を活用した仮想ブラウザ（Virtual Browser）の導入が注目されていることに着目した。

仮想ブラウザとは、ユーザの端末上で直接 Web ページを開くのではなく、クラウドや仮想環境上でブラウジング処理を実行し、そのレンダリング結果のみをユーザーに提供する技術である。この方式を採用することで、悪意のあるスクリプトやマルウェアの影響を回避し、安全なインターネット利用を可能にするものである。

仮想ブラウザの仕組みとその利点、さらに導入に伴う課題について考察し、東北大学病院で実証することとした。

- **仮想ブラウザの仕組みと特性**

仮想ブラウザは、大きく分けてクラウド型仮想ブラウザ、サーバベース型仮想ブラウザ、コンテナ型仮想ブラウザの三つの方式に分類される。クラウド型では、Web サイ

トのレンダリング処理をクラウド環境で実行し、ユーザ端末には画像や仮想セッションのストリームのみを転送する。この方式は、ユーザの端末に Web コンテンツを一切ダウンロードしないため、マルウェア感染のリスクを大幅に軽減する。特に、ゼロトラスト環境の構築に適しており、高度なセキュリティ対策を求める組織において導入が進められている。

一方、サーバベースの仮想ブラウザは、企業や組織の内部サーバ上でブラウジング環境を構築し、リモートデスクトップ方式でユーザに提供する仕組みである。この方式では、ユーザの端末に Web コンテンツが直接配信されることがないため、フィッシング攻撃やランサムウェア感染のリスクを抑制できる。また、特定の業務環境に適応しやすく、オンプレミス環境において高いセキュリティを確保する手段として利用されている。

さらに、コンテナ型仮想ブラウザは、ユーザの端末上に仮想コンテナを作成し、その中でブラウザを実行する方式である。この方式では、ブラウザのセッションが終了するとコンテナ内のデータが自動的に削除されるため、マルウェアが端末のシステムに影響を与えるリスクを最小限に抑えられる。

- **仮想ブラウザの利点**

仮想ブラウザの最大の利点は、サイバー攻撃の感染リスクの低減にある。通常、Web サイトを閲覧する際には、JavaScript や各種スクリプトがユーザの端末上で実行されるが、仮想ブラウザを利用すれば、Web ページの実行処理がクラウドや仮想環境上で完結するため、悪意のあるコードが端末に直接影響を及ぼすことがない。

たとえば、電子カルテシステム端末を直接インターネットに接続することなく、仮想ブラウザを介して外部サイトを閲覧することで、安全性を確保できる。

- **仮想ブラウザの課題と運用上の考慮点**

仮想ブラウザには上記のような、多くの利点がある一方で、運用上の課題も存在する。第一にクラウド環境やリモート環境でブラウザを実行するため、レスポンスの遅延が発生する可能性がある。特にレスポンスを重要視する電子カルテ端末においては重要な課題となる。

また運用コストの問題も重要な課題である。クラウド型やサーバベース型の仮想ブラウザは、導入および維持に一定のコストが発生する。特に大規模な組織では、サーバーリソースの確保やネットワーク帯域の増強が必要となるため、コスト対効果の検討が求められる。

- **仮想ブラウザの評価**

これまでの説明の通り、仮想ブラウザは、Web 分離技術を活用し、マルウェアやフィッシング攻撃のリスクを低減する有効な手段として期待されている。特に医療機関などのセキュリティが求められる環境において、その導入が進んでいる。Web コンテンツがユーザの端末上で直接実行されないという特性により、ランサムウェアやゼロデイ攻撃に対する強固な防御策となる。

しかしながら、レスポンスの遅延や運用コストの増加、特定の Web サービスとの互換性といった課題も存在するため、導入に

際しては慎重な検討が求められる。

そこで実際の商用サービスを検討したところ、年間ライセンス型で、既存のサーバ類を利活用することで対応できる、コンテンツ型の仮想ブラウザがあった。これは実際に音声には対応していないものの、既に東北大学病院では実装されているもので、クラウド型 AI サービスの実行を想定して、音声対応版を用意して実際に試験を行うこととした。

- **東北大学病院での実装試験**

本実証においては、院内導入の構成図および地域医療ネットワークシステム上に展開する設計図を、図 4 および図 5（文末）に示す通り実装した。

また東北大学病院が試行していた音声会話を SOAP 形式に変換するサービスを、本実証環境において動作可能かどうかの検証を行った。検証の過程で、電子カルテ端末のメモリが 8GB であり、AI サービス側が要求する端末スペックに満たないという課題が明らかとなった。これに対し、メモリ増設を行うことで対応を準備したが、実際には、サーバ側での処理が途中の仮想ブラウザサーバを経由しても遅延を生じることなく、そのまま活用可能であることが確認された。

さらに、本環境ではコンテナ型のアーキテクチャを採用しており、感染防御を維持しながら、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できた点は大きな意義を持つ。

この方式を導入することで、安全性を確保しつつ、十分な処理速度を維持しながら、既存環境に大きな変更を加えることなく運用できることが示唆された。

加えて地域医療ネットワークシステム上に同様のサーバを設置することで、同じ環境を参加施設にも提供できる設計を行った。この仕組みを活用することで、人材不足が懸念される医療機関や、外部サービスの利用を前提とするクリニックなどにとっても、高い利便性をもたらすことが期待できる。

そこで図 6、ならびに図 7 に地域医療ネットワークシステムを活用したシステム設計案を作成した。これらはローカル側(医療機関側)のネットワーク環境の変更は最小限であり、コスト課題なども十分に配慮がされたものと考える。

来年度は、設計した通りにデコイシステムおよび仮想ブラウザを地域医療ネットワークシステム上に構築し、その動作や利便性の評価を実施する予定である。

D. 健康危惧情報

代表者報告書で適時記載

E. 研究発表

1. 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)

2. **学会発表**
   - ① 第 44 回医療情報学連合大会

シンポジウム

1. 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（第 25 回日本医療情報学会学術大会）,2024/11/21-24, 日本医療情報学会 第44回医療情報学連合大会論文集:医療情報学 44（Suppl）p358-359,2024.
2. 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（第 25 回日本医療情報学会学術大会）,2024/11/21-24, 日本医療情報学会第 44 回医療情報学連合大会論文集:医療情報学 44 （ Suppl ） p368-370,2024.
3. 藤井進 中村直毅 野中小百合 園部真也,医療AIの研究と開発、社会実装を大学と企業の立場で考える, 第52回日本救急医学会総会・学術集会, 2024/10/13-15,第 52 回日本救急医学会総会・学術集会 p ,2024.
4. 藤井進, 医療データの利活用を推進する組織と臨床利用AI によるデータ収集～東北大学病院での事例並びに地域医療ネットワークシステムの活用に向けて～」,日本医師会-PhRMA ラウンドテーブル,東急キャピタルホテル,講演,2024/12/13
5. 藤井進, 医療データの利活用を推進する組織と臨床利用AI によるデータ収集～東北大学病院での事例並びに地域医療ネットワークシステムの活用に向けて～」,日本医師会医療 IT 委員会,日本医師会本部,講演,20245/2/5
6. 藤井進 中村直毅 野中小百合 園部真也,医療情報の利活用を進めるための取り組みについて」,CRIETO,2025/2/21

F. 知的財産権の出願

・なし

添付

A1. 地域連携システムにおけるセキュリティ対応のニーズ調査　アンケート内容：

No	質問	回答
自院の状況についてご質問です		
1	病床規模を教えてください。	1：クリニック 2：病院（400 床以上） 3：病院（200～399 床） 4：病院（200 床未満） 5：薬局 6：介護施設 7：歯科
2	自院のセキュリティ人材が不足していると感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
3	自院ではセキュリティ対策がきちんとできていると思いますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
4	MMWIN には参加していますか？	1：はい 2：いいえ
地域医療連携システムの情報共有についてご質問です		
5	地域医療連携システムを使って、画像の共有ができることに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
6	地域医療連携システムを使って、検査結果、薬歴、病名の共有ができることに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない

7	地域医療連携システムを使って、紹介、逆紹介、診療予約ができることに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
地域連携システムを使うことによって、医療情報の共有だけでなく、以下のセキュリティ対策がなされるとするとメリットがあるかに関するご質問です		
8	**医療機器や電子カルテシステムのリモート保守に対する向上することに魅力を感じるか。**	
8-1	リモート保守の向上１：複数ある“VPN回線（ベンダー毎の保守回線）”や“外部との接続方法”が、１つに集約されることに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
8-2	リモート保守の向上２：“VPN サーバ”や“リモートログインサーバ”の保守から解放されることに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
8-3	リモート保守の向上３：外部委託業者（例えば給食）の“外部持ち込みサーバとの接続管理”から解放されることに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
9	**部門システムや電子カルテシステムの“バックアップを地域連携システムが稼働するクラウド上に保管”することに魅力を感じるか**	
9-1	地域連携の“クラウド上に院内の医療情報システムのバックアップができる”ことに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
9-2	地域連携の“クラウド上にバックアップを置くことで**ランサムウェアの対策**を兼ねる”のであれば、魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない

		4：あまり感じない 5：まったく感じない
9-3	**災害対策**として“クラウドにバックアップデータが保存される”ことに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
10	**地域医療連携システムのネットワークを活用したその他の用途について**	
10-1	地域連携システムを通して、AI(診断補助やカルテ作成などの医師の業務支援など)が使えることに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
10-2	地域連携システムを通して、AI(診断補助やカルテ作成などの医師の業務支援など)を使うときに、患者の診療情報が地域連携システムを通して安心安全(三省のガイドラインに準拠)に情報共有されるとしたら、利用したいと考えますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない

表３　要因分析

有効データ数＝308

＜因子負荷行列と寄与率＞　（バリマックス法）

変数名	因子1	因子2	因子3	因子4	因子5	因子6	因子7	共通性
施設規模	0.003	0.037	0.043	-0.031	0.102	0.057	0.284	0.098
自施設のセキュリティ人材が不足していると感じますか？	0.192	0.139	-0.15	0.042	0.904	0.031	0.311	0.995
自施設ではセキュリティ対策がきちんとできていると思いますか？	0.082	-0.013	-0.103	-0.011	-0.359	-0.008	-0.015	0.147
画像の共有ができることに魅力を感じるか	0.797	0.246	0.166	0.14	-0.036	0.162	-0.003	0.77
検査結果、薬歴、病名の共有ができることに魅力を感じるか	0.874	0.27	0.134	0.107	0.001	0.13	-0.009	0.883
地域医療連携システムを使って、紹介、逆紹介、診療予約ができることに魅力を感じるか	0.781	0.266	0.131	0.211	-0.009	0.031	0.085	0.75
リモート保守の向上１：複数あるVPN回線（ベンダー毎の保守回線）や外部との接続方法が、１つに集約されることに魅力を感じるか	0.353	0.406	0.665	0.2	0.019	0.129	0.244	0.849
リモート保守の向上２：VPNサーバやリモートログインサーバの保守から解放されることに魅力を感じるか	0.28	0.317	0.693	0.178	0.203	0.408	0.026	0.9
リモート保守の向上３：外部委託業者（例えば給食）の外部持ち込みサーバとの接続管理から解放されることに魅力を感じるか	0.28	0.287	0.34	0.17	0.03	0.774	0.3	0.995
地域医療連携の連携のクラウド上に院内の医療情報システムのバックアップができることに魅力を感じるか	0.278	0.687	0.191	0.243	0.065	0.138	0.12	0.682
地域医療連携のクラウド上にバックアップを置くことでランサムウェアの対策を兼ねるのであれば、魅力を感じるか	0.231	0.749	0.289	0.204	0.054	0.16	0.075	0.774
災害対策としてクラウドにバックアップデータが保存されることに魅力を感じるか	0.301	0.762	0.073	0.093	0.096	0.066	0.039	0.7
地域医療連携システムを通して、AI(診断補助やカルテ作成などの医師の業務支援など)が使えることに魅力を感じるか	0.409	0.434	0.187	0.465	0.106	0.167	-0.265	0.716
AI(診断補助やカルテ作成などの医師の業務支援など)を使うときに、安心安全に情報共有されるとしたら、利用したいと考えるか	0.336	0.391	0.195	0.818	0.038	0.126	-0.068	0.995
固有値	2.835	2.527	1.335	1.173	1.029	0.924	0.432	
寄与率	0.203	0.181	0.095	0.084	0.073	0.066	0.031	
累積寄与率	0.203	0.383	0.478	0.562	0.636	0.702	0.732	

[R-4.3.3 factanal() : Factor Analysis で算出]

表４　分散分析表

<< ３レベル被分かれ分散分析版 >>

分散分析表(簡略版)

変数名	施設規模変動				自施設のセキュリティ人材が不足していると感じますか？変動				自施設ではセキュリティ対策がきちんとできていると思いますか？変動				残差変動		補正計算	
	MS	df	F	P	MS	df	F	P	MS	df	F	P	MS	df	施設規模	じますか？
画像の共有ができることに魅力を感じるか	0.76	4	0.571	0.6889	1.33	12	0.679	0.75426	1.96	23	1.774	0.01748	1.11	280	No	No
検査結果、薬歴、病名の共有ができることに魅力を感じるか	0.62	4	0.367	0.8275	1.7	12	1.29	0.28863	1.32	23	1.243	0.20767	1.06	280	No	No
地域医療連携システムを使って、紹介、逆紹介、診療予約ができることに魅力を感じるか	0.76	4	0.438	0.77883	1.73	12	1.217	0.32965	1.42	23	1.297	0.16792	1.1	280	No	No
リモート保守の向上１：複数あるVPN回線（ベンダー毎の保守回線）や外部との接続方法が、１つに集約されることに魅力を感じるか	1.71	4	1.676	0.21977	1.02	12	0.825	0.62549	1.24	23	1.173	0.26886	1.06	280	No	No
リモート保守の向上２：VPNサーバやリモートログインサーバの保守から解放されることに魅力を感じるか	1.14	4	0.403	0.80286	2.83	11	2.574	0.02843	1.1	22	1.125	0.31892	0.98	272	No	No
リモート保守の向上３：外部委託業者（例えば給食）の外部持ち込みサーバとの接続管理から解放されることに魅力を感じるか	2.27	4	0.907	0.4932	2.51	11	1.928	0.09155	1.3	22	1.236	0.2164	1.05	272	No	No
地域医療連携の連携のクラウド上に院内の医療情報システムのバックアップができることに魅力を感じるか	0.59	4	0.188	0.93991	3.11	12	1.752	0.11972	1.78	23	1.441	0.09038	1.23	280	No	No
地域医療連携のクラウド上にバックアップを置くことでランサムウェアの対策を兼ねるのであれば、魅力を感じるか	1.07	4	0.437	0.77951	2.44	12	2.212	0.04924	1.11	23	1.201	0.2428	0.92	280	No	No
災害対策としてクラウドにバックアップデータが保存されることに魅力を感じるか	0.6	4	0.211	0.92758	2.83	12	1.728	0.12552	1.64	23	1.865	0.01075	0.88	279	No	No
地域医療連携システムを通して、AI(診断補助やカルテ作成などの医師の業務支援など)が使えることに魅力を感じるか	0.5	4	0.323	0.85691	1.55	12	1.118	0.39235	1.39	23	1.434	0.09339	0.97	280	No	No
AI(診断補助やカルテ作成などの医師の業務支援など)を使うときに、安心安全に情報共有されるとしたら、利用したいと考えるか	0.28	4	0.246	0.90638	1.16	12	0.747	0.69471	1.55	23	1.585	0.04597	0.98	280	No	No

表 5　変動成分表：各変動成分の SD と CV、および残差 SD に対する SD 比(SDR)

変動成分表：各変動成分のSDとCV、および残差SDに対するSD比(SDR)

変数名	N	総平均	施設規模成分			自施設のセキュリティ人材が不足していると感じますか？成分			自施設ではセキュリティ対策がきちんとできていると思いますか？成分			残差成分	
			SD	CV	SDR	SD	CV	SDR	SD	CV	SDR	SD	CV
画像の共有ができることに魅力を感じるか	319	3.64	0	0	0	0	0	0	0.31	8.48	0.293	1.05	28.92
検査結果、薬歴、病名の共有ができることに魅力を感じるか	319	3.78	0	0	0	0.15	4.11	0.151	0.17	4.48	0.164	1.03	27.27
地域医療連携システムを使って、紹介、逆紹介、診療予約ができることに魅力を感じるか	319	3.77	0	0	0	0.15	3.85	0.139	0.19	5.05	0.182	1.05	27.8
リモート保守の向上１：複数あるVPN回線（ベンダー毎の保守回線）や外部との接続方法が、１つに集約されることに魅力を感じるか	319	3.52	0.15	4.14	0.142	0	0	0	0.14	4.05	0.139	1.03	29.23
リモート保守の向上２：VPNサーバやリモートログインサーバの保守から解放されることに魅力を感じるか	309	3.54	0	0	0	0.3	8.45	0.302	0.12	3.27	0.117	0.99	27.94
リモート保守の向上３：外部委託業者（例えば給食）の外部持ち込みサーバとの接続管理から解放されることに魅力を感じるか	309	3.42	0.14	4.14	0.138	0.25	7.43	0.248	0.17	4.83	0.161	1.03	30
地域医療連携の連携のクラウド上に院内の医療情報システムのバックアップができることに魅力を感じるか	319	3.58	0	0	0	0.28	7.85	0.253	0.25	6.86	0.222	1.11	30.97
地域医療連携のクラウド上にバックアップを置くことでランサムウェアの対策を兼ねるのであれば、魅力を感じるか	319	3.92	0	0	0	0.27	6.95	0.284	0.14	3.66	0.149	0.96	24.5
災害対策としてクラウドにバックアップデータが保存されることに魅力を感じるか	318	4.18	0	0	0	0.27	6.54	0.292	0.29	6.96	0.311	0.94	22.42
地域医療連携システムを通して、AI(診断補助やカルテ作成などの医師の業務支援など)が使えることに魅力を感じるか	319	3.74	0	0	0	0.12	3.25	0.123	0.22	5.79	0.22	0.98	26.34
AI(診断補助やカルテ作成などの医師の業務支援など)を使うときに、安心安全に情報共有されるとしたら、利用したいと考えるか	319	3.66	0	0	0	0	0	0	0.25	6.89	0.255	0.99	27

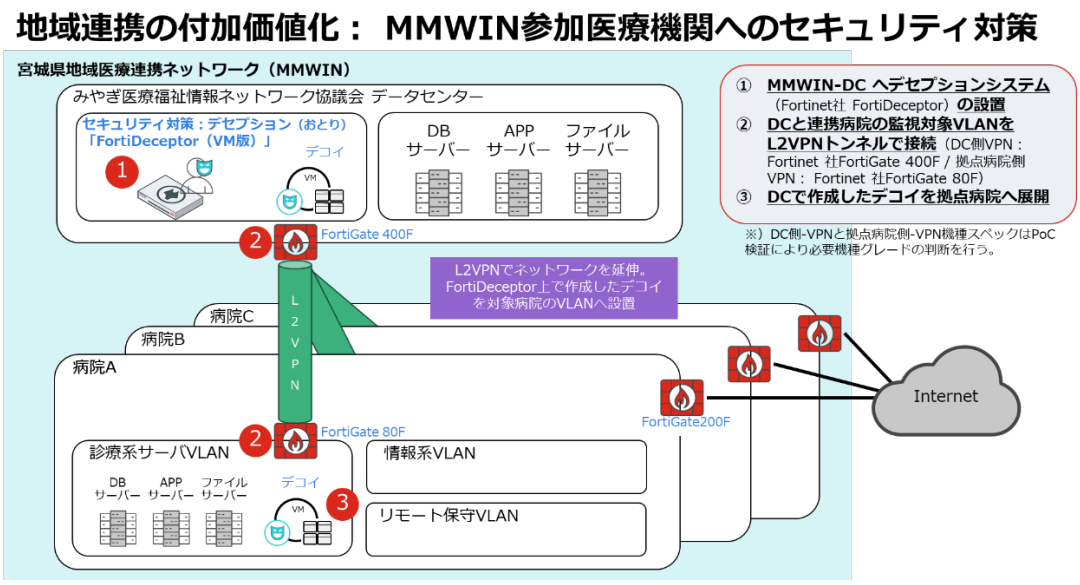


図 2　地域連携の付加価値化： MMWIN 参加医療機関へのセキュリティ対策

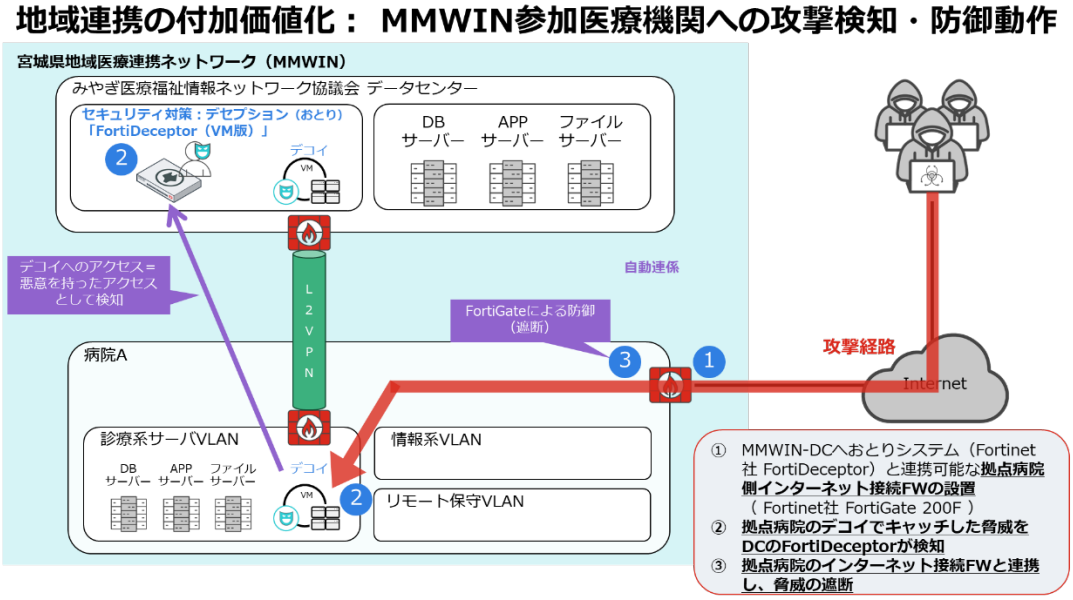


図 3　地域連携の付加価値化： MMWIN 参加医療機関への攻撃検知・防御動作

図 2・3 は日本医療情報学会での発表スライドから引用。フォーティネットジャパン合同会社様から研究用に提供されたものを使用しています。資料の再利用等はご注意ください。

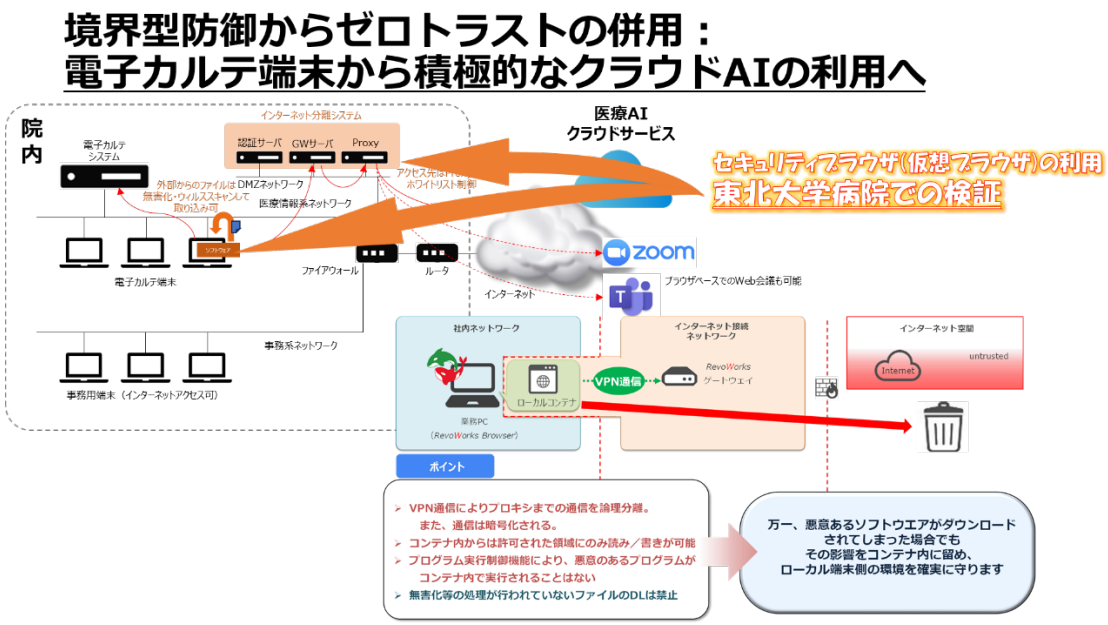


図 4　境界型防御からゼロトラストの併用

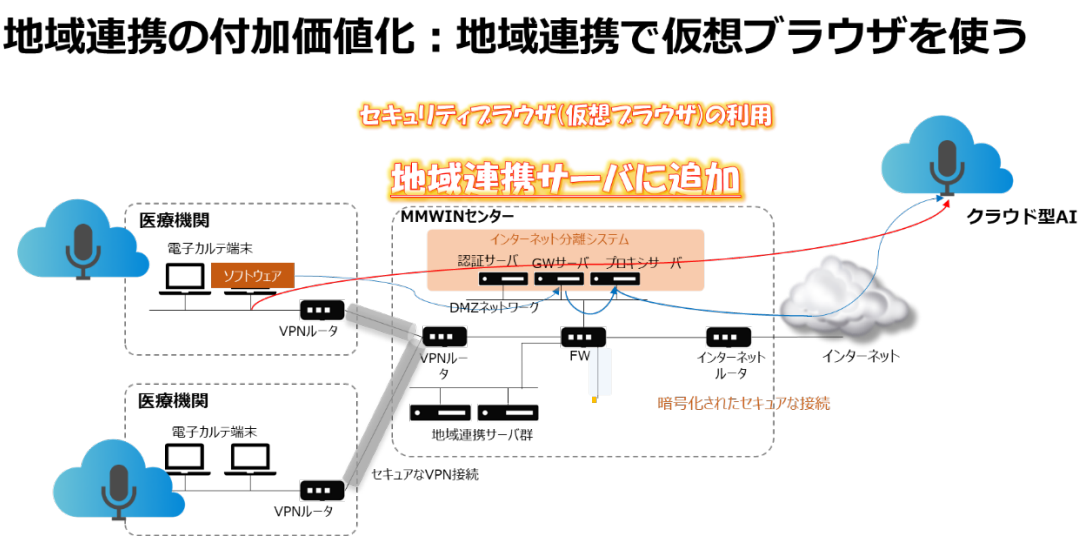


図 5　地域連携の付加価値化：地域連携で仮想ブラウザを使う

図 2・3 は日本医療情報学会での発表スライドから引用。ジェイズ・コミュニケーション株式会社様から研究用に提供されたものを使用しています。資料の再利用等はご注意ください。

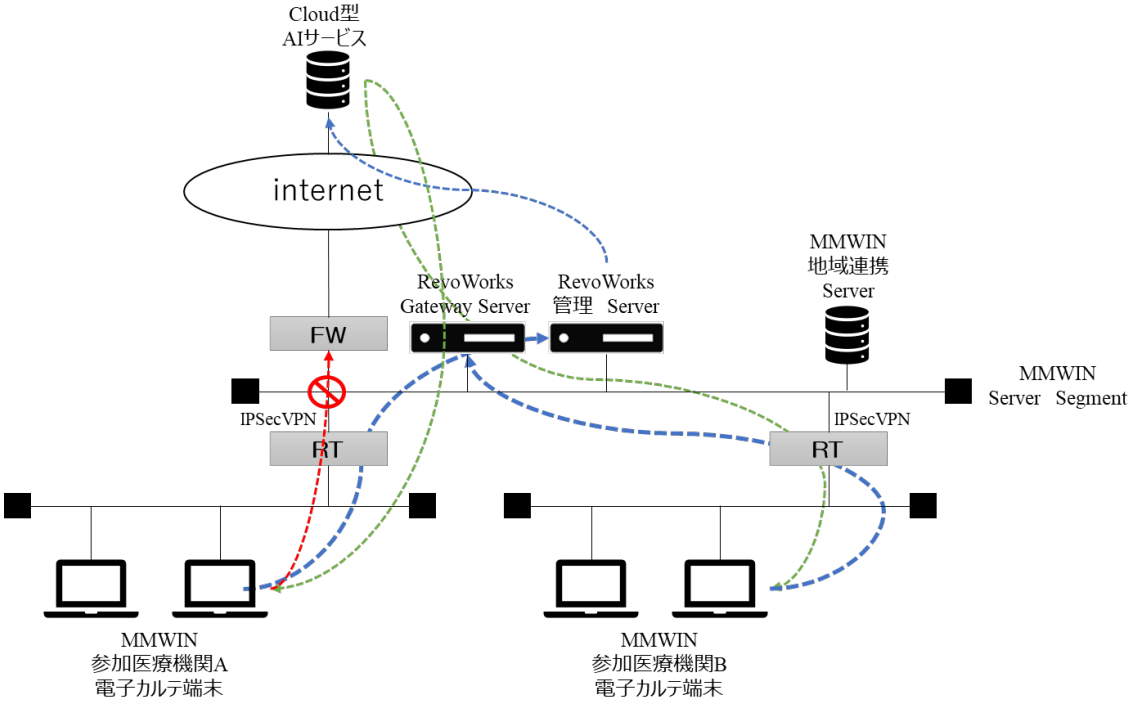


図 6　地域連携の付加価値化：地域医療連携システムで仮想ブラウザを使う場合の設計案

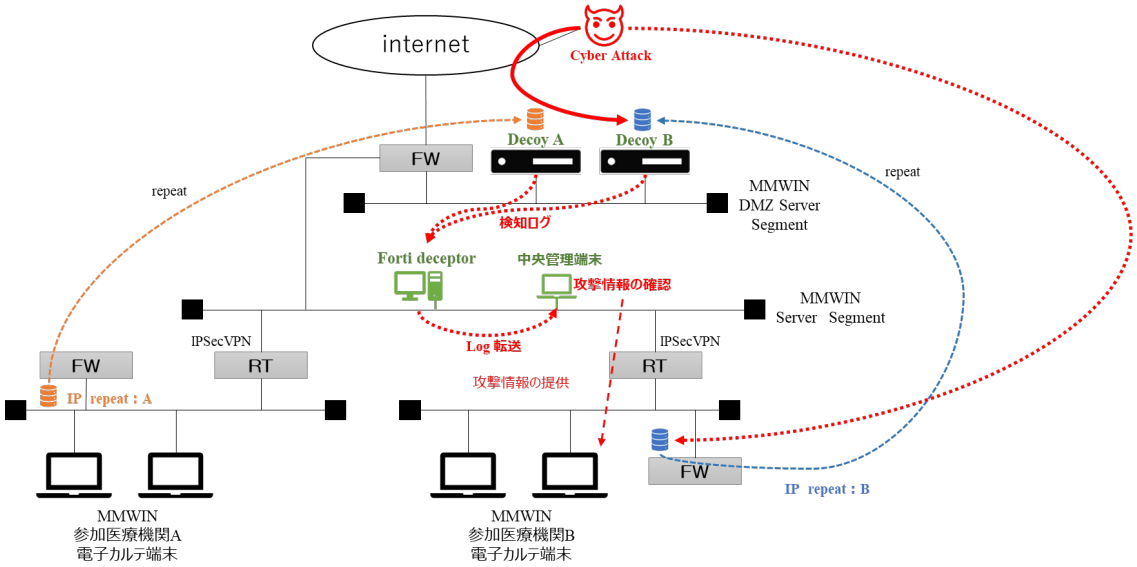
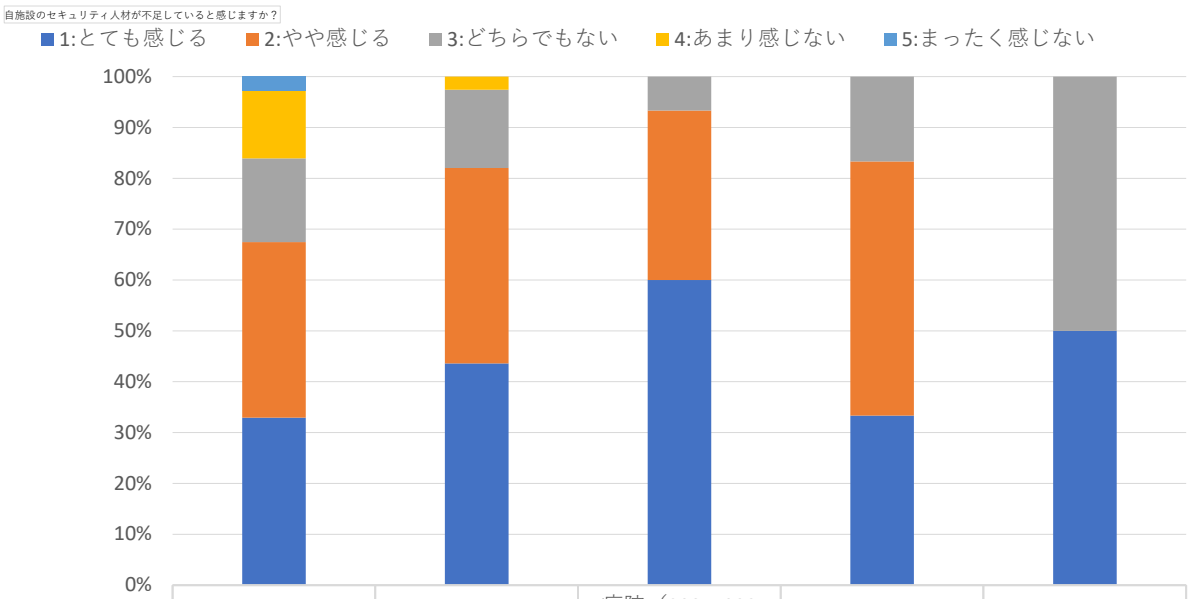


図 7　地域連携の付加価値化：地域医療連携システムでデコイシステムを使った中央管理を行う場合の設計案

自院のセキュリティ人材が不足していると感じますか？

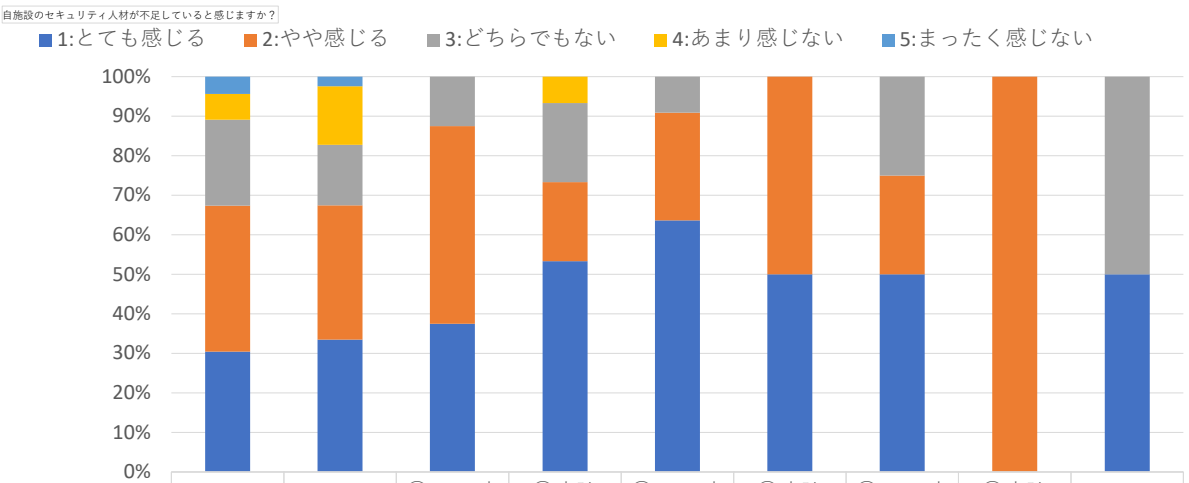
個数 / No



	クリニック ①	病院（200床未満） ②	病院（200～399床） ③	病院（400床以上） ④	介護施設 ⑤
5:まったく感じない	7				
4:あまり感じない	34	1			
3:どちらでもない	42	6	1	1	2
2:やや感じる	88	15	5	3	
1:とても感じる	84	17	9	2	2

医療機関の種類・規模を教えてください。2医療機関の種類・規模を教えてください。

個数 / No

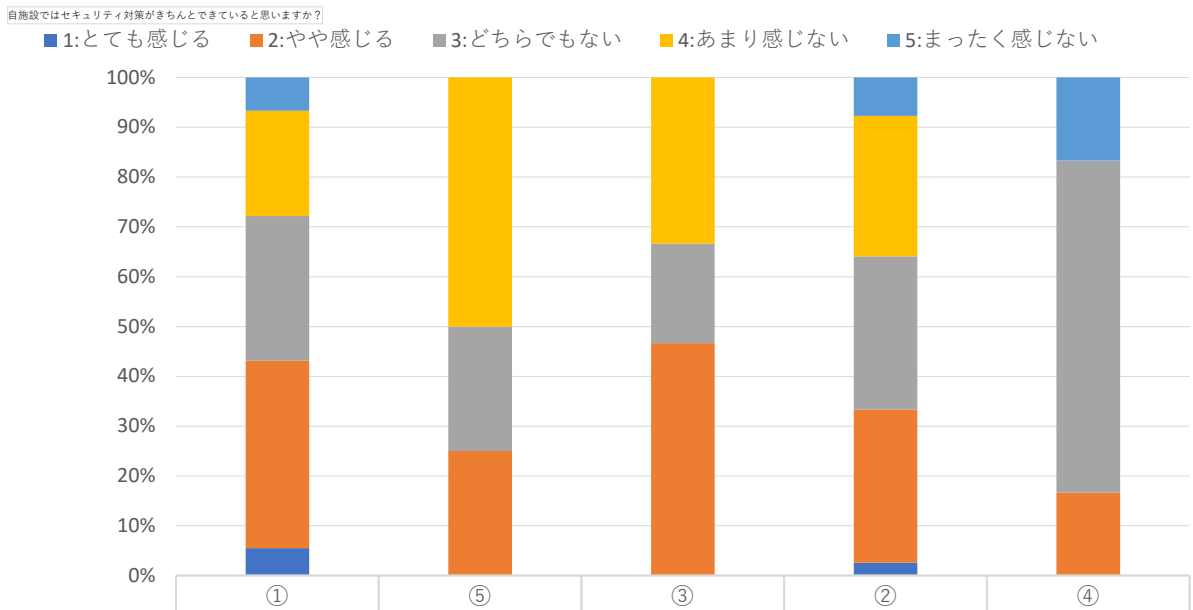


	①MM_クリニック	①クリニック	②MM_病院（200床未満）	②病院（200床未満）	③MM_病院（200～399床）	③病院（200～399床）	④MM_病院（400床以上）	④病院（400床以上）	⑤介護施設
	①_クリニック		②_病院（200床未満）		③_病院（200～399床）		④_病院（400床以上）		⑤_介護施設
5:まったく感じない	2	5							
4:あまり感じない	3	31		1					
3:どちらでもない	10	32	3	3	1		1		2
2:やや感じる	17	71	12	3	3	2	1	2	
1:とても感じる	14	70	9	8	7	2	2		2

グループグループ名

自院ではセキュリティ対策がきちんとできていると思いますか？

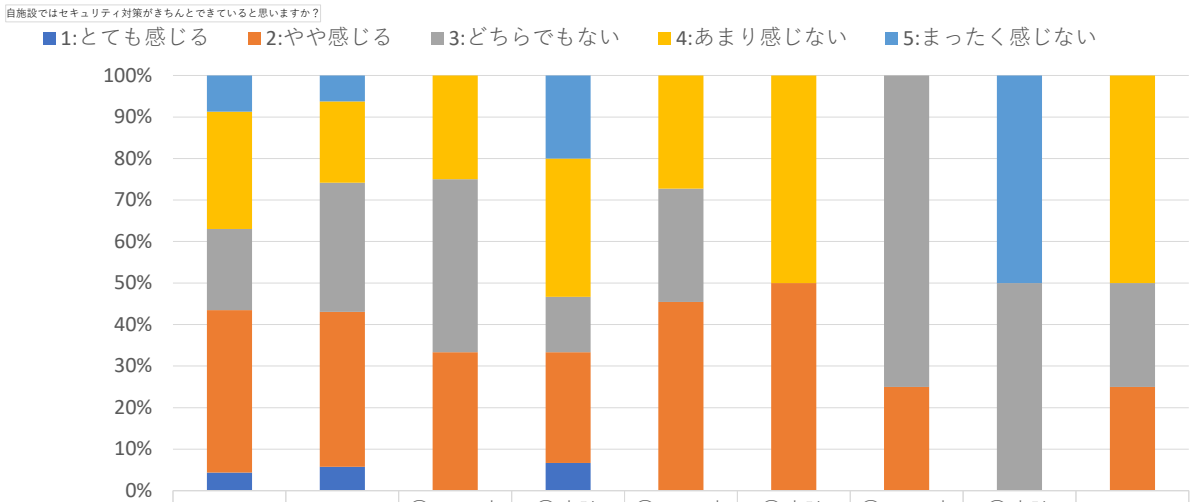
個数 / No



	① クリニック	⑤ 介護施設	③ 病院（200～399床）	② 病院（200床未満）	④ 病院（400床以上）
5:まったく感じない	17			3	1
4:あまり感じない	54	2	5	11	
3:どちらでもない	74	1	3	12	4
2:やや感じる	96	1	7	12	1
1:とても感じる	14			1	

医療機関の種類・規模を教えてください。医療機関の種類・規模を教えてください。2

個数 / No

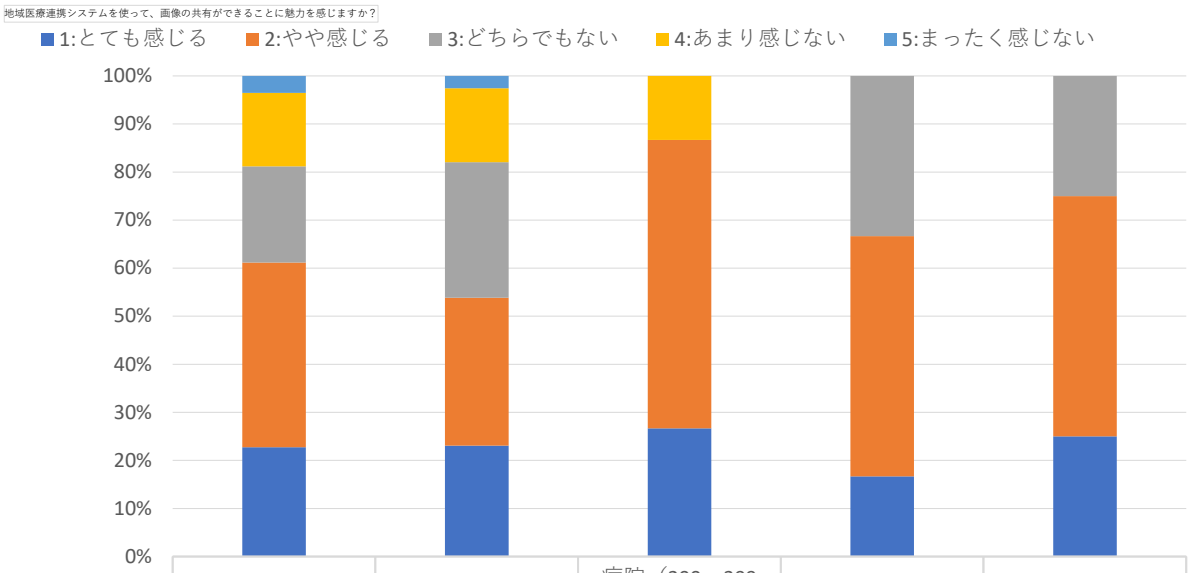


	①MM_クリニック	①クリニック	②MM_病院（200床未満）	②病院（200床未満）	③MM_病院（200～399床）	③病院（200～399床）	④MM_病院（400床以上）	④病院（400床以上）	⑤介護施設
	①_クリニック		②_病院（200床未満）		③_病院（200～399床）		④_病院（400床以上）		⑤_介護施設
5:まったく感じない	4	13		3				1	
4:あまり感じない	13	41	6	5	3	2			2
3:どちらでもない	9	65	10	2	3		3	1	1
2:やや感じる	18	78	8	4	5	2	1		1
1:とても感じる	2	12		1					

グループグループ名

地域医療連携システムを使って、画像の共有ができることに魅力を感じますか？

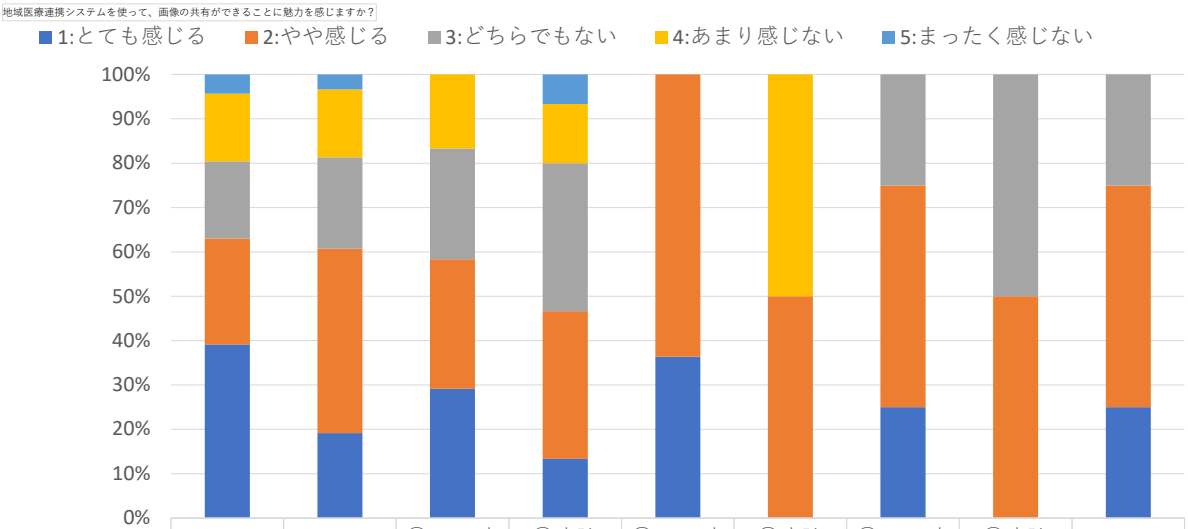
個数 / No



	クリニック ①	病院（200床未満） ②	病院（200～399床） ③	病院（400床以上） ④	介護施設 ⑤
5:まったく感じない	9	1			
4:あまり感じない	39	6	2		
3:どちらでもない	51	11		2	1
2:やや感じる	98	12	9	3	2
1:とても感じる	58	9	4	1	1

医療機関の種類・規模を教えてください。2医療機関の種類・規模を教えてください。

個数 / No

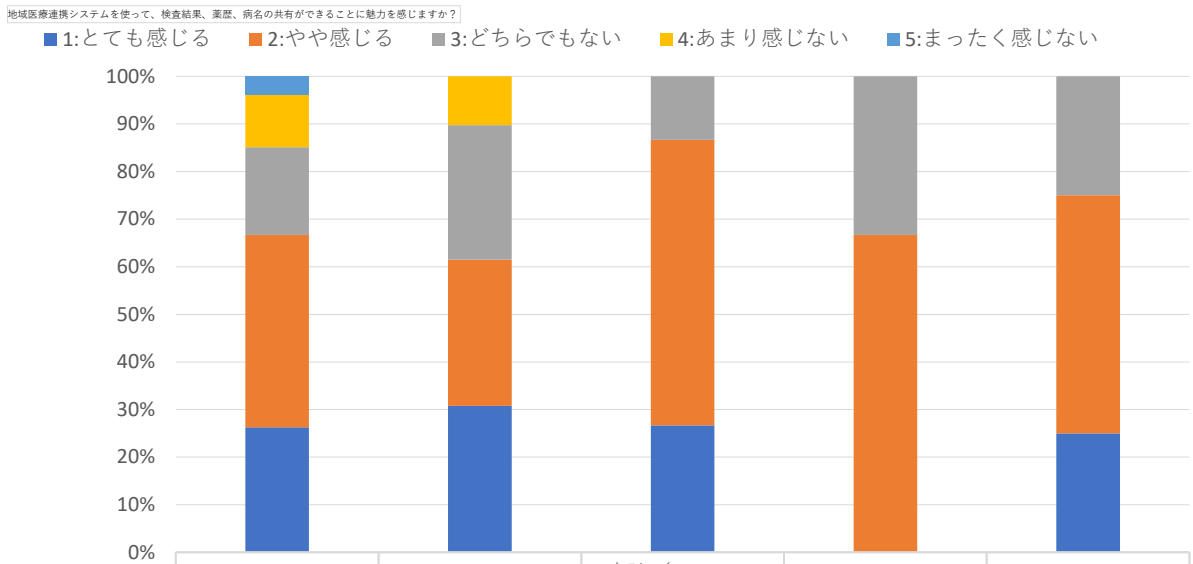


	①MM_クリニック	①クリニック	②MM_病院（200床未満）	②病院（200床未満）	③MM_病院（200～399床）	③病院（200～399床）	④MM_病院（400床以上）	④病院（400床以上）	⑤介護施設
	①_クリニック		②_病院（200床未満）		③_病院（200～399床）		④_病院（400床以上）		⑤_介護施設
5:まったく感じない	2	7		1					
4:あまり感じない	7	32	4	2		2			
3:どちらでもない	8	43	6	5			1	1	1
2:やや感じる	11	87	7	5	7	2	2	1	2
1:とても感じる	18	40	7	2	4		1		1

グループグループ名

地域医療連携システムを使って、検査結果、薬歴、病名の共有ができることに魅力を感じますか？

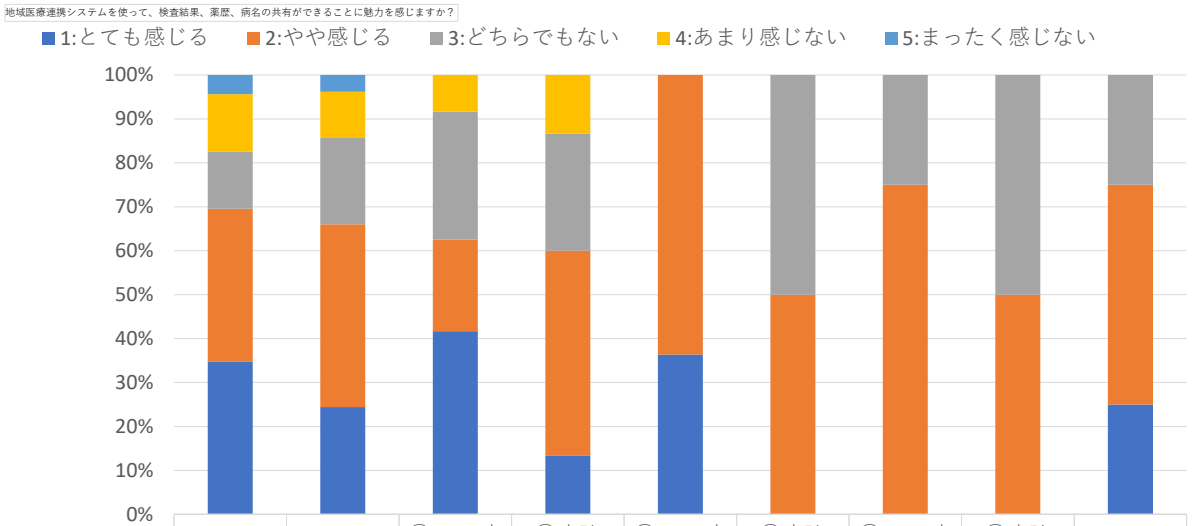
個数 / No



	クリニック ①	病院（200床未満） ②	病院（200～399床） ③	病院（400床以上） ④	介護施設 ⑤
5:まったく感じない	10				
4:あまり感じない	28	4			
3:どちらでもない	47	11	2	2	1
2:やや感じる	103	12	9	4	2
1:とても感じる	67	12	4		1

医療機関の種類・規模を教えてください。2医療機関の種類・規模を教えてください。

個数 / No

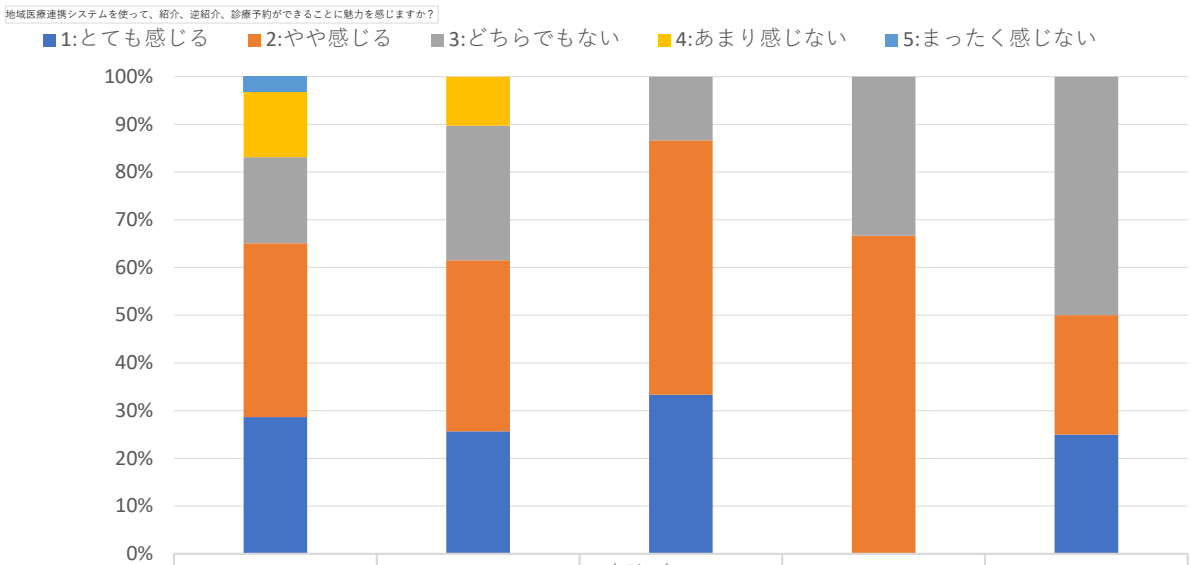


	①MM_クリニック	①クリニック	②MM_病院（200床未満）	②病院（200床未満）	③MM_病院（200～399床）	③病院（200～399床）	④MM_病院（400床以上）	④病院（400床以上）	⑤介護施設
	①_クリニック		②_病院（200床未満）		③_病院（200～399床）		④_病院（400床以上）		⑤_介護施設
5:まったく感じない	2	8							
4:あまり感じない	6	22	2	2					
3:どちらでもない	6	41	7	4		2	1	1	1
2:やや感じる	16	87	5	7	7	2	3	1	2
1:とても感じる	16	51	10	2	4				1

グループグループ名

地域医療連携システムを使って、紹介、逆紹介、診療予約ができることに魅力を感じますか？

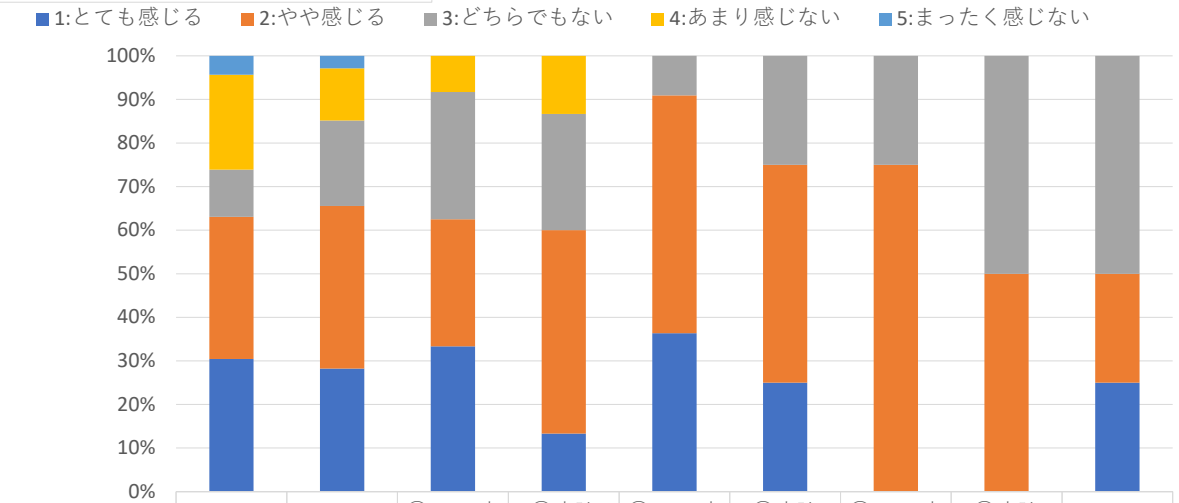
個数 / No



	クリニック ①	病院（200床未満） ②	病院（200～399床） ③	病院（400床以上） ④	介護施設 ⑤
5:まったく感じない	8				
4:あまり感じない	35	4			
3:どちらでもない	46	11	2	2	2
2:やや感じる	93	14	8	4	1
1:とても感じる	73	10	5		1

医療機関の種類・規模を教えてください。2医療機関の種類・規模を教えてください。

個数 / No

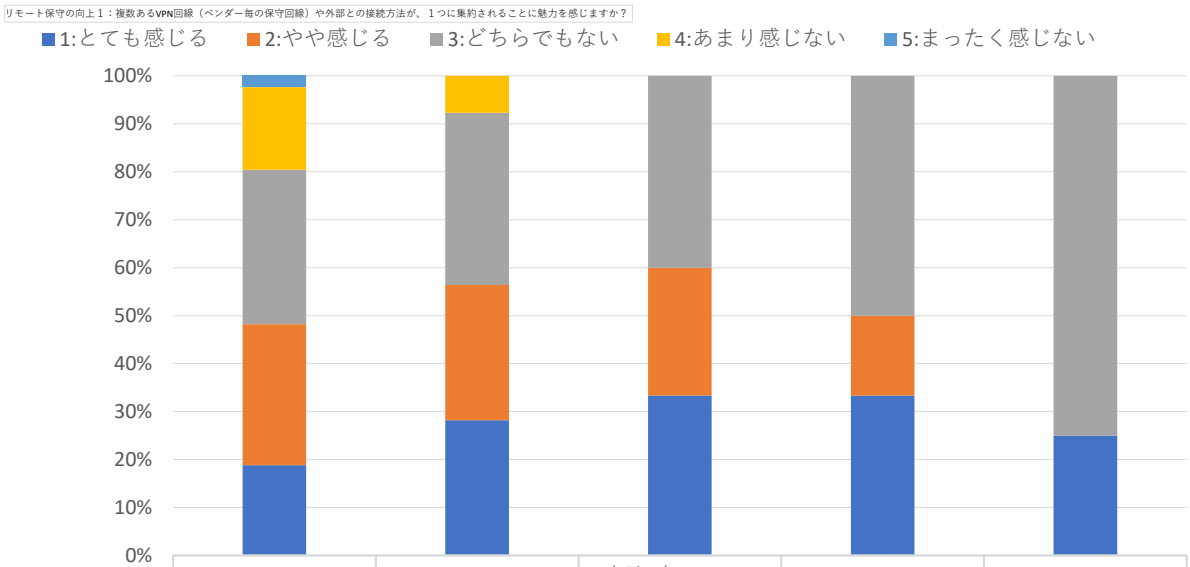


	①MM_クリニック	①クリニック	②MM_病院（200床未満）	②病院（200床未満）	③MM_病院（200～399床）	③病院（200～399床）	④MM_病院（400床以上）	④病院（400床以上）	⑤介護施設
	①_クリニック		②_病院（200床未満）		③_病院（200～399床）		④_病院（400床以上）		⑤_介護施設
5:まったく感じない	2	6							
4:あまり感じない	10	25	2	2					
3:どちらでもない	5	41	7	4	1	1	1	1	2
2:やや感じる	15	78	7	7	6	2	3	1	1
1:とても感じる	14	59	8	2	4	1			1

グループグループ名

リモート保守の向上１：複数ある“VPN回線（ベンダー毎の保守回線）”や“外部との接続方法”が、１つに集約されることに魅力を感じますか？

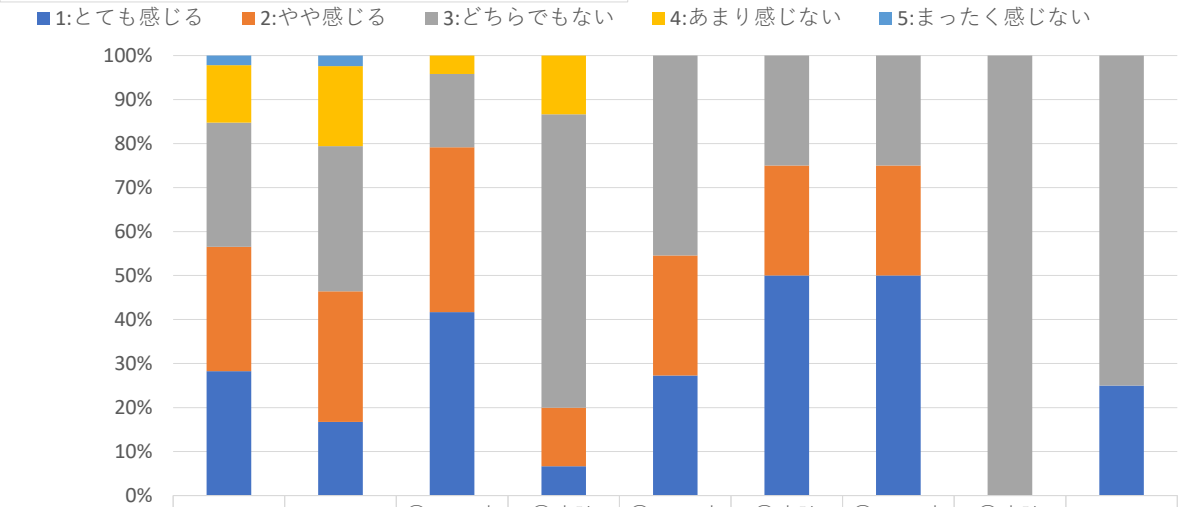
個数 / No



	クリニック ①	病院（200床未満） ②	病院（200～399床） ③	病院（400床以上） ④	介護施設 ⑤
5:まったく感じない	6				
4:あまり感じない	44	3			
3:どちらでもない	82	14	6	3	3
2:やや感じる	75	11	4	1	
1:とても感じる	48	11	5	2	1

医療機関の種類・規模を教えてください。2医療機関の種類・規模を教えてください。

個数 / No

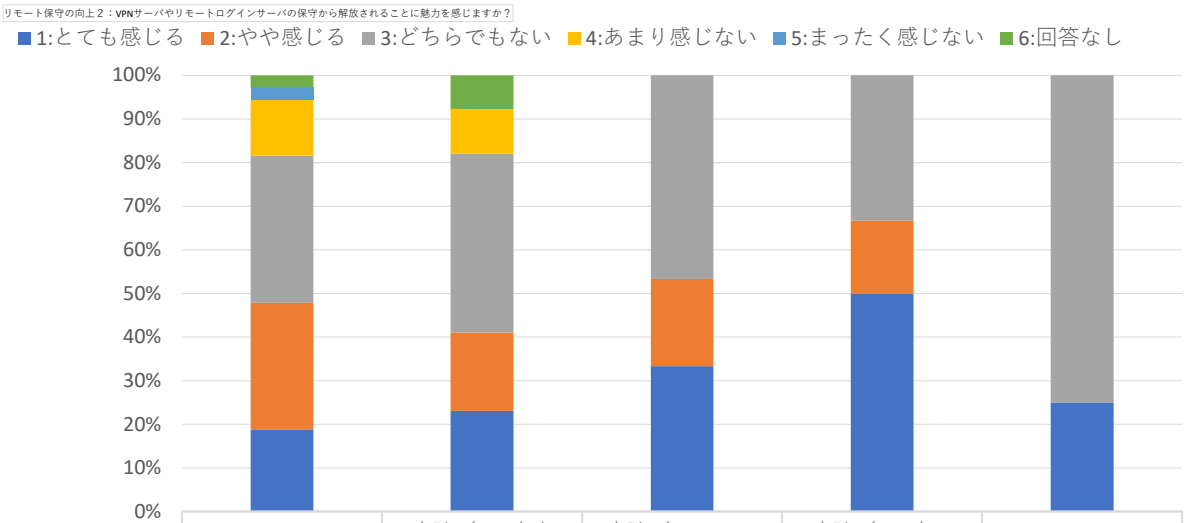


	①MM_クリニック	①クリニック	②MM_病院（200床未満）	②病院（200床未満）	③MM_病院（200～399床）	③病院（200～399床）	④MM_病院（400床以上）	④病院（400床以上）	⑤介護施設
	①_クリニック		②_病院（200床未満）		③_病院（200～399床）		④_病院（400床以上）		⑤_介護施設
5:まったく感じない	1	5							
4:あまり感じない	6	38	1	2					
3:どちらでもない	13	69	4	10	5	1	1	2	3
2:やや感じる	13	62	9	2	3	1	1		
1:とても感じる	13	35	10	1	3	2	2		1

グループグループ名

リモート保守の向上２：“VPNサーバ”や“リモートログインサーバ”の保守から解放されることに魅力を感じますか？

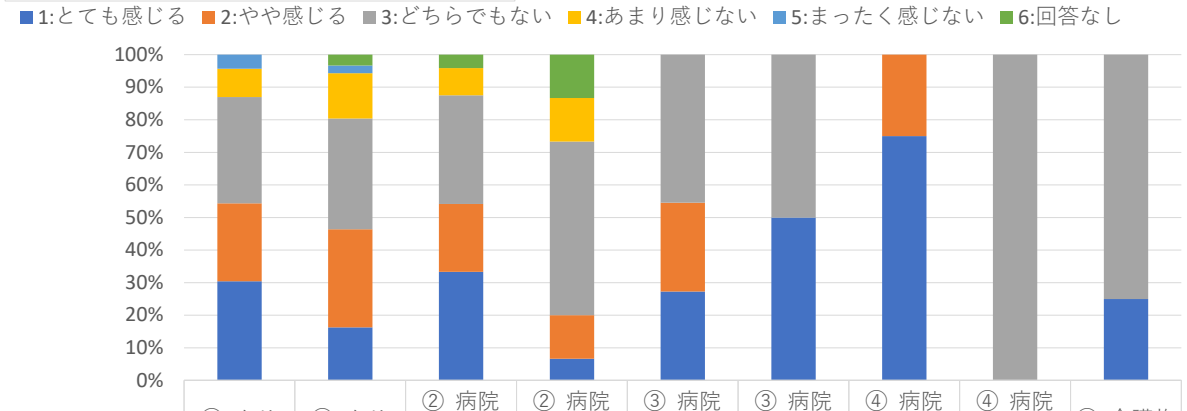
個数 / No



	クリニック ①	病院（200床未満） ②	病院（200～399床） ③	病院（400床以上） ④	介護施設 ⑤
6:回答なし	7	3			
5:まったく感じない	7				
4:あまり感じない	33	4			
3:どちらでもない	86	16	7	2	3
2:やや感じる	74	7	3	1	
1:とても感じる	48	9	5	3	1

医療機関の種類・規模を教えてください。2医療機関の種類・規模を教えてください。

個数 / No

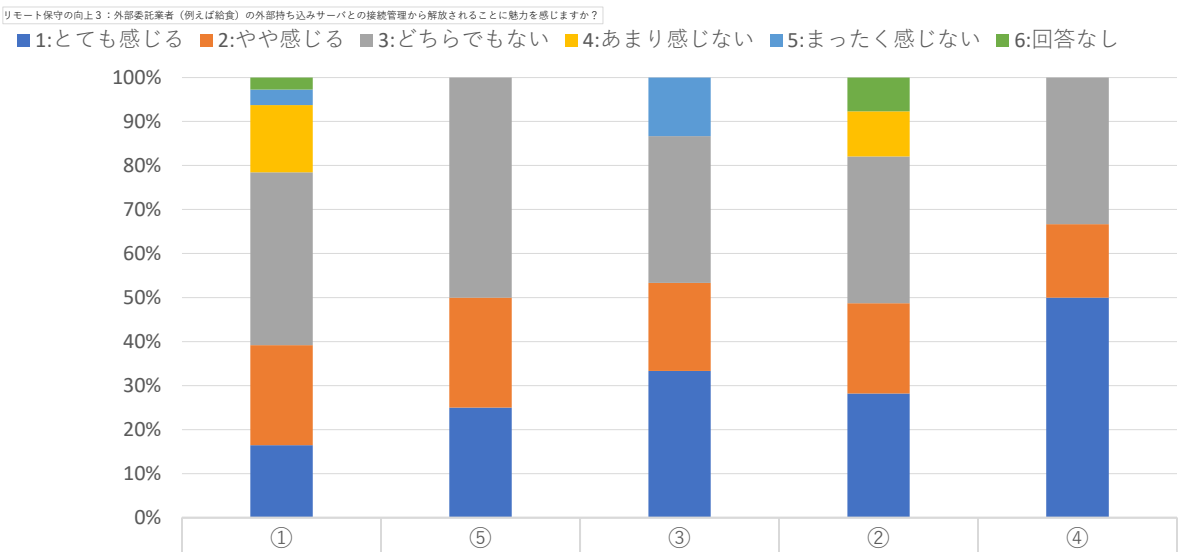


	①_クリニック ①MM_クリニック	①_クリニック ①クリニック	②_病院（200床未満） ②MM_病院（200床未満）	②_病院（200床未満） ②病院（200床未満）	③_病院（200～399床） ③MM_病院（200～399床）	③_病院（200～399床） ③病院（200～399床）	④_病院（400床以上） ④MM_病院（400床以上）	④_病院（400床以上） ④病院（400床以上）	⑤_介護施設 ⑤介護施設
6:回答なし		7	1	2					
5:まったく感じない	2	5							
4:あまり感じない	4	29	2	2					
3:どちらでもない	15	71	8	8	5	2		2	3
2:やや感じる	11	63	5	2	3		1		
1:とても感じる	14	34	8	1	3	2	3		1

グループ名グループ

リモート保守の向上３：外部委託業者（例えば給食）の“外部持ち込みサーバとの接続管理”から解放されることに魅力を感じますか？

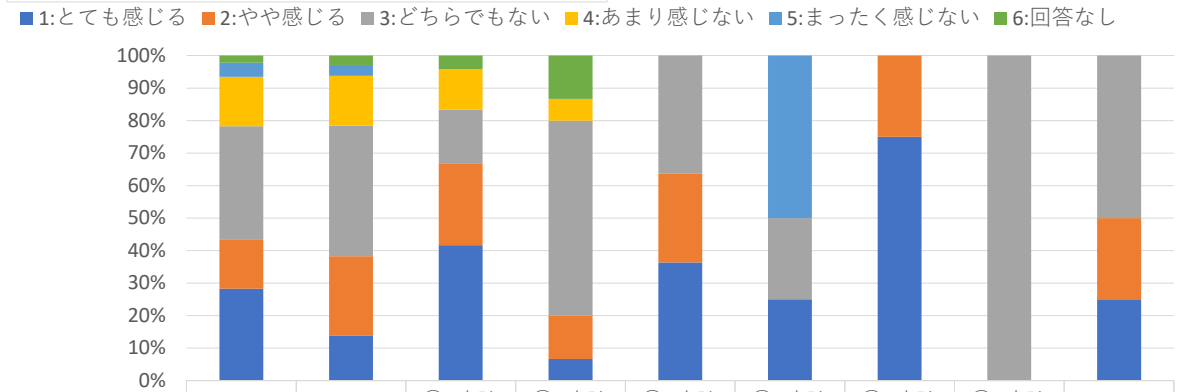
個数 / No



	① クリニック	⑤ 介護施設	③ 病院（200～399床）	② 病院（200床未満）	④ 病院（400床以上）
6:回答なし	7			3	
5:まったく感じない	9		2		
4:あまり感じない	39			4	
3:どちらでもない	100	2	5	13	2
2:やや感じる	58	1	3	8	1
1:とても感じる	42	1	5	11	3

医療機関の種類・規模を教えてください。医療機関の種類・規模を教えてください。2

個数 / No

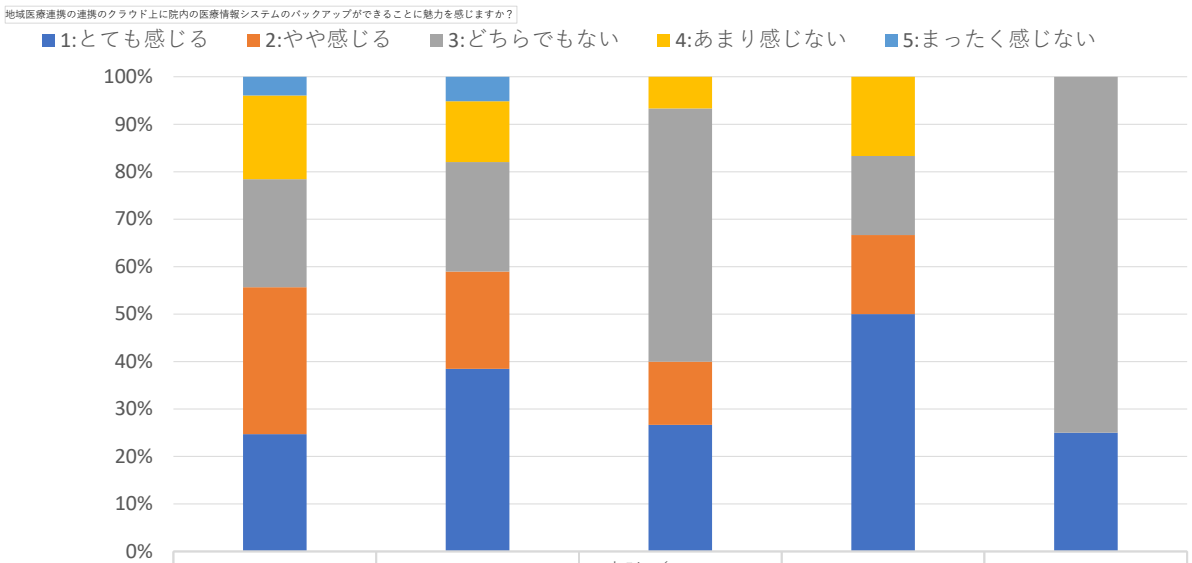


	①_クリニック ①MM_クリニック	①_クリニック ①クリニック	②_病院（200床未満） ②MM_病院（200床未満）	②_病院（200床未満） ②病院（200床未満）	③_病院（200～399床） ③MM_病院（200～399床）	③_病院（200～399床） ③病院（200～399床）	④_病院（400床以上） ④MM_病院（400床以上）	④_病院（400床以上） ④病院（400床以上）	⑤_介護施設 ⑤介護施設
6:回答なし	1	6	1	2					
5:まったく感じない	2	7				2			
4:あまり感じない	7	32	3	1					
3:どちらでもない	16	84	4	9	4	1		2	2
2:やや感じる	7	51	6	2	3		1		1
1:とても感じる	13	29	10	1	4	1	3		1

グループ名グループ

地域連携の“クラウド上に院内の医療情報システムのバックアップができる”ことに魅力を感じますか？

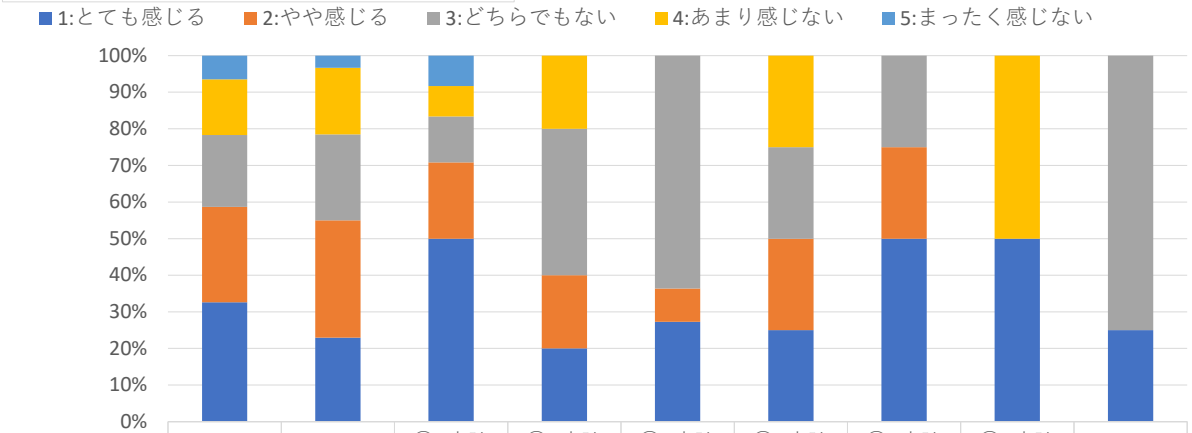
個数 / No



	クリニック ①	病院（200床未満） ②	病院（200～399床） ③	病院（400床以上） ④	介護施設 ⑤
5:まったく感じない	10	2			
4:あまり感じない	45	5	1	1	
3:どちらでもない	58	9	8	1	3
2:やや感じる	79	8	2	1	
1:とても感じる	63	15	4	3	1

医療機関の種類・規模を教えてください。2医療機関の種類・規模を教えてください。

個数 / No

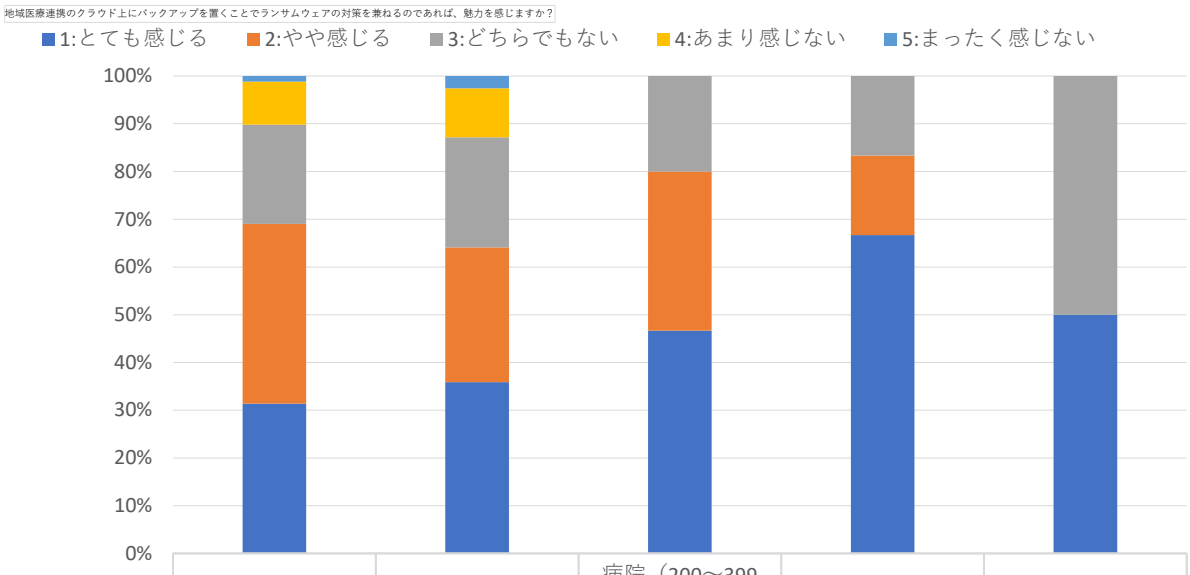


	①_クリニック ①MM_クリニック	①_クリニック ①クリニック	②_病院（200床未満） ②MM_病院（200床未満）	②_病院（200床未満） ②病院（200床未満）	③_病院（200～399床） ③MM_病院（200～399床）	③_病院（200～399床） ③病院（200～399床）	④_病院（400床以上） ④MM_病院（400床以上）	④_病院（400床以上） ④病院（400床以上）	⑤_介護施設 ⑤介護施設
5:まったく感じない	3	7	2						
4:あまり感じない	7	38	2	3		1		1	
3:どちらでもない	9	49	3	6	7	1	1		3
2:やや感じる	12	67	5	3	1	1	1		
1:とても感じる	15	48	12	3	3	1	2	1	1

グループ名グループ

地域連携の“クラウド上にバックアップを置くことでランサムウェアの対策を兼ねる”のであれば、魅力を感じますか？

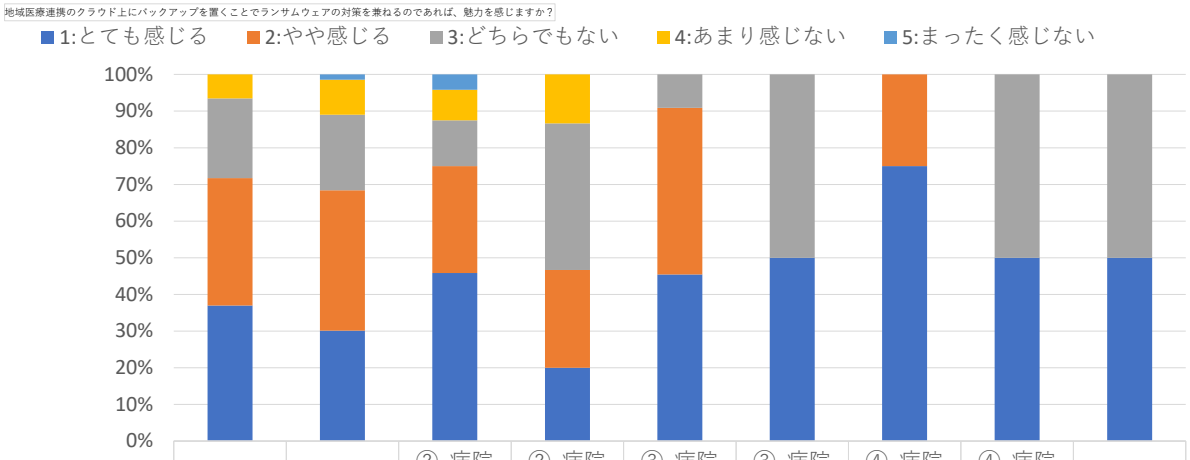
個数 / No



	クリニック ①	病院（200床未満） ②	病院（200～399床） ③	病院（400床以上） ④	介護施設 ⑤
5:まったく感じない	3	1			
4:あまり感じない	23	4			
3:どちらでもない	53	9	3	1	2
2:やや感じる	96	11	5	1	
1:とても感じる	80	14	7	4	2

医療機関の種類・規模を教えてください。2医療機関の種類・規模を教えてください。

個数 / No

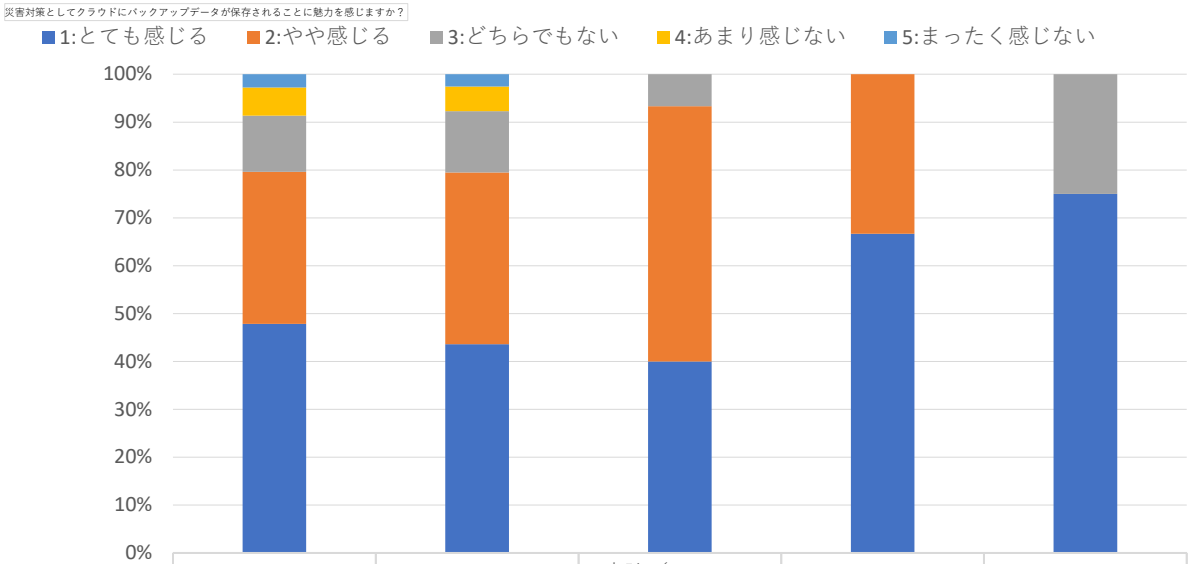


	①_クリニック ①MM_クリニック	①_クリニック ①クリニック	②_病院（200床未満） ②MM_病院（200床未満）	②_病院（200床未満） ②病院（200床未満）	③_病院（200～399床） ③MM_病院（200～399床）	③_病院（200～399床） ③病院（200～399床）	④_病院（400床以上） ④MM_病院（400床以上）	④_病院（400床以上） ④病院（400床以上）	⑤_介護施設 ⑤介護施設
5:まったく感じない		3	1						
4:あまり感じない	3	20	2	2					
3:どちらでもない	10	43	3	6	1	2		1	2
2:やや感じる	16	80	7	4	5		1		
1:とても感じる	17	63	11	3	5	2	3	1	2

グループ名 グループ

災害対策として“クラウドにバックアップデータが保存される”ことに魅力を感じますか？

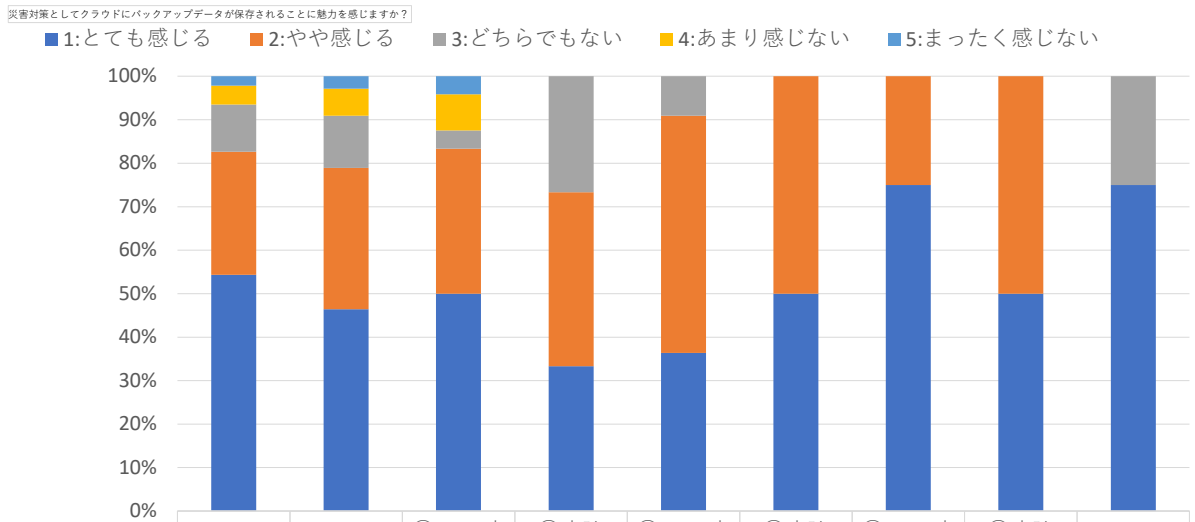
個数 / No



	クリニック ①	病院（200床未満） ②	病院（200～399床） ③	病院（400床以上） ④	介護施設 ⑤
5:まったく感じない	7	1			
4:あまり感じない	15	2			
3:どちらでもない	30	5	1		1
2:やや感じる	81	14	8	2	
1:とても感じる	122	17	6	4	3

医療機関の種類・規模を教えてください。2医療機関の種類・規模を教えてください。

個数 / No

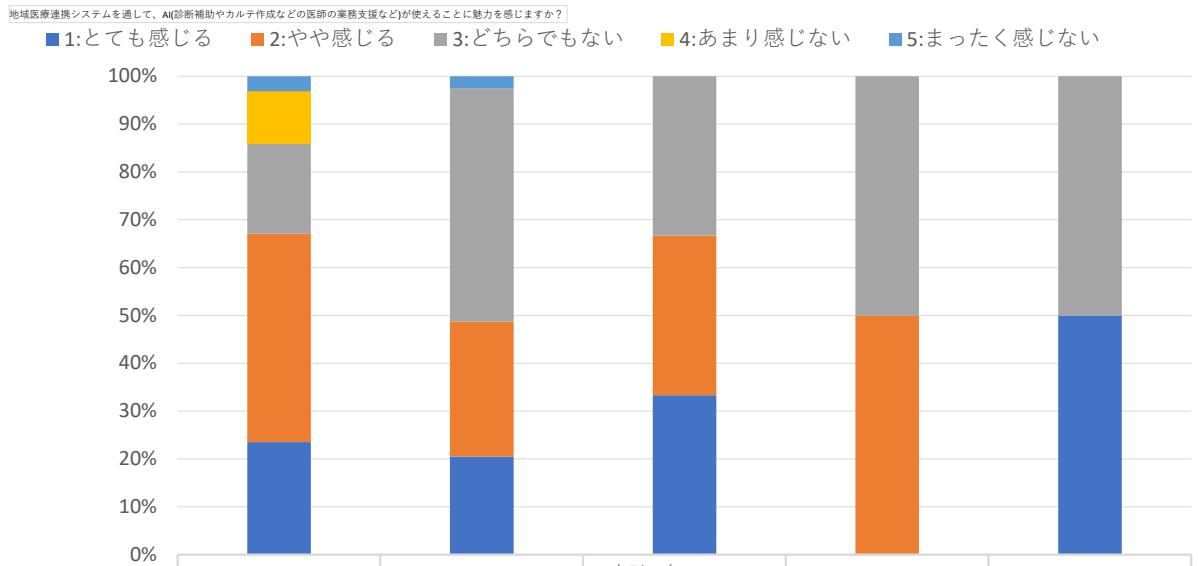


	①MM_クリニック	①クリニック	②MM_病院（200床未満）	②病院（200床未満）	③MM_病院（200～399床）	③病院（200～399床）	④MM_病院（400床以上）	④病院（400床以上）	⑤介護施設
	①_クリニック		②_病院（200床未満）		③_病院（200～399床）		④_病院（400床以上）		⑤_介護施設
5:まったく感じない	1	6	1						
4:あまり感じない	2	13	2						
3:どちらでもない	5	25	1	4	1				1
2:やや感じる	13	68	8	6	6	2	1	1	
1:とても感じる	25	97	12	5	4	2	3	1	3

グループグループ名

地域連携システムを通して、AI(診断補助やカルテ作成などの医師の業務支援など)が使えることに魅力を感じますか？

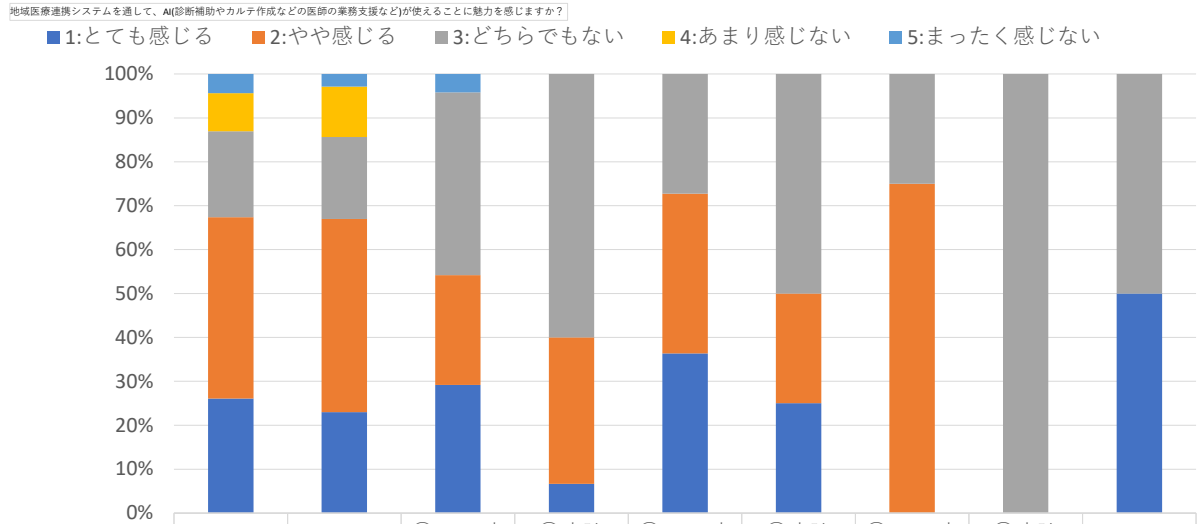
個数 / No



	クリニック ①	病院（200床未満） ②	病院（200～399床） ③	病院（400床以上） ④	介護施設 ⑤
5:まったく感じない	8	1			
4:あまり感じない	28				
3:どちらでもない	48	19	5	3	2
2:やや感じる	111	11	5	3	
1:とても感じる	60	8	5		2

医療機関の種類・規模を教えてください。2医療機関の種類・規模を教えてください。

個数 / No

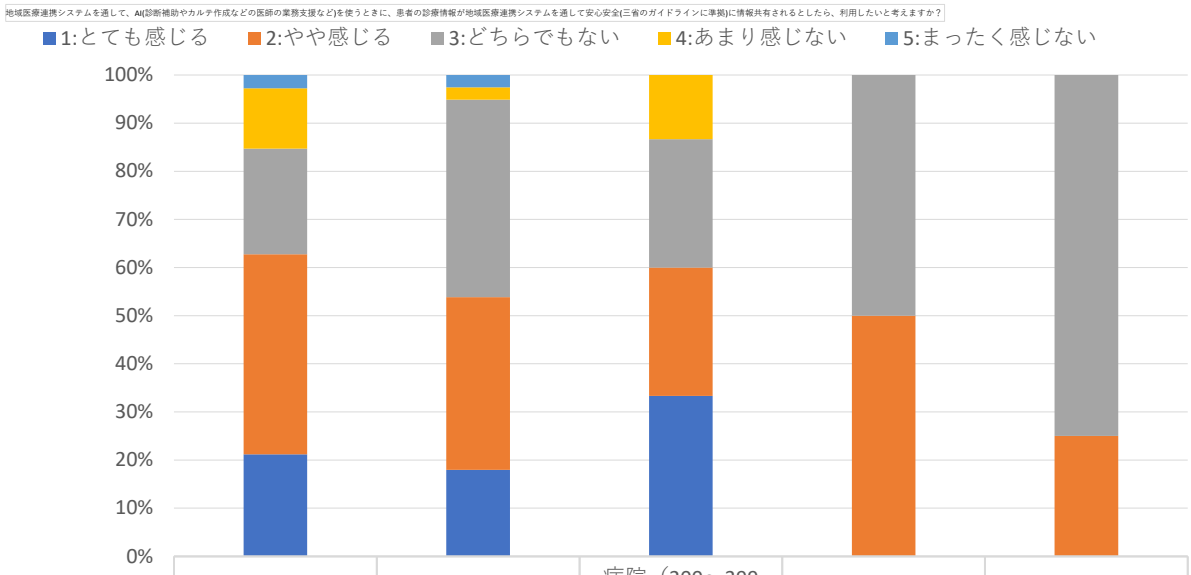


	①MM_クリニック	①クリニック	②MM_病院（200床未満）	②病院（200床未満）	③MM_病院（200～399床）	③病院（200～399床）	④MM_病院（400床以上）	④病院（400床以上）	⑤介護施設
	①_クリニック		②_病院（200床未満）		③_病院（200～399床）		④_病院（400床以上）		⑤_介護施設
5:まったく感じない	2	6	1						
4:あまり感じない	4	24							
3:どちらでもない	9	39	10	9	3	2	1	2	2
2:やや感じる	19	92	6	5	4	1	3		
1:とても感じる	12	48	7	1	4	1			2

グループグループ名

地域連携システムを通して、AI(診断補助やカルテ作成などの医師の業務支援など)を使うときに、患者の診療情報が地域連携システムを通して安心安全(三省のガイドラインに準拠)に情報共有されるとしたら、利用したいと考えますか？

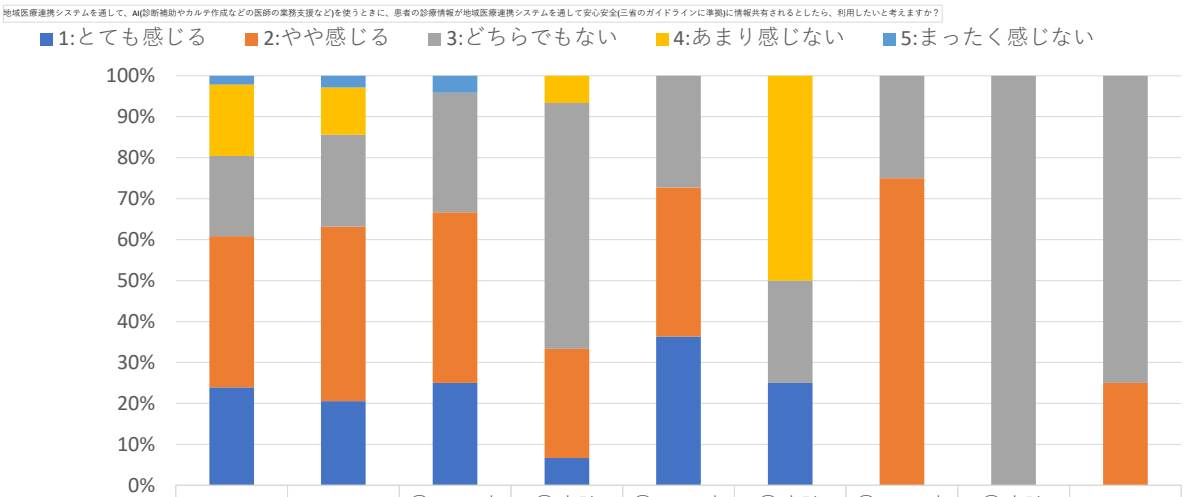
個数 / No



	クリニック ①	病院（200床未満） ②	病院（200～399床） ③	病院（400床以上） ④	介護施設 ⑤
5:まったく感じない	7	1			
4:あまり感じない	32	1	2		
3:どちらでもない	56	16	4	3	3
2:やや感じる	106	14	4	3	1
1:とても感じる	54	7	5		

医療機関の種類・規模を教えてください。2医療機関の種類・規模を教えてください。

個数 / No



	①MM_クリニック	①クリニック	②MM_病院（200床未満）	②病院（200床未満）	③MM_病院（200～399床）	③病院（200～399床）	④MM_病院（400床以上）	④病院（400床以上）	⑤介護施設
	①_クリニック		②_病院（200床未満）		③_病院（200～399床）		④_病院（400床以上）		⑤_介護施設
5:まったく感じない	1	6	1						
4:あまり感じない	8	24		1		2			
3:どちらでもない	9	47	7	9	3	1	1	2	3
2:やや感じる	17	89	10	4	4		3		1
1:とても感じる	11	43	6	1	4	1			

グループグループ名

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
BIPROGY 株式会社 パブリックサービス第三本部公共サービス部 第四室長

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 度は医療機関から外部接続するユースケースを整理した。2025 年度は 2023 年～2025 年の調査整理を行い、提言に向けて整理を行う予定である。

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。

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。

（倫理面への配慮）

本研究においては特段なし。

C. 研究結果

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。（No3 は 2025 年度に構成を継続検討中）

ユースケース1は、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。

ユースケース 2 は、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ている。2025 年度継続予定。

ユースケース3は、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・W

eb 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。

ユースケース 4 は、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。

ユースケース5は、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。

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 年度に引き続き 2024 年度も実施した。

- 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

いかにして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 を支えるかが今後の課題であり、特に医療機関及び患者にとって費用対効果がでるソリューションを普及させるかが我々にとっての重要なテーマである。

次年度は、ユースケース 2 の実証の継続並び医療機関だけではなく、保守メンテナンスを行っているベンダへのヒアリングを行い、現状のセキュリティに関する課題を抽出し、提言に取りまとめていく予定である。

F. 健康危惧情報

総括研究報告書に記載

G. 研究発表

なし

H. 知的財産権の出願

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

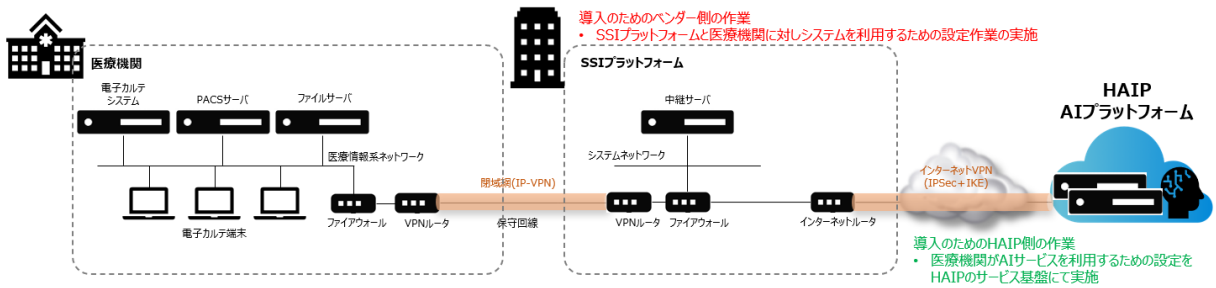


図２　ユースケース１の概要図

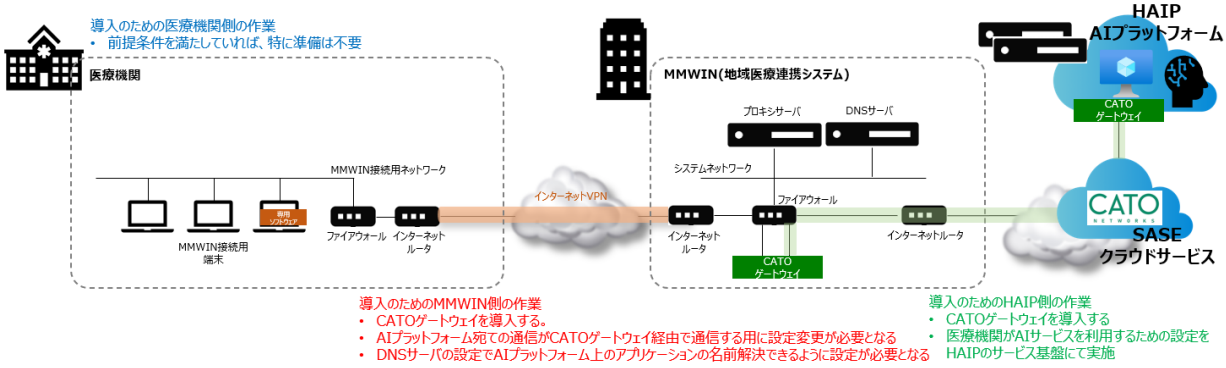


図３　ユースケース２の概要図

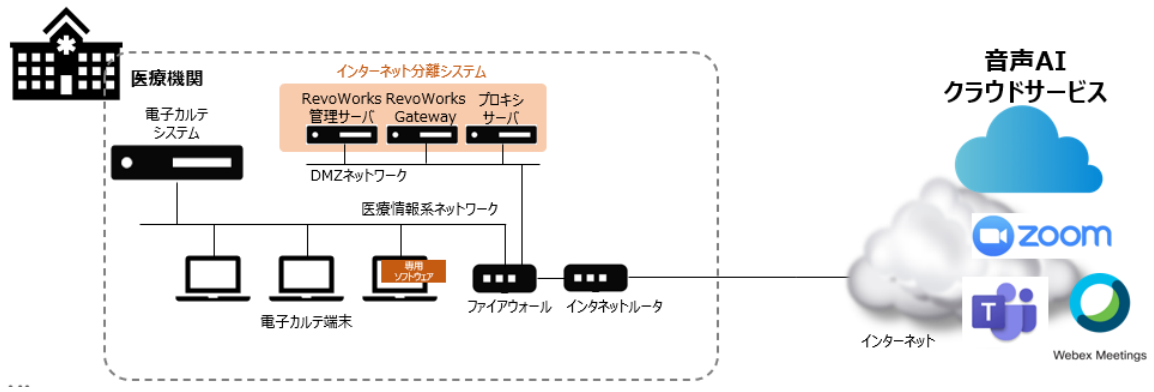


図４　ユースケース３の概要図

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

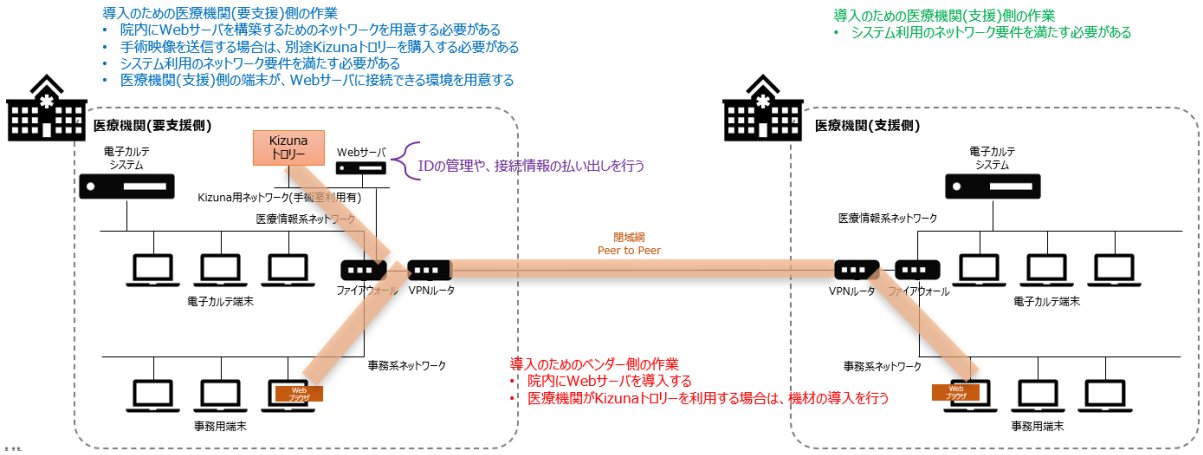


図６　KizunaWeb(ボーダレス・ビジョン社製品)

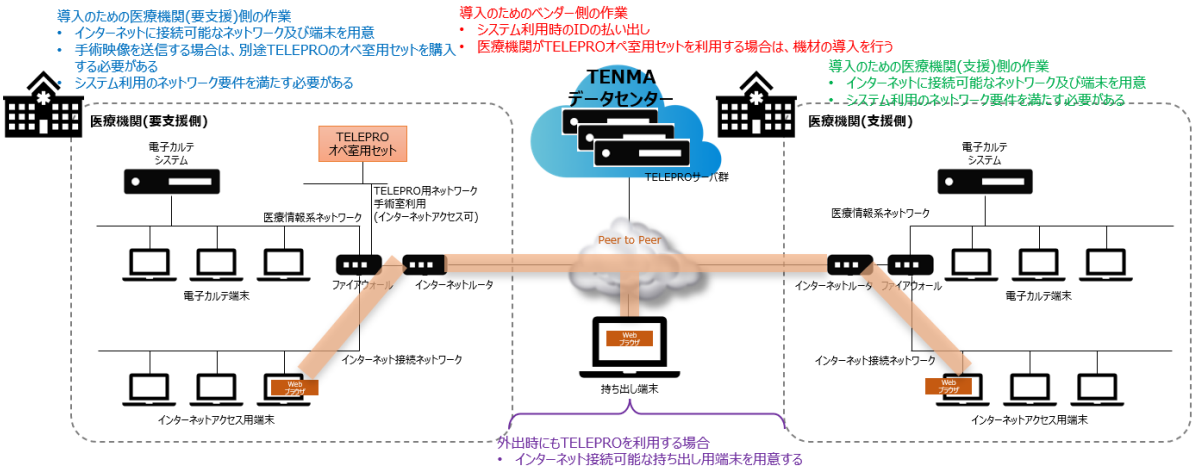


図７　TELEPRO(天馬諮問株式会社製品)

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）

R6 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　専務理事

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ていく。

本成果を基に、医療機関がリーズナブルなコストで導入しやすいクラウド上の AI サービスの実証やヒアリングを複数箇所で実施し、その結果に基づいたネットワークセキュリティ構成の提言やシステムセキュリティ監査方法の提言を行う予定である。

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。

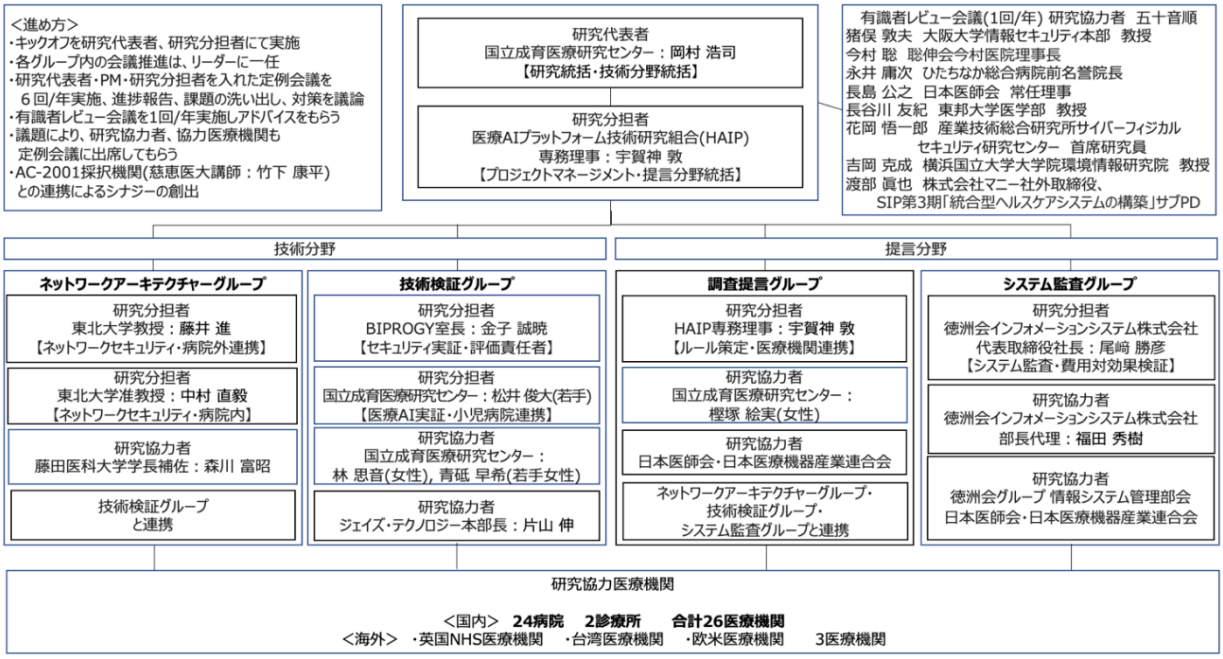
本研究は、医療機関の類型化に基づいた最適なネットワークセキュリティ構成やシステムセキュリティ監査のルールを示す事により、全国の医療機関が安全、安心かつリーズナブルな費用で医療 AI サービスが利用できることを目的とする。

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。

（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

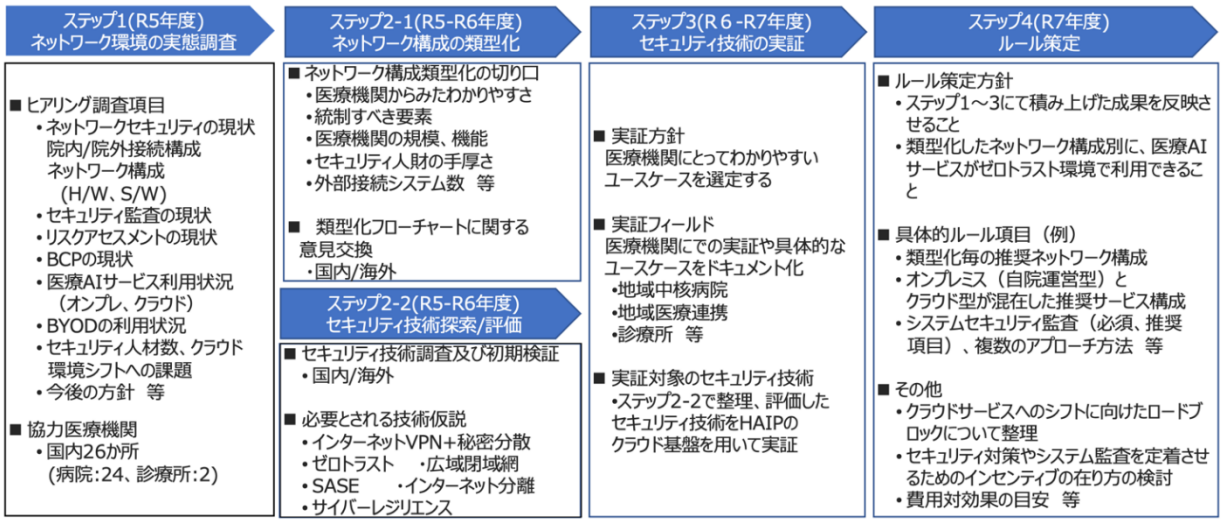
従来実施されていたアンケート調査と本研究の大きな違いは、回答数とそのアプローチ方法である。本研究では、医療機関数は 26 である。医療機関の選定は、設立母体、病床数、地域ができるだけばらつく様に考慮した上で、２４病院、２診療所の計２６医療機関を選定した（付録 1）。医療機関の実態を把握

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

目的：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行う



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。

⑤BCP

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く計画である。

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5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）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。

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いる医療機関がセキュリティ強化のサイクル（現状把握→セキュリティ対策→対策の確認→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を行う必要がある。

① 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できること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する。また、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する。これらは、厚労省医療機関向けのチェックリストを包含する様に策定を行う。

② セキュリティ対策

ネットワーク類型化のレベルに合った施策

を具体的に示す提言を行う必要がある。また、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。

③ 対策の確認

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。しかしながら、医療機関の規模や人材によっては、システムセキュリティ監査を実行することが難しい医療機関が存在する。システムセキュリティ監査の代わりに、①現状把握で述べた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。

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と、ランサムウェアによる被害の拡大もあり、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ネットワークの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。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きたい。

多忙の中、協力していただいた２８の医療機関（付録２）に深謝いたします。

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. 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

H, 知的財産権の出願

なし

資料　協力医療機関

付録１：協力医療機関の構成

協力医療機関の構成

１．ヒアリング調査（病院）　**計26医療機関**

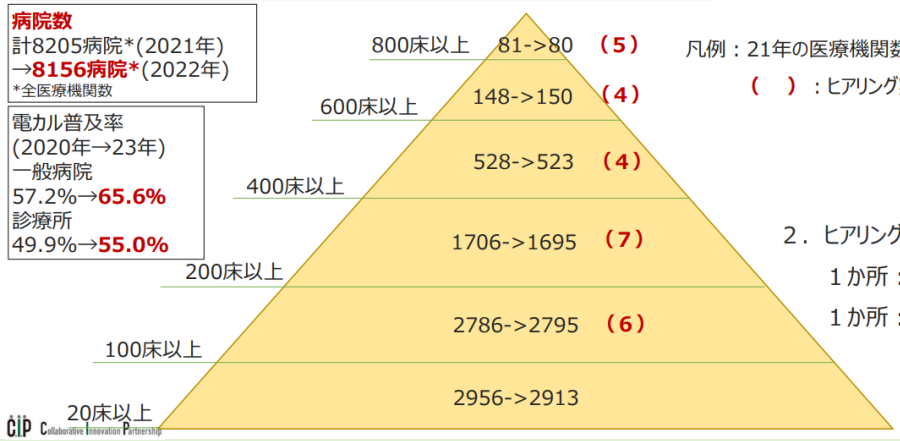
設立母体・病床数・地域を考慮し、かつ電カル導入済みの医療機関から選定を行った。

設立母体：国立大学病院、私立大学病院、NC病院、公的医療グループ、医師会病院、民間医療グループ、公立病院、民間病院、企業立病院等

所在地：宮城・茨城・埼玉・東京・神奈川・愛知・石川・福井・滋賀・京都・大阪・奈良・福岡

病院数
計8205病院*(2021年)
→**8156病院***(2022年)
*全医療機関数

電カル普及率
(2020年→23年)
一般病院
57.2%→**65.6%**
診療所
49.9%→**55.0%**



凡例：21年の医療機関数→22年の医療機関数
（　）：ヒアリング実施の医療機関数を示す

２．ヒアリング調査（診療所）　**計2診療所**
１か所：**電カルなし**、レセコン、オン資あり
１か所：**電カルあり**、レセコン、オン資あり

CIP Collaborative Innovation Partnership

1

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

CIP Collaborative Innovation Partnership

(*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

2

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（民間に運営を委託）
２１	賛育会病院	東京都墨田区	199	社会福祉法人
２２	公立刈田総合病院	宮城県白石市	199	公立（民間に運営を委託）
２３	板橋区医師会病院	東京都板橋区	192	日本医師会
２４	JR仙台病院	宮城県仙台市青葉区	164	企業立病院
２５	博愛会病院	福岡県福岡市中央区	145	民間
２６	豊橋ハートセンター	愛知県豊橋市	130	民間

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
2	斎藤医院	東京都板橋区	0	民間

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 代表取締役社長
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、一方病院を中心に医療機関の電子カルテ等はインターネットから分離し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監査（サイバーセキュリティ監査）を行ってきた。このシステム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ている。Ｒ５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、また徳洲会グループ病院の監査からフィードバックを行って監査項目や監査方法の改善を実施し、標準化に向けた土台作りを行った。続くＲ６年度においては徳洲会グループ３病院で監査を実施して前年同様に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１病院での監査を実施した。この監査では監査項目や提出資料などを大幅に見直し、また監査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第一歩を踏み出すことができたと考える。

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、一方病院を中心に医療機関の電子カルテ等はインターネットから分離し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監査（サイバーセキュリティ監査）を行ってきた。このシステム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「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「システム監査チェックシート」にもとづきＲ５年度に４病院、Ｒ６年度にも次の４病院でシステム監査を実施し、それぞれの結果をフィードバックして監査項目や監査方法の見直しを行い、次回の監査で検証とフィードバックを行う形で実施した。特にＲ７年３月に実施したＡ病院は初の徳洲会グループ外の施設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、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】

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）

C. 研究結果

ここでは主にＲ７年３月に実施した徳洲会グループ外のＡ病院での監査について、その準備と実施について記述する。

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、遵守に運用されている	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 ②は実際に使われた（記載のある）もの生データが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する。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

A病院の監査では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。

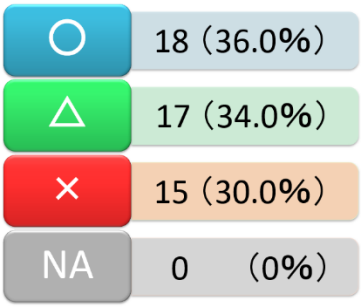
３．監査の実施と結果

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（いずれも現地監査当日の総評で病院へ報告したもの）。

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

D．考察

１．初のグループ外病院監査における考察

・監査チェックシートは大幅な修正を行ったが、なお標準化に不十分だった項目がある、また類似した内容の項目が複数あるなどさらなる検討と改善が必要。

・事前の資料準備での病院負担を軽減するため、現場の状況は写真提出ではなく当日確認としたが、現場訪問のルート設定がやや曖昧でこれを明確にすればより効率的にラウンドできたと考える。

・文書監査後にその結果を送付するだけでなく、Web 会議等で結果の説明、現地監査の段取りや準備等についてコミュニケーションを取れればお互いに理解を深め、より良い監査に繋がると考える。

２．監査結果の考察

・セキュリティに配慮された運用が見られる一方、情報漏えいやウイルス感染に繋がるセキュリティリスクが存在することも確認された。

・最も大きな課題は厚労省ガイドラインにもとづく「情報システム運用管理規程」の内容が不十分であり、診療情報の電子的な取り扱いと情報システムの運用に関する安全管理のルールが確立していない点である。

・まずは運用管理規程の整備により情報システムのセーフティ／セキュリティのルールとその責任者および運用体制を明確に定めること、次にそのルールを院内に周知し、ル

ールに沿った運用を行うことが診療情報や情報システムの安全に繋がると考える。
・大規模停電やサイバー攻撃の際の備えが十分でないことも懸念される点である。システムを停止させないこと、また停止した場合の診療継続については院内で検討の上早急な対応が必要と考える。
・ＳＥは専任１名・兼任１名、知識や経験もあり精一杯業務に取り組まれていると感じたが、いかんせん医療機関での IT 関連業務は多岐にわたり、厚労省を含め国の施策もあり増加の一途である。情報を的確につかみ対応していくこと、特に十分なセキュリティ対策を取ることは現状の体制ではかなり難しいと思われる。

E. 結論

Ｒ６年度は徳洲会グループ病院でこれまでどおりシステム監査を実施しながらその都度フィードバックとシステム監査チェックシートや監査方法の改善を行い、次の監査で試行するというサイクルで継続的なブラッシュアップを行った。Ｒ７年３月には初の徳洲会グループ以外の病院でのシステム監査を実施し、目的である監査の標準化に向けてのファーストステップを踏むことができ、またこの取り組みに関わった監査員のレベル向上にも繋がったと評価する。
システム監査は現状のセキュリティ上の問題点を洗い出すことが目的だが、この問題点を改善しなければ病院のセキュリティレベルは向上しない。しかし「改善を」「ルールの策定を」「関係書類の作成と適切な運用を」と言っても SE をはじめシステム管理体制に余力がない病院においては病院外からの支援がなければ難しいことをあらためて認識した。この支援についての方法と体制についても徳洲会グループでの改善支援活動をベースにＲ７年度の研究課題として取り組みたい。

F. 健康危惧情報

総括研究報告書に記載

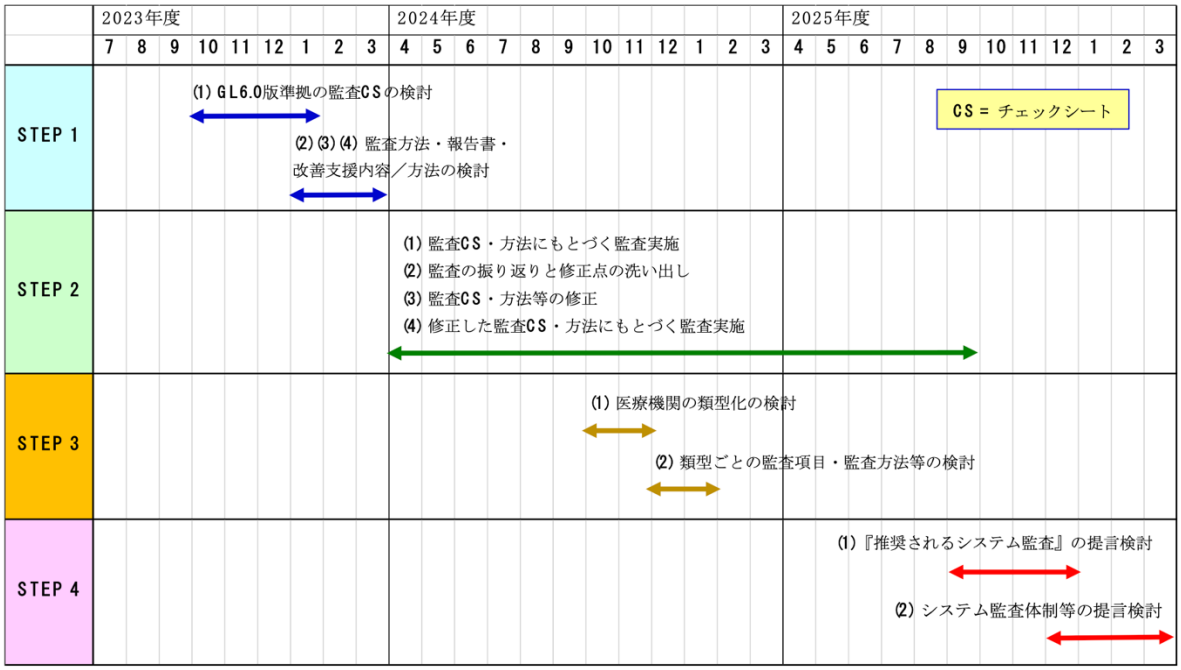
G. 研究発表

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

H. 知的財産権の出願

なし

資料　システム監査グループの全体スケジュール



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

画像認識等 AI 技術の進歩は医療分野にも大きな可能性をもたらし、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などを目指した取り組みが活発に進められている。国立成育医療研究センター(NCCHD)では、医療 AI サービスを開発、医療 AI プラットフォーム技術研究組合(HAIP)と連携し、国内多くの医療機関がクラウドから公開されるサービスを安全に使うことができる環境の整備を目指して研究を進めている。NCCHD では免疫不全患者や臓器移植後の免疫抑制剤投与患者など、感染症に対してハイリスクな患者を多数抱えており、グラム染色画像からの感染症起因菌同定支援システムの開発を進め、特許出願を行った。互いに異なる培養条件に対応する複数のモデルを構築し、判別対象菌の培養条件に応じて選択することで、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いる。また、ファブリー病のスクリーニングシステムでは、尿沈渣顕微鏡写真からマルベリー小体を自動検出する技術を実現した。早期発見により適切な治療が可能となるため、学校検尿との連携による効率的なスクリーニング実現を目指している。これらのサービスはコンテナ化しているが、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、サーバレスアーキテクチャへの移行を進めている。この過程で、電子カルテ端末からの安全な利用を実現するため、ゼロトラストセキュリティモデルの実装についての検討も行った。サーバレスアーキテクチャは、その特性上、従来のネットワーク境界に依存したセキュリティ対策ではなく、アイデンティティベースのアクセス制御を前提としており、ゼロトラストの実装に適している。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た。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いて、プロバイダ間でのサービス機能の対応関係を体系的に整理し、要求に応じた最適なサービス選定の指針を提供した。本研究を通じて、医療 AI サービスの実用化に向けた技術的課題の解決とともに、セキュリティ面での実証を重ねることで、患者および市民の参画を促し、さらなる医療技術の発展につなげることを目指している。特に、電子カルテネットワークからの安全なアクセスの実現は今後の重要な課題であり、セキュリティ対策の実績を積みながら、管理者や患者、市民に対する分かりやすい説明を継続的に行っていく必要がある。

A. 研究目的

ディープラーニングによる画像認識の飛躍的な精度向上はその後の社会を大きく変えることとなった。皮膚がんの診断など医療における AI の有用性が示されて以来、医療の質や効率の向上、地域格差の解消、医療従事者の負担軽減などを目指した医療 AI の研究開発が盛んに進められている。自動車の自動運転や、世界最強棋士を破った囲碁プログラムで注目を浴びた強化学習についても、個別医療の最適化、手術に使われる医療ロボットの制御など、さまざまな活用が考えられている。これらの技術はハードウェアとソフトウェアの技術開発をも促進してきた。その結果、さまざまな実行環境がクラウドとオンプレミスで構築された複雑なシステムの上に組み合わされている状況を作り出し、一方で個人情報保護や患者不利益等への配慮が求められる時代背景にあって、ランサムウェアをはじめとするサイバー攻撃の危険性がますます高まっている。

我が国では内閣府が主導する戦略的イノベーション創造プログラムにより AI ホスピタルの取り組みが 2018 年から始まり、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)とともに採択され、医療データを共有し、一体となって AI 開発を進めてきた。国内多くの医療機関が、このようなサービスを、安全に、安価に利用できる環境を提供することを目的に、共同で調査等も行っている。いずれ、カルテ端末、さらには患者を含めた一般市民の端末からも利用されることを目指すには、どのような対策が必要かを考る必要がある。

現在、HAIP サービス事業基盤において、感染症起因菌同定支援、腎細胞がん病理画像のグレーディング支援、ファイブリー病スクリーニングの 3 つの医療 AI サービスがコンテナとして実装されており、公開範囲は限定されているものの、利用できる状況にある。ここでは、感染症起因菌同定支援、ファイブリー病スクリーニングについて報告する。また、近年の生成 AI の医療への活用は無視できるものではなく、NCCHD では医療的ケア児の支援体制、遺伝カウンセリング支援について開発を進めており、以下では後者について現状を報告する。

これらのサービスは Linux サーバにおいてウェブアプリケーションとして開発され、開発効率の向上、運用コストの削減、運用管理の簡素化、柔軟性の向上などを目的としてコンテナ化を行い、さらに、医療データを扱うという観点からセキュリティを強化するためにデスクトップ仮想化(VDI)を行ってクラウドから公開されている。現在、それぞれに対し、サーバレス環境への移行を進めており、その際にゼロトラストセキュリティモデルを実装し、電子カルテ端末からの利用、また一般ユーザからの安全な利用と普及を目指している。現在の AI 技術は教師あり学習に基づいており、実用化においては質と量の両方を伴ったビッグデータの収集が不可欠である。個人情報保護の観点からの制約により、思うように研究開発が進んでいない面もあるが、安全なシステムの実証により患者および市民の参画(PPI)を促し、さらなる医療技術の発展へと繋げることができると考えている。

B. 研究方法

顕微鏡画像からの教師データ作成には 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 Python スクリプトで行った。

感染症起因菌同定支援では、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、Amazon EC2 のインスタンスタイプ g4dn.xlarge を利用した。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 ラボ基盤、および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。

C. 研究結果

小児科として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ているなど、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。そこで菌血症患者の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

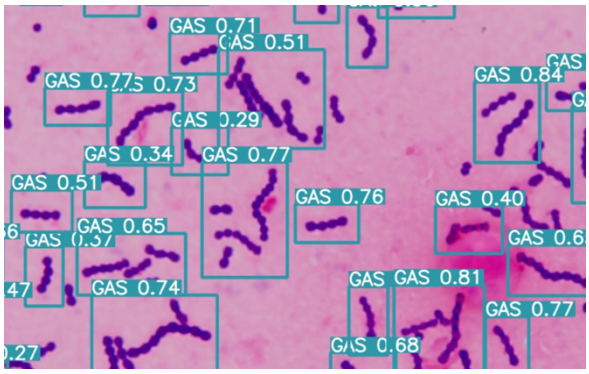


図 1 人食いバクテリア、化膿レンサ球菌の検出

に対してアノテーションを行い、グラム陽性桿菌、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。内訳は、腸内細菌科、緑膿菌、エンテロコッカス属、コアグラーゼ陰性ブドウ球菌、バシラス属、黄色ブドウ球菌、B 群 β 溶血性レンサ球菌、レンサ球菌属、ヘモフィルス属、肺炎レンサ球菌、化膿レンサ球菌、リステリア、シュードモナス属、コリネバクテリウム、グラム陰性球菌、カンジダであり、これらに赤血球を加えた 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)。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。

図 2 VDI でクラウドのウェブカメラを利用

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いるので、患者や家族にとっては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、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。わずか 240 枚の写真しかないが、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り、ブラウザから利用できるようにした(図 3)。

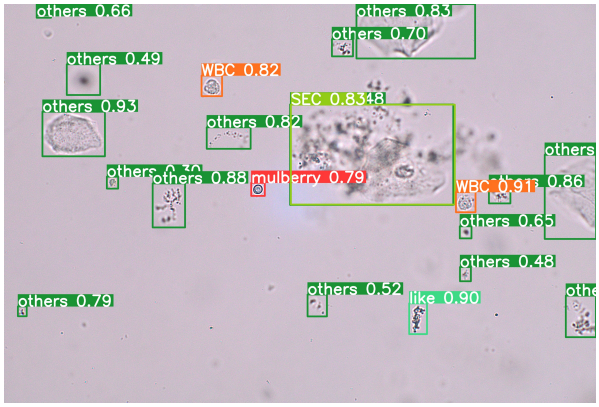


図 3 尿沈渣顕微鏡写真からのマルベリー小体検出

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。2024 年 6 月末、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

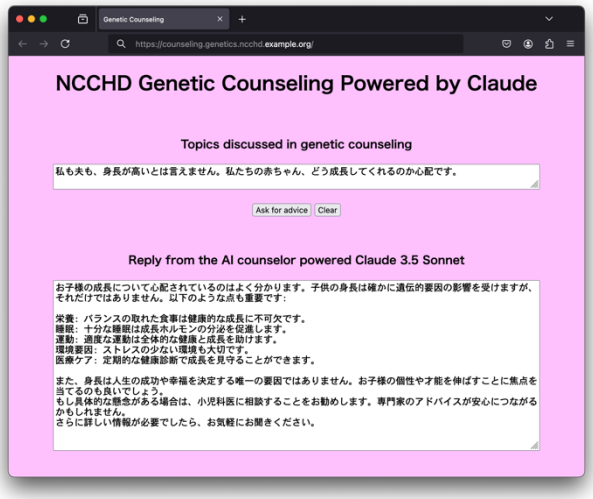


図 4 遺伝カウンセリングを生成 AI で代替

いるが(図 4)、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。

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 5)。

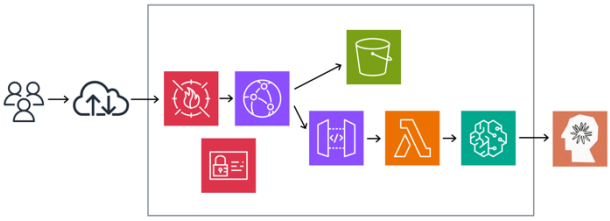


図 5 サーバレスのビルディングブロック例

最後に、医療機関のクラウド移行におけるセキュリティサービス選定を支援するため、主要クラウドプロバイダのセキュリティサービス群に関する比較調査研究を実施した。各社が提供する有償・無償セキュリティサービスについて、サービス名称の相違による選定困難性の課題に着目し、機能要件に基づく対応関係の分析を行った(資料)。調査により、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いて、プロバイダ間でのサービス機能対応を体系化し、組織のセキュリティ要求に応じた最適なクラウドセキュリティサービス選定のための実践的指針を提供した。

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持たせ、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(図 5)、仮想マシンが不要となる。クラウド上でサーバが不要になるわけではなく、ユーザが用意する仮想マシンが不要になることがサーバレスである。

プロバイダ側の利点は、そのままユーザ側の利点ともなる。セキュリティの観点では、攻撃範囲の限定、範囲が狭いことによる迅速な脆弱性対応、動的な実行環境による攻撃対象からの回避、細粒度必要最小限の権限付与によるリスクの低減、ブロックに特化した対策に集中、監視ログの細分化による問題特定の容易化、そしてセキュリティ技術の入れ替えも細分化されていればその一つ一つは決して困難ではない。このような状況では、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、マイクロサービスアーキテクチャの欠点のようにも見えてしまうが、アイデンティティによるアクセス制御、つまり ID ベースのアクセス制御が必要になる。これは、ゼロトラストと盛んに言われる以前から、クラウドプロバイダ側には当然の対策であった。イベント駆動型のサーバレスコンピューティングサービスの中で最も歴

史が長く、機能も充実していると思われる AWS Lambda では、SigV4 というリクエスト署名によるクライアント認証により、実行権限のある正当なユーザから出された改竄されていないリクエスであることが確認される。ユーザー管理、グループ管理、ロールベースのアクセス制御、ポリシー管理は AWS IAM によって行われ、Microsoft Azure や Google Cloud では、それぞれ、Microsoft Entra ID、Google Cloud IAM が対応する。そしてサーバレス環境では、データの保存や転送時の暗号化が標準的に行われている。サーバレスを採用することでそのままゼロトラストセキュリティモデルを実現することができるわけではないが、見通し良くある程度のセキュリティを確保できそうである。

このような状況でも、実際の電子カルテネットワークから医療 AI サービスへのアクセスは許されておらず、現状インターネット側に出て行けるのは、NTP サーバとの同期、MDM サーバの認証のみとのことで、逆向きに、サービス側からのアクセスは言うまでもなく許されていない。

E. 結論

開発を行った医療 AI サービスに対し、運用コストの面からサーバレスへの移行を進めているが、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持っており、掴みどころがないように思われたゼロトラスに対する理解を深めることができた。一方、ゼロトラストを謳う統合的なサービスの仕様を眺めると、やはり複雑で分かりにくく、必要性が不明な高機能、それに付随する高価格を目にすれば、気安く導入できるようなものではない。実際、目標とする電子カルテからのアクセスは実現できておらず、ゼロトラストの言葉をもって管理者、患者や市民に安心を与えられるわけではない。ゼロトラストセキュリティは開発者側を鼓舞する上で便利な言葉ではあるものの、ユーザ側を納得させ、医療 AI サービスのより広範な活用を図るためには、セキュリティ対策の実績を積むとともに、分かりやすい説明を続けるという地道な作業が必要であるように思われる。

F. 健康危惧情報

総括研究報告書に記載

G. 研究発表

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

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*, 2024, **52**, 19

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　クラウドプロバイダのセキュリティサービスの比較

ユースケース	A社	費用	O社	費用
ID とサービスおよびリソースへのアクセスを安全に管理	AWS Identity and Access Management (IAM)	無償	IAM Identity Domains	無償/有償
複数のアカウントやアプリケーションへのワークフォースのアクセスを一元管理	AWS IAM アイデンティティセンター (SSO の後	無償	IAM Identity Domains	無償/有償
安全でフリクションレスなカスタマー ID およびアクセス管理の実装と拡張	Amazon Cognito	有償	IAM Identity Domains	無償/有償
カスタムアプリケーション内できめ細かい権限と承認を管理	Amazon Verified Permissions (プレビュー)	有償	IAM Identity Domains	無償/有償
フルマネージドのマイクロソフトアクティブディレクトリサービスで効率化	AWS Directory Service	有償	-	-
複数のアカウント間でリソースを簡単かつ安全に共有	AWS Resource Access Manager	無償	OCI（built-in）	-
リソースをスケーリングする際に、環境を一元管理	AWS Organizations	無償	OCI（built-in）	-
セキュリティチェックの自動化とセキュリティアラートの一元化	AWS Security Hub	有償	Cloud Guard	無償
インテリジェントな脅威検出でアカウントを保護	Amazon GuardDuty	有償	Cloud Guard /Threat Intelligence	無償
大規模な自動化された継続的な脆弱性管理	Amazon Inspector	有償	Vulnerability Scanning	無償
数ステップでセキュリティデータを自動的に一元化	Amazon Security Lake	有償	Observability & Management Logging/Logging Analytics	有償
リソースの設定を評価、監査、評価する	AWS Config	有償	Cloud Guard	無償
オンプレミスおよびクラウド上のリソースとアプリケーションを観察および監視	Amazon CloudWatch	無償/有償	Observability & Management	有償
ユーザーアクティビティと API 使用状況の追跡	AWS CloudTrail	無償/有償	Cloud Guard /Threat Intelligence	無償
			Observability & Management Logging/Logging Analytics	有償
IoT デバイスとフリート全体のセキュリティ管理	AWS IoT Device Defender	有償	-	-
アカウント全体のファイアウォールルールを一元的に構成および管理	AWS Firewall Manager	有償	VCN, Security List, etc	無償
VPC 全体に Network Firewall セキュリティをデプロイ	AWS Network Firewall	有償	Network Firewall	有償
マネージド DDoS 保護でアプリケーションの可用性と応答性を最大化	AWS Shield	無償/有償	OCI（built-in） Layer3,4	
VPN なしで企業アプリケーションに安全にアクセス	AWS Verified Access	有償	IAM Identity Domains	無償/有償
一般的な攻撃からウェブアプリケーションを保護	AWS Web Application Firewall (WAF)	有償	Web Application Firewall	有償
VPC のアウトバウンド DNS トラフィックのフィルターと制御	Amazon Route 53 Resolver DNS Firewall	有償	-	-
大規模な機密データを検出して保護する	Amazon Macie	有償	Data Safe	無償
データを暗号化またはデジタル署名するためのキーを作成および管理	AWS Key Management Service (AWS KMS)	有償	Vault	無償/有償
シングルテナントのハードウェアセキュリティモジュール (HSM) の管理	AWS CloudHSM	有償	Vault	無償/有償
サービスと接続されたリソースを使用した SSL/TLS 証明書のプロビジョニングと管理	AWS Certificate Manager	無償	Certificates	無償
リソースを識別してデータを保護するためのプライベート証明書を作成	AWS Private Certificate Authority	有償	Certificates	無償
シークレットのライフサイクルを一元的に管理	AWS Secrets Manager	有償	Vault	無償/有償
セキュリティデータを分析および視覚化して、潜在的なセキュリティ問題を調査	Amazon Detective	有償	Cloud Guard	無償
			Logging Analytics（OCI Auditログ, VCN Flowログ）	有償
スケーラブルでコスト効率性に優れたアプリケーションの復旧	AWS Elastic Disaster Recovery	有償	OCI（built-in）	-
コンプライアンスレポートにオンデマンドでアクセスできるセルフサービスポータル	AWS Artifact	-	Oracle Cloud Compliance	-
使用状況を継続的に監査して、リスクとコンプライアンスの評価を簡素化	AWS Audit Manager	有償	Cloud Guard	無償

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)

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**, 3, 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. 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**, 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)

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)

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. *月刊インナービジョン* **37**, 第 7 号, 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, 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)

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.* [doi: 10.1002/bcp.70026], 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)

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）

令和 7 年 5 月 21 日

厚生労働大臣 殿

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 6 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 利用推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 （23A1001）

３．研究者名 （所属部署・職名） システム発生・再生医学研究部 ・ 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）	□	☑	□		□
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 7 年 5 月 28 日

厚生労働大臣 殿

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 八田 泰秀

次の職員の令和 6 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 利用推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　（23A1001）

３．研究者名　（所属部署・職名）　理事会 ・ 専務理事

（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）	□ ☑	□		□
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７年５月９日

厚生労働大臣　殿

機関名　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６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 7 年 5 月 28 日

厚生労働大臣 殿

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 八田 泰秀

次の職員の令和 6 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 利用推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　（23A1001）

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）	□ ☑	□		□
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 7 年 5 月 21 日

厚生労働大臣 殿

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 尾﨑 勝彦

次の職員の令和 6 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 利用推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　（23A1001）

３．研究者名　（所属部署・職名）　役員 ・ 代表取締役社長

（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）	□	☑	□		□
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 7 年 5 月 21 日

厚生労働大臣 殿

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 6 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 利用推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 （23A1001）

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）	□	☑	□		□
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７年３月７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６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。