別紙 3

厚生労働科学研究費補助金
政策科学総合研究事業 (臨床研究等 ICT 基盤構築・人工知能実装研究事業)

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

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

研究要旨

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

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

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

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

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

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

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

A. 研究目的

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

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

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

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

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

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

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

B. 研究方法

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

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

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

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

とが示された。

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

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

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

C. 研究結果

1. ネットワークアーキテクチャーの再検討

■サイバーセキュリティは「診療継続性」の問題

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

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

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

2. 最近の被害事例からみた課題

■アサヒグループ事例：対策していても突破され、事業が止まる

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

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

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

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

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

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

■医療機関の被害事例：病院規模に関係なく診療が止まる

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

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

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

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

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

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

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

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

3. 攻撃の見取り図

■ランサムウェアは「突然暗号化するウイルス」ではない

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

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

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

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

■攻撃経路の類型

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

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

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

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

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

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

4.　情報部門の優先順位の再定義

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

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

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

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

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

5. 早期発見手段としての Decoy

■EDR、NDR、Decoy の比較

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

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

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

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

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

■Decoy を地域で共同利用する合理性

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

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

図 1　地域医療ネットワークシステムの見張り番を参照

図 2　decoy の配置図を参照

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

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

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

6. 仮想ブラウザによるクラウド型 AI 利用環境

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

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

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

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

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

7. IT-BCP の本質

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

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

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

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

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

8. 前年度アンケート結果との接続

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

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

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

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

9. 地域医療連携ネットワークの新たな価値

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

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

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

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

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

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

図 3　教育だけでは解決しないを参照

10. 政策提言としての位置づけ

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

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

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

11. まとめ

本年度の研究により、以下の点が明らかとなった。

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

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

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

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

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

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

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

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

D. 健康危惧情報

代表者報告書で適時記載

E. 研究発表

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

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

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

F. 知的財産権の出願

- なし

資料　大学病院を核とした地域医療ネットワークの高度化と安全な運用

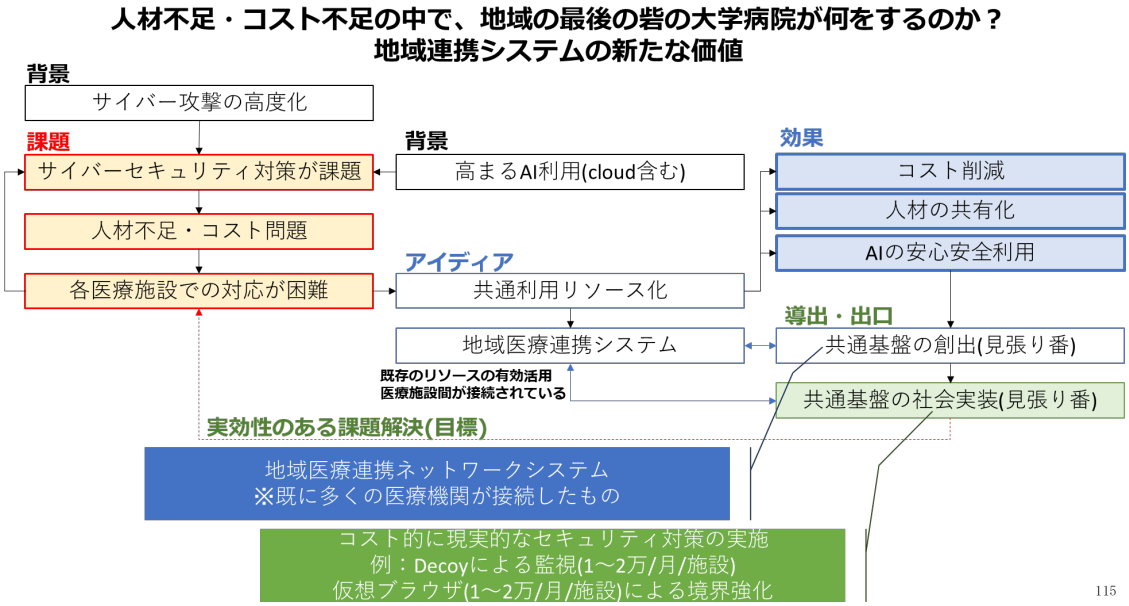

図１　地域医療ネットワークシステムの見張り番を参照

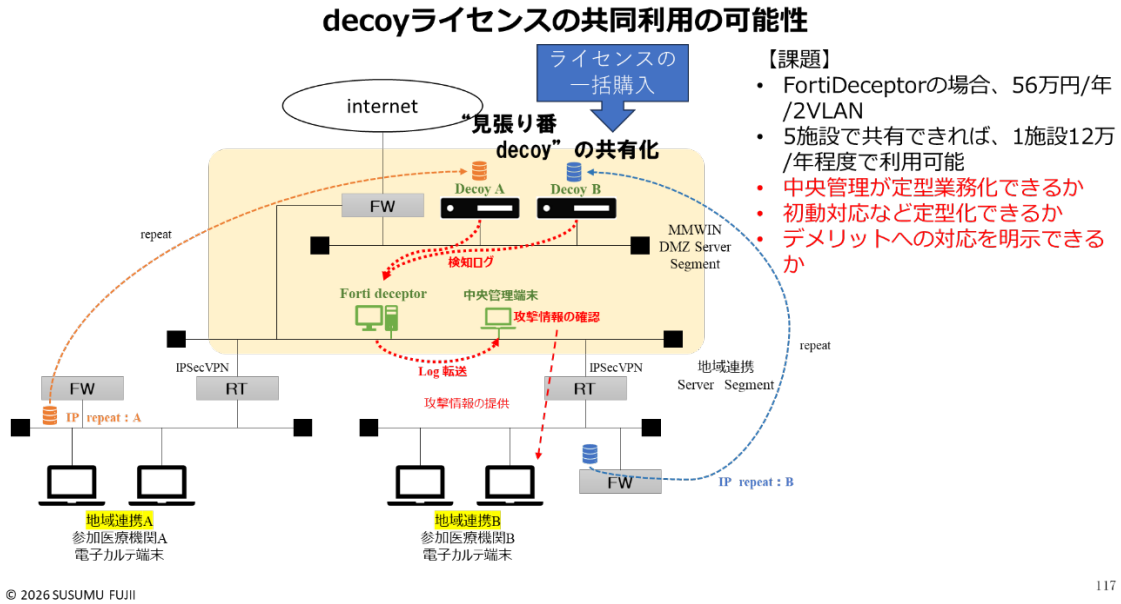

図２　decoy の配置図を参照

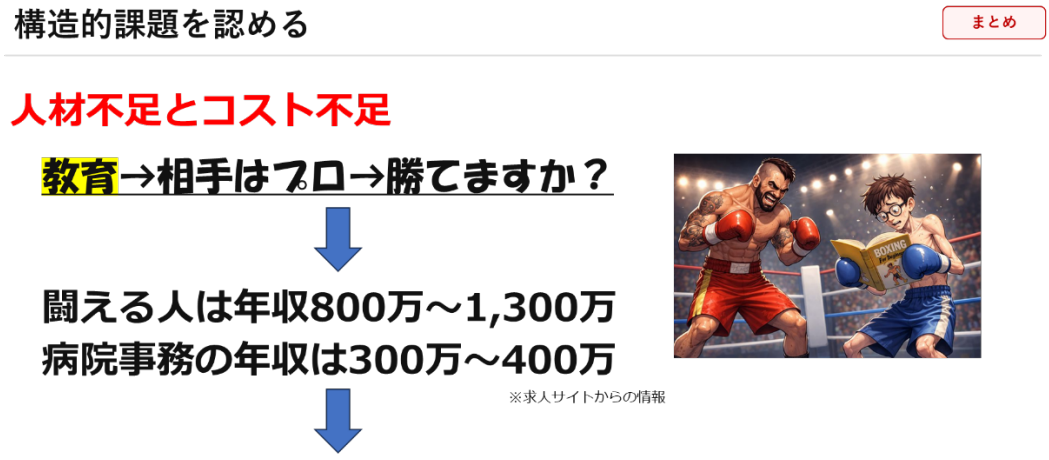

図３　教育だけでは解決しないを参照