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5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 (2024) 年 1 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

医療従事者の働き方改革や医療の均霑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 医療機関に対して実態調査を行った。対面のヒアリング実施前に、事前アンケート調査票を送付し、その回答を入手した後にヒアリングを実施することにより、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の上、効率的に確認すべき内容を明確にすることができた。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、医療機関のシステム構成を技術面から 3 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。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になった。技術面では、医療機関とクラウドシステムを安全・安心に接続するための必要とされる 4 種類のセキュリティ領域について、技術調査と整理を行った。システムセキュリティ監査については、2023 年 5 月に発行された 3 省 2 ガイドライン 6.0 版の内容をセキュリティチェックリストへ反映、システム監査の実施方法の検討や報告書内容の検討を行った。本研究チームは、実際の医療データを用いて独自の医療 AI サービスの開発も行なっており、コンテナ化、および仮想デスクトップ基盤を利用して、医療 AI プラットフォームへの実装まで行うことができた。これまでの電子カルテネットワークは境界型防御によりセキュリティ対策が取られてきたが、ランサムウェアをはじめとしたさまざまな攻撃事例を目の当たりにし、ゼロトラスト・セキュリティモデルの実装が求められつつある。仮想デスクトップ基盤に加え、ゼロトラストの一ソリューションである SASE、セキュアブラウザを利用するインターネット分離も導入し、電子カルテ端末から安全に、そして安心して医療 AI サービスを利用できるための環境整備、その検証を進めている。

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・再生医学研究部・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

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、個人情報保護への配慮が求められる現在、ランサムウェアをはじめとしたサイバー攻撃の危険性が高まっている。

国立成育医療研究センター(NCCHD)は、AI ホスピタルの中で 30 以上の医療 AI サービス開発を本研究代表者が中心となって進め、それらの有用性を複数の小児医療機関で実証し、医療 AI サービス利用上の課題等を先行して把握してきた。一方、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。クラウド上の AI プラットフォームの実証を NCCHD の医療データを用いて、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った。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

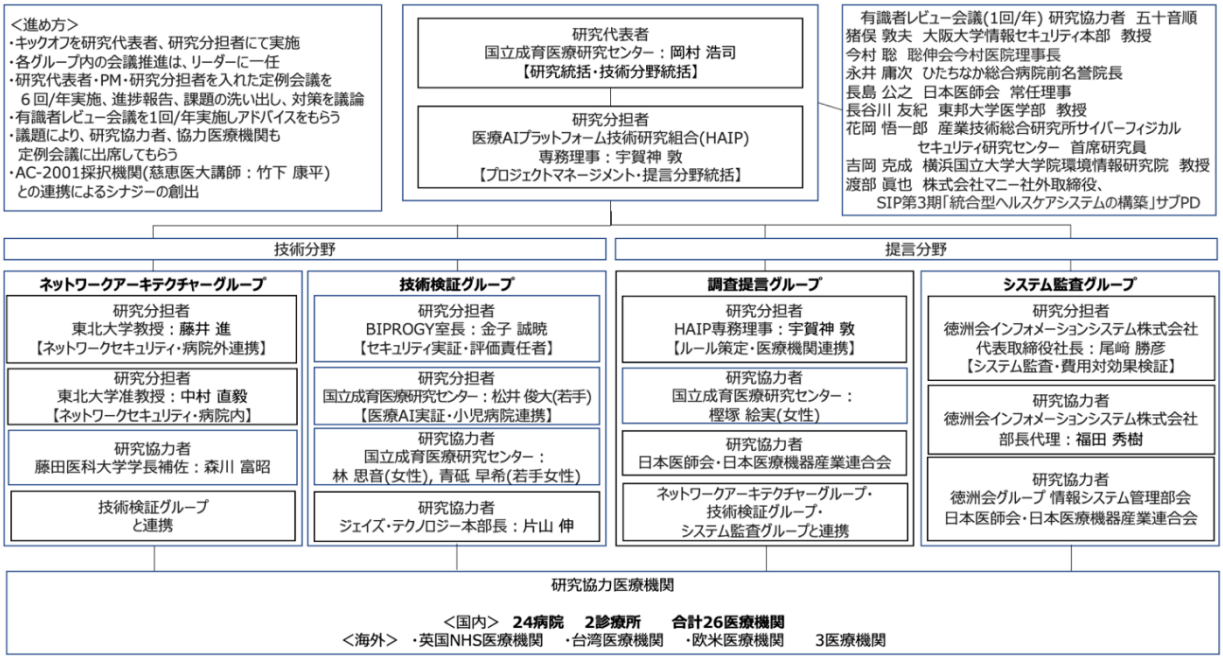
国内 24 の医療機関に対し、アンケートによる事前調査を行なった上で、対面によるネットワークセキュリティのヒアリングを実施する。そこで得られた規模に応じた機能、セキュリティ人材の有無、外部接続システム数などに関する情報を基にネットワーク構成の類型化を行い、クラウドシフトを加速するための課題を明らかにする。

システムセキュリティ監査に関しては、更新されたガイドラインをチェックリストに反映させ、実際に医療機関を訪問して監査を行う。初年度は徳洲会グループの病院を対象とする。

NCCHD から得られた実際の医療データを用いて医療 AI サービスのウェブサービスとしての開発を行う。ゼロトラスト・セキュリティモデルに沿う環境を整えるために、仮想デスクトップ基盤、SASE、インターネット分離を導入し、検討を行う。

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

付録に添付した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。その際、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。

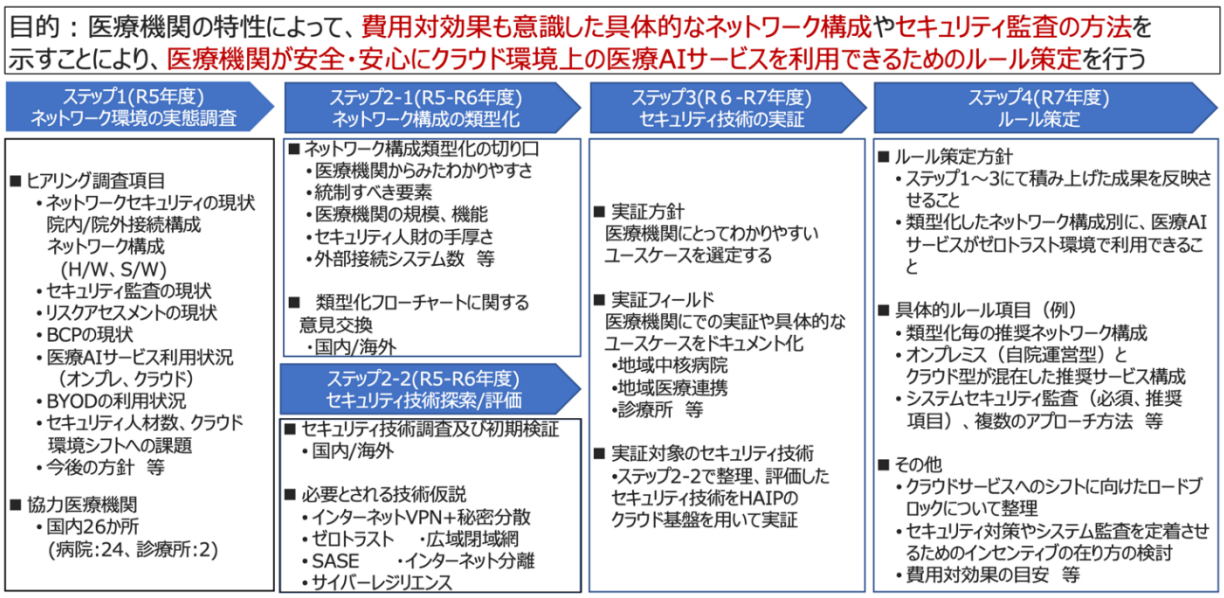
（2） 医療機関の選定及び調整

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（計画時は 20）であるが、医療機関の実態を把握するために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）。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ことになり、またタイトなスケジュールの中で日程調整に応じて頂いた。ご協力頂いた医療機関の皆様に感謝申し上げると共に、皆様非常に協力的であり、かつセキュリティは専門性が高く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

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。

（5）セキュリティ製品調査・検証

まずは、医療機関のネットワーク構成汎化モデルを作成した。その上で、セキュリティ製品調査領域を 4 種類に分類し、Web 調査を行った。製品選定基準は、Gartner, Inc.社(米国)のマジッククアドラント、カスタマレビューなどを参考に選定した。Gartner 社は世界的な IT 市場の調査分析を行っている企業である。製品ジャンルの定義、製品シェア、技術トレンドなどの情報を数多く提供している。製品ジャンルの定義は、Gartner 社が発信した情報がデファクトスタンダードになるケースも多い。本研究では、Gartner 社が公開しているマジッククアドラントに選定されている製品の中からレビュー数が多く、日本でもある程度の知名度があるものを選定し、机上評価を行った。

（6）システムセキュリティ監査

徳洲会グループ病院のシステム監査で使用している監査チェックシートの内容に医療情報システムの安全管理に関するガイドラ

イン 6.0 版の改定ポイントを全て確認した上で、特に重要な項目をシステム監査チェックシート項目として採用した。採用した項目は以下の 2 項目である。①災害、サイバー攻撃、システム障害等の非常時における対応や対策②ネットワーク境界防御型思考／ゼロトラストネットワーク型思考

さらに、厚労省から発行された医療機関におけるセキュリティ対策チェックリストをシステム監査でも有効活用するために、『【厚労省 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】は医療機関確認用と事業者確認用が作成、保管されている』という項目を追加した。今後は、ブラッシュアップしたシステムセキュリティチェックリストを徳洲会グループ病院だけではなく、他の医療機関へ適用し、さらに使いやすいチェックリストにしていく計画である。

（7）ゼロトラスト・セキュリティモデル

クラウド環境のネットワークアクセスの安全性を確保するため、仮装デスクトップ基盤に加え、ゼロトラストの一ソリューションである SASE の検証を医療機関と行う事とした。検証を行う製品の選定は、前述したセキュリティ製品の調査に基づいて行った。実際には Cato Networks 社がサービスを展開している Cato SASE クラウドプラットフォーム(CATO)の調達を行い、利用できる環境が整った。またセキュアブラウザを利用するインターネット分離については、ジェイズ・コミュニケーション社の RevoWorks を調達し、セキュリティ対策の選択肢を増やした。このような状況で NCCHD の電子カルテネットワークでの試用、電子カルテネットワークへのリモートアクセス案(資料)を打診したが、残念ながら一時的な利用であっても現状において許可は得られていない。

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。更新された医療情報システムの安全管理に関するガイドラインを反映させることはもちろんのこと、実態を踏まえた手順の作成により、システムセキュリティ監査の実施が、医療機関側にとっても、実施側にとっても容易になると期待される。今回明確になったセキュリティ人材の不足は早急に解決すべき問題であり、地域医療連携によるセキュリティ対策を効率的に行うアプローチなどを提言する必要があると考えている。

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・セキュリティモデルの導入が叫ばれている。しかしながら、これまで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を変えることは、技術に対する理解不足、コスト、管理者の責任問題から容易でない状況が明らかとなった。最新技術の検証、実証、実装を着実に進め、調査に協力していただける医療機関を見つけ、社会全体にアピールして行く必要がある。

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。個人情報保護とセキュリティへの懸念から思うように研究開発が進んでいない面もあるが、本提案による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。

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。さらに、医療機関のシステム構成を技術面から 3 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。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た。また、実際の医療データを用いて独自の医療 AI サービスの開発を行ない、さらにコンテナ化によりウェブアプリケーションとして医療 AI プラットフォームへの実装を行った。仮想デスクトップ基盤に加え、SASE、インターネット分離といったゼロトラスト・セキュリティモデルに沿う最新技術も導入し、電子カルテ端末から安全に、そして安心して医療 AI サービスを利用できるための環境整備、その検証を進めているが、境界型防御によりセキュリティ対策が取られてきた電子カルテネットワークへの導入は単純に進められるものではなく、次年度以降への大きな課題となっている。

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

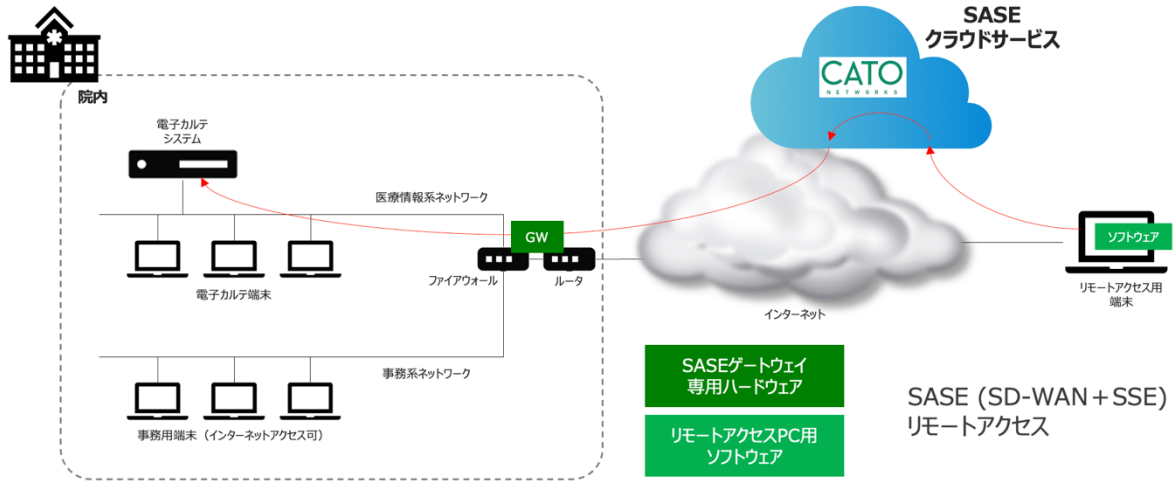
4. 藤井 進, 野中 小百合, 中村 直毅. 地域医療連携ネットワークシステムを活用したゼロトラストのニーズ調査. *医療情報学*, 2024, **44(Suppl.)**, 368-370

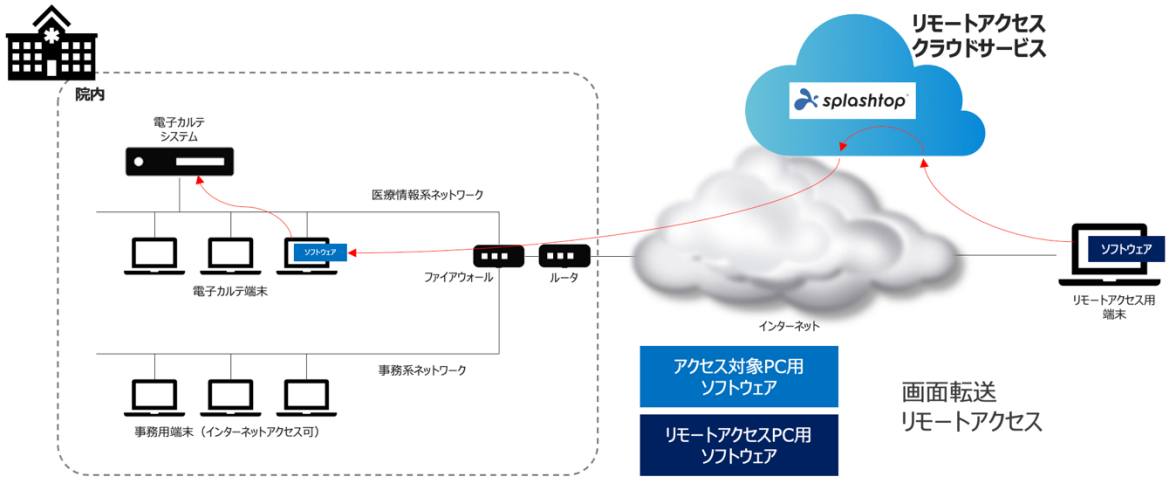
5. 宇賀神 敦. クラウド型AIサービス活用の課題と将来の展望について. *医療情報学*, 2024, **44(Suppl.)**, 371

H. 知的財産権の出願

なし

資料 電子カルテシステへのリモートアクセス２案





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 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いた最適なネットワークセキュリティ構成やシステム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。医療 AI は、深層学習による画像認識や生成系 AI の飛躍的な精度向上により医療への有用性が示されるが、個人情報保護への配慮やランサムウェアなどのサイバー攻撃の対応も喫緊の課題となっている。本分担班は東北大学が主導的に運用する地域医療ネットワークシステム MMWIN：Miyagi Medical and Welfare Information Netowork を通して、これら相反する課題を同時解決できないか検討した。

ガイドラインや医療機関へのヒアリングを参考に、ネットワークセキュリティに関するアンケート調査を超急性期病院(東北大学病院)の立場や地域医療ネットワーク(MMWIN)の立場で実施した。また AI 利用とセキュリティ対応が同時に成立するシステム構成の設計を、AWS を想定したクラウド基盤の前提で設計した。

ランサムウェア被害は近年高度化し、境界型防御を前提にしたセキュリティ対応が難しい現状が確認できた。またゼロトラスト型セキュリティ対応をガイドラインに合わせて導入したくとも、人材不足や資金の面で課題があることがわかった。これらセキュリティ対応において、地域医療連携システムを介して実現するならば有益であるとの見解もアンケート調査から確認ができた。また AWS 上に配置した特定のサーバと、医療施設内に設置したサーバがクラウド接続を通して、バックアップファイルの転送やリモート保守用途の接続、AI 利用に向けた API 連携ができることを確認した。

地域医療連携システムを活用することで、人材不足や投資抑制を補いながら、網羅的に多くの医療施設を課題解決できることが示唆された。来年度はこれらを具体的に検証し、実運用上の課題などを明らかにしながら、詳細なネットワークアーキテクチャーに落とし込む予定である。

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 センター長/東北大学病院 メディカル IT センター 副センター長 中村直毅：東北大学病院 メディカル IT センター 副センター長・准教授

A. 研究目的

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。医療 AI は、深層学習による画像認識や生成系 AI の飛躍的な精度向上により医療への有用性が示されるが、個人情報保護への配慮やランサムウェアなどのサイバー攻撃の対応も喫緊の課題となっている。本分担班は東北大学が主導的に運用する地域医療ネットワークシステム MMWIN: Miyagi Medical and Welfare Information Netowork を通して、これら相反する課題を同時解決できないか検討した。

地域医療連携システムなどを介し、多くの医療施設が抱える人材不足や投資負担の軽減を目指し、実効性のある安心安全な AI 利用基盤のネットワークアーキテクチャーを明らかにする。

B. 研究方法

近年の本邦でのランサムウェア被害を調査し、その被害や原因を知ると同時に、医療機関の実態を明らかにする。また安心安全のための厚労省らのガイドラインや医療機関へのヒアリングを参考に、医療機関での課題を明らかにしながら、地域医療連携システムを介して解決が計れるか検討する。宮城県内の医療施設にネットワークセキュリティに関するアンケート調査を実施し、超急性期病院(東北大学病院)の立場や地域医療ネットワーク(MMWIN)の立場で解析を進める。また AI 利用とこうしたセキュリティ対応が同時に成立するシステム構成の設計を、AWS を想定したクラウド基盤の前提で設計する。

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調査

2022 年 10 月 31 日に発生した大阪急性期・総合医療センターでのランサムウェア被害がある。2023 年 3 月 28 日の新聞報道では、被害総額は 10 億円超と報告されている。また外来診療の全面再開は翌年の 2023 年 1 月 11 日となっており、システム復旧に係る費用以外にも、病院経営や地域の医療提供にも大きな影響を与えていることが再認識された。

報道等からの情報では、2016 年以降の医療機関でのランサムウェア被害は 19 件、21 年には 5 件、22 年は 8 件と急増している。主なランサムウェア被害例は、福島医大病院(2017)、新潟大学医歯科学総合病院(2017)、宇陀市立病院 (2018)、多摩北部医療センター(2019)、市立東大阪医療センター (2021)、つるぎ町立半田病院(2021)、春日井リハビリテーション病院(2022)、日本歯科大学附属病院(2022)、青山病院(2022)、鳴門山上病院(2022)などがあった。

病床規模の大小、急性期や療養期など機能や役割に関係がない、被害を受けたシステムは検査システムや治験システム、遠隔読影システム、電子カルテシステム、医事会計システム、院内の研究用 PC などであり、ターゲットも広範囲になっている。さらにはバックアップデータも被害を受けた事例もあった。

■境界型防御の実態調査

今でも多くの医療機関では、医療情報システムは外部との接続をしないローカルエリアネットワーク(院内の閉域網)を構築す

ることを原則にしている。東北大学病院も例には漏れない。最低限の外部との接続はFW やウィルス対策、IDS/IPS などガイドラインに準拠してシステムは構築がされている。

一方で電子カルテシステムがあるネットワークは安全かつ信頼できるものとして、端末とサーバ間の認証や通信監視は極めて簡単なものになっている。信頼するエリア内の端末はウィルスチェックや USB 管理、ID やパスワード管理が中心であり、こうしたものは導入時からパッケージングで対応がなされている感がある。

電子カルテシステムが接続されるネットワークは信用できるネットワーク網(閉域網)であり、利用者のログイン認証など最低限の検証を行うセキュリティモデルを構築してきた。いわゆる境界型防御を前提にしたセキュリティ対応であることが、今回の研究調査で再認識がされた。

こうした境界型防御を前提にしたセキュリティ対応がどこの医療施設でも一般的であり、実際に被害を受けた医療施設では、パスワードや VPN のバージョン管理に不備があったなど報告があるものの、方針的にはどこも同じであることも確認ができた。

先の大阪急性期・総合医療センターの調査報告書[1]では、VPN ソフトのバージョン管理やパスワード・ID の不適切な運用などが指摘され、何かしらの運用上の課題が示されているものの、近年のサイバー攻撃の巧妙化は、こうした方針では対応できないことを示し、外部からの侵入し、無防備な内部からバックアップを含めて医療情報を暗号化、システム停止・診療機能の停止へとつながることへの対応が喫緊の課題であることが再確認された調査結果となった。

■外部接続の必要性からの実態調査

医療施設はシステム機器の保守だけでなく、自営式でない病院では給食などの委託サービスなど外部接続することが増えている。一般社団法人医療 ISAC が実施した実態調査アンケートがある[2]。回答した医療施設数は 1,279 件であるが、リモートメンテナンスを許可している医療施設は実に 76%もある。そのうちリモートメンテナンスに利用している機器・製品のバージョン情報等を把握している組織は 47%という低いレベルで、危険な状態にあることも示唆された。

過去の事例(徳島県のつるぎ町立半田病院)では、ＶＰＮソフトのバージョン管理などから生じる脆弱性が原因のひとつとして指摘された。同じＶＰＮソフトを利用している医療機関は 456 あり、そのうち脆弱性対応が未了の組織は 1 割程度あったことが報告されている。つまり既知の脆弱性だけでも 45 病院が危険にさらされていて、たまたま感染していないだけの状態ともいえる。

このようなこれまでのアンケート調査からも、多くの医療施設では外部との接続は行われており、そもそも安全な閉域網という考え方が成立していない現実があった。

■境界型防御(閉鎖網)を前提とした環境におけるサーバ OS における最新化検証

多くの医療機関では、厚労省からの指導もありシステムの最新化を要求されている。しかしながら医療システムは 24 時間稼働であり、また安定的に動作することが求められていることから、検証がされていない

OS バージョンとアプリケーションの組み合わせによる稼働は慎重にならざる得ない事情もある。また自施設で対応するにも、ＯＳのアップデートだけでなくサーバＯＳサポート切れに伴って、新ＯＳでのサーバ構築まで拡大する可能性があり、費用面も課題になることがある。

そこで実例として宮城県地域連携システムである MMWIN の環境にて検証し、どのような課題があるかを検討した。

令和５年度は Windows 2012 サーバの OS（済）と Linux サーバの最新化（済）が完了し、 現在～令和６年度初め（現在進行中）では、Windows2012 Server から Windows 2016 Server へのインプレースアップグレード（in-place upgrade）による更新を試みている。

※OS の入れ替えの方法の一つで、稼働中のシステムで、稼働したままアップグレードする方式で、システムの再セットアップが不要となる。

実際には、Linux サーバにおいて、ファイルシステムの mount 系のプログラムと java のソフトウェアの仕様変更に伴って、一部のプログラムが動作しなくなったという障害が出たが、設定変更で仕様変更に伴う不具合を回避して、大きな問題なくアップグレードできた。

しかしながら、技術的な検証はできたものの、こうしたアプローチを思いつく知識、作業が実施できるスキルを持つ人材がいる医療施設は少ないと考えている。もしくは外注に依頼する場合の費用は高額になることも予測される。OS やミドルウェア、サーバソフトの脆弱性が重要な対処事項となることは間違いなく、対処するべきことと理解できる。ただしシステムを持つことで生じるメンテナンス・システム維持に係るコスト・人材不足から脱却を図ることも課題と考えられる調査事例となった。

■環境面からの実態調査

地域医療の課題には「医療施設の最適配置」や「医師の偏在の是正」、「国民との適切な受診の推進」がある。医療の役割分担の推進であり、従来からの地域完結型医療が求められている。これを推進するために地域医療連携システムが期待され、施設間で医療情報を共有することが求められている。また医師不足の解消に、今後は臨床業務で医師が院外から情報システムを利用する機会も増える可能性がある。

つまり閉域網にある院内システムは外部との接続がこの環境面からも求められているのが現実である。またデータ Health 改革や「医療 DX 令和ビジョン 2030」[3]にあるように、国民との適切な受診の機会となれば、国民が自らの医療情報にアクセス可能な PHR などにより、患者との双方向性から外部接続が前提になる可能性が高い。

■ガイドラインなどの現状調査

「医療情報システムの安全管理に関するガイドライン 6.0」[4](2023 年 5 月に更新)がある。ガイドラインでは、ゼロトラスト型のセキュリティ対応へのシフト・併用による解決を求めている。従来の境界型防御：情報セキュリティに対する考え方を整理し(ネットワークの安全性の考え方や認証のあり方)、ゼロトラスト型防御を併用した対策の考え方を示している。また IT-BCP などサイバー攻撃を含む非常時に対する具体的

な対応についても言及している。

■新たな課題

しかしながら、ゼロトラスト型セキュリティ対応を、既存の境界型防御と併用するとしても、新たにクラウド型のセキュリティ対応や動的ポリシーなどが求められることになる。つまり一部は根本からの見直しであり、導入コストの負担が医療施設にとっては重大な懸念事項になる。

さらに保守対応する部門には、こうした新たなネットワークスキルを求めることとなり、人材育成や確保が現実の課題となる。そして新たなセキュリティ負荷からレスポンスを含め利便性の低下も懸念される。この対応に、システム自体も大幅な改修が必要となるかもしれなく費用負担がここでも懸念される。

こうした「導入コストや運用上の課題・人材育成と確保」と、「サイバー攻撃の巧妙化への対応や新たな外部接続(社会的)要求への対応」が相反することとなるが、社会にとって重要なインフラである医療では、ゼロトラスト型セキュリティ対応へ進むことは間違いないと考えるべきである。つまりネットワークアーキテクチャーの検討を行うのであれば、(1)病院側のコスト負担が軽減される方向であり、また(2)人材が少ない中で実現可能なこと、(3)地域連携や保守・外部委託先など外部接続があることが前提で、かつ(4)どこの医療施設でどんなシステムでも取りこぼさない仕組みが必要となる。つまり地域でのインクルーシブセキュリティ対応が求められることになる。

そこでネットワークアーキテクチャーのSWGでは、「地域連携システム上にゼロトラスト型防御を実現し、そこに接続する医療施設を取りこぼすことないようにセキュリティ対応が可能かを検討することとした。これが実現可能であれば、多くの医療施設を効率的にかつ短期間に対応できることが期待できることになる。

2. 【地域連携システム上に求めるセキュリティ対応の考察】

まず上図1に示す通り、病院情報システムの境界が曖昧になってきている。従来の病院情報システム内だけに閉域網を作り、

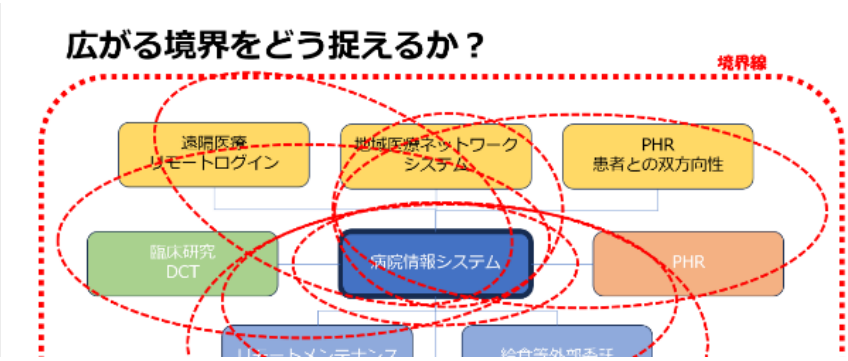


図1　境界型防御の境界はどこにあるのか

病院情報システムが中心にあるが、実際はリモートメンテナンスや外部委託、地域連携システムなど接続していることが多い。また将来的にPHRやクラウド型サービスなどのニーズから外部との接続が増えることが考えられる。そうなると境界型防御の境界をどこに設定するかの課題が生じるだろう

その内側を安全領域にするだけではセキュリティが成立ないことも理解できる。従来の院内における境界型防御：電子カルテシステムは外部接続しない、接続するにしてもファイヤーウォールやリバースプロキシを導入することで、内側は安心としてきている。つまり、端末とサーバ間の認証や通信監視は省略してきた(不正な要求を検知できない)経緯がある。

一方で USB など直接に端末に持ち込まれる悪意に対して、ウィルス対策ではウィルス対策ソフトのインストール、メール添付ファイルの取り扱い注意などの教育と啓発、USB 管理としてはポート制御、USB そのものの暗号化や認証機能を有するように多機能化することで対応を行ってきた。刑事的な罰則がある情報漏洩には不正アクセスの把握や教育と啓発によるもので、内部犯行には十分な対応がされているとは言えない状況ともいえる。

つまり水際戦略を実施しており、境界型防御と教育で、セキュリティは万全である(安全神話)という考え方である。サイバー攻撃の巧妙化はこうした安全神話を崩壊させ、外部からの侵入により無防備な内部からバックアップを含めて暗号化し、システム停止へと追い込むことから、この神話が成り立たないことは事実である。

海外事例でいえば、Tufts Medicine がある。Tufts Medicine は、クラウドのプラットフォーム上で、4 病院の 6 つの電子カルテや 40 以上のアプリケーションを統合・連携させることで、医療従事者が、PC からでもスマートフォンからでも、病院のデータに安心・安全にアクセスできる仕組みを構築している。これにより病院機能や働き方の改善を実現し、本業である医療への集中とデータ利活用の促進、20%のコスト削減が達成できたとしている。

※引用 AWS re:Invent 2022 “Realizing the full value of your EHR with a digital health ecosystem (HLC202)”, https://www.youtube.com/watch?v=7GhWW3JD5Sg
https://aws.amazon.com/jp/solutions/case-studies/tufts-case-study/

この事例ではクラウド型アーキテクチャの実装を通じてゼロトラスト型の高いセキュリティレベルを実現している。“*AWS の Well-Architected Framework に従うことで、チームが目線を同じくして、セキュリティ対策に取り組むことが出来、最初のセキュリティレビューでは、驚くべきことに、5 点満点中 4.8 の非常に高い評価を得ることが出来た。(レビューアーは) これも、AWS のフレームワークに基づく推奨項目のすべてに、一つ一つに着実に従ったおかげだと明言している”(Jeremy Marut, Chief of Digital Modernization, Tufts Medicine)。※引用 AWS re:Invent 2022, “Realizing the full value of your EHR with a digital health ecosystem(HLC202)”, https://www.youtube.com/watch?v=7GhWW3JD5Sg*
https://aws.amazon.com/jp/solutions/case-studies/tufts-case-study/

“これが業界の従来のやり方で、機能してきた。サーバを自分たちの机の下で管理しているから患者さんが生き残るのだ。”いう考えに

挑戦する必要があります。ナンセンスです。私たちのチーム全員が、日々、命を救っていると信じています。以前なら復旧に 6 週間かかる障害が起きても、救命救急を止めずに済みました(Jeremy Marut, Chief of Digital Modernization, Tufts Medicine)の言葉にあるように、セキュリティ対応の真の目的は、「Saving lives, not drives! 救うのは患者の命、ドライブではない!」

※引用 AWS re:Invent 2022, "Realizing the full value of your EHR with a digital health ecosystem (HLC202)", https://www.youtube.com/watch?v=7GhWW3JD5Sg

https://aws.amazon.com/jp/solutions/case-studies/tufts-case-study/

これらのように、セキュリティ対応の目的は患者の命であり、医療機能を停止しないことが重要である。こうした命題に対して、現状を正しく把握し、クラウド利用など従来の技術に拘らず対応していくことが重要である。

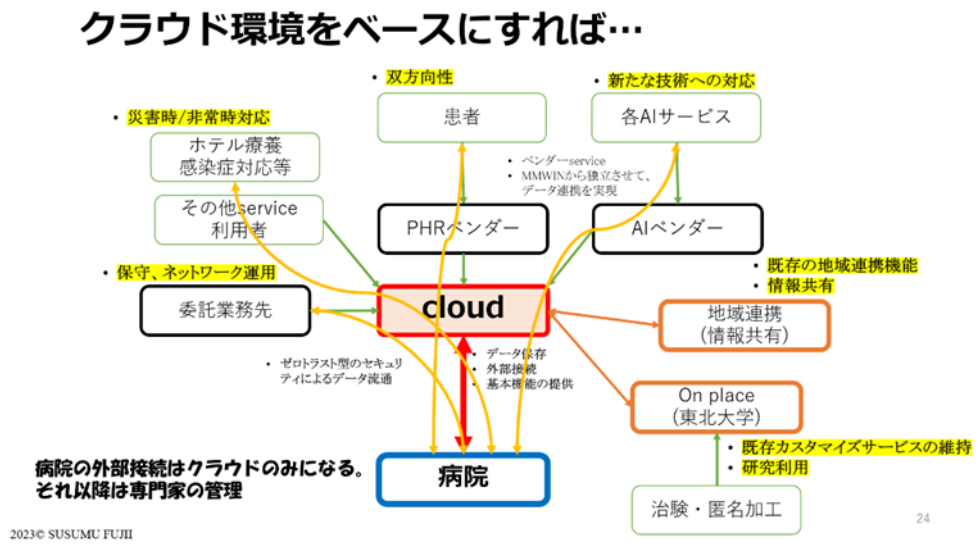


図 2 クラウドによる課題解決の関係

病院は外部接続がクラウド接続に集中できることで、境界型を強化しつつ、サービスがクラウド上での接続になることで全体解でのゼロトラスト型セキュリティ対応も行われる。

そこで SWG では、まずクラウド導入により医療施設がもつ課題をどの程度改善できるかを検討した。図 2 に課題対応できる関係性を示した。

図 2 に示す通り、クラウドを経由してリモート保守や外部委託先との接続、地域連携システムとの接続、将来的なニーズを含む患者との双方向性、AI サービスなども接続可能となる。この場合、医療施設ではクラウド接続する 1 つの接続線を管理すれば良く、運用における管理対象が大幅に軽減される。クラウド上に展開されるサーバや接続サービスはクラウドベンダーやその先のベンダーによるものとなり、こうした管理からも解放される可能性が高い。

そこで SWG では図 3 に示す通り AWS 上で

図 2 に示した内容を実現することが可能かをアマゾン・ウェブ・サービス・ジャパン合同会社の協力を得て調査した。

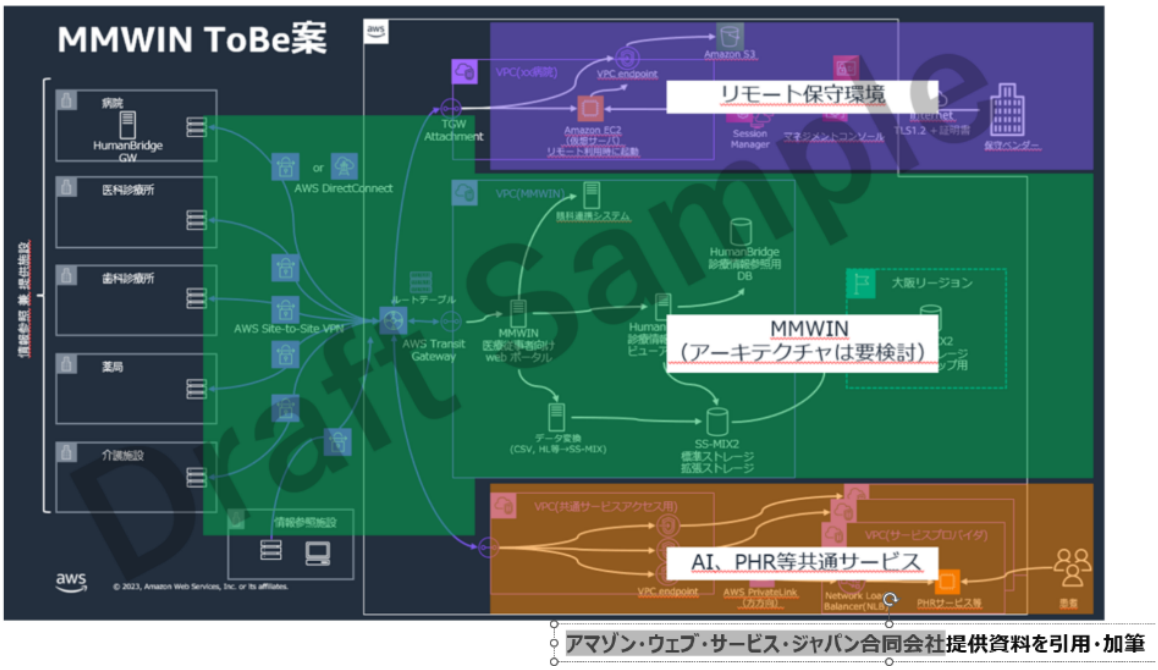


図 3　AWS を使ったセキュリティ対応モデルの設計

基本的に外部からの保守契約は、クラウド内にサーバ A、サーバ A のみが院内にあるサーバ X に到達できるような設定サービスで可能であり、外部委託サーバも同様に設定可能である。また外部委託サーバ自体をクラウド上のサービスに変更できれば、より安全性が高まることも考えられた。AI や PHR サービスは既に AWS などのクラウド上で展開されている事例が多く、AWS 内でのサーバ接続で対応可能であった。

一方で backup に関しては、遠隔地保存自体が災害や火事などの事象には有効な手段であるが、ランサムウェアなどにおいては全てが解決できる状況にないこともわかった。クラウド上に保存した backup は外部と遮断されていることから、backup データにあるウィルスが発症して悪意のある動作をしても問題が発生しにくい。また変更そのものができないから、暗号化されてしまうなどの被害を食い止めることは可能である。しかしながら、既に感染した情報であることは否定できないので、そこからリストアすることは再感染を起こす可能性があり、単純には利用できるデータにはならない。なにかしら感染を検知する事前の処理が必要となるだろう。

しかしながら、多くの課題が解決できることと、これがパッケージングされて導入すればゼロトラスト型セキュリティ対応の一部になるのであれば、その実効性も高いものになる。つまり地域連携システムのように今後は必要となるであろうシステム上に、もしくは宮城県のように 739 施設が参加するシステム上に、cloud 環境を有効に使

うことで、これまで院内だけの境界線を地域の医療システム全体を境界線とし、合わせてゼロトラスト型セキュリティ対応を併用できることになる。これはコストの面や人材育成・確保という課題解決にもつながるものであり、合理性が高いアプローチと考える。ただし backup や外部接続なども鑑みながら、動的ポリシーなどにより要求を管理して安全性を高めることがなければ、成立しない安全性もあることを踏まえていく必要がある。

2023 年度の SWG では、これまでの実態調査からゼロトラスト型セキュリティ対応の必要性を再認識し、ゼロトラスト型セキュリティ対応の導入時の課題を整理し、人的リソースや導入コストを指摘した。また具体的にどのようなサービスが必要なのかをユースケースとして検討した。そこでクラウド環境を利用することで多くが解決できる可能性があることを示唆した。

2024 年度はこれら知見をより詳細に定義し、クラウドベンダーの比較や疑似環境を通して課題を調査しながら、最終年度の実証に向けて研究を進める予定である。

3. 【地域連携システム上にゼロトラスト型セキュリティ対応ができることの意識調査】

宮城県内にある医療施設(介護施設内にある診療室を含む)1753 施設に WEB によるアンケートを実施した(2024 年 3 月)。内容には地域連携システムにおいてクラウドを活用し、そこでゼロトラスト型セキュリティ対応が実現するとしたら、ニーズがあるのかを調査である。

従来の境界型防御(電子カルテネットワーク内は安全)というセキュリティ対策から、ゼロトラスト型セキュリティ(安全な領域はない)の併用への転換を厚労省からも推奨している。しかしながら、これに対応したくとも、スキルを持った人材の育成や人材確保が難しいことを説明し、地域連携システムを通して外部接続やバックアップがされることで、ランサムウェア対策を兼ねることが可能であれば、医療機関にはメリットがあるかのニーズを調査となっている。

速報値でいえば 60～70%が地域医療連携システムを介してセキュリティ対応がなされるのであれば、前向きな回答となった。詳細は次年度にまとめて設計に活かす。

なおアンケート項目は文末に「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」に添える。

参考文献

1) 情報セキュリティインシデント調査委員会. 調査報告書. 地方独立行政法人大阪府立病院機構大阪急性期・総合医療センター, 2023. https://www.gh.opho.jp/pdf/report_v01.pdf

2) 全国保険医団体連合会/日本病院会. セキュリティアンケート結果調査. 一般社団法人医療 ISAC, 2023. https://m-isac.jp/wp-content/uploads/2023/08/report_20230120.pdf

3) 「医療 DX 令和ビジョン 2030」厚生労働省推進チーム. 医療ＤＸ. 厚生労働省, 2022. https://www.mhlw.go.jp/content/10808000/000992373.pdf,

https://www.mhlw.go.jp/stf/shingi/other-isei_210261_00003.html
4) 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.厚生労働,
2023.[https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html]

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 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
      1. 医療情報システムにおけるプラス・セキュリティとは -起きることを待つ、から起きていることを当たり前に(猪俣敦夫：研究班有識者)
      2. 境界型防御からゼロトラストへ　医療機関からの視点(藤井進・中村直毅：東北大 SWG)
      3. 地域連携システムや PHR システムでのゼロトラストの考え方(名田茂)
      4. 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(宇賀神敦：研究班主担当)
   ② 第 29 回日本災害医学会総会・学術集会
      1. 災害時の医療情報提供に関する意識調査

3. 大会論文集・査読付き詳細な抄録
   ① 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 -, Vol43 Supplement, 43 回医療情報学連合大会論文集(24 回日本医療情報学会学術大会), p141, 2023/11.
   ② 藤井進　野中小百合　金秀明　浅見太一　江川　新一, 災害時の医療情報提供に関する意識調査, Vol28 Supplement,Japanese Journal of Disaster Medicine, p454, 2024/02.

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

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 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、医療機関の設立母体、病床数、地域などの特性を踏まえて 26 医療機関（24 病院、2 クリニック）に対して実態調査を行った。対面のヒアリング実施前に、事前アンケート調査票を送付し、その回答を入手した後に、25 医療機関については対面のヒアリング（1 医療機関はアンケート調査項目の回答）を実施することにより、効率向上とヒアリングで確認すべき内容を明確にすることができた。本ヒアリングを通して、医療機関の IT 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を把握及び医療現場が抱える課題を把握することができた。また、本ヒアリングから、医療機関のシステム構成を技術面から 3 種類に類型化することができた。類型化については 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。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、またベンダ依存体制が浮き彫りになった。技術面では、医療機関とクラウドシステムを安全・安心に接続するための必要とされる 4 種類のセキュリティ領域について、技術調査と整理を行った。今年度の成果を基に、医療機関がリーズナブルなコストで導入しやすい技術の実証を複数箇所で実施し、それに基づいたネットワークセキュリティ構成の提言を実施する予定である。

A. 研究目的

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ている。
2023 年度は、国内医療機関へのヒアリングを実行し、医療機関が外部ネットワークに出る際の類型化案を策定する。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の、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。

B. 研究方法

国内医療機関へ対面でネットワーク環境の実態調査のためのヒアリングにあたり事前アンケート調査票を提示し、医療機関にて記入後ヒアリングを実施した。
アンケート調査票とヒアリング内容をもとに、統計化および類型化を実施した。その際に JASO TP15002 を活用し、脅威・リスクを抽出した。
脅威・リスク及び現状のセキュリティ状況を理解した上で、最新クラウドセキュリティに関する整理を机上にて実施した。
（倫理面への配慮）
本研究においては特段なし。

C. 研究結果

26 医療機関にヒアリングを実施した。対面は 25 医療機関、1 医療機関はアンケート調査項目の回答のみであった。
ヒアリング前に以下の項目のアンケート調査項目を取得した。
調査項目は、病床数・平均外来来院数・機関組織・開設主体・病院機能・診療科区分・システム導入状況・サイバーセキュリティ対策チェックリストに記入状況・システム担当者の有無・セキュリティ人材の有無・院内でのセキュリティ監査の実施の有無・院内のリスクアセスメント実施状況の有無・BCP 対策の状況・ハイブリッドクラウドの採用の有無・診療系ネットワークにおける外部通信の有無・医療 AI サービスの利用状況・BYOD の利用状況・今後クラウドシフトへの想いなど、24 項目である。
添付（A1.　医療機関へのネットワークセキュリティ事前アンケート内容）
24 項目の回答状況をもとに、平均 1.5 時間程度医療機関へのヒアリングを実施し、図 1 のイメージでヒアリング結果をまとめた。
ヒアリングの中でアンケート調査項目のみでは回答しきれない現状の外部通信に関する医療機関内のネットワークに関する内容も確認し、ネットワークパターンを 3 つに類型化した。それが図 2～4 である。

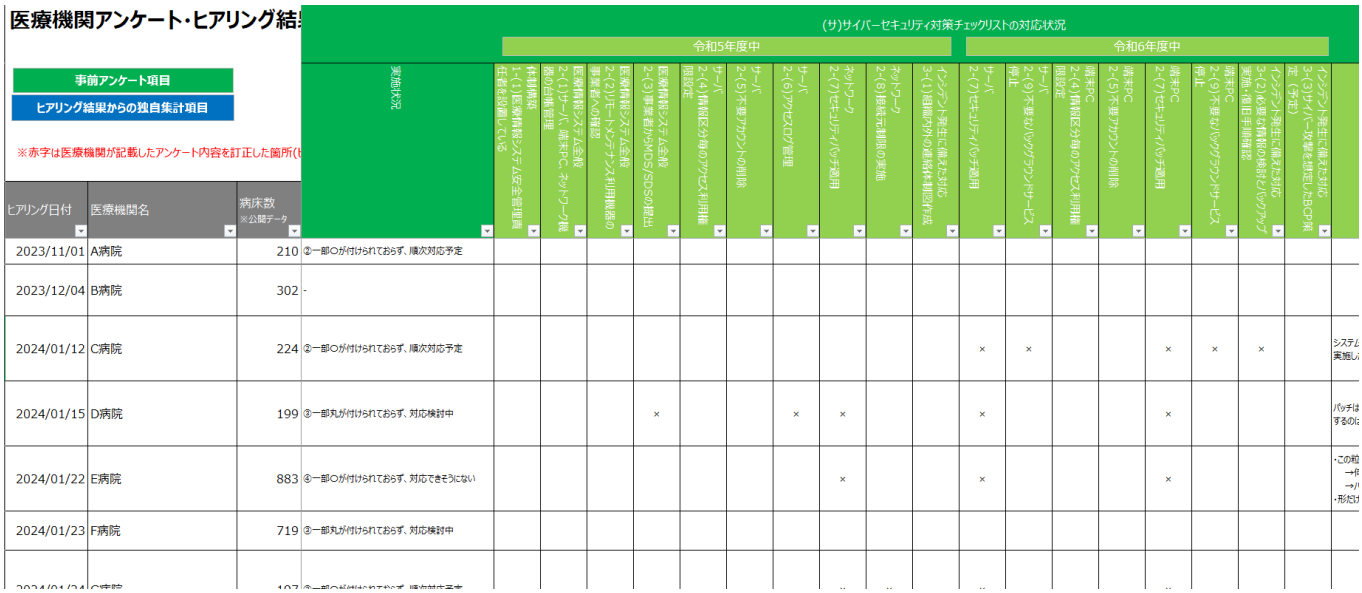


図１　ヒアリング結果イメージ

医療機関ネットワークモデル（レベル1）

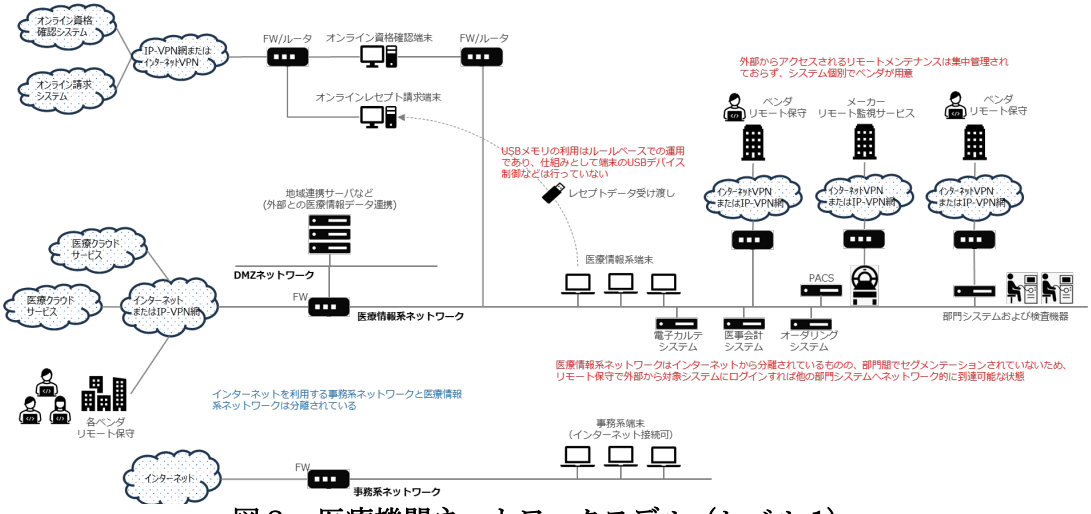


図２　医療機関ネットワークモデル（レベル 1）

医療機関ネットワークモデル（レベル2）

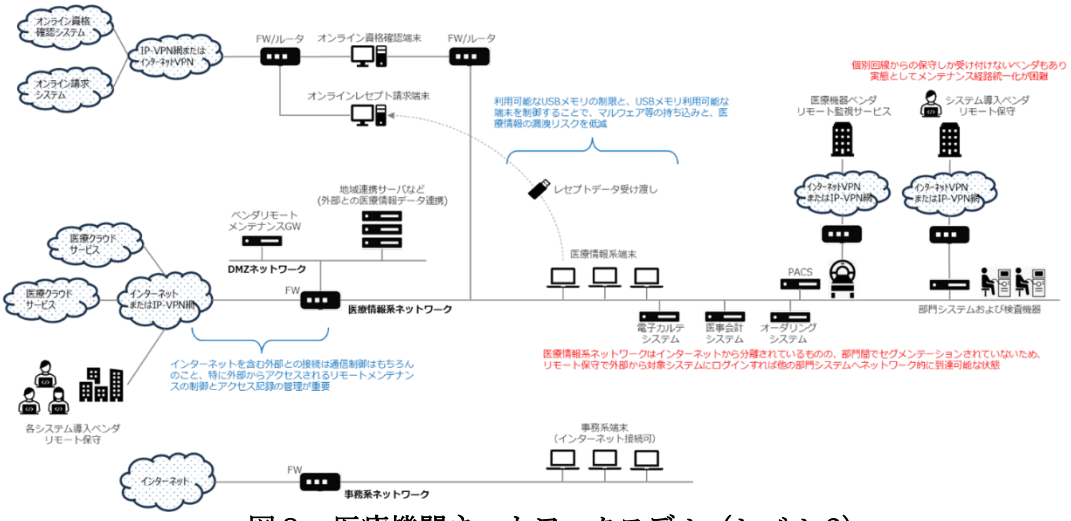


図３　医療機関ネットワークモデル（レベル 2）

医療機関ネットワークモデル（レベル3）

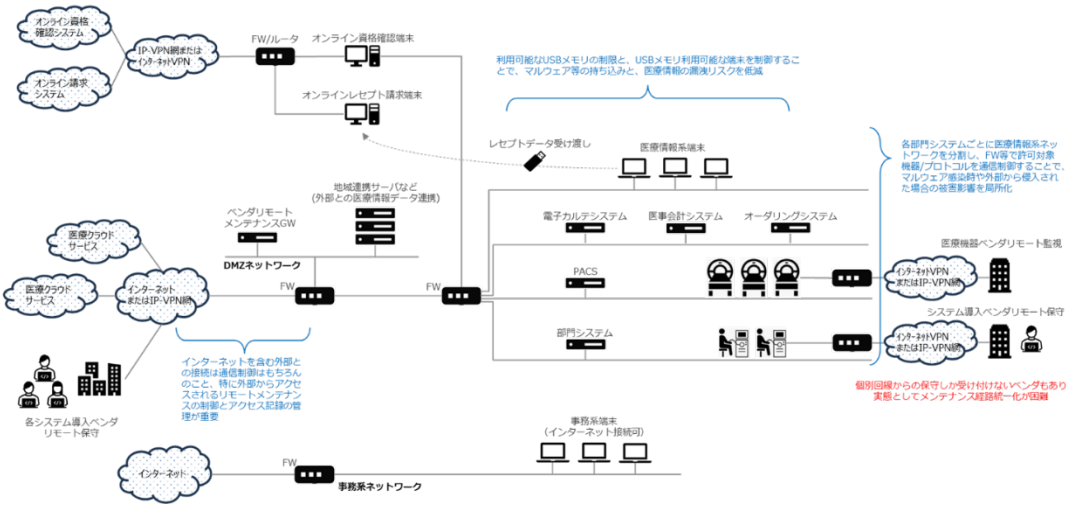


図４　医療機関ネットワークモデル（レベル 3）

今回の調査における医療機関ネットワークモデルの分類の状況としては、3 つのレベルに類型化した。
レベル 1 は、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。レベル 2 は、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。また、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。
レベル 3 は、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。また、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。さらに、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。
それらを図 5 の形で整理した。

医療機関のネットワークセキュリティを考察する上で、個別構成の議論にならないよう以下の観点で凡化モデルを作成した。汎化モデルを作成するうえで、以下を定義した。

- 電子カルテ、PACS などシステム個々ではなく、保護すべき医療情報として一つの塊とみなす（昨今の医療情報システムは、各システムが TCP/IP ネットワークを通じでつながっている）
- 医療情報（システム）へアクセスする主体を特定する
  - 院内の職員、院外からのリモートアクセス、外部連携システムなど
- ネットワークセキュリティ対策を施す領域を分類し凡化モデルにマッピングする（本書では以下の 4 つに分類した）
  - アカウント層：ID・認証情報の管理や権限管理を行う領域
  - エンドポイント層：医療情報システムへアクセスする端末
  - ネットワーク層：外部との接続を中心にセキュアなネットワーク接続を実現する領域
  - 監視・検知層：ネットワークや端末、サーバなどシステム全体にわたってセキュリティの監視や検知を実現する領域

上記を前提に、図 6 に汎化モデル図を作成した。

レベル	統制の主な内容	外部NW接続統制	記憶媒体利用統制	内部NW統制	分布割合	コメント
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	△	△	×	45% (10)	いずれの医療機関でも、医療情報とインターネットとの分離は実現済み。
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	○	○	×	45% (10)	USBメモリなど外部媒体の利用制限を、ルールと仕組みの両面で実現している医療機関は比較的多かった。 また、ベンダリモート保守のアクセス方法を院内統一化をめざし、ベンダ個別にID・パスワード発行のうえ、アクセス先システムを制御している機関も一定数あり。ただし、その接続方式を受け入れないベンダもあり、アクセス方式の完全統一は慣習上困難であるのが実情。 尚、各部門システムのネットワーク（VLAN）を分けている機関はいくつかあったが、通信制御までは実現できていないため、レベル2でもセキュリティリスクは存在。 • ランサムウェアに感染した場合に医療情報系ネットワークで被害が拡散 • ベンダリモートアクセスにおいて、対象システムにログイン後に、別の部門システムへ容易にネットワーク侵入が可能
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	○	○	○	9% (2)	部門システムごとにネットワークをセグメンテーションし、必要な通信のみ許可するよう制御している医療機関は2件のみだった（NWセキュリティに精通した人材が医療機関全体を把握し、各医療機器ベンダと会話しながら通信フローを把握する必要あり）

図 5　医療機関ネットワークモデル分類状況

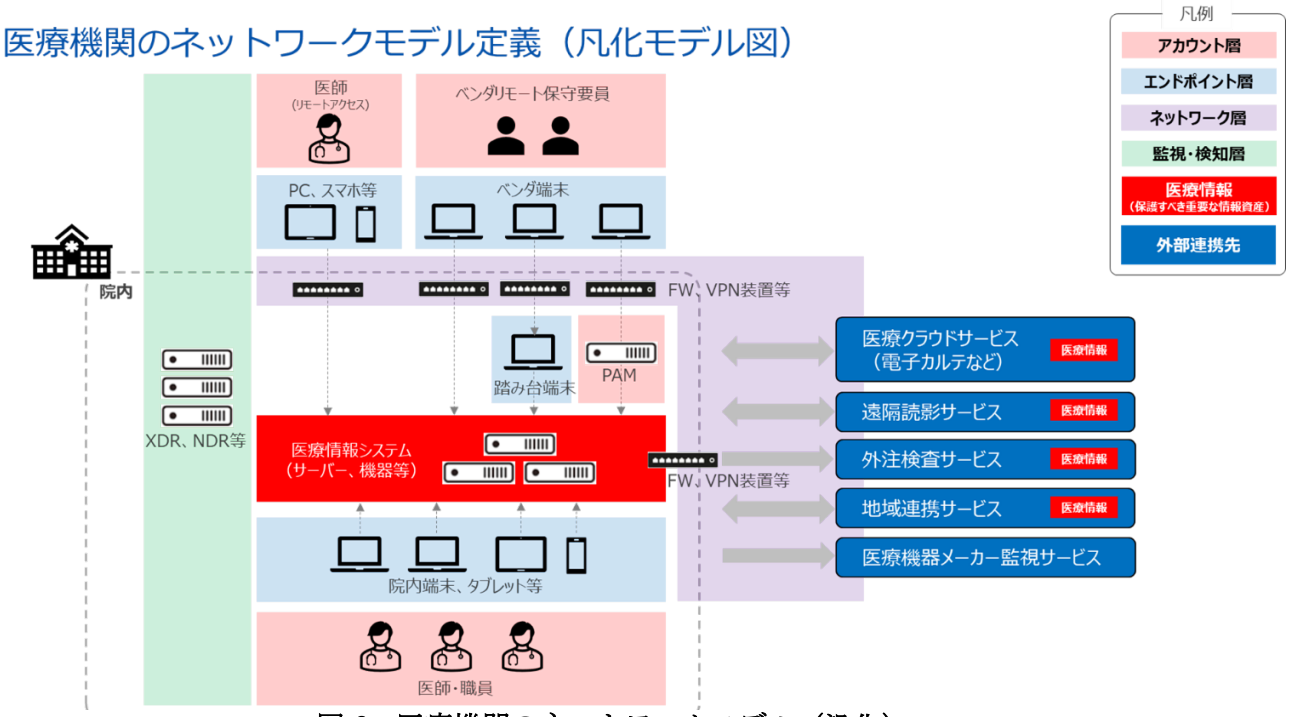


図 6　医療機関のネットワークモデル（汎化）

汎化したモデル図に対して脅威事象を抽出するにあたり、以下の基本的なセキュリティ対策は実施済と仮定した。

- 医療情報システム（サーバ、及び関連 NW 機器）はマシンルームや施錠されたラック等、物理的に関係者以外がアクセスできない場所に設置されているものとする
- 医療情報システム（サーバ、及び関連 NW 機器）が第三者（患者など）に物理アクセス可能な場所に設置されている場合は、不正操作の対策がされているものとする
  - 対策例 1:システムが設置されている部屋に入室する場合は職員が立ち会い、勝手に第三者に操作されない運用を行う
  - 対策例 2:ネットワークスイッチの未使用ポートはシャットダウンしておき、機器を接続してもネットワークにアクセスできない状態とする
  - 対策例 3：離席時はタイマー等で PC のスクリーンロックが自動的にかかる設定とし、第三者が不正に PC を操作しない対策を行う
- 医療情報システム（サーバ、及び関連 NW 機器）の、OS やアプリケーションは利用者ごとに ID が払い出され、パスワードが適切に管理されているものとする
  - NG 例 1：ユーザーに必要のない権限（特に管理者権限など）を付与している
  - NG 例 2：複数の利用者で ID を共用している
  - NG 例 3：複数のシステムや機器で共通の ID/パスワードを設定している
  - NG 例 4：初期設定のパスワードや機器のデフォルトパスワードを使い続けている
- 医療情報システムを設置設定およびメンテナンスするベンダ作業者の身元確認、作業内容確認を、医療機関職員が確認している
- 医療情報システムを設置設定およびメンテナンス（リモート含む）を行うベンダの作業用 PC は、アンチウィルスソフト導入などセキュリティ対策がされ、マルウェアに感染していないものとする
- 医療情報システム、及びそのシステムにアクセスするネットワークや端末は、直接的にインターネットに接続されていないものとする
- 特にインターネットに暴露されている NW 機器は、設定不備による意図しない外部からのアクセスはないものとする

本仮定を前提したアクセスパスごとに具体的な脅威を図 7 に洗い出した。

アクセスパス	具体的な脅威事象	備考
院内ネットワーク	悪意のある第三者が不正に院内ネットワーク（LAN）に対して接続し、医療情報の閲覧・搾取が行われる	特にWi-Fiは電波が届く範囲は盗聴可能となるため、適切な認証方式と暗号化強度で利用することが必須。
	悪意のある第三者が不正に院内ネットワーク（LAN）に対して接続し、マルウェア感染や医療情報システムが破壊される	特にWi-Fiは電波が届く範囲は盗聴可能となるため、適切な認証方式と暗号化強度で利用することが必須。
院内医療情報端末（タブレット等含む）	マルウェアが仕組まれたUSBデバイスを院内端末で利用することでウィルスに感染して、医療情報の搾取や、医療情報システムが破壊される	
	USBメモリなど外部記憶媒体を利用し、医療情報が外部に漏洩する（故意による持出し、不注意によるUSBメモリ紛失など）	
	他の医師や職員のIDを利用して、なりすましで医療情報システムを操作する	特にパスワードを変えずに運用し続けたり、退職済み職員や、一時作業用IDが放置されるとリスクが高くなる。
院外からの医療情報システムアクセス	職員がリモートでアクセスし、故意に医療情報の持ち出しを行う	
	職員がマルウェア等に感染した端末等で医療情報システムにアクセスし、ウィルスが院内に感染、医療情報システムが破壊されたり、医療情報が搾取される	端末が直接ネットワークでつながる形態だと感染被害が広がりやすいが、限定的なアプリケーションでのアクセスや、画面転送方式であれば、被害が局所化できると想定される。
	職員用のリモートアクセスルートから第三者が不正にアクセスし、医療情報の不正閲覧や医療情報搾取が行われる	特にインターネット経由で職員が医療情報システムに接続されるネットワーク形態の場合、不特定多数からアタックを受けやすい。 また、多要素認証の未活用、単純なパスワード設定、パスワード情報漏洩によりリスクが高くなる。
院外からの医療情報システムアクセス	職員用のリモートアクセスルートから第三者が不正にアクセスし、ウィルス感染を含む医療情報システムの破壊や、医療情報搾取が行われる	特にインターネット経由で職員が医療情報システムに接続されるネットワーク形態の場合、不特定多数からアタックを受けやすい。 また、単純なパスワード設定、パスワード情報漏洩、多要素認証の未活用などによりそのリスクは高くなる。
	インターネットに露出されているNW機器の脆弱性を突かれて、インターネット経由で第三者が侵入、ウィルス感染を含む破壊活動や医療情報搾取が行われる	医療情報システムが、間接的にでも物理的にインターネットに接続される場合は、インターネット境界のセキュリティ維持は非常に重要。
ベンダリモートメンテナンス	ベンダリモートアクセスのルートにて第三者が不正にアクセスし、ウィルス感染を含む医療情報システムの破壊や、医療情報搾取が行われる（単純なパスワード設定、パスワード情報漏洩、多要素認証の未活用などを原因として）	認証情報（パスワードや多要素認証の情報）がベンダで適切に管理されていない場合、リスクが高くなる。 また、インターネット経由でリモートメンテナンスされるネットワーク形態の場合、インターネット境界のセキュリティ維持は非常に重要。
	インターネットに露出されているNW機器の脆弱性を突かれて、インターネット経由で第三者が侵入、ウィルス感染を含む破壊活動や医療情報搾取が行われる	インターネット境界のセキュリティ維持は非常に重要。
	ベンダが医療情報システム（サーバやNW機器）にアクセスしたうえで、悪意をもって保守範囲外の別システムにアクセスし、医療情報を不正に閲覧したり情報搾取を行う	部門システム間で自由なNWの疎通ができる状態だと、サーバにログインさえ出来れば、他のサーバへラテラルムーブメントが可能。管理レベルの低い部門システム保守ベンダにより、院内システム全体がリスクにさらされる。
	ベンダが医療情報システム（サーバやNW機器）にアクセスしたうえで、悪意をもって保守範囲外の別システムにアクセスし、ウィルス感染を含む破壊活動を行う	部門システム間で自由なNWの疎通ができる状態だと、サーバにログインさえ出来れば、他のサーバへラテラルムーブメントが可能。管理レベルの低い部門システム保守ベンダにより、院内システム全体がリスクにさらされる。
外部サービス連携	医療情報システムと接続している外部のシステムや組織経由で、第三者が不正にリモートでアクセスし、医療情報の不正閲覧や医療情報搾取が行われる	閉域網で接続されていても発生する。セキュリティ強度の低い組織と接続することで自院のリスクも高まる。
	医療情報システムと接続している外部のシステムや組織がウィルスに感染したり、外部システム経由の不正アクセスで院内にウィルス感染が波及、医療情報システムの破壊や、医療情報搾取が行われる	閉域網で接続されていても発生、セキュリティ強度の低い組織と接続することで自院のリスクも高まる。 大阪急性期・総合医療センターのランサムウェア被害も、外部接続したシステムからの侵入が原因の一つであった。
	インターネットに露出されているNW機器の脆弱性を突かれて、インターネット経由で第三者が侵入、ウィルス感染を含む破壊活動や医療情報搾取が行われる	インターネット境界のセキュリティ維持は非常に重要。

図 7　脅威の事象

各脅威に対する対策有効性を評価するにあたり、汎化モデルで定義した各領域の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として以下をピックアップした。

- 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。
実態調査に関する考察としては、医療情報システムに求められるネットワークセキュリティを実現するためには、医療機関個々の取組みだけでなく、行政や地域連携、関係団体など多面的な支援が必要と考えられる。
ヒアリング通じて、具体的に以下の 4 点が感じられた。

- セキュリティ要件に対応するための具体的なノウハウ不足：具体的な対応手順や対策例、また対応すべき優先順位など、現場ですぐに活用可能なノウハウを行政や関連団体から積極的に展開し、現場担当者のスキルを補う対応は急務であると考えられる。例えば本調査と並行で実施されているシステム監査グループの成果物は、現場が必要としている具体的な監査ノウハウとして有効である考えられる。
- セキュリティ要件に対応する工数捻出：情報担当者が展開されたノウハウを活用し対応の見通し（期間・工数含む）を立てることと併せて、行政からも医療機関の経営者・管理者にセキュリティ対応の重要性と人員・コストの必要性を啓蒙することも重要である。
- セキュリティ対策コスト捻出：セキュリティレベルの底上げは医療業界全体の課題であるからには、各医療機関がセキュリティ対策に対してインセンティブが働くよう、行政が主導しアメ（補助金など）とムチ（診療報酬の減額や罰則など）を活用するマクロ的な取り組みは有効であると考えられる。
- 医療情報担当者の人員不足：多くの医療機関では医療情報担当者の待遇面は事務職扱いであるためエンジニアが集まりづらい。待遇改善による採用改善を試みることも必要だが、例えばネットワーク機器の継続的なパッチ適用は専門ベンダに外注することや、クラウドの活用など、人口減少時代に外部リソースの活用は避けて通れない打ち手となる。

また、電子カルテ及び周辺システム（オーダリング・医事会計）は比較的管理されているが、部門システム（例えば PACS、検査システム等）は部門担当者任せであるケースが多いため、院内ネットワーク全体の外部接続を把握している職員がかなり少ない状況であることがわかった。このような体制ではそれぞれの医療機関がセキュリティリスクに対応するのは困難であり、医療情報を扱う端末やシステムからセキュアに外部の医療クラウドサービスへ接続する仕組みを、今後新たに示す必要があると考えられる。
次年度には PoC の検証する候補として、今回調査にて各接続形態を医療機関と、クラウドサービス事業者の両者の視点から比較検討を行った。
図 8 は比較検討結果であるが、以下の 2 つの接続形態は今後の PoC 評価対象として有力な候補として SASE/SSE 及びセキュアブラウザとし、次年度 PoC 評価を行う予定である。

D. 考察

実態調査に関する考察としては、医療情報システムに求められるネットワークセキュリティを実現するや医療機関でのクラウド促進ためには、医療機関個々の取組みだけでなく、行政や地域連携、関係団体など多面的な支援が必要と考えられる。

E. 結論

医療機関の体制ではそれぞれの医療機関でセキュリティリスクに対応するのは困難であり、医療情報を扱う端末やシステムからセキュアに外部の医療クラウドサービスへ接続する仕組みを、今後新たに示す必要があると考えられると感じた。
次年度は医療機関から外部にでるユースケースを検討し、PoC を行う予定である。
PoC 評価対象として有力な候補として SASE/SSE 及びセキュアブラウザとし、次年度 PoC 評価を行う予定である。

接続形態	医療機関にとって様々な医療クラウドサービスを利用しやすい接続形態であるか	医療機関のセキュリティ確保がしやすい構成であるか	クラウド事業者が準備しやすい接続形態であるか	クラウド事業者側のセキュリティ確保がしやすい構成であるか	評価コメント
①専用線	サービスごとに回線を敷設するのはコスト的に困難であり、IPアドレス体系の重複は導入上の制約・課題となることが想定される。	外部と閉域網で接続されるため、セキュリティ確保が容易。	利用する医療機関ごとに回線を敷設する必要があり、またIPアドレス体系の重複は導入上の制約・課題となることが想定される。	外部と閉域網で接続されるため、セキュリティ確保が容易。	クラウド事業者の接続形態として一般的ではないため、PoC対象から除外。
②IP-VPN	（同上）	（同上）	（同上）	（同上）	クラウド事業者の接続形態として一般的ではないため、PoC対象から除外。
③拠点間VPN	（同上）	VPN機器がインターネットに晒されるが、論理的には閉域網で構成されるため、セキュリティ確保が比較的容易。	多くの医療機関とのVPN接続を収容できるNW機器が必要。またIPアドレス体系の重複は導入上の制約・課題となることが想定される。利用機関の増減に合わせてVPN接続のメンテナンス運用が必要。	VPN機器がインターネットに晒されるが、論理的には閉域網で構成されるため、セキュリティ確保が比較的容易。	クラウド事業者の接続形態として一般的ではないため、PoC対象から除外。
④リモートアクセスVPN	端末に専用ソフトウェア導入が必要。仕組み上、接続時は院内LANへのアクセスが制限されることが想定される。	アクセス先をクラウドサービスに絞ることで、セキュリティの確保が比較的容易。	専用のリモートアクセスVPN装置が必要。利用機関の増減に合わせてIDの発行・失効メンテナンス運用が必要。	インターネットの不特定多数にアクセスされる状態となるため、アクセス装置は特にタイムリーなパッチ適用などセキュリティ維持は必須。	④・⑤は技術的な差異はあるが、類似した接続形態となる。いずれも比較的枯れた技術であり候補となり得るが、敢えて検証を行う必要性は低いと考える。
⑤SSL-VPN	（同上）	（同上）	専用のSSL-VPN装置が必要。利用機関の増減に合わせてIDの発行・失効メンテナンス運用が必要。	（同上）	（同上）
⑥SASE/SSE	（同上）	アクセス先をSASEサービスに絞ることで、セキュリティの確保が比較的容易。	SASEの導入が必要。利用機関の増減に合わせてIDの発行・失効メンテナンス運用が必要。	常時SASEサービスへ接続され、各医療機関とも論理的な閉域網を構成するため、セキュリティ的に保護された状態となる。	単なる経路の暗号化だけでなく、様々なセキュリティ機能を有している。今後の評価対象の一つとして有力な候補であると考える。
⑦端末のブラウザを直接利用	利用しやすい。ただし、セキュリティ確保のためProxyサーバ等でのアクセス先制限は必須。	アクセス先をクラウドサービスに絞ることで、セキュリティの確保が比較的容易。	一般的なインターネットへのWeb公開と同等。	インターネットに直接公開するWebシステムとなるため、多層防御（FW、IPS、WAF、DDoS対策など）が必要	単に端末からインターネットへアクセスする構成となるため、敢えて検証を行う必要は無いと考える。
⑧セキュアブラウザ	利用しやすい。ただし、セキュアブラウザのシステム導入が必要。	アクセス先をクラウドサービスに絞ることで、セキュリティの確保が比較的容易。万が一不正なコードやファイルをダウンロードした場合でも、隔離された領域でブラウザが稼働するため端末の安全性が確保される。	（同上）	（同上）	今回のヒアリングにおいて、電カル端末からインターネット参照を実現するために採用している医療機関が一定数存在した。また、今後セキュアに電カル端末からインターネット上の医療クラウドサービスへのアクセス需要が増えると考えられる。 そのため、安全なファイル授受の機能も利用可能なセキュアブラウザは、今後の評価対象の一つとして有力な候補であると考える。
⑨仮想デスクトップアクセス（クラウド事業者側で用意）	比較的利用しやすい。 ただしVDIの種類によっては、端末に専用ソフトウェア導入が必要。	アクセス先をクラウドサービスに絞ることで、セキュリティの確保が比較的容易。 またVDIでの作業となるため、端末側の安全性が確保される。	VDIシステムを準備する必要があるため、この接続形態を採用するクラウド事業者は多くないことが想定される。	VDIシステムのパッチ適用などセキュリティ維持は必須。	広く展開するクラウドサービスとして、実際の採用は稀であることが想定されるため、PoC対象から除外。

図 8 次年度評価対象一覧（接続形態）

F. 健康危険情報

包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　医療機関へのネットワークセキュリティ事前アンケート内容

回答者の情報	本アンケートの回答を頂く病院名と部署名を記入してください。	（記入欄）
	本アンケートの回答者の職種を教えてください。①②の場合は○、③の場合は記入お願いします。	①医師 ②情報システムの担当者 ③それ以外の場合は自由記載してください （③の記入欄）
病院基本情報	（ア）該当する病床数を○につけてください。 ①50床未満　②　50～100床未満　③100～200床未満　④200～400床未満　⑤400～600床未満　⑥600～800床未満　⑦800床以上	
	（イ）1日の平均外来来院数に○をつけてください。 ①50人未満　②　50～100人未満　③100～200人未満　④200～400人未満　⑤400～600人未満　⑥600～800人未満　⑦800人以上	
	（ウ）機関・組織に○をつけてください。 ①病院　②有床診療所　③無床診療所　④健診施設	
	（エ）開設主体に○をつけてください。 ①厚生労働省　②独立行政法人国立病院機構　③国立大学法人　④独立行政法人労働者健康安全機構　⑤国立高度専門医療研究センター ⑥独立行政法人地域医療機能推進機構　⑦都道府県、市町村、地方公共団体の組合　⑧国民健康保険団体連合会及び国民健康保険組合 ⑨日本赤十字社　⑩社会福祉法人恩賜財団済生会　⑪厚生農業協同組合連合会　⑫社会福祉法人北海道社会事業協会 ⑬全国社会保険協会連合会　⑭厚生年金事業振興団　⑮船員保険会　⑯健康保険組合及びその連合会 ⑰共済組合及びその連合会　⑱国民健康保険組合　⑲私立学校法人　⑳公益社団法人　㉑公益財団法人　㉒社会医療法人 ㉓社会福祉法人　㉔医療法人　㉕医療生協　㉖会社　㉗個人　㉘その他の法人	
	（オ）病院機能に○をつけてください。 ①特定機能病院　②地域医療支援病院　③臨床研究中核病院　④国立高度専門医療研究センター（National center） ⑤がん診療連携拠点病院　⑥救急医療　⑦へき地医療拠点病院　⑧災害拠点病院　⑨エイズ診療拠点病院　⑩総合周産期母子医療センター	
	（カ）該当する診療科区分に複数○をつけてください。 ①内科　②心療内科　③精神科　④神経科　⑤呼吸器科　⑥消化器科　⑦循環器科　⑧アレルギー科　⑨リウマチ科　⑩小児科 ⑪外科　⑫整形外科　⑬形成外科　⑭美容外科　⑮脳神経外科　⑯呼吸器外科　⑰心臓血管外科　⑱小児外科　⑲皮膚泌尿器科 ⑳性病科　㉑肛門科　㉒産婦人科　㉓眼科　㉔耳鼻咽喉科　㉕気管食道科　㉖リハビリテーション科　㉗放射線科　㉘神経内科 ㉙胃腸科　㉚皮膚科　㉛泌尿器科　㉜産科　㉝婦人科　㉞呼吸器内科　㉟循環器内科　㊱歯科　㊲歯科矯正科　㊳小児歯科 ㊴糖尿病科　㊵腎臓内科　㊶腎移植科　㊷血液透析科　㊸代謝内科　㊹内分泌内科　㊺救急医学科　㊻血液科　㊼血液内科 ㊽麻酔科　㊾消化器内科　51消化器外科　52肝胆膵外科　53糖尿内科　54大腸肛門科　55眼形成眼窩外科　56不妊内分泌科 57膠原病リウマチ内科　58脳卒中科　59腫瘍治療科　60総合診療科　61乳腺甲状腺外科　62新生児科　63小児循環器科	
	（キ）システム導入状況に○をつけてください。 ①医事会計システムを導入 ②オーダリングシステムを導入 ③電子カルテシステムを導入 ④電子レセプトオンライン請求を導入 ⑤マイナンバーカードの健康保険証利用のためマイナ受付の導入 ⑥電子処方箋の導入 ⑦外注検査依頼と結果のオンラインサービス ⑧遠隔読影のオンラインサービス ⑨その他院内のシステムと外部接続しているサービスがあれば自由記載	①導入済　②検討中　③未導入 ①導入済　②検討中　③未導入 ①導入済　②検討中　③未導入 ①導入済　②検討中　③未導入 ①導入済　②検討中　③未導入 ①導入済　②検討中　③未導入 ①導入済　②検討中　③未導入 ①導入済　②検討中　③未導入 （記入欄）
	（ク）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を知っていますか。（https://www.hospital.or.jp/site/news/file/1686540766.pdf） 該当箇所に○をつけてください。	①知っている　②知らない
	（ケ）サイバーセキュリティ対策チェックリストの記入しましたか。該当箇所に○をつけてください。	①記入した　②記入中　③記入していない
	（コ）サイバーセキュリティ対策チェックリストの対応状況はいかがですか。該当箇所に○をつけてください。	①全て○がつけられた ②一部○がつけられておらず、順次対応予定 ③一部○がつけられておらず、対応検討中 ④一部○がつけられておらず、対応できそうにない
	（シ）サイバーセキュリティ対策チェックリストを記載している医療機関において、チェックリストを本プロジェクトに公開していただくことは可能ですか。該当箇所に○をつけてください。	①可能 ②WEB会議で投影のみで説明だけであれば可能 ③不可能
	（ス）医療機関の中に、電子カルテシステム等の院内担当者はいますか。該当箇所に○をつけてください。	①医療情報部/情報システム課のような形で専属の部や室がある ある場合は、在籍人数を教えてください。（　　名） ②総務部や経理部といった部のメンバーが担当している システムを担当されている方は何名ですか。（　　名） ③院長が責任している ④その他（　　） ⑤全くいない。
	（セ）上記（ス）でカウントされた方の中に、セキュリティに詳しい人材はいますか。該当箇所に○をつけてください。	①自らセキュリティ対策を自発的に考え、委託しているシステムベンダーと会話することができる。 ②資格は有していないが、委託をしているシステムベンダーが言ったことを理解できる、 または学会等に参加する中で情報を得ている人数 ③委託しているシステムベンダーの言っていることをそのまま信用して対策を講ずるしか手段がない。 ④その他（　　）
	（ソ）セキュリティの外部資格を有している人材がいましたら何人いますか。該当箇所に○をつけてください。 セキュリティの外部資格候補例は以下です。 ・情報処理安全確保支援士試験 ・情報セキュリティマネジメント試験 ・SPREAD情報セキュリティサポーター能力検定 ・SPREAD情報セキュリティマイスター ・情報セキュリティ管理士認定試験 ・金融情報セキュリティマネージャー	①1名 ②1名程度 ③1名以上（この場合は＿＿名在籍） ④0名
	（タ）医療機関内で、セキュリティ監査を行っていますか。該当箇所に○をつけてください。 セキュリティ監査とは、病院が保有する情報資産を守るために正しく対策がとられているかを、第三者的な目線でチェックすることです セキュリティルール、組織のガイドラインを用意し、 セキュリティ対策を正しく実施し機能しているかを定期に検証や評価を行うことをいいます。	①はい、行っている ②いいえ、行っていない ①と回答した場合は、どのような形で監査しているか簡単でよいので記載してください （記入欄）
	（チ）医療機関内で、リスクアセスメントを行っているますか。該当箇所に○をつけてください。 リスクアセスメントとは、病院が抱える情報資産に対するリスクの洗い出しや分析、評価を行い、許容できるかどうかを決めるプロセスのことを表します。	①はい、行っている ②いいえ、行っていない ①と回答した場合はどのような形でリスクアセスメントしているか簡単でよいので記載してください （記入欄）
	（ツ）医療機関内で、BCPの対策は上っていますか。該当箇所に○をつけてください。 BCPとは、医療施設の災害対応のための事業継続計画を指します。	①はい、厚生労働省の医療施設の災害対応のための事業継続計画に基づいて、 または自院内の個別ルールに基づいてBCP対策を行っている、もしくは計画中である。 ※①は、院内に災害対策委員会等の常設、災害対策本部の立ち上げルール、 災害対策マニュアルの整備といったシステム外の対策がメインとなる質問です。 ②はい、①まではできていないが、システムバックアップ等の保管場所の工夫や、クラウドを利用した参照用のシステムを構築しており、システム面では診療を続けられる対策がとれている。 ③いいえ、①・②ともに行っていない ①②と回答した場合は、どのような形でBCP対策を行っているのか簡単に記載してください （記入欄）
	（テ）医療機関内で、ハイブリッドクラウドを採用していますか。該当箇所に○をつけてください。 ハイブリッドクラウドとは、パブリッククラウド、プライベートクラウド、院内の物理サーバを組合せて使うクラウドのことです。	①はい、採用している ②検討したが、採用はしていない（検討したものを簡単でよいので記載してください） ③聞いたことがあるが、具体的に検討をしたことがない ④初めて聞いた言葉である ①②と回答した場合は、どのようなソリューションを検討されたのか簡単に記載してください （記入欄）
	（ト）医療機関内で電子カルテの診療系ネットワークにおいて外部との通信している個所はどのようものがありますか。該当箇所に○をつけてください。 電子カルテが使えるネットワークを診療系ネットワークと表現しています。	①昼夜メンテナンス時に委託会社がアクセスするため接続方法について （接続方法はご存じの場合、閉域網、HW-VPN、SW-VPN、LTE、モバイル、その他） ①で答えた場合は、どのシステムが回線で接続されているのか記載してください。 （記入欄）サンプル　電子カルテシステムは閉域網、PACSはHW-VPN、リハビリシステムはSW-VPN ②マイナンバーカードによるオンライン資格確認のため ③レセプトオンライン提出のため ④クラウドサービス利用のため ①と回答した場合は、どのような外部クラウドサービスを使われているのか記載してください。 （記入欄） ⑤地域連携用に外部とのアクセスがある ⑥電子カルテの診療系ネットワークにて、他に外部との通信を行っているものがある ①と回答した場合は、どのような用途で使われているのか記載してください。 （記入欄）
	（ナ）医療機関内で、医療AIサービス利用状況を教えてください。該当箇所に○をつけてください。	①利用している（利用している場合は、商品名を記載してください。） ①-1　オンプレで利用しているか　商品名（　　） ①-2　クラウドで利用しているか　商品名（　　） ①-2-1　クラウド利用に踏み切った際に、注意した事項はなにかありますか。 （記入欄） ①-2-2　クラウド利用を行うにあたり、医療機関内で反対の声はありましたか。 （記入欄） ②検討中である ②と回答した場合は、どのような外部クラウドサービスを検討されているのか記載してください。 （記入欄） ③興味があるが、利用まで至っていない ④聞いたことがない
	（ニ）医療機関内で、職員や患者のスマートフォン等BYODを利用されているケースはありますか。該当箇所に○をつけてください。 BYODとは、業務に個人のスマートフォンやパソコンを持ち込んで利用する捉えてください。	①利用している ①で利用している場合は、サービス名もしくは用途を教えてください。（　　） ②検討中である ②で検討中場合は、サービス名もしくは用途を教えてください。（　　） ③利用していない
	（ヌ）医療機関内から外部に出ている点を中心にヒアリング時にネットワーク構成を教えて頂けますか。該当箇所に○をつけてください。	①ヒアリング時に説明してもよい ②ネットワーク構成のお話しはできない。 ②の場合は、なぜできないか可能な範囲で教えてください。 （記入欄）
	（ネ）電子カルテを含めた医療情報システムのクラウドシフトや今後の方針について、思われることを簡単でよいので記載してください。	（記入欄）

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

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 3 種類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になった。

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。

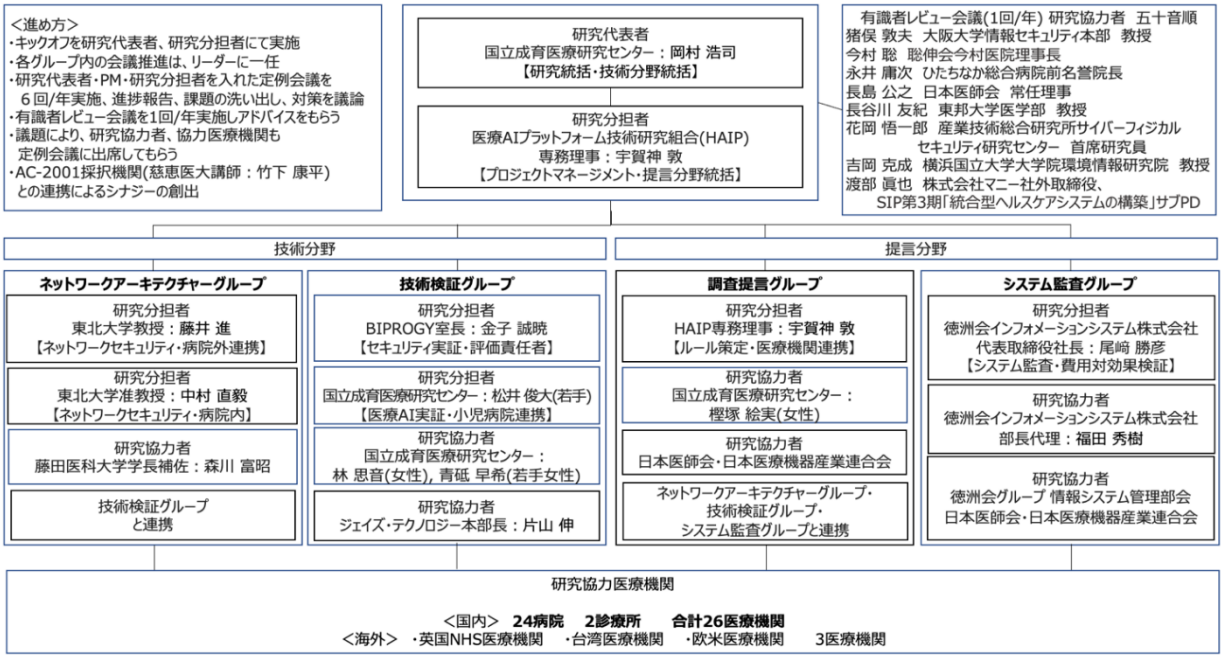
本研究は、医療機関の類型化に基づいた最適なネットワークセキュリティ構成やシステムセキュリティ監査のルールを示す事により、全国の医療機関が安全、安心かつリーズナブルな費用で医療 AI サービスが利用できることを目的とする。

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。

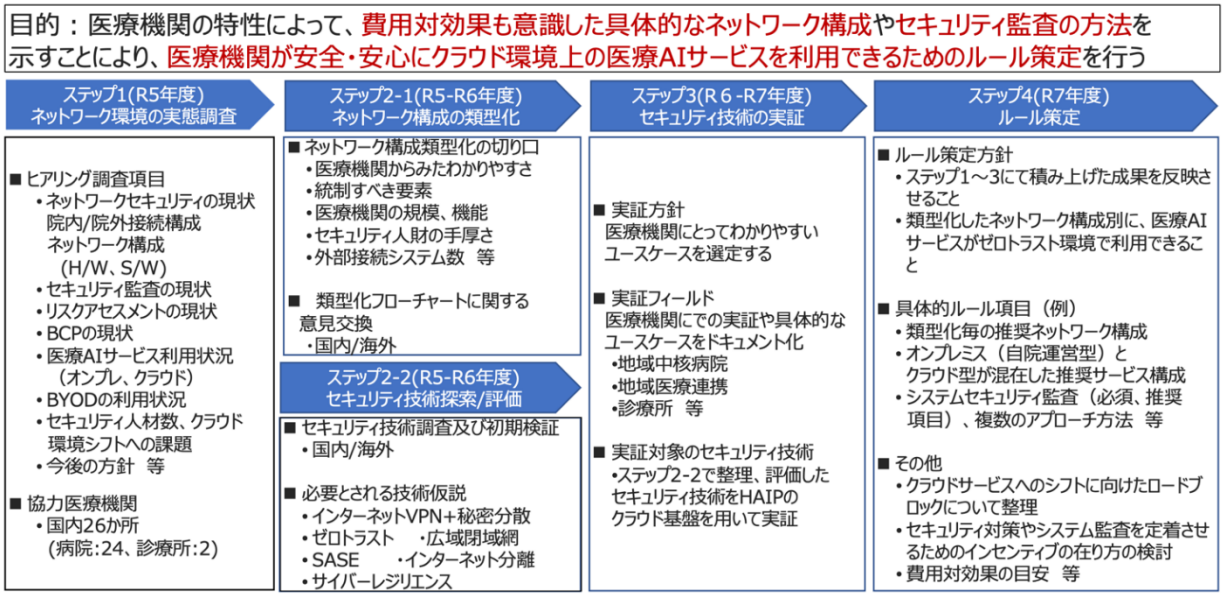
（2） 医療機関の選定及び調整

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（計画時は 20）であるが、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



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

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。さらに、医療機関のシステム構成を技術面から 3 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。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。

F. 健康危惧情報

総括研究報告書に記載

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　ヒアリングに協力頂いた医療機関名称

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	飯塚病院	福岡県飯塚市	1048	会社
4	大阪赤十字病院	大阪府大阪市天王寺区	883	日赤
5	横須賀共済病院	神奈川県横須賀市	740	共済組合
6	国立国際医療研究センター	東京都新宿区	719	国立
7	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
8	国立成育医療研究センター	東京都世田谷区	490	国立
9	越谷市立病院	埼玉県越谷市	481	公立
10	恵寿総合病院(*1)	石川県七尾市	426	民間
11	淡海医療センター	滋賀県草津市	420	民間
12	仙台病院	宮城県仙台市泉区	384	JCHO
13	済衆館病院	愛知県北名古屋市	331	民間
14	みやぎ県南中核病院	宮城県大河原町	310	公立
15	日立製作所ひたちなか総合病院	茨城県ひたちなか市	302	会社
16	仙台徳洲会病院	宮城県仙台市泉区	250	民間
17	練馬総合病院	東京都練馬区	224	公益財団法人
18	生駒市立病院	奈良県生駒市	210	公立
19	賛育会病院	東京都墨田区	199	社会福祉法人
20	公立刈田総合病院	宮城県白石市	199	公立
21	板橋区医師会病院	東京都板橋区	192	医師会
22	JR 仙台病院	宮城県仙台市青葉区	164	会社
23	博愛会病院	福岡県福岡市中央区	145	民間
24	豊橋ハートセンター	愛知県豊橋市	130	民間

(*1)24/1/1　能登半島地震のため、事前アンケート調査票のみ入手

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。R 5 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えたと考える。

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 版に準拠するよう、システム監査で用いる「システム監査チェックシート」上の監査項目の再編を行った。さらにＲ５年度に実施した徳洲会グループ３病院でのシステム監査結果のフィードバックからも監査項目や監査方法の見直しを実施した。

C. 研究結果

１．監査チェックシートの再編

① 厚労省ガイドラインの反映

厚労省ガイドラインの改定ポイント・内容を運用管理規程に反映させ、そこから特に重要と考えるものを監査チェックシートの項目として採用した。その一例を示す。

表１　システム監査チェックシート（抜粋）

	チェック内容	チェック対象資料等	資料提出	結果	監査員コメント
2	情報システム委員会が設置され各部署から委員が選出されている	①組織図 ②役務任命簿	事前	○	問題ない
11	不要な電子カルテのユーザIDの残存有無が定期的に確認されている	不要な電子カルテのユーザIDの存在有無の点検が行われたことが確認できる資料 （別紙9_ID・権限棚卸結果報告書・別紙10_ID・権限棚卸結果管理書 等）	事前	×	退職時に総務課で利用者マスタに退職チェックを入れる運用だが、定期的な棚卸しは行われていない
15	ウイルス対策ソフトは適正なライセンス数を購入し、サーバおよび端末にインストール、定義ファイルを定期的に更新している	①ウイルス対策ソフトのライセンス購入と本数が確認できる資料 ②端末管理台帳 ③ウイルス対策ソフトのパターンファイルの日付が確認できる画面	事前および当日	△	アンチウイルスのライセンス数が端末数より少ない/実際にアンチウイルスがインストールされていない端末がある
18	端末からデータを抜き出せない設定を行っている	①USBメモリ/CD等の制御設定が確認できる画面のハードコピー （ActiveDirectory ・ESET） ②USBメモリ利用許可端末の一覧等（部署名・用途が記載されたもの）	事前および当日	△	ActiveDiretoryの設定は適正だが、アンチウイルスの入っていない端末では任意のUSBメモリを差すことが可能な状態
22	ランサムウェア等のウイルスの感染が発生した際の初動対応が周知されている	①ランサムウェア感染時の初動対応が記載された資料（ランサムウェア感染時：対応チェックリスト 等） ②その周知方法が確認できる資料	事前および当日	○	各部署に『ランサムウェア感染時対応チェックリスト』が配付され、現場の職員にも周知されている

厚労省ガイドライン：災害、サイバー攻撃、システム障害等の非常時における対応や対策

監査チェックシート：項番 22『ランサムウェア等のサイバー攻撃が発生した際の初動対応が周知されている』

厚労省ガイドライン：ネットワーク境界防御型思考／ゼロトラストネットワーク型思考

監査チェックシート：項番 24『医療機器保守用回線のネットワーク機器（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』

また厚労省から出されたチェックリストを監査でも有効活用すべく、次の項目も追加した。

監査チェックシート：項番 25『【厚生労働省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】は医療機関確認用と事業者確認用が作成、保管されている』

② 監査項目内容・項目数の変更

従来院内 SE の業務内容なども含めていた監査項目をサイバーセキュリティ／セーフティ関連のものに絞り、また 1 項目をより深く見て議論でき、かつ監査を効率的に実施できるよう項目数を従来の 70 → 50 とした。

③ 準備資料等の明確化

病院側の準備と監査がスムーズに行えるよう、監査で確認する書類や写真等を監査チェックシートの添付資料として具体的に提示した。

2．監査方法の見直し

① 事前のオンライン面談実施

従来は病院から事前に提出された資料等にもとづき文書監査を行い、その後現地監査を実施していた。今年度は文書監査後に監査メンバーと病院 SE で状況と課題を共有するオンライン面談を試行、これにより病院側の理解が深まり、現地監査の円滑化にも繋がった。

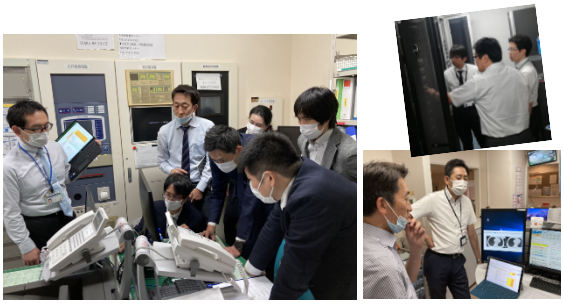


図 1　システム監査：現地監査の様子

② 監査報告提出後の改善フォロー実施

従来は現地監査後に監査報告書を送付し、病院はこれにもとづき指摘事項の改善作業を行っていた。しかし病院側の理解が不十分で改善になかなか手を付けられないなどのケースがあったため、監査報告提出後に監査メンバーと病院 SE で指摘された項目の改善方法やスケジュール、支援の方法などについてオンラインで話し合う場を持った。これにより改善作業がより円滑に開始・実行されるようになったと考える。

表 2　システム監査結果報告書（抜粋）

2．監査結果概要

監査は計 50 の項目について実施しました。カテゴリごとに『充足』『一部充足』『未充足』の 3 段階で評価（運用ルールはあるが実績がないものは『該当なし』）を行い、結果は次のとおりです。
このうち『未充足』の 3 項目と『一部充足』の 9 項目については次の 3．指摘事項 にその内容を記載しています。

監査カテゴリ／監査項目数		監査結果			
カテゴリ	項目数	充足 項目数	一部充足 項目数	未充足 項目数	該当なし 項目数
管理体制	3	2	1	0	0
個人情報保護対策	3	3	0	0	0
セキュリティ管理（管理者権限）	2	1	1	0	0
セキュリティ管理（アプリケーション）	6	4	2	0	0
セキュリティ管理（サーバ・端末）	6	5	0	0	1
セキュリティ管理（サイバー攻撃対策等）	5	4	1	0	0
パスワード管理	3	3	0	0	0
文書・マニュアル等の管理	7	5	1	1	0
サーバ運用	9	4	3	2	0
端末運用	4	4	0	0	0
システム管理室関連	2	2	0	0	0
	計 50 項目	計 37 項目	計 9 項目	計 3 項目	計 1 項目

（指摘事項：計 12 項目）

3．3　指摘事項の詳細

【未充足項目】

カテゴリ／項番	問題・課題と改善策	指摘事項の内訳
文書・マニュアル等の管理／項番 30	◆電子カルテ等院内システムがダウンした際の訓練が実施され、手順の見直しが定期的に行われている： 電子カルテ等が利用不能となったことを想定した訓練が行われておらず、有事に診療の継続等対応が適切に行えない可能性がある。 → サイバー攻撃やシステム障害に備え（また R6 年度より診療録管理体制加算 I の要件となったことも合わせ）、システムダウン時の訓練を実施し、その結果に基づく手順の見直しを行ってください。その後、訓練が実施されたこと・手順の見直しを行ったことが確認できる資料を提出してください。	①
サーバ運用／項番 38	◆サーバのバックアップは適切に取得・保管されている： 電子カルテサーバのデータバックアップは取得されているが、システム管理者がその世代管理や保管場所等を十分把握できておらず、障害時に円滑な対応ができない可能性がある。SE 部会提供の資料も参考にバックアップ運用について把握しておくことが推奨される。 → 電子カルテサーバのバックアップ運用を理解し、それを示した資料を提出してください	①
サーバ運用／項番 42	◆サーバ室は災害時に被害を受けにくい場所にある： 電子カルテサーバ等が設置されたサーバ室が地下 1 階にあり、浸水等により電子カルテが利用不能となることが考えられる。 → 現在各システムサーバの 5 階への移設が進められており、電子カルテサーバの移設も検討し移転時期やサーバラック内の設置予定場所等を示した計画書を提出してください。	①

【一部充足項目】

カテゴリ／項番	問題・課題と改善策	指摘事項の内訳
管理体制／項番 3	◆情報システム委員会は月 1 回程度開催され、機能している： コメディカル部門から新たに委員を選出し適切な体制となったが、新体制による委員会がまだ開催されていない。 → 新体制による委員会の 2 回分の議事録（必要な署名あるいは押印がされたもの：PDF）を提出してください。	③
セキュリティ管理（管理者権限）／項番 7	◆管理者 ID（サーバ OS の ID や電子カルテのスーパーユーザ等）は必要最低限の ID のみが登録されている／また不要な管理者 ID の残存有無が定期的（年 1 回程度）に確認されている： 管理者 ID（電子カルテのスーパーユーザー等）の棚卸しが行われておらず、必要のない職員に大きな権限が付与されたままになる可能性がある。 → 運用管理規程：別紙 9【ID・権限棚卸結果報告書】および 10【ID・権限棚卸結果管理表】にもとづき管理者 ID の棚卸しを行い、これらの書類（必要な署名あるいは押印がされたもの：PDF）を 1 部ずつ提出してください。	①

D．考察

「C.1．監査チェックシートの再編」においては厚労省ガイドライン第 6.0 版の内容の反映、項目内容と項目数の見直し、準備資料等の明確化を行うことでより Up to Date かつ効果的・効率的なチェックシートとすること

ができた。また「C.２．監査方法の見直し」では、事前のオンライン面談と監査報告提出後の改善フォローを通じて病院と監査員とのコミュニケーションの機会を増やしたことにより、監査をスムーズに行えるようになっただけでなく、病院がサイバーセキュリティの重要性や課題の理解を深めることにも繋がったと考える。

E. 結論

Ｒ５年度はこれまで徳洲会グループで実施してきたシステム監査について監査項目や方法の見直しを検討、見直した内容にもとづいた監査を行い、フィードバックを実施というサイクルで継続的なブラッシュアップを行った。次年度の徳洲会グループ以外の病院でのシステム監査実施、つまり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。

F. 健康危惧情報

総括研究報告書に記載

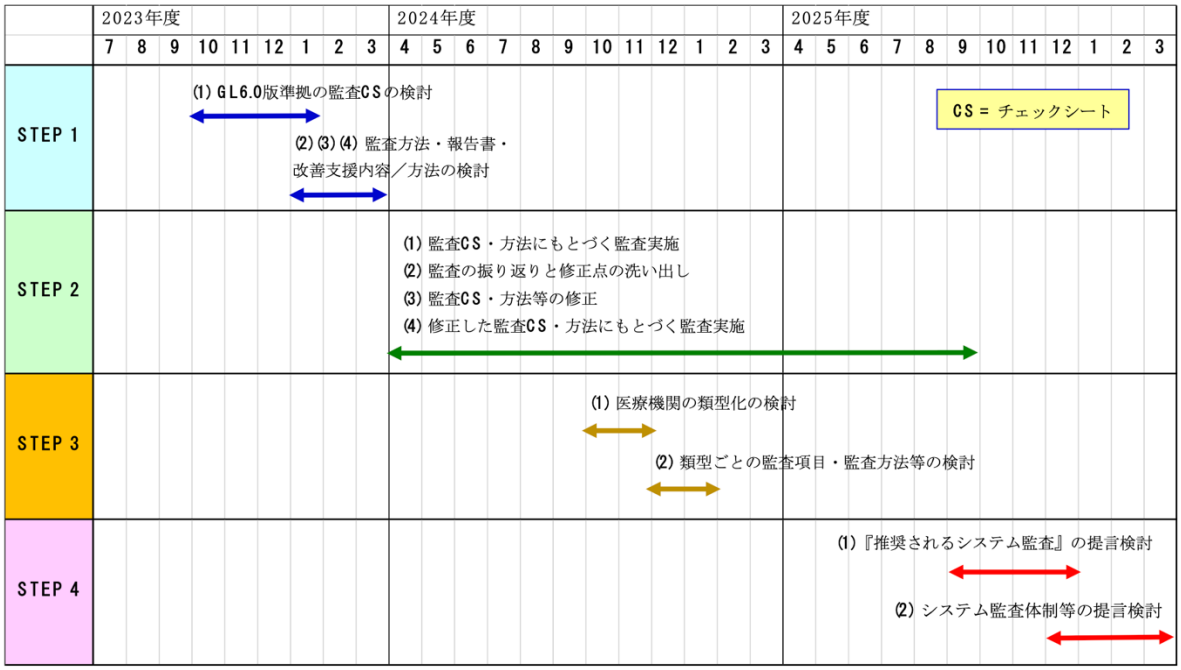
G. 研究発表

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

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

ディープラーニングを中心とした人工知能の発展は医療にも大きな影響を与え、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等により、医療の質や効率の向上だけでなく、地域格差の解消、医療従事者の負担軽減など多岐にわたる検証が進められている。国立成育医療研究センターでは 2018 年の AI ホスピタル事業採択を機に、研究所の研究者、病院の医師だけでなく、全ての職員を対象としたデータサイエンスの啓蒙、教育活動からスタートし、顕微鏡写真からの感染症起因菌同定支援、病理画像のグレーディング支援システムなどの開発を行い、実際の診療における補助手段としての試用も開始した。クラウドシフトによる大小さまざまな医療機関からの利用を見据え、医療 AI プラットフォーム技術研究組合との協力体制でこれらウェブアプリケーションのコンテナ化と仮想デスクトップ基盤を介した安全な通信環境の構築も行い、最終的な目標は、各医療機関の電子カルテ端末からこのようなサービスを自由に、かつ安全に利用できるようにすることである。しかしながら、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高まり、個人情報保護や患者不利益等への配慮がますます求められる状況にあっては、従来からの境界型防御に加え、ゼロトラストを前提としたシステム構築を避けることはできない。それだけでなく、信頼されうる安全性の実証が不可欠であり、かつ現状の最大の課題ともなっている。安心できる環境の実現は、患者および市民参画をも促し、ビッグデータに依存する医療 AI のさらなる発展を期待することもできる。本研究では、感染症起因菌同定支援サービスの開発、クラウドからの公開、そしてユーザが安全かつ信頼性の高い環境下で利用できるように SASE アーキテクチャの試験的な導入、さらにはセキュアなブラウザ経由での利用を想定したインターネット分離を実装し、電子カルテ端末から医療 AI サービスを安全に、そして安心してアクセスできる環境を整えるための技術検討を行い、現状の課題を明確にした。

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、一体となって医療 AI サービスの開発を進めてきた。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。今回、NCCHD で開発を進めていた感染症起因菌同定支援のサービスをコンテナ化し、HAIP の医療 AI プラットフォームから公開することを試みた。

独自サービスを用意することで、安全な利用環境の検討にさまざまな最先端技術を試すこともできる。本研究では、環境をサーバ上に集約させる仮想デスクトップ基盤(VDI)、ゼロトラストの一ソリューションである SASE、またセキュアブラウザを利用するインターネット分離を取り上げ、いずれ実現させたい電子カルテ端末からの医療 AI サービス利用を検討した。

B. 研究方法

感染症起因菌同定支援においては、NCCHD における小児菌血症患者の検体から 23,753 画像の顕微鏡写真データを取得し、Microsoft VoTT を利用して 347,234 箇所を手作業で切り出し、16 種類の細菌真菌を区別するアノテーションを行った。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 形式への出力は Python スクリプトを用いた。

最初に 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、起因菌の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 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 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。

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、細菌感染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 真菌を物体検出で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 画像から 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)。

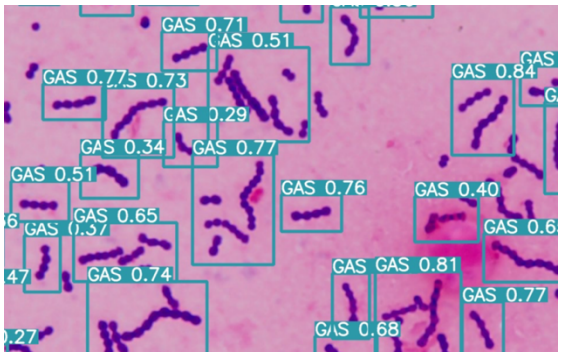


図 1.化膿レンサ球菌の検出

検出モデルをウェブサービスに組み込み、ブラウザからの画像データアップロードで瞬時に、かつインターネット接続ができればどこからでも結果が得られる仕組みを作り上げた。そして Docker によりコンテナ化を行い、作成したコンテナがオンプレミスに加え、AWS でも動作することを確認し、扱う医療データを安全にやり取りする目的で、HAIP サービス基盤が導入している Microsoft Azure の VDI 環境で公開することができた。利用可能ユーザは限定しているものの、申請があれば誰でも利用できる体制を整えた。

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)。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、直結されたクラウド側に存在するウェブカメラでのデータ扱いとなる。

図 2. VDI でクラウドのウェブカメラを利用

さらにクラウド環境のネットワークアクセスの安全性を確保するため、ゼロトラストの一ソリューションである SASE を導入することとし、実際には Cato Networks 社がサービスを展開している Cato SASE クラウドプラットフォーム（CATO)の調達を行い、利用できる環境が整った。またセキュアブラウザを利用するインターネット分離については、ジェイズ・テクノロジー社の RevoWorks を調達し、セキュリティ対策の選択肢を増やした。このような状況で NCCHD の電子カルテネットワークでの試用を打診したが、残念ながら一時的な利用であっても許可は得られていない。

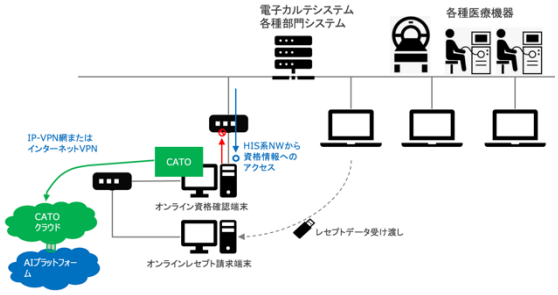


図 3. SASE として CATO の導入

D. 考察

感染症起因菌同定支援システムは臨床検査技師をはじめとする医療関係者の力量を上回る結果が出ている一方で、訓練データが単一機器から習得されていることもあり、他施設で期待したほどの認識精度が得られていないという実態がある。実装可能であることは示すことができたが、社会実装を進めるためには、より広範囲なビッグデータの収集が必要になる。

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。このような状況に対し、サーバレスアーキテクチャを採用した場合、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できる可能性がある。サーバのセットアップ、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はずで、さらにはアイデンティティベースの認証など、ゼロトラストの考え方と一致する面もある。次年度の取り組みとして検討を進める必要があると考えている。

E. 結論

クラウド上の医療 AI サービス利用促進のためのネットワークセキュリティ構成をゼロトラストの観点も含めて提案し、電子カルテネットワークあるいは電子カルテ端末からの利用を試したいと考えていたが、境界型防御を通してきた電子カルテのネットワークを改変することは、技術面だけでなく、セキュリティに対する不安や、管理者の責任問題から非常に困難である現状が明らかとなった。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、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。また、ゼロトラストの言葉をもって管理者、さらには患者や市民に安心を与えられる状況ではない。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

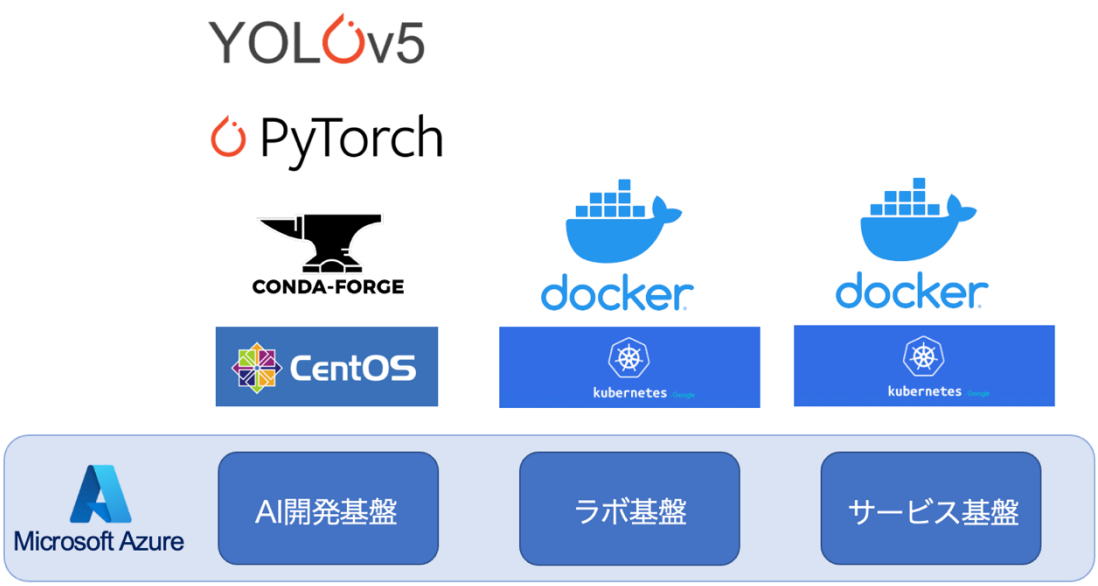
G. 研究発表

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

H. 知的財産権の出願

なし

資料　医療 AI プラットフォームにおける開発基盤



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）

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, 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* **Vol.282 No.10**: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* **Vol.58 No.2**:45–50, 2022

藤井 進（研究分担者）

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）

植松直哉, 真辺篤, 福田秀樹, 藤村義明, 髙橋則之, 尾﨑勝彦, 大橋壮樹, 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** No.7, 2022

松井 俊大（研究分担者）

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. 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 6 年 11 月 30 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 5 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 6 年 11 月 30 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 5　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。

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 6 年 11 月 30 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 災害科学国際研究所長

氏　名 栗山 進一

次の職員の令和 5　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）　災害科学国際研究所 ・ 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 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 6 年 11 月 30 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 5　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 6 年 11 月 30 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 5　　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）　尾崎 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 6 年 11 月 30 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 5 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。

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 6 年 11 月 30 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 東北大学病院長

氏　名 張替 秀郎

次の職員の令和 5　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）　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 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。