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

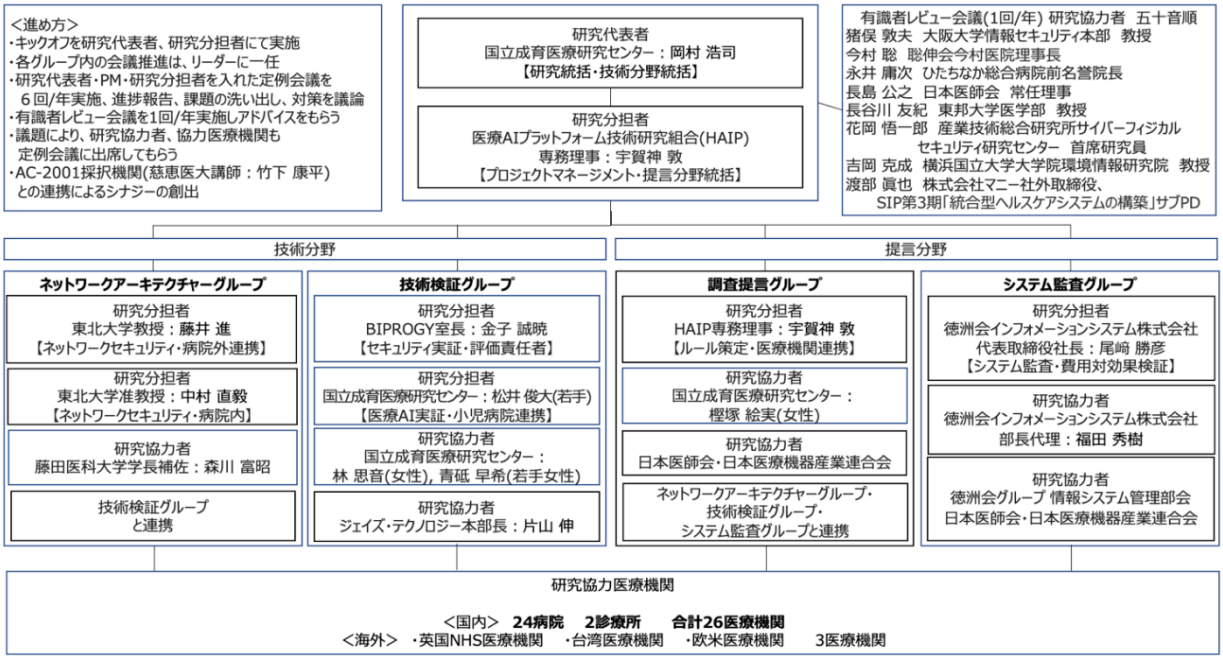
国内 24 の医療機関に対し、アンケートによる事前調査を行なった上で、対面によるネットワークセキュリティのヒアリングを実施する。そこで得られた規模に応じた機能、セキュリティ人材の有無、外部接続システム数などに関する情報を基にネットワーク構成の類型化を行い、クラウドシフトを加速するための課題を明らかにする。

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。

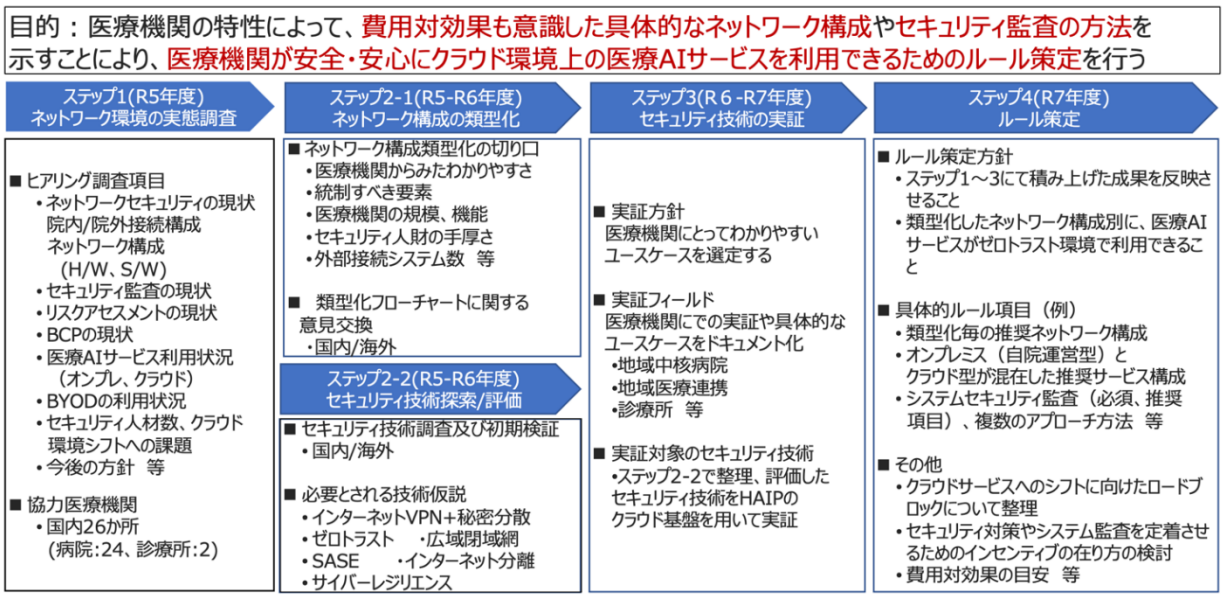
（2） 医療機関の選定及び調整

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