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）

R7 年度　分担研究報告書（調査提言グループ・プロジェクトマネージャ）
クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言

分担研究者　宇賀神　敦　医療 AI プラットフォーム技術研究組合　理事長

研究要旨

医療従事者の働き方改革や医療の均てん化を実現するためには、医療従事者と医療 AI との協調が鍵となる。質の高い医療データに基づいて開発された医療 AI サービスが次々に生まれているものの、幅広い医療機関で利用されているとは言い難く、クラウドの利用に加えて利用しやすい価格設定が不可欠である。本研究では、医療機関のセキュリティの実態を把握するために、医療機関の設立母体、病床数、地域などの特性を踏まえて、24 病院、2 診療所の合計 26 医療機関に対して 2 段階で調査を行った。Step1 は、対面でのヒアリング実施前にアンケート調査票を対象の医療機関に送付して、訪問前に回答を入手し回答内容の確認を行った。Step2 は、アンケート調査の回答内容を正しく理解した上で、各医療機関に直接訪問してヒアリングを実施した。2 段階のプロセスを踏むことで、対面のヒアリングを効率的かつ深く掘り下げることが可能となり確認すべき内容を明確にすることができた。訪問に際しては、本研究班の技術検証グループに必ず同行してもらい、技術的な深掘りを行うと共に一部の医療機関のサーバ室を見学した。また一部のヒアリングには厚生労働省厚生科学課の担当官も同席し医療現場が抱える課題を直接聞いてもらった。今後の政策立案に少しでも役立つことを期待したい。この調査を通して、医療機関の ICT 導入状況、ネットワーク構成、人員体制、リスクアセスメント実施状況、システムセキュリティ監査状況、保健所によるセキュリティ立ち入り検査対応状況などの実態、医療現場が抱える課題等を把握することができた。さらに、医療機関のネットワーク構成をセキュリティガバナンスの点から 4 段階に類型化しそれぞれのセキュリティ対策を整理した。医療機関は平均して 100 床あたり 1 名のシステム要員で電子カルテシステムの導入、運用、トラブル対応やセキュリティ対策を実施しており、リソース不足が顕著である。また、新しい知識を吸収する時間が確保出来ない事やベンダーへの依存体制が顕著である事などが浮き彫りになった。さらに、医療機関に有益なユースケースのヒアリング調査のために追加で 2 医療機関の協力を得た。ユースケースについては、技術検証グループにてその成果をまとめた。

本成果を基に、以下に示す提言策定を行った。提言の構成は、アセスメント - 対策 - 監査 - 訓練 - 人材育成・意識改革のそれぞれの項目について、ツールの準備、具体的なユースケース、システムセキュリティ監査の具体的手法を示している。また、これらの PDCA サイクルを定期的かつ継続的に実施するために必要となる制度的支援についても言及した。

A. 研究目的

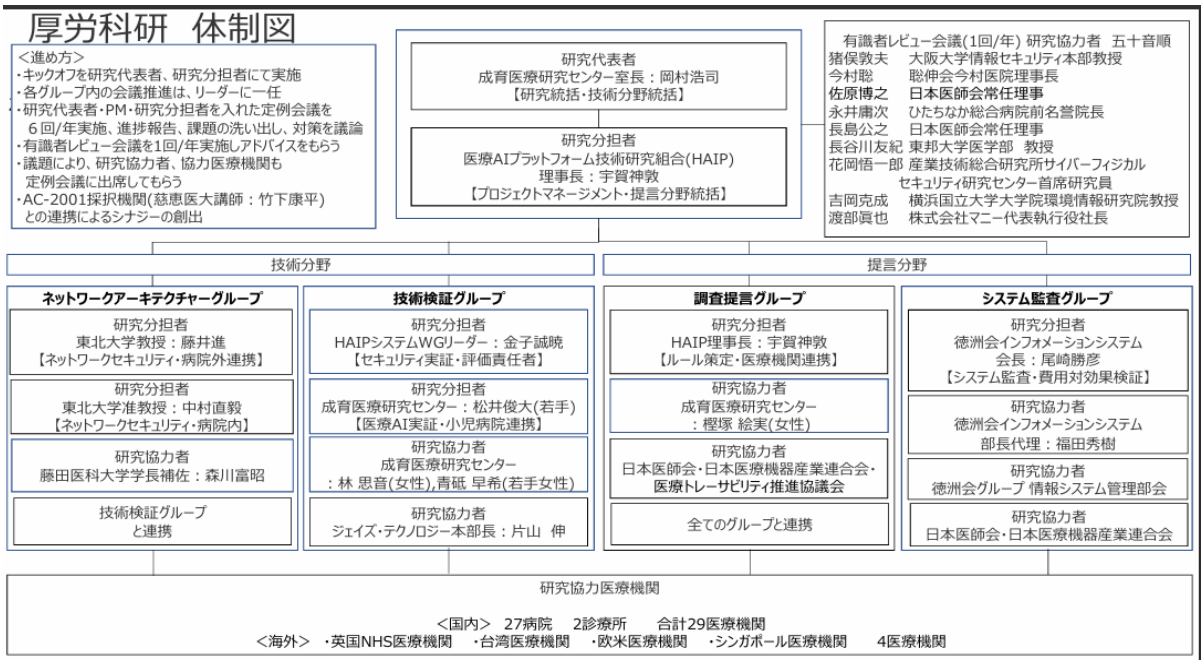
医療 AI は、深層学習による画像認識の飛躍的な精度向上により医療への有用性が示され、国内では内閣府による AI ホスピタル事業にて医療の質向上や医療従事者の負担軽減などの実証が進められた。一方で、医療機関における医療 AI サービスの利用は 10%程度との報告もあり、まだまだ導入が進んでいない。医療の提供環境にも変化が起こっている。ひとつは、2024 年 4 月から開始された医師の時間外労働の上限規制（年間９６０時間）による医療従事者の働き方改革であり、もうひとつは、2025 年に全人口の 18%（2180 万人）が後期高齢者となることに起因する医療・介護の担い手不足の深刻化である。今後医療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。

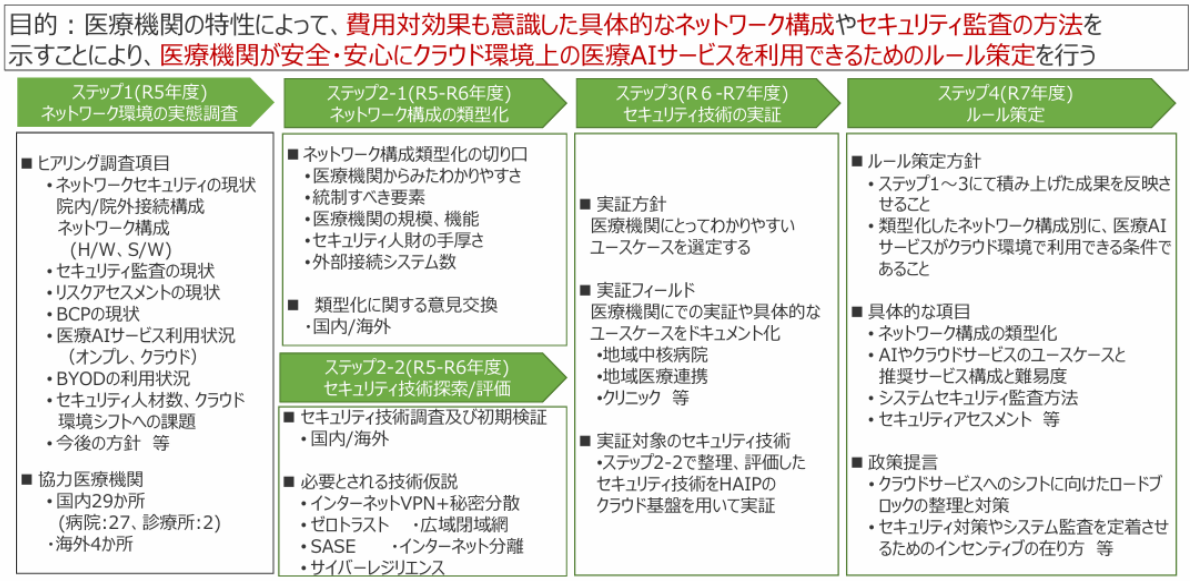
本研究は、医療機関が簡単に自己チェックを行えるアセスメントツールの検討、医療機関のネットワークガバナンスによる類型化と自己チェック、システムセキュリティ監査のルール策定、IT-BCP 訓練、医療 AI やクラウドサービスを医療機関が検討・導入しやすくするためのユースケースを示している。また、これらを定期的かつ継続的に行うためには、原資が必要となるため、そのための制度的支援案についても示している。全国の医療機関が安全、安心かつリーズナブルな費用で医療 AI サービスが利用できることにより、医療機関の経営改善や医療の質を高めることを目的とする。

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

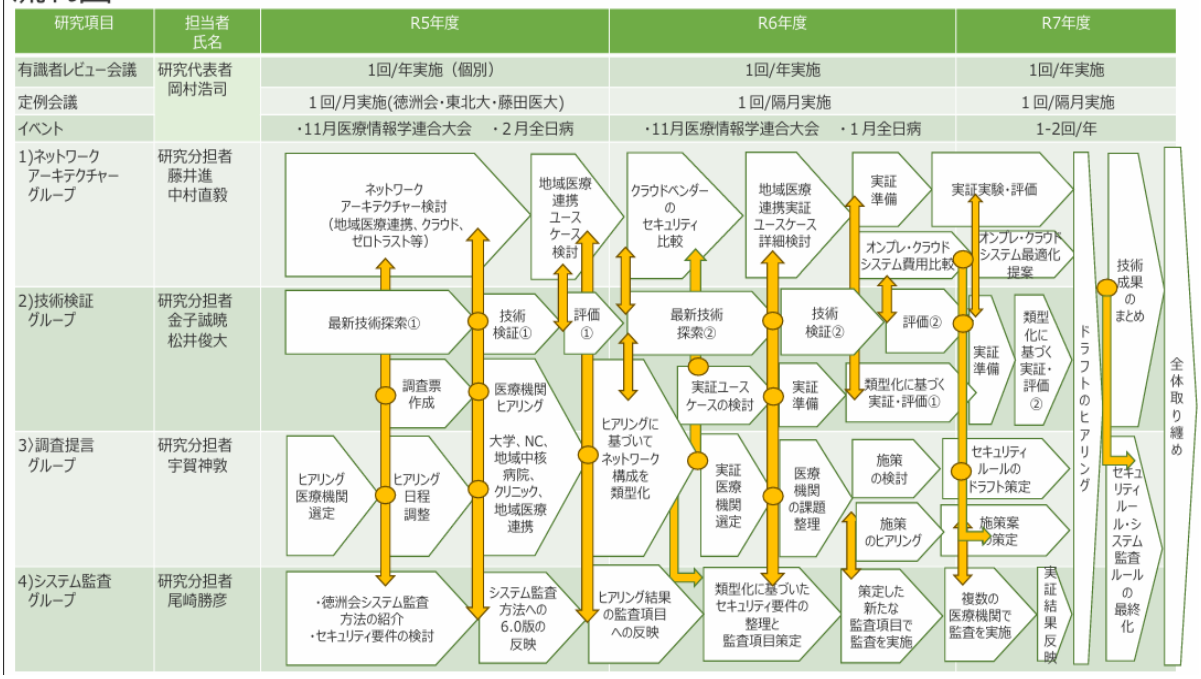


研究計画：各ステップにおける実施内容



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

流れ図



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。2026 年 1 月『情報セキュリティ１０大脅威 2026』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であり、二大脅威であることに変わりはない。特筆すべきは、3 位に AI の利用をめぐるサイバーリスクが初登場したことである。生成 AI がサイバー攻撃を行う時代になっており、この進化が著しいため、もはや境界防御型セキュリティやゼロトラスト型セキュリティによる防御という概念だけでは防ぎき

れなくなっている。そこで、重要になるのが例えサイバー攻撃を受けても被害をできるだけ最小化して、医療の継続をおこなうサイバーレジリエンスの考え方を実践する事である。

（1）事前アンケート調査票の作成

事前アンケート調査票を研究班全体でレビューを実施し、23 項目の調査票を完成させた。調査項目の作成においては、今までに実施されていた厚労省、全日本病院協会、日本医師会総合政策研究機構の調査を参考にしつつ、今回の研究目的に必要な項目を策定した。

（2）医療機関の選定及び調整

従来実施されていたアンケート調査と本研究の大きな違いは、回答数とそのアプローチ方法である。本研究では、医療機関数は 26 である。医療機関の選定は、設立母体、病床数、地域ができるだけばらつく様に考慮した上で、２４病院、２診療所の計２６医療機関に協力いただいた（注：その後、ヒアリングについてさらに3医療機関の協力をいただき 27 医療機関、2 診療所の計 29 医療機関（付録 1)、海外ではシンガポール 2 病院、MoH に協力いただいた)。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。

⑤ BCP

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いた。

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 ✓ 部門システムとごと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・プトロコルのみ通信できる構成とする

（5）ユースケース

医療機関にとって、有効な６つのユースケー

ス（①医療機関の既設ネットワークを利用した医療 AI サービス利用②地域医療連携ネットワークを活用したセキュアなインターネット利用③インターネット分離システムを利用した Web 会議や音声 AI サービスの利用④医師が院外からセキュアな環境で電子カルテのアクセス⑤遠隔医療システムを活用した手術支援、⑥ネットワーク結節点の集約によるセキュリティ安全性の担保）の選定を技術検証グループと共同で行った。上記の中で、医師が院外からセキュアな環境で電子カルテのアクセスのユースケースについて、3 つの医療機関のヒアリング先を選定し、技術検証グループと共にヒアリングを実施した。

（6）アセスメント

ヒアリングから医療機関が自組織のセキュリティ状況を容易かつ安価に実施できる方策が必要との考えに至った。その解決手段として汎用的な Web ベースのアセスメントツール（ISMS ベースで 175 問、5 段階評価）を参考にして、医療機関向けにできるだけ質問数を絞り込んでシンプルにした。また、用語解説を追加し 3 段階評価とした。かつ、医療情報システムの安全管理ガイドライン 6.0 版や R7 年度版セキュリティチェックリストの内容を質問に反映させて再構成を行った。用途別には、病院の IT 部門向け（80 問）、病院の経営層向け（15 問）、診療所向け（13 問）の 3 種類を準備した。病院の IT 部門向けは、病院のセキュリティについて、組織・運用面、技術面の 21 項目について数問ずつ設問を用意し、病院のセキュリティ全体を俯瞰できる内容とした。病院の経営層向けは、経営層（理事長、院長、事務長）がセキュリティに対する理解が不十分な病院は、システムセキュリティ監査の結果が低い結果がでており、経営層の意識改革が不可欠と判断して、作成した。診療所向けは、病院に比べ構成がシンプルな診療所に向けである。これら 3 種類を β 版として、70 を超える医療機関や関係部門にて試行を実施した。

D. 考察

今回の調査で多数の医療機関から多方面にわたる生の情報を取得し、多くの課題を抽出することができたとともに、ネットワークセキュリティ構成の類型化を行うことができた。研究開始時に策定した研究計画を進めるにあたって、とるべきアクションがより明確になった。

具体的には、セキュリティ人材が不足しており、かつ、経営が厳しい医療機関が多い中で、医療機関がセキュリティ強化のサイクルである、アセスメント（現状把握）→セキュリティ対策→監査・訓練（対策の確認）→人財育成・意識改革（組織の強化）→アセスメント（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が重要である。つまり、提言の中で示すべき方針は大きく２つあると考える。一つ目は、できるだけ少ない IT 投資で病院のセキュリティレベルをいかに向上するか。二つ目は、医療機関の IT 投資へのインセンティブをつけるための制度設計である。

① アセスメント（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することが可能な 2 種類のツールを開発した。一つめは、ガバナンスにフォーカスした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した。二つめは、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した。前述のとおり、本アセスメントツールは、用途別に病院の IT 部門向け、病院の経営者層向け、診療所向けを準備し、β版のトライアルをおこなった。結果としては、概ね好評であり、軽微な改善の要望については今後改善を行う。本アセスメントツールは、医療システムの安全管理に関するガイドライン(６.０版)や R7 年度版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に準拠しており、自組織の強みや弱みを正確に現状把握するためだけではなく、ベンダーとの対話を具体的に進めるためのツールとしても利用が可能と考えている。本研究終了後は、医療システムの安全管理に関するガイドライン(６.1 版)の公開や R8 年度版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チェックリストの公開行われるため、本ツールへの反映を行う計画である。

② セキュリティ対策

前述のネットワーク類型化レベルを確認するフローチャートに則った対策案を示すこととしている。また、Web セキュリティアセスメント結果に則った対策案を具体的に示している。さらに、医療機関に役立つクラウド利用のためのユースケースを複数提示する。具体的には、安全・安心にクラウド上の AI サービスを利用する方法、自宅などのリモートから院内システムへのアクセスを行う方法、運用管理が不十分な外部ネットワーク結節点（モダリティ、サブシステム、電子カルテ等の保守回線や給食システムなどの外部サービス）を集約する方法、地域医療連携ネットワークにおいて、セキュリティ体制が脆弱な多くの医療機関をセキュリティ体制が整っている組織がまとめて面倒を見る方法などである。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。Web セキュリティアセスメントの結果、点数が低い部分（3 点満点で 1.5 点以下）の対策案を提示する。また、さらに、医療機関が具体的なアクションを起こしやすい様に Health ISAC Japan、医療トレーサビリティ推進協議会、ソフトウエア ISAC、ＩＰＡなどと連携してマップを策定する計画である。

③ 対策の確認・訓練

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。システムセキュリティ監査は、医療機関の規模や体制によって、受査することが困難な医療機関が多数存在すると考えている。また、監査する側の組織や体制整備も大きな課題であり、今後関係各所の知見を借りながら定着をめざすための具体化を進めていきたい。当面は、ある規模以上の医療機関（200 床以上）は 3 年に一度の外部監査の実施を、内部監査については、毎年一度の実施を推奨する。監査を補完する役割である、①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。

訓練については、ネットワークアーキテクチャーグループが研究を進めている。

前述のとおり、生成 AI がサイバー攻撃を行う時代となり、攻撃の高度化が顕著であるため、サイバー攻撃を完全防御することは極めて困難になってきてる。従って、万一サイバー攻撃を受けた場合に、どうやって医療の継続的な提供を行うかが重要となっており、そのための包括的なアプローチであり上位概念がサイバーレジリエンスの考え方である。IT-BCP は、サイバーレジリエンスの考え方の内、障害からの復旧計画と実際の復旧を示すことが多い。IT-BCP は、計画の立案は重要であるが、災害時の避難訓練のように、実際の訓練をすることが極めて重要である。

1 年に 1 回は実際の訓練を行って、計画と現実の GAP を確認して IT-BCP の計画を継続的にブラッシュアップしていくことが重要である。日頃より、訓練をしていないと有事の際に間違いなく対処ができないと考えておいた方がよい。本提言でも IT-BCP について提言で言及している。

④ 人財育成・意識改革

人財育成については、組織として継続的な実施が必要である。医療機関に属する全員が必修として受講すべき基本的な研修と IT やセキュリティ業務として必要な専門的な研修を組み合わせて行う必要がある。本提言では、

研修の内容については深く掘り下げないが、提言のコンテンツは研修で使われる事を意識して、スライド形式で纏めている。是非、活用をしていただけるとありがたい。また、厚生労働省　ＮＩＳＴに掲載されているコンテンツを研修で活用することが大変有効と考える。さらに、生成ＡＩを医療機関で用いるケースが増えてきているため、生成 AI の利用者向けガイドラインも研修コンテンツとして有効である。

意識改革については、病院経営層の意識改革が極めて重要である。経営層のセキュリティに対する意識が低い医療機関はシステムセキュリティ監査の結果が悪く、意識が高い医療機関は結果が良いというデータがある。むしろ、ＩＴ人財の多い少ないよりも影響が大きい。

⑤ インセンティブ

官のインセンティブは、診療報酬の施設基準緩和が一番重要である。また、導入補助金の様な一過性のものではなく、継続した打ち手を高く評価してインセンティブにフィードバックする仕組みが必要であろう。

民のインセンティブは、出金を抑えるインセンティブとして、金融機関からの借入れ金利のディスカウントや損保会社のサイバー保険割引率アップなどが考えられる。収入を増やすインセンティブは、具体的なユースケースを共有したり、安全・安心なネットワーク経由で匿名化あるいは仮名化された医療データを提供することに対するインセンティブが考えられる。さらに、治験への参画を積極的に行うことによる収入アップも重要であろう。

⑥　認定制度

他の医療機関の見本となるセキュリティ対策を行っている医療機関、生成ＡＩなどのＡＩの活用を医療機関全体で行っており、業績改善や医療の質向上の定量的なアウトカムを示した医療機関を認定し、⑤に代表されるインセンティブを獲得できる仕組みの提案を行う。認定制度は、あくまで手段であり、目的はデジタル化、クラウド活用、AI 活用に向けた取組み、具体的なユースケースを他医療機関への共有と失敗事例の共有を行うことにより、同じ隘路に陥らない様にすること、及びセキュリティ投資や AI への投資へのインセンティブを一過性ではなく、社会システムとして継続できるようにすることである。認定するための項目整理と認定を行うプロセス、組織の検討を本研究が終了した後に検討を深めたい。

⑦ Human Centric Healthcare の実現

サイバーセキュリティ対策は、医療 DX、データ利活用、医療従事者の働き方改革を支える基盤と考えている。物流が劇的に発展した背景には、高速道路網などのインフラ整備によるものであり、医療 DX、データ利活用、

医療従事者の働き方改革の進展もそれをささえるインフラ整備が必須である。この場合のインフラの大きな要素は、安全・安心なネットワーク環境の整備であり、医療機関や自治体、介護施設、市民・患者に代表されるステークホールダーのセキュリティ対策である。これらが、インフラとして整備されると現在の医療機関を中心とした医療（場所中心の医療ともいえる。病院、診療所など特定の場所に市民・患者が出向く）からひと中心の医療（市民・患者が最適な医療を選択できて、医療過疎地域の方々へのリモートモニタリング、遠隔診療など）とのミックスが重要だと考える。また、ここでいうひとは、必ずしも市民・患者だけを指している訳ではなく、医師・看護師・薬剤師や医療従事者も含んでいる。これらの方々の過重労働、バーンアウト問題の解決や高度な専門スキルの継続（休職、退職後の再就職など、高度なスキルを活かす枠組み）問題を解決すべく、活動していきたい。

E. 結論

国内 26 医療機関に対して、事前アンケート調査を行った上で、対面による実態調査を行った。医療機関の ICT 導入状況、ネットワーク構成、人員体制、リスクアセスメント実施状況、システムセキュリティ監査状況、保健所によるセキュリティ立ち入り検査対応状況などの実態、医療現場が抱える課題等を把握することができた。また、医療機関のシステム構成を技術面から 4 種類に類型化し、それぞれのメリット、デメリットを整理した。さらに、医療機関に役立つ具体的な 6 種のユースケースの洗い出しとヒアリングを行った。

医療機関は平均して 100 床あたり 1 名のシステム要員で院内システムのトラブル対応やセキュリティ対策を実施しており、リソース不足や知識不足、またベンダー依存体制が浮き彫り、早急な対策が必要であると考えられる。サイバー攻撃の増加し、ランサムウェアによる被害が拡大している状況の中、境界防御型セキュリティに加えて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のネットワーク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。さらに、生成 AI によるサイバー攻撃が激増し攻撃が高度化

しているため、境界防御型セキュリティとゼロトラスト型セキュリティを組み合わせた完全防御をめざすセキュリティ対策では守り切れない時代になってきている。これからは、サイバー攻撃リスクは、常に存在し、万一サイバー攻撃にあっても医療の提供をとめないことが最重要の課題となる。組織全体でサイバーレジリエンス対応による予測・耐性・回復・適応能力を高め、IT-BCP により、サイバー攻撃からの回復及び医療提供の継続の計画を立案し、日ごろより実践訓練を行うことが唯一の解だと考える。これらを体系立てて提言としてまとめ、公開することにより、クラウド上の医療 AI 利用、医療 DX 及び医療機関やステークホールダー間のデータ利活用の促進や医療従事者の働き方改革の推進に少しでも貢献できれば幸いである。最終的には、医療機関中心の医療からひと中心の医療である Human Centric Healthcare へのシフトが進むことを期待してやまない。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く所存である。

最後に、多忙の中、協力していただいた 29 の医療機関（付録２）に深謝します。

F. 研究発表

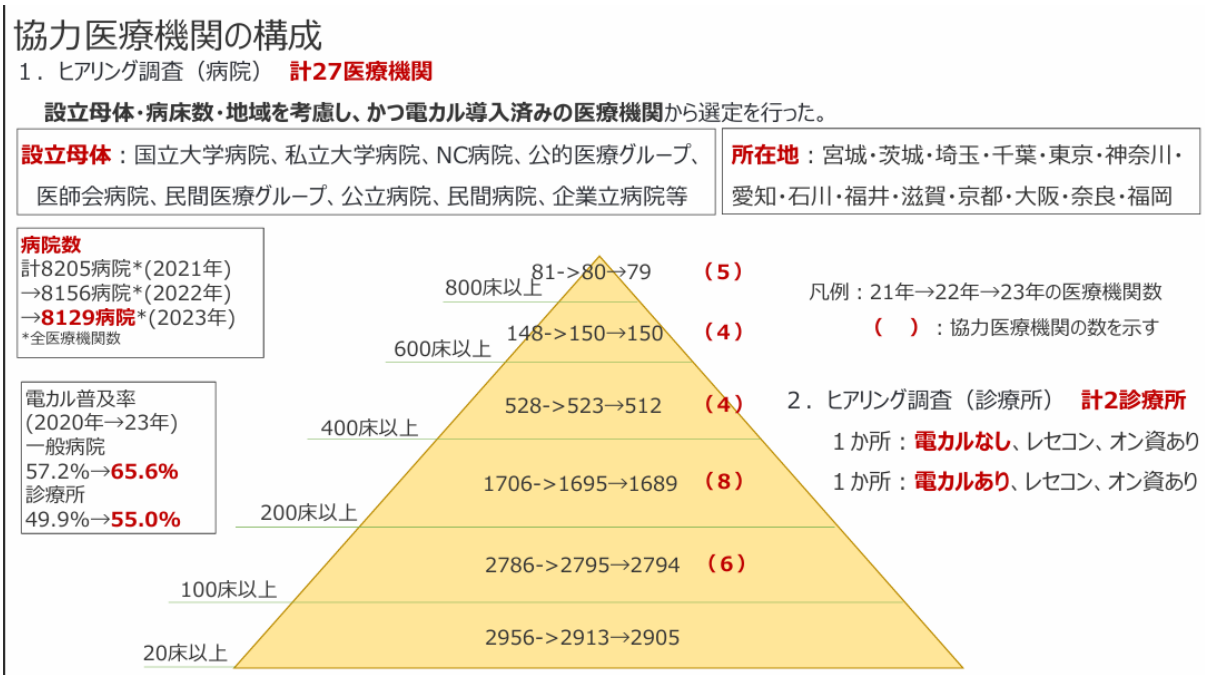
1. 宇賀神 敦, 医療機関に求められるサイバーセキュリティ対策とクラウド型AIサービスの活用, *週刊医学のあゆみ* 12月28日号, 2024, **Vol. 291 Nos12, 13**, 1123-1129
2. 宇賀神 敦, クラウド型AIサービス活用の課題と将来の展望について, *医療情報学*, 2024, **44(Suppl.)**, 371
3. 宇賀神 敦, AIサービス普及のための情報セキュリティのあり方, *INNERVISION*, 2024, **39**, 17-20
4. 宇賀神 敦, 医療機関の経営者は今こそ情報セキュリティに対する投資優先度を上げるべき, *月刊新医療*, 2023, **50**, 22－27
５. 宇賀神　敦、正しく恐れて、積極的に活用しよう！‐医療機関が押さえておくべき「医療・ヘルスケア分野における生成 AI 利用ガイドライン（第 2 版)」のポイント‐, ITvision, 2025, 55, 14－15
６. 宇賀神　敦, 医療 AI の活用や医療 DX 推進に求められるセキュリティやガバナンス‐安心して医療 AI が利用できるデータ連携基盤やサイバーセキュリティの制度的支援の考察 ‐, 第 45 回医療情報学連合大会, 2025, 45(4-B-1-08), 1－6
７. 宇賀神　敦, 中小医療機関が直面するサイバーセキュリティー課題と対策　論考②, 日本医療法人協会ニュース, 2026, 2026/5

G. 知的財産権の出願

該当なし

資料　ネットワークセキュリティ構成類型における協力医療機関

付録１：協力医療機関の構成



付録２：協力医療機関の一覧

協力医療機関一覧（１）

１．病院

#	医療機関名称	所在地	病床数	開設主体
1	藤田医科大学病院	愛知県豊明市	1376	私立学校法人
2	東北大学病院	宮城県仙台市青葉区	1160	国立大学法人
3	京都大学医学部附属病院	京都府京都市左京区	1131	国立大学法人
4	飯塚病院	福岡県飯塚市	1048	企業立病院
5	大阪赤十字病院	大阪府大阪市天王寺区	883	日本赤十字
6	横須賀共済病院	神奈川県横須賀市	740	共済組合
7	国立国際医療研究センター	東京都新宿区	719	国立研究開発法人
8	仙台医療センター	宮城県仙台市宮城野区	660	国立病院機構
9	福井大学医学部付属病院	福井県吉田郡永平寺町	600	国立大学法人
１０	国立成育医療研究センター	東京都世田谷区	490	国立研究開発法人
１１	越谷市立病院	埼玉県越谷市	481	公立
１２	恵寿総合病院 *1	石川県七尾市	426	民間
１３	淡海医療センター	滋賀県草津市	420	民間、地域医療連携推進法人

*1:24/1/1　23年度は能登半島地震のため、事前アンケート調査票の提出のみのご協力

協力医療機関一覧（２）
１．病院

#	医療機関名称	所在地	病床数	開設主体
１４	仙台病院	宮城県仙台市泉区	384	JCHO
１５	済衆館病院	愛知県北名古屋市	331	民間
１６	みやぎ県南中核病院	宮城県大河原町	310	公立
１７	日立製作所ひたちなか総合病院	茨城県ひたちなか市	302	企業立病院
１８	仙台徳洲会病院	宮城県仙台市泉区	250	民間
１９	練馬総合病院	東京都練馬区	224	公益財団法人
２０	生駒市立病院	奈良県生駒市	210	公立（医療法人徳洲会*2）
２１	柏市立柏病院	千葉県柏市	200	公立
２２	賛育会病院	東京都墨田区	199	社会福祉法人
２３	公立刈田綜合病院	宮城県白石市	199	公立（医療法人仁誠会*2）
２４	板橋区医師会病院	東京都板橋区	192	日本医師会
２５	JR仙台病院	宮城県仙台市青葉区	164	企業立病院
２６	博愛会病院	福岡県福岡市中央区	145	民間
２７	豊橋ハートセンター	愛知県豊橋市	130	民間

＊２：指定管理者として民間医療機関が公立病院の運営を行っている

協力医療機関一覧（３）
２．診療所

#	医療機関名称	所在地	病床数	開設主体
1	今村医院	東京都板橋区	0	民間（元日本医師会筆頭副会長）
2	斎藤医院	東京都板橋区	0	民間（板橋区医師会長）

１）診療所への更なる協力依頼、Webセキュリティアセスメントツール、地連への調査（日医総研）に関して、日本医師会長島常任理事、佐原常任理事に相談に伺った