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。

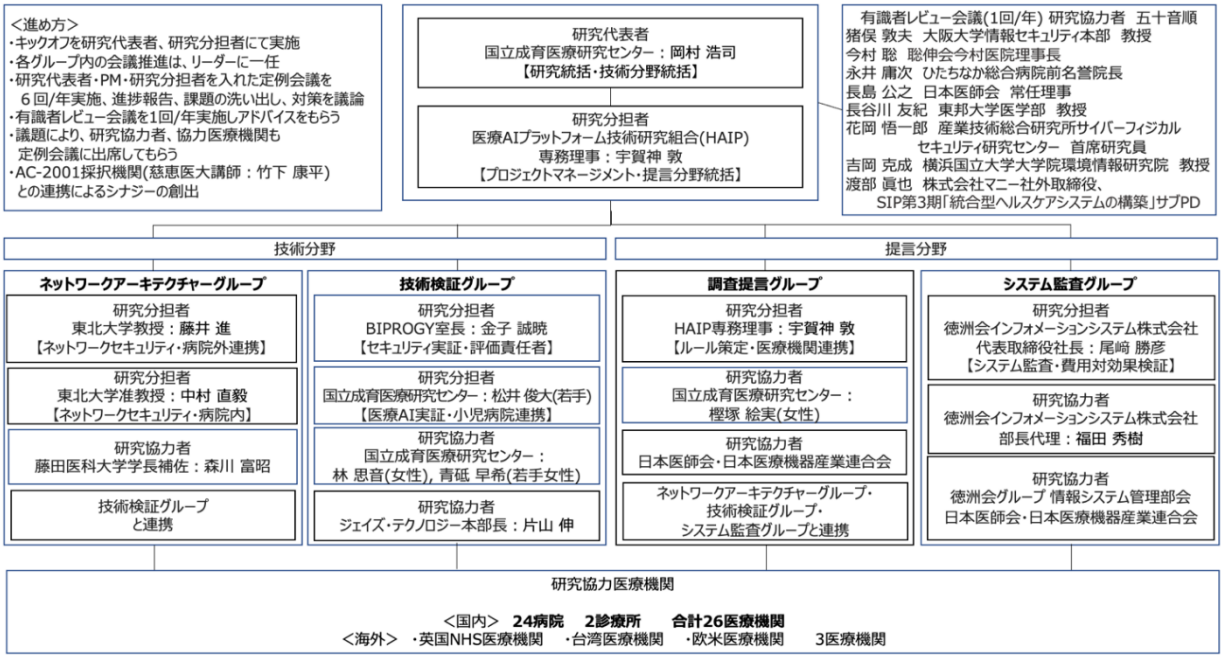
本研究は、医療機関の類型化に基づいた最適なネットワークセキュリティ構成やシステムセキュリティ監査のルールを示す事により、全国の医療機関が安全、安心かつリーズナブルな費用で医療 AI サービスが利用できることを目的とする。

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。

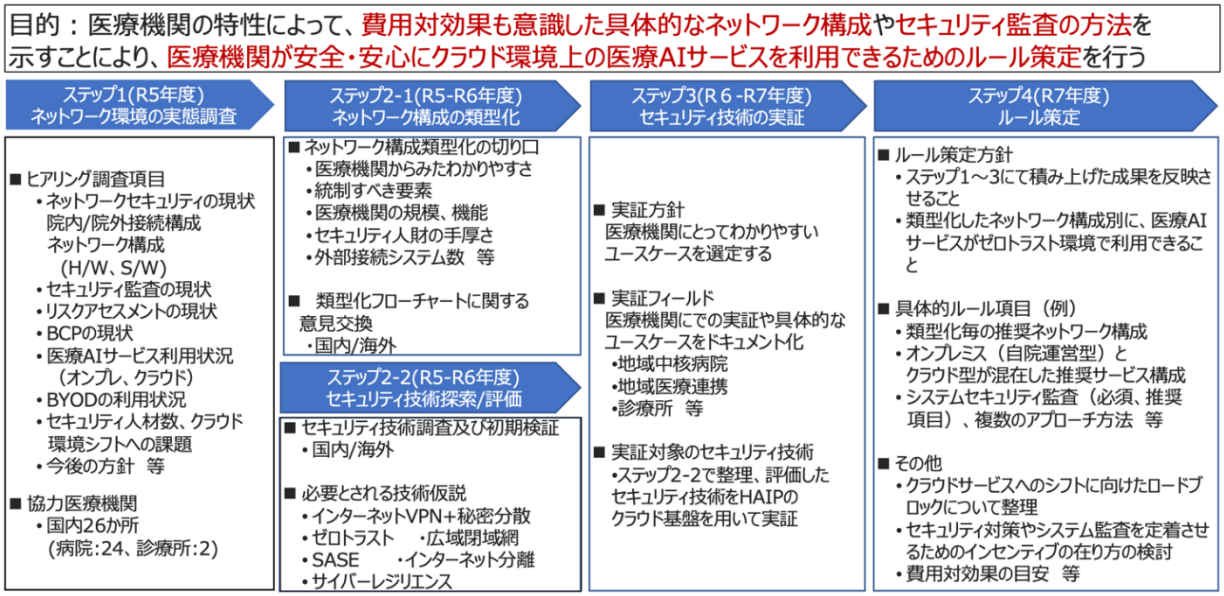
（2） 医療機関の選定及び調整

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