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・分担 研究年度終了報告書

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

岡村浩司（研究代表者）・宇賀神敦・金子誠暁・松井俊大・尾﨑勝彦

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 医療機関について対面のヒアリング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。なお、一部のヒアリングには厚労省厚生科学課にも同席してもらい、医療機関のリアルな実態を把握してもらった。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、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。システム監査については、23 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。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、システムセキュリティチェックリストに基づいた監査の実施と監査方法の提言を実施する予定である。

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
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
金子誠暁：医療 AI プラットフォーム技術研究組合システム WG リーダー
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小児内科系専門診療部医員

A. 研究目的

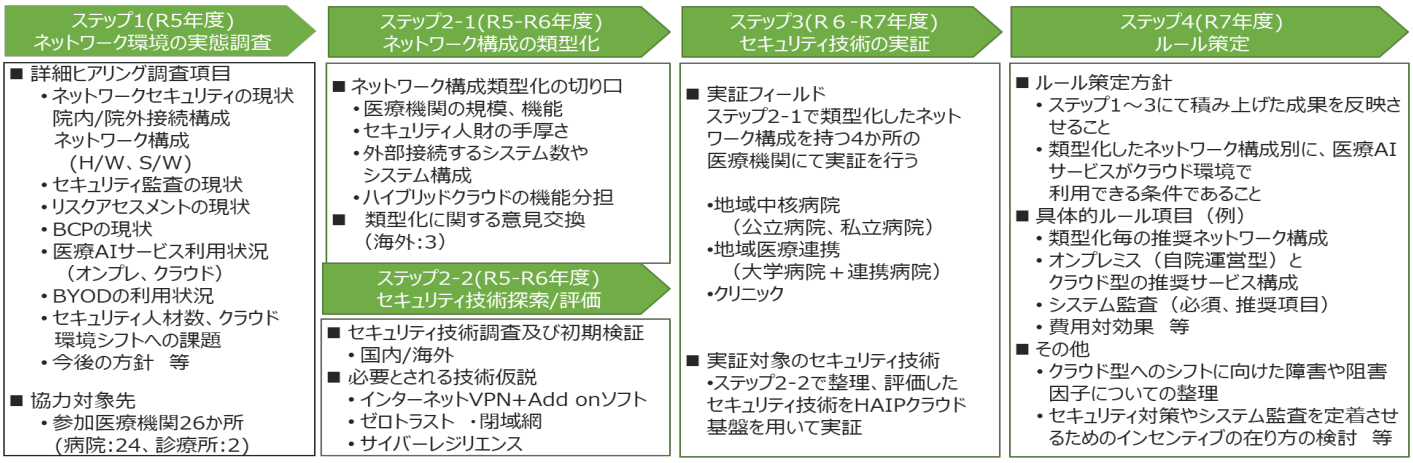
医療従事者と医療 AI との協調は、医療従事者の働き方改革の実現や医療の均てん化には重要である。質の高い医療データに基づいて開発された医療 AI サービスが次々に生まれ、幅広い医療機関で利用されるためには、利用しやすい価格とクラウドの利用が不可欠である。本研究では、医療機関の特性によって、費用対効果も意識した具体的なネットワーク構成やセキュリティ監査の方法を示すことにより、医療機関が安全・安心にクラウド環境上の医療 AI サービスを利用できるためのルール策定を目的とする。

B. 研究方法

本研究では、1 年目にガイドラインやアンケート調査を参考に、ネットワークセキュリティのヒアリングを国内 24 の医療機関に実施した。規模・機能、セキュリティ人材の有無、外部接続システム数などを基にネットワーク構成の類型化を行った。また、国内外の最先端セキュリティ技術の評価を行った。2 年目は、ネットワークセキュリティ技術調査を継続して実施すると共に、医療機関から見たネットワーク構成の類型化を完了し国内外医療機関と意見交換を行う。類型化に基づいて 4 か所の医療機関単体及び地域医療連携を想定したクラウド環境を利用した実証を開始し、有効性と費用対効果の検証に着手する。3 年目は、医療機関との実証を終了し、その有効性と費用対効果の検証を行い成果物としてまとめる。これまでの成果を踏まえて、類型化に基づき最適なネットワークセキュリティ構成やシステム監査方法についてルール策定を行う。さらにクラウドシフトを加速するための課題を明らかにする。

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。

情報セキュリティ10大脅威 2024（2024年1月）

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）	2023年からの変化
1	ランサムウェアによる被害	2016年	9年連続9回目	→　±0
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目	→　±0
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目	↗　+1
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目	↘　−1
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目	↗　+1
6	不注意による情報漏えい等の被害	2016年	6年連続7回目	↑　+3
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目	↗　+1
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目	↘　−1
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目	↓　−4
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目	→　±0

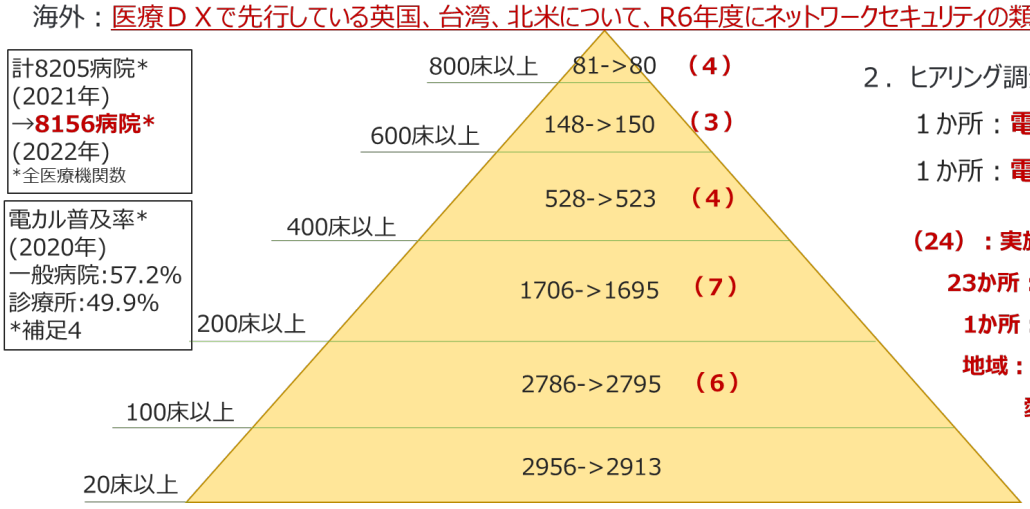
出典：情報処理推進機構　https://www.ipa.go.jp/security/10threats/10threats2024.html

1．ヒアリング調査（病院）　**計24医療機関（計画比：+4医療機関）**

国内：**設立母体・病床数・地域を考慮し、かつ電カル導入済みの医療機関**から選定を行った。（国立大学病院、私立大学病院、NC、国立・公的医療グループ、医師会病院、民間医療グループ、公立病院、民間病院、企業立病院等）

本研究では、**①事前アンケート送付、②事前に回答を入手、③対面でのヒアリング**(1.5時間/1医療機関)を実施した。

海外：医療ＤＸで先行している英国、台湾、北米について、R6年度にネットワークセキュリティの類型化に関する意見交換を計画



2．ヒアリング調査（診療所）　**計2か所**

1か所：**電カルなし**、レセコン、オン資あり

1か所：**電カルあり**、レセコン、オン資あり

（24）：実施医療機関数

23か所：事前アンケート、ヒアリング実施

1か所：事前アンケートのみ実施

地域：宮城・茨城・埼玉・東京・神奈川・愛知・滋賀・大阪・奈良・福岡・石川

以下、本研究の成果を報告する。

１．医療機関の実態調査

（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、全日病、日本医師会、医療 ISAC のアンケートも参考にした。

（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られてた。

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しているものの、双方向での会話にならず、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。

③ 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） ネットワークセキュリティ構成の類型化

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

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	具体的な施策例
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	△	△	×	✓ 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	● 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	○	○	×	(レベル1に加え) ✓ 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	● 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	○	○	○	(レベル2に加え) ✓ 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・プトロコルのみ通信できる構成とする

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

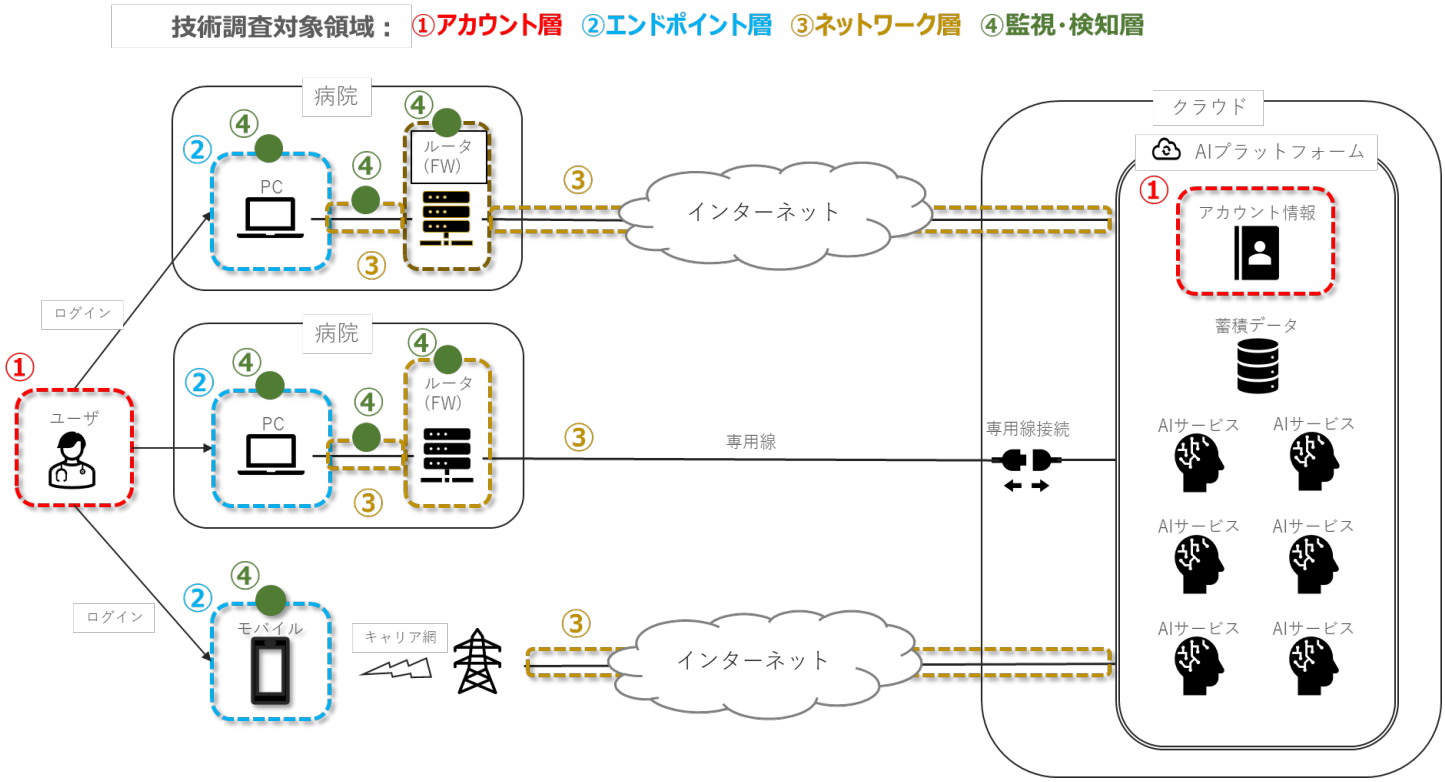
まずは、医療機関のネットワーク構成汎化モデルを作成した。その上で、セキュリティ製品調査領域を 4 種類に分類し、Web 調査を行った。

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 3 省 2 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。

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 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：本研究班調査提言グループ)

② 24年2月23日全日本病院協会『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（宇賀神敦：本研究班調査提言グループ）

3. 大会論文集・査読付き詳細な抄録

なし

F. 知的財産権の出願

・なし

以上

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：

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日の平均外来患者数に○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　⑦一き地医療拠点病院　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）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経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院長が兼任している 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 ・公認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実際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の対策はとっていますか。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、災害対策本部のなり上げルール、 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 非常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保守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の回答した場合は、どのシステムがどの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:閉域網、PACS:HW-VPN、リハビリシステム:SW-VPN
	（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。	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請求のため ④クラウドサービス利用のため ④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データセスがある ⑥電子カルテの診療ネットワークにて、他に外部との通信を行っているものがある ⑥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）
		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がありますか。 （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 利用すると捉えてください。	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）

添付 A2：　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