厚生労働行政推進調査事業（地域医療基盤開発推進研究事業）
研究報告書

医療分野の情報化の推進に伴う医療機関等におけるサイバーセキュリティ対策のあり方に関する調査研究
令和３年度　総括報告

研究代表者　近藤博史
特定非営利活動法人日本遠隔医療協会
研究分担者
山本隆一　財団法人医療情報システム開発センター
美代賢吾、星本弘之　国際医療研究センター
長谷川高志　特定非営利活動法人日本遠隔医療協会

研究要旨
医療分野の情報化の推進に伴う医療機関等におけるサイバーセキュリティ対策のあり方に関する調査研究として、技術状況や課題の総合的検討、複数の病院のセキュリティ管理状況調査、管理状況に関するアンケート調査のパイロットスタディ、医療情報システムの安全管理ガイドラインへ反映すべき課題の調査、院内へのサイバーセキュリティ訓練の手法の調査等を行った。令和３年度～4 年度の研究だが、複数病院の調査を広範に進めるため、令和３年度分の研究期間を延長して、2 年間実施した。

1．研究総括報告
（1）目的
重要インフラに該当する医療分野において、医療機関等のサイバーセキュリティに対する取り組みを強化することは喫緊の課題である。病院情報システムは、これまで外部と隔絶した情報ネットワークであった状況に対し、データヘルス改革、働き方改革、オンライン診療、モバイルヘルス(m-Health)等の導入で外部ネットワークへの接続が始まっている。情報化が進んでいなかった小規模病院、診療所における電子カルテの導入・普及も進みつつある。また、今後、拡大する m-Health 機器（携帯に連携した継続的なモニタリングと適時な介入をする治療アプリを含む。）は病院、診療所のシステムと連携され、研究基盤として活用されることも考慮する必要がある。同時に、進化するクラウド技術により、医療機関内にあったサーバをクラウド上に移行することも現実的になりつつある。
一方、サイバーセキュリティ対策も閉じたネットワークの出入口監査から、エンドポイント検知、ゼロトラストと言われるような内外の区別が無く直接個々の端末を対策する取組が重視されるようになってきた。このように変化と対策の将来像は双方合致した状況に見えるが、正反対の現状から理想の将来像に如何に安全に効率的に移行するかが喫緊の課題と言える。
本研究では、国内及び諸外国の EMR、EHR、PHR、m Health および臨床研究ネットワークも含めた対象について調査を行い、医療機関等の現場に即したサイバーセキュリティ対策を次世代技術や他分野の手法も踏まえて整理し、現在および今後の状況に即した対策のあり方を教育・情報共有も含め検討する。
具体的には、医療分野におけるサイバーセキュリティ対策と課題について医療機関の規模・ユースケース等ごとに整理するとともに、医療機関同士が相互にサイバーセキュリティ対策に関する情報共有・相談を行う体制のあり方等を検討し、医療機関等への対策強化の普及・促進策等を検討する。さらに、諸外国の先進的な医療クラウドの事例調査と、国内における医療情報システムのクラウド化などの先例調査と現場意向調査を行い、日本のニーズから近未来化を効率的かつ迅速に進めるためのクラウド化の方向性を検討する。最後に現状の医療機関のサイバーセキュリティ対策の強化を迅速に広範囲に適合するための方策について、クラウド化を含めて提案し、その手引き等

の作成を行う。

（2）研究結果概要

医療のクラウド利用への変化は診療所用クラウド型電子カルテと、歩数、脈拍、体重、血糖値などの計測モバイルヘルス系のクラウド利用が進んでいる。一方、大規模病院のクラウド移行については鳥取大学が 2020 年にクラウドサーバのオンプレミス構築がクラウドサーバ移行の技術的可能性は明確にした。同時に、シンクライアントによる地域連携システムのスマートフォン通信を介した高速表示は専用回線と共に利用して通信切断時の予備通信回線の技術的課題をクリアしたと言える。2021 年には福井大学病院のクラウドサーバ移行が具体的な実現を示した。ただ、そのコストはオンプレミスと同程度であったので、今後のクラウドサービス利用の増加によるスケールベネフィット効率化を待つ必要があることがわかった。クラウドサービスにおけるセキュリティに関しては AWS から 2 回聴取し、クラウドサービスにおけるセキュリティの責任分界点と利用者の設定ミス時の利用者責任部分の課題が明確になり、その対策として十分な説明資料のサービスの充実が図られていた。一方、シンポジウムにおいて医療情報システムの安全管理ガイドラインに掲載された CSIRT 組織化については、医療機関からの困難な状況の指摘があり、具体的要件情報の収集のため、金融系 CSIRT 委託事業者と IPA から事情を聴取し、攻撃後ではなく、攻撃前の調査の重要性が明確となった。具体的には外部接続の確認、これには接続の FW, VPN ルータの機種、ソフトウェアのバージョン、設定内容、保守体制を含む。また、外部接続と内部ネットワーク全体図、そこにおけるサーバとクライアント端末の関係も資料作成が必須であった。ただ、医療機関の場合は種々のネットワーク、機器が次期と部署が異なり統合管理部署がないことも明確になった。例えば、情報システムと放射線部門の購入する C T、M R I などの検査機器とそのオンライン保守回線があげられる。現地保守契約でもコロナ禍でいつの間にかオンライン保守化した事例もあった。事前調査の困難さが明確になった。また、NHK のインタビュー体験から一般への説明の困難さ、これは ISAC 内での情報共有の困難さにも関係するが、知識のある専門家間では相対的安全性の議論がされることの理解の重要性が明確になった。

今回のアンケート調査では既存技術でセキュリティレベルを上げる仕組みの理解度を聞くことにした。

複数病院のサイバーセキュリティ実態調査が最後になったが、現状の攻撃と対策技術の調査の後の現場の実態調査は順序として適切であったと考える。ベンダーが情報を公開し医療機関と共にリスク分析をして対応する新たな手法は始まったばかりで、理解されていない状況がわかり、具体的な病院管理者の対応の指導が必要であった。実際の医療機関の外部接続は数個の FW に集約された理想系から、部門システム、検査機器毎の保守回線が多数存在する病院が多かった。一度にまとめて導入されることのない中小病院では専門の技術者もおらず、全体のリスク想定と対策は難しいと考えられた。特に放射線機器の保守回線を LTE で導入する場合、無線のため病院のネットワーク管理者と協議する必要もなく接続できるので情報部門が放射線部門や検査部門の機器の保守契約に関与する体制が必須になっている。

（3）実施経過

医療システムのクラウド移行については鳥取大学病院、福井大学病院の情報収集を行い、診療所電子カルテ、医療 D X に関係するモバイルヘルス系システムは遠隔医療学会、医療情報部長会からの情報収集から得た。一方、クラウドサービスにおけるセキュリティ、医療関係者等の意見を聞く場として分担者である山本隆一氏に「医療情報システムの安全管理ガイドライン」の解説を加えて、6 月の医療情報学会、10 月の遠隔医療学会、11 月の医療情報学連合大会、2 月の遠隔医療学会スプリングカンファレンスでシンポジウムを企画した。ここではセキュリティベンダー、クラウド事業者、CSIRT 事業者、IPA, 医療機器工業会にも発表頂きそれぞれの情報収集と同時に視聴者の医療関係者の意見を聞いた。CSIRT 委託事業者、I P A からの CSIRT の事前情報収集としての医療機関内のネットワークと

外部接続の把握に関して、代表近藤はデータ調査会社のオンラインデータ取得における事業者の「匿名保存する」の説明に対して名寄せ可能性から「匿名化されていない」接続をしていることを指摘した。また、別途、「遠隔画像診断サービス」においても「匿名化保存」の説明の下で画像サーバにオンライン接続している実態を発見した。研究班内で検討し危険な接続の可能性として扱うこととした。また、美代、星本は画像検査機器等の保守契約においてコロナ禍でオンライン保守に移行され、詳細が情報担当部門に連絡されない実態を報告した。類似の情報は医療情報部長会でも愛媛大学の木村教授からも指摘があり、契約において責任取らない旨の内容を見つけ報告した。6 月の東大阪病院、徳島県半田病院の事例もあり、データの安全な保存技術について、昔の磁気テープ保存の見直し、販売の増加情報を得たが、直接ストレージ機器ベンダー、ネットワーク機器ベンダーに聴取しハードウェアに暗号化されない、消されないバックアップ機器の開発がされている情報を得た。また、ＮＨＫからのインタビューは情報機器を知らない一般人への説明の困難さも明確になり医療系 ISAC 立ち上げ時に参加者への説明に問題になることがわかり、ICT の安全性は繋がっていること自体は危険であり、相対的に安全になる技術を推奨する立場であることの教育の重要性が明確になった。これを踏まえて、今年度のアンケート調査は「相対的に安全になる技術、推奨される技術」に関する知識を問うことにすることを研究班内で協議した。最新の「医療情報システムの安全管理ガイドライン」にも仮想ブラウザなど技術の名称が記載されるようになった。

複数病院のサイバーセキュリティ実態調査では、病院会から紹介された病院を中心に１１病院を選択し調査した。経営者、システム管理者、利用者のチェエクリストのチェックから始めた。１１病院のデータを並べ、〇の多い項目、少ない項目について項目内容と病院の状況を想定して検討した。経営者では、予算化や組織の作成などは多くの医療機関で〇がつくが、具体的な体制、管理規則は個人情報保護対応ほどはされていない状況が見える。また、具体的方法の明示のない監査の実施、現状調査は丸が少ない。ただ、セキュリティ対策の公表はリスクもあり意見の別れるところであり、何らかの提案が必要と思われた。システム管理者では、これまでの個人情報保護法に基づいた医療情報システムの安全管理ガイドラインの内容についてはほとんど〇の状況だが、監査の実施については詳細の提案がないためやや数字は落ちる、契約内容についても担当部署でない可能性もあり数字が低くなる。医療情報システム系でもベンダーへの規則の改定部分の MDS の医療側対応はまだ普及しておらず、医療側の具体的対応も指導が必要と感じる。IoT 関係も同様でベンダー側の規則が成立したのが昨年度であり、医療者側の対応の具体的指導は今後のことであり、これから整備される ISAC も成績は悪い。外部への Web サービスがほとんどされていない日本の医療機関では答えられないものも多い。利用者では、個人情報保護のガイドラインに従って教育されている結果で〇が大半だいが、医療機関で導入されているシステムに依存した部分は X も存在する。

外部通信を含んだネットワーク全体図、情報系機器の資産台帳の作成は日々の脆弱性対策にも、攻撃発生時の CSIRT 活動に必須のことであり、各病院が個別に作成し、更新すべきものである。しかし、業者任せで全体を把握していない病院にとっては手立てもわからず、その作成に協力することは重要である。また、本研究において作成のノウハウを作ることも重視した。そのため、2022 年度の調査を実施したセコム山陰に協力して頂き、新たな調査ベンダーにはセコム山陰の指導のものとに調査することにした。また、情報担当で管理されていない外部接続を探す、一定期間内に機器の事実を調査することは、定番の方法が無く、コスト計算も大小なることが予想されたので、厳密に人数と時間の記録をとり、人員の単価はベンダーに依存することで調査を実施した。情報管理の契約については、病院と遠隔医療協会、遠隔医療協会と各ベンダーで契約した。各病院の情報は、研究代表、分担者とセコム山陰で共有した。

作成された外部接続を含むネットワークの全体像、と資産台帳からは、7 つの外部接続

に集約した病院から、最大 47 の外部接続を有する病院まで存在した。サブシステムや検査機器の保守に https サーバに接続する SSL-VPN 接続が見られた。放射線機器の保守系で LTE 回線も見られた。また、サービス終了が近い ISDN 接続も残っていた。放射線機器の保守回線が見られない医療機関が一つあり、放射線機器の保守回線が忘れられている可能性があった。

2. 複数病院のサイバーセキュリティ実態調査管理方式開発
（担当　研究分担者　長谷川高志）
各病院の調査は、サイバーセキュリティに関する技術を有するシステム技術系企業６社に委託した。その調査結果を研究代表者、研究分担者が統括する視点から整理、分析した。５社で１１病院の調査を実施するにあたり、各社・各施設が公平かつ共通・一定に作業するべく、各社との情報保護や業務方式のルールや手続や文書類を共通化した。各施設とも依頼書、作業手順書、情報保護の誓約書等を共通の書式や方式で実施した。また調査内容の技術レベルを均質にするために、調査会社中の一社で令和４年２～３月に一施設でパイロット調査を担当した企業が、技術および工程の共通管理やレビューを担当した。これにより、具体的な調査事項のブレの抑制が抑制された。この管理方式は、本研究のみならず、今後サイバーセキュリティに関する施設調査を実施する際の“調査結果の質の安定化”に資する手法となった。なお調査対象施設は研究班による個別選別と、一般社団法人日本病院会での募集の二系統から選んだ。この募集および令和４年度研究での調査活動について、一般社団法人日本病院会からの支援は大変有益だった。

3. サイバーセキュリティに関する意識調査
（担当　研究分担者　長谷川高志）
（1）目的
医療機関に於けるサイバーセキュリティの管理体制を調べるために、組織で実施しているセキュリティ対策、施設内の規定、セキュリティインシデント発生時の対応、侵入対策やウイルス対策の状況、サイバーセキュリティ対策への意識や理解度などをアンケート調査する。単なる意識調査ではなく、回答者の知識水準などを具体的に抽出する設問を作る。
（2）結果概要
詳細を把握するために、106 問の設問にまとめた。これだけ設問数が多い、負担感の大きいアンケートにも関わらず全対象者の約 1 割 9%が回答した、サイバーセキュリティに関するリテラシーの存在を感じた。

（3）実施経過
準備に時間を掛け、令和 4 年 3 月の短期間に日本遠隔医療学会会員を対象に実施した。

4. 医療分野におけるサイバーセキュリティ対策と課題について
（担当　研究分担者　山本隆一）
（1）研究概要
「医療情報システムの安全管理ガイドライン 5.2 版」に対する医療機関やシステムベンダーからの質疑、意見等から社会の反応とその対応を検討し、今後のガイドラインからのアプローチの現状と可能性、今後の方策について調査を行った。また、随時、関係各位からの聴取を行ない、方策を検討して、新たに発出予定である第 6.0 版への提言を行った。また、患者を対象としたオンライン診療の現状把握や調査を行い、前年度結果との比較分析をし、研究期間中の状況の変化の把握、患者の意識の変化や、社会情勢の影響の有無など検討を行った。

（2）実施経過
患者を対象としたオンライン診療の現状把握や調査を行い、前年度結果との比較分析をし、研究期間中の状況の変化の把握、患者の意識の変化や、社会情勢の影響の有無など検討を行った。

5. 医療機器等に関連した調査と対策および医療機関のセキュリティ対応状況と教育等の対策の整理
（担当　研究分担者　美代賢吾、星本弘之）
（1）目的
ICT 化、医療機器の IoT 化が進む中で求められる医療機関のサイバーセキュリティ対策について、医療機関のサイバー攻撃リ

スクの観点から、サイバーセキュリティ指針案の策定に資する。

（2）結果概要

医療機関におけるサイバーセキュリティ対策調査として、日本国内 4000 の病院（精神科を含む）に調査票を送付し、用意した Web 上の回答フォームに 508 の医療機関から回答があった（回答率 12.7%）。その結果、IoT 機器の利用が進む状況の中、現在 IMDRF 文書に記載されるサイバーセキュリティリスクへの対応については、多くの医療機関が十分に対応できていないことが明らかになった。今後の対応として、IoT 機器に対するサイバー攻撃のリスク評価と対応基準の検討、IMDRF 文書のセキュリティ要件に対応するための医療機関を支援する組織の必要性、日々進化するサイバー攻撃に対応し、的確な教育を行う仕組みの組織的な提供により、日本の医療機関全体のサイバー攻撃への対処能力の向上につなげる必要性が示唆された。

（3）実施経過

コロナ禍で移動制限のある中、NCGM のセンター病院の状況・事例を含め実態の調査を行うとともに、より幅広く日本全体のサイバーセキュリティ対策の実態を把握するために国内の病院の半数にあたる 4000 の医療機関に調査票を送付し、508 の医療機関から回答を得た。この回答をもとに、現在の状況と今後の対応について検討をおこなった。

成果の刊行に関する一覧表：後述
成果による知的財産権の出願・取得状況：なし

（4）成果の今後の活用・提供：

国の重要インフラの一つである医療機関のサイバーセキュリティ対策を実態に合わせて進めるための資料として活用する。

6．健康被害情報

なし

7．謝辞

本研究にあたり、一般社団法人日本病院会殿および会員施設の皆様、調査にご協力いただいた全ての病院、関係者の皆様にたいへんお世話になりました。ここに深く感謝を述べさせていただきます。