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
総合報告

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、　国際医療研究センター
星本弘之、辻岡和孝
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、日本病院会会員施設へのセキュリティ管理状況に関するアンケート調査、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。

1．総合報告

（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）研究結果の概要

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ＣＴ、ＭＲＩ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。令和 3 年度、4 年度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。

医療機関内にあるサーバをクラウド上に移行する方法についてはオンプレミスでクラウドサーバ類似のサーバを導入した鳥取大学医学部附属病院の事例や実際に現状でクラウドサーバの利用を開始した福井大学医学部附属病院の事例の情報収集をしていたが、2021 年度に発生した VPN と FW の複合機の脆弱性をついたサイバー攻撃事例の頻発により、シンポジウム等を介した情報収集は IPA の CSIRT 活動を中心に始めた。日本医療情報学会春季学術大会では事前の①事前のネットワーク調査、②ネットワーク・サーバ機器の資産台帳の整備、③脆弱性が判明した場合の医療機関の知るタイミング、知った後の対応の問題。攻撃後では③ネットワーク、機器の情報収集の時間の必要性、④ハッカーの潜入機関が 100 日以上になる場合がある。⑤画像のような大容量データも一部の暗号化の場合がある。⑥暗号化されたデータの複合化をしても前の状態と同じかの証明ができない問題。などが明確になった。これによりデータバックアップと BCP の問題が明確になったため、日本遠隔医療学会総会ではストレージに絞って情報収集し、①フラッシュ系ストレージ会社から、ハードウェア依存型バックアップやストレージ専用 OS によるバックアップにより OS に依存しないバックアップの提案があり、これらはテープよりも高速に利用可能であるメリットが示された。また、②ネットワーク系ベンダーからの提案で接続時間を書き込み時のみに制御し暗号化を免れる方法の提案があった。一方、③テープバックアップからは垂直磁場の利用で 5TB が 5 万円のテープが近い将来 500TB になり、一回書き込み（WriteOnce）の実現性が指摘された。これは上述の④ハッカーの潜入機関が 100 日以上への対応を可能にする方法であり期待できる。鳥取大学病院で 1 年間の電子カルテデータ SS-MIX2 で 1 TB であるが、地域医療ネットワークの公立病院では 5 年で 1 TB 未満であり、地域でのバッ

クアップサービスの利用の可能性も考えられた。日本医療情報学連合大会では①大阪府急性期医療センターのサプライチェーン経由型の攻撃を話題にしたが、企業と医療機関が基本的な情報公開とリスク分析を行っていなかったからと言った議論になり、具体的な対策を参加者に提示できなかった。しかし、日本遠隔医療学会春季学術大会では現場調査の CISCO を含めたネットワーク会社を中心に議論した。①攻撃後も前も NDR の必要性が明確になった。②システム導入時の管理者権限のわかりやすい ID, パスワードの利用が指摘された、筆者も③NIST が言うゼロトラストアーキテクチャーにおける端末と人の Authentication Authorization の後者、権限付与が日本では配慮が薄いと考えていた。つまり「閉じたネットワーク神話」もあり、これまで保守ベンダーは管理者権限のわかりやすい ID, パスワードを利用し、病院や関連ベンダーに簡単に情報共有してきた。このことはソフトのインストールなど対応が容易なこと、逆に言えば、ソフトの管理などあまり重視していなかったことと共通する。実際、サプライチェーン経由でハッカーが侵入しても管理者権限が容易に取得できなければ攻撃は難しいものであり今後この部分の教育、管理の徹底が必要である。

別途、放射線機器のオンライン保守中心に安価な携帯デジタル通信①LTE による専用回線接続の増加を聞いた。携帯電話の大きさで USB 接続できる機器が、ネットワーク機器、PC, 画像検査機器に直結して多くの保守がされている。また、②https サーバに接続する PC 等を用いて遠隔保守や遠隔画像診断をするサービスも増加している。DICOM 画像の取得、レポートの返信、検査機器のログ情報の取得などほとんどの通信が PC 経由でできる状況になっている。現状この医療機関内の PC の内容はブラックボックス化されている。外部接続する内部ネットワーク内の PC について病院は①通信内容の情報を知る必要があり、②モニタリング、監視するべき、あるいはモニタリング情報を知らされるべきである。また、③この PC が乗っ取られることを想定して DMZ など同 PC から病院内ネットワークに自由に通信できる環境におくべきではないと考えられる

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）研究の実施経過

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、2021 年 6 月の医療情報学会、2021 年 10 月の遠隔医療学会、2021 年 11 月の医療情報学連合大会、2022 年 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。シンポジウム開催による専門家からの情報収集と参加者への情報提供では、2021 年に増加し、電子カルテ、病院の機能停止の大問題から脆弱性をつくサイバー攻撃対策として CSIRT 活動を実際に行なっている IPA の担当者の話を日本医療情報学会春季学術大会で企画した。また、日本遠隔医療学会総会では診療データのバックアップに焦点を当てた。2022 年 11 月の日本医療情報学連合大会、2023 年の日本遠隔医療学会スプリングカンファレンスでは 2022 年に発生したサプライチェーン経由の攻撃に焦点を当て、ネットワーク会社 2 社に講演をして頂いた。また、別途、現場から聴取した情報を元に ISDN のサービス終了に変わる安価で簡単な携帯デジタル通信を用いた LTE 専用回線利用の保守契約の増加を確認した。

また、遠隔画像診断サービスについて https 接続を使った DICOM 画像と診断レポートの通信のセキュリティも積極的調査対象にした。どちらも放射線機器、放射線遠隔画像診断に関係するため、日本医療画像システム工業会 JIRA の DICOM 委員会、日本医学放射線学会の電子情報・AI 委員会の遠隔画像診断ガイドライン更新の小委員会の委員として現場で情報収集した。また、現場の状況を取得するため放射線技師学会での招待講演時にシンポジウムに参加し、ベンダーと放射線技師の考えを聞いた。

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. 病院調査の管理方式
（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
　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った。日本病院会の会員施設を対象として、各施設の現実の状況を捉えた。プレ調査として、令和 3 年度に日本遠隔医療学会会員にパイロット調査を行った。
（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された。令和 4 年度に本格的に実施した。日本病院会の会員を対象として、2489 会員に案内して、581 件（23.3%）の回答を得た。昨年度の小規模集団での回答率の 2 倍以上を得た。多忙な病院現場にも関わらず、設問数の多いアンケートへの積極的な対応と受け止めた。　回答は学会実施と比べて、知識水準等に差異は無かった。コストや人員不足、対策技術の方向性の不統一など現場の厳しい状況が明らかとなった。
実施経過：アンケート用紙は昨年度研究と同じ書式を用いた。一般社団法人日本病院会殿に協力いただき、会員施設にインターネット経由で 9 月 21 日～11 月 7 日にアン

ケートを実施した。結果はNTTデータ経営研究所に一次分析を依頼した。
研究成果の刊行に関する一覧表：　特になし
（3）成果の今後の展開
日本病院会殿を通して、各施設に結果を知らせる。この結果から、対策技術の方向性を整理すべきことを様々な場に提唱する。

4. 医療情報システムの安全管理ガイドラインの調査・精査および患者を対象としたオンライン診療の現状把握や調査
（担当　研究分担者　山本隆一）：
（1）目的
医療分野における喫緊の課題であるサイバーセキュリティ対策と課題について、迅速かつ効果的な解決の方策を検討、提言を行う。
（2）結果の概要
昨年度に引き続き、山本本人が改定作業班の主査として主導し、取り纏めを行った「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。
（3）実施経過
改定作業班の主査として改定を主導した「医療情報システムの安全管理ガイドライン 5.2 版」に対しての社会の反応や対応を検討し、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い、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。
（4）研究により得られた成果の今後の活用・提供
今後も適宜見直し改定が予定されている「厚労省医療情報システムの安全管理に関するガイドライン」に関して、今後検討を行うにあたり重要なポイントを複数掲げられたこと、並びに「オンライン診療の適切な実施のためのガイドライン」に関しても、アンケート調査により受診した患者側の状況や意見など今後の改定等の参考となりえる提言が出来た。

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、辻岡和孝）
（1）目的
医療機関、とくに中小規模の民間医療機関などにおいては情報システムや情報セキュリティの担当者が適切に設置されておらず、システム管理やセキュリティ対応において様々な問題を抱えている。さらに、近年多発している医療機関に対するサイバー攻撃に適切に対応を行うには、医療機関の情報システムを適切に管理運用する体制の整備に加え、一般の職員などのITおよびセキュリティリテラシーの向上が必要と考えられる。以上から、本分担研究としては、一般職員等に対するセキュリティ訓練プラットフォームの検討とリファレンスシステムの開発を行うことを目的として研究を実施した。
（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。

令和 3 年度に開発検証したプロトタイプシステムを元に、実運用が可能な迷惑メール対応訓練システムを開発した。本システムにより、一般的な迷惑メール（マルウェア添付、URL 記載）に類似した訓練メールの発信とそのメールの開封・URL アクセス・添付ファイル参照などに関する受信者の行動把握が可能となり、適切なセキュリティ対応に関する訓練を実施するシステムの実現が可能となった。今後は、このシステムを用いたセキュリティ訓練サービスの提供などについて検討を行っていく予定であるが、それと合わせて中小医療機関を適切に支援する体制の整備が必要である。

4．健康被害情報

なし

5．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。