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４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、　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．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)等の展開で外部ネットワークへの接続が進み、患者等にまで利用が拡大する方向性にある。情報化が遅れていた小規模病院、診療所における電子カルテの普及も進みつつある。また、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状況もある。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。変化と対策の将来像は双方合致した状況に見えるが、現状から理想の将来像に安全に移行できるかが喫緊の課題である。
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調査を行うとともに、2021 年に発生したランサムウェアを用いた組織的攻撃による電子カルテの消失事例も踏まえ、対策の遅れる中小病院等に注力した調査と対策を追加的に検討し、医療機関等の現場に即したサイバーセキュリティ対策のあり方を次世代技術や他分野の手法も取り入れて明らかにする。
具体的に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し、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や、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、現場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

（3）研究の実施経過

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。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。

（4）研究により得られた成果の今後の活用・提供

サイバー攻撃の現状と現在の対策技術、現場の状況の情報収集ができたので、現状の広報すべき情報の戦略ができたと言える。緊急にするべき対策は①把握されていない、医療機関のネットワーク全体図、外部接続、それらの機器の設定情報を含んだ情報機器資産台帳の作成と最新の脆弱性情報の収集チェック方法の確立。②外部接続していない神話に基づく手抜き管理の是正。例えば、管理者権限のベンダー間共有など。③利用者教育は完全ではないので仮想ブラウザーの導入など利用者経由の侵入対策技術の普及。④それでも侵入された場合の端末での検出 EDR, ネットワークでの検出の NDR 導入、およびこれらの検出を容易にする統合仮想サーバ、ネットワークの導入推進。⑤サイバー攻撃を考慮した BCP として遠隔バックアップと携帯等での参照基盤の提唱をする。(WannaCry 以降ネットワーク内に隠れているウイルス排除には時間を要し、その間ネットワークと端末の利用が難しいことから地域医療連携おしどりネットで実施するバックアップ SS-MIX2 の携帯からの常時参照サービスを実施しており、この有効性を想定した。)

2. 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

日本病院会の会員施設のサイバーセキュリティの意識調査を行い、各施設の現実の状況を捉える。

（2）結果概要

昨年度の小規模集団にパイロット調査を行ったアンケートについて、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。

（3）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。

（4）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。

3. 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。

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。

4. 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、教育等の対策、教育方法と評価方法の整理

（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

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。

（3）研究により得られた成果の今後の活用・提供

本研究で開発したシステムについて、当センター迷惑メール対応訓練の実施において活用するとともに、関係機関と協力し、外部の医療機関などにおいて迷惑メール対応訓練などのセキュリティ対応訓練を実施する際にサービスの提供を行うことを検討している。

5. 健康被害情報

なし

6. 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。