別紙3

厚生労働行政推進調査事業費補助金（地域医療基盤開発推進研究事業）
総括研究報告書

テーマ：医療機関におけるサイバーセキュリティ対策向上に向けた実態調査に関する研究

研究代表者　武田理宏　大阪大学大学院医学系研究科　医療情報学　教授

研究要旨

本研究は、医療機関におけるサイバーセキュリティ対策の現状と課題を明らかにし、厚生労働省「医療機関におけるサイバーセキュリティチェックリスト」の実効性向上に資する方策を検討することを目的としている。研究では、全国の医療機関を対象とした Web アンケート調査、先進的な対策を実施している医療機関へのインタビュー調査、ならびに電子カルテベンダーへのインタビュー調査を行った。

アンケート調査では全国 550 施設から回答を得た。その結果、多くの施設で CISO や医療情報システム安全管理責任者の設置、規程類の整備、オフラインバックアップ、IT-BCP 策定など、チェックリストに基づく対策が進展していることが確認された。一方で、サイバーセキュリティ専門人材の不足、ネットワーク機器を含む資産管理の不十分さ、アクセスログの分析不足、不要アカウント管理の不徹底など、運用面における課題が明らかとなった。特に、サーバや端末 PC へのセキュリティパッチ適用率や、サーバ・ネットワーク機器に対する二要素認証導入率は十分とは言えず、医療情報システムの安定稼働との両立が大きな障壁となっていた。

施設インタビュー調査では、先進施設において「侵入防止」を重視した従来型対策から、「早期検知と迅速復旧」を重視するレジリエンス型対策への移行が進んでいることが示された。具体的には、オフラインバックアップを用いた復旧訓練、IT-BCP に基づく災害訓練など、実際のインシデント発生を想定した訓練が実施されていた。また、リモートメンテナンス回線管理、MDS/SDS を活用したベンダー管理、資産管理ツールの活用など、実効性を重視した取り組みも確認された。一方で、多くの施設では専門人材不足やベンダー依存、システムの属人化が課題となっていた。

ベンダーインタビュー調査では、各社とも近年のサイバー攻撃被害を受けてセキュリティ意識の向上とソリューション提供体制の充実が確認できた。一方、地方ではサイバーセキュリティを担う人材不足を課題として捉えていた。現行システムで対応が難しい項目でも、システム更新のタイミングで対策を提供することができることが確認できた。一方、対策にはハードウェアコストや SE 人件費が必要となるため、医療機関のコスト負担が課題になると考えられた。

以上から、チェックリストのうち実施困難な項目として、特に「二要素認証を実装している。または令和9年度までに実装予定である。（2-⑩）」、「セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。（2-⑥）」、「サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。（2-①）」が挙げられた。二要素認証（2-⑩）については、踏み台サーバ、リモートメンテナンス経路等の管理操作部分から優先的に導入し、次期システム更新時に調達仕様へ明記することやクラウド型電子カルテの導入が考えられる。セキュリティパッチ（2-⑥）については、適用範囲、頻度、検証方法、停止時間、費用負担をシステム導入時又は更新時に保守契約へ含めることで対応することが想定される。台帳管理（2-①）については、資産管理ツール、ネットワークスキャン、物理棚卸、構成図更新を組み合わせ、外部接続点の把握と一体的に管理することが有効と考えられた。

A. 研究目的

医療分野は、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活または社会経済活動に多大なる影響を及ぼす恐れが生じる重要インフラ分野の1つに定められている。政府においては、医療分野における DX を、スピード感を持って進めているところ、近年、医療機関におけるサイバー攻撃被害が増加しており、地域医療を支える医療機関が、実際に、サイバー攻撃により、長期にわたり診療が停止し、地域医療の安全性を脅かす事案が発生している。

医療機関等におけるサイバーセキュリティ対策について、厚生労働省は「医療情報システムの安全管理に関するガイドライン」のうち、まずは医療機関が優先的に取り組むべき事項を「医療機関におけるサイバーセキュリティチェックリスト」（以下「チェックリスト」という」としてまとめている。しかし、チェックリストについては、令和 6 年 2 月から 3 月にかけて実施された「病院における医療情報システムのサイバーセキュリティ対策に係る調査」（以下「サイバーセキュリティ調査」という）の結果、一部の医療機関において対応できていない項目が存在することが明らかとなっている。対応困難な項目について対応できないまま放置することはサイバーセキュリティ対策として好ましくないことは当然である。一方、医療機関ごとの努力での解決を求めていては、多くの医療機関で対応の遅れが継続することになると想定され、保健所の立入検査やサイバーセキュリティ調査では解明できない、医療機関や電子カルテメーカ側の課題を明らかにすることが重要である。

本研究では、全国の医療機関に対する Web アンケート、チェックリスト対応ができている医療機関へのインタビュー調査、病院情報システム導入事業者との意見交換を通じ、チェックリストの項目の中で対応が難しい項目の洗い出しとその解決方法の提示を行うことを第一の目標とする。さらに、チェックリストの新規追加項目の検討を医療情報システムの安全管理に関するガイドライン」との整合性を確認しながら実施する。本取り組みにより、全国の医療機関にとってよりチェックリストがより実効性の高いものとなり、医療機関が広くサイバーセキュリティ対策を講じる社会の実現をサポートすることを目的とする。

B. 研究方法

1. チェックリストへの対応状況アンケート調査

チェックリストは令和 6 年度版と令和 7 年度版の双方を対象とすることとした。

各施設の対応状況をできるだけ正確に把握するため、質問項目に対する回答選択肢はできるだけ具体的な内容を記載することとした。質問項目は令和 6 年度版チェックリストに従い作成し、令和 7 年度版チェックリストで追加された質問項目を追加する形とした。研究代表者と研究分担者で議論を行い作成した質問項目を別添資料1 「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」への対応状況調査項目に示す。アンケートの質問内容は 8 つのセクション、合計 89 問の質問項目で構成される。最後に、本アンケート調査後に予定された施設インタビュー調査への協力の有無を確認した。

アンケートは Microsoft Office 365 の Form を用いた Web アンケート調査とした。全国自治体病院協議会、全日本病院協会、地域包括ケア病棟協会、日本リハビリテーション病院・施設協会、日本医療法人協会、日本私立医科大学協会、日本社会医療法人協会、日本精神科病院協会、日本病院会、日本慢性期医療協会、労働者健康安全機構、国立大学病院医療情報

部長会、公立大学病院医療情報協議会、日本赤十字社（順不同）の事務局に調査の趣旨を伝え、会員施設にメーリングリスト等を用いて調査協力依頼の発出を依頼した。アンケートへの回答は任意とした。情報セキュリティ対策が不十分な施設にも回答いただけるように、施設を特定できる情報は収集しないことを原則とした。インタビュー調査を行う医療機関の選定の都合上、インタビュー調査を行う医療機関のみ施設情報の収集を行った。ただし、アンケート調査結果の解析作業では施設情報は削除し、匿名の状態で解析を行った。

2. チェックリストへの対応状況の施設インタビュー調査

チェックリストへの対応状況のアンケート調査で 68 施設（12.4%）がインタビュー調査に協力すると回答があった。アンケート調査で対応が分かれる質問項目、対応が難しい質問項目で研究代表者、研究分担者が、対応が進んでいると判断した医療機関を選定し、インタビュー調査依頼を行った。インタビュー調査は研究分担者 1 名が訪問調査し対面で調査、意見交換を行い、研究代表者や他の研究分担者は Web 会議で接続をして議論に参加することを原則とした。併せて、研究分担者の所属施設のサイバーセキュリティ対策状況についても調査を行った。研究代表者より 11 施設にインタビュー調査依頼を行い、承諾が得られた 9 施設に訪問調査を行った。研究分担者所属施設を含め、調査対象となったのは以下の 11 施設である。研究代表者、分担者で定めたインタビュー調査内容を別添資料2に示す。

施設	特徴
A	大都市圏に位置する大規模な高度急性期病院。救命救急、循環器、がん、難病など専門性の高い診療を担い、広域医療圏の三次救急中核として機能する。行政系病院として災害医療や感染症対応にも強みを持つ。
B	地域中核都市に立地する大規模急性期総合病院。高度救急医療を担い、周産期・小児・救命救急体制が充実している。幅広い診療科を備え、地域住民の基幹病院として機能している。
C	工業地域に立地する中～大規模の急性期病院。企業系病院として発展し、循環器や外科系診療、救急医療に強みを持つ。地域医療と先進医療を両立し、職域医療の色彩も特徴的である。
D	地方中核地域に位置する大規模地域基幹病院。救命救急や災害医療、がん診療を担う公的病院であり、周辺地域から重症患者が集まる。災害派遣や地域連携にも積極的である。
E	大都市中心部に立地する大規模大学病院。高度先進医療、臨床研究、教育機能に優れ、全国から難治例が集まる。専門外来や低侵襲治療も充実した高度医療機関である。
F	首都圏近郊にある中～大規模急性期病院。地域医療支援病院として救急・周産期・がん診療を幅広く提供する。災害拠点機能を持ち、広域医療圏の中核病院として役割を果たしている。
G	地方圏に位置する大規模大学病院。高度急性期医療と研究を担い、先端放射線治療など高度専門医療に特色を持つ。地域医療の最後の砦として広域患者を受け入れている。
H	地方地域に立地する中～大規模大学病

	院。地域人口は比較的少ないが、広域の高度医療を一手に担う役割が大きい。地域医療連携や高齢者医療にも力を入れている。
I	大都市圏に位置する国内有数の大規模大学病院。再生医療、ゲノム医療、高度手術など先端医療を展開し、研究力にも優れる。広域から重症例が集まる高度医療拠点である。
J	地方地域にある中規模病院で、回復期・慢性期医療の比重が高い。地域密着型の医療提供を行い、高齢患者の継続診療やリハビリテーションに特徴がある。地域包括ケアへの関与も強い。
K	大都市近郊の住宅地域に立地する中規模の精神科・慢性期中心病院。高齢者医療や認知症、長期療養支援に力を入れ、地域包括ケア病床やリハビリ機能も備える。生活支援型医療を担う施設である。
L	伝統ある医学教育機関に附属する大規模大学病院。高度専門医療を提供し、周産期、移植、がん診療などに強みを持つ。教育・研究活動と地域連携を両立している。

3. チェックリストへの対応状況のベンダーインタビュー調査

インタビューに対応可能であった大手電子カルテベンダー3 社を対象に、セキュリティ対策の支援状況や運用上の課題についてインタビュー調査を行った。対象とした 3 社は、主に中規模から大規模の医療機関向けに電子カルテシステムの導入・保守を行うベンダーであり、医療情報システムの基盤構築、運用支援、保守対応などに関与している。これらのベンダーを対象とすることで、医療機関におけるサイバーセキュリティ対策に対して、ベンダー側がどのような支援を行っているか、また医療機関との役割分担や実務上の制約がどのように生じているかを把握することを目的とした。

（倫理面への配慮）

本研究は医療機関や電子カルテベンダーに対するアンケート、インタビュー調査であり、人を対象とする研究は含まれず、倫理的配慮は該当しない。

C. 研究結果

1. チェックリストへの対応状況アンケート調査

550 施設から回答を得た。詳細は別添資料 3「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」への対応状況調査結果に示す。

【医療情報システム安全管理責任者を設置している。(1-(1))】

CISO と医療情報システム安全管理責任者（以下、安全管理責任者）を配置していないと回答した施設は 6.4%にとどまり、チェックリストの項目とすることで設置が進んでいることが確認できた。CISO の知識レベルは「一定の専門知識はあるが支援が必要」と「ほとんど知識がない」が同程度で最も多かった。安全管理責任者は「ほとんど知識がない」の割合は下がり、「一定の専門知識はあるが支援が必要」が多くを占めた。IPA の資格、試験を取得している割合は高くなかった。

医療情報システム管理部門の設置は 80.0%の施設で行われていた。アンケート回答施設の選択バイアスが入っている可能性はあるが高い割合であった。しかし、IPA IT スキル標準レベル 4 以上相当を有する情報セキュリティ人材を配置している施設は 5.3%、専門知識を有する情報セキュリティ人材を配置している施設は 38.0%にとどまった。

組織体制は整ってきているが、専門知識がついてきていない状況が明らかになった。専門知識獲得に向け、サイバーセキュリティ教育のさらなる充実やIPAの資格、試験の取得奨励が必要と考えられた。

【サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。(2-(1))】

台帳管理を行っていない施設はほとんどなかったが、全機器を把握している施設は、サーバ 70.7%、端末 PC62.0%、ネットワーク機器48.2%であり、特にネットワーク機器の網羅的管理の難しさが明らかになった。台帳管理はほとんどの施設がエクセル等の汎用ソフトであった。資産管理ツールを導入することで網羅的な管理に近づくと考えられるが、導入コストが必要となる。費用対効果を説明するため、好事例を示す実例を作ることが必要と思われる。

外部接続回線を全て把握している施設は70.5%で、回線削減の必要性を感じている施設は 79.6%に上った。回線数を減らす努力は多くの施設が感じていたが、実際に努力を実施している施設の割合は、全てを把握している施設では 51.3%、一部のみ把握している施設では36.6%と大きく差があり、回線を全て把握することと回線数を減らす努力が表裏一体であることがうかがわれた。適切に管理可能な回線数は「10回線以内」が大半であった。

【リモートメンテナンス(保守)を利用している機器の有無を事業者等に確認した。(2-(2))】

自施設が管理するリモートメンテナンス環境を持つ施設は62.9%であったが、その仕組みのみを許可している施設は18.2%にとどまり、ベンダー側の理由で例外を認めざるを得ない状況が明らかになった。リモートメンテナンスの全容を把握できていない施設が18%存在し、ベンダー依存による管理不足が明らかとなった。

医療機関では、自施設でリモートメンテナンスの仕組みを構築し、可能な限り例外は認めず、例外を認める場合は、例外で接続するリモートメンテナンス回線を把握し、管理することが求められると考えられた。

【事業者から製造業者/サービス事業者による医療情報セキュリティ開示書(MDS/SDS)を提出してもらう。(2-(3))】

MDS/SDSの提出を受けている施設は93.5%と高率であったが、内容を確認し具体的対策まで実施している施設は25.5%にとどまった。多くは提出を受けるのみで、十分な活用には至っていなかった。一方で、二要素認証やパッチ対応の要求など、積極的に活用する事例も認められた。

【利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))】

サーバやネットワーク機器では、ユーザごとにIDと利用権限を設定し、パスワードは機器群ごとに異なっていることが理想であるが、これが実現できている施設はサーバで 11.3%、ネットワーク機器で 10.2%にとどまった。組織外からのセキュリティ対策と組織内のセキュリティ対策を考えると、前者では機器群ごとに異なるパスワードの設定を行うこと、後者ではユーザごとに異なる ID と利用権限を設定することが大切になる。パスワードが機器群ごとに異なっている施設の割合は、サーバで 67.3%、ネットワーク機器で 61.8%である程度の医療機関が対応していることが明らかになった。

端末PCではOSのユーザ認証を行っている施設の割合は32%、OSは同一ユーザ、ソフトウ

ェアでユーザ認証を行っている施設が 63.3%であった。OS は administrator 権限で自動ログインを行っている施設も 17.5%認める状況であった。端末 PC のエンドユーザに対するアクセス利用権限は約半数の施設が個別のユーザ ID を発行し、使いまわしをしているユーザ ID はなかったが、管理者権限の ID の使いまわしがあると回答した施設も少なくなかった。管理者権限の ID 使いまわしがあると回答した施設も一定数見られ、改善が必要と考えられた。

【退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))】

全て、削除または無効化できていると回答した施設の割合はサーバが 73.5%、端末 PC が 71.1%であった。リアルタイムに不要なアカウントを削除または無効化している施設の割合はサーバが 63.1%、端末 PC が 62.7%であったが、年に1回など棚卸作業をしている施設を含めるとサーバが 91.6%、端末 PC が 93.1%であった。削除または無効化できていないアカウントを如何に減らすかを検討することが、セキュリティ担保に必要と考えられた。

【アクセスログを管理している。(2-(6))】

多くの施設が全て、あるいは一部のアクセスログを残していたが、定期的にアクセスログを確認している施設は多くなかった。アクセスログの保管期間を把握していない医療機関も少なくなかった。アクセスログを漫然と残している医療機関はその取扱いについて、保守事業者と議論をする機会を持つことも必要と考えられた。

【セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))】

サーバに対するセキュリティパッチを適用していない施設の割合は 47.8%、端末 PC に対しては 53.8%、ネットワーク機器に対しては 34.5%であり、その割合は低くなかった。セキュリティパッチを適用している施設でも、セキュリティパッチを適用するタイミングは適用が必要なセキュリティパッチが出てきたタイミング、セキュリティパッチを当てる範囲は保守事業者が推奨するセキュリティパッチとした施設が多く見られ、定期的にセキュリティパッチを当てる、あるいは医療機関がセキュリティパッチの必要性を判断するといった施設は多くなかった。

サーバや端末 PC に対するセキュリティパッチの適用は医療情報システムの安定稼働のリスクとなり、保守事業者の検証作業が必須となる。保守事業者にとっては、検証作業にはシステムエンジニアの人件費が必要となる。セキュリティパッチを適用する費用は保守費用に含まれると回答した施設が約 8 割であったが、これらの施設で医療情報システム導入時にこれらの費用が十分に見込まれていたかは明らかではない。作業費用を勘案すると、定期的なセキュリティパッチの適用は見送りとなっているケースも懸念される。また、保守事業者主導で適用範囲を決めていることも適切な判断となっているか、医療機関側からの判断は難しい。

セキュリティパッチの適用時はサーバ再起動などでシステム停止が必要となる。一方、端末 PC はエンドユーザが適用するタイミングを調整することでその影響は最小限にすることができる。以上を考えると、特にサーバへのセキュリティパッチの適用の回数は慎重に考える必要がある。

以上を考えると、医療機関と保守事業者はできればシステム導入時にセキュリティパッチの適用のあり方について意見交換を行い、その作業費用を見込んだ保守費用を見込むことが、

もっとも適切なセキュリティパッチの適用タイミングと適用範囲の決定につながると考える。

【接続元制限を実施している。(2-(8))】

ネットワーク機器で接続元制限を実施している施設は 79.8%であった。管理や監視は病院とネットワーク事業者の共同対応が多く、一部は事業者任せとなっていた。ネットワーク事業者任せにせず、医療機関が関わっていく姿勢が大切と考えられた。

【バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))】

不要ソフトウェアやサービスの停止は約 9 割の施設で実施されていたが、多くは導入時確認のみで、定期点検は少なかった。エンドユーザによるソフトウェア導入は制限され、管理者のみがインストール可能とする施設が多かった。一方で、不要ソフトウェアの判別が困難との意見もあった。

【パスワードは英数字、記号が混在した 8 文字以上とし、定期的に変更している。※二要素認証、または 13 文字以上の場合は定期的な変更は不要(令和 7 年度 2-⑦)】
【パスワードの使いまわしを禁止している(令和 7 年度 2-⑧)】
【二要素認証を実装している。または令和9年度までに実装予定である。(令和 7 年度 2-⑩)】

パスワードは、英数字、記号が混在した 13 文字以上としている、あるいは、パスワードは、英数字、記号が混在した 8 文字以上とし、定期的に変更していることを実現できていない施設がサーバ)、端末 PC、ネットワーク機器ともに半数以上を占めた。

医療情報システムの安全管理に関するガイドラインでは、医療情報システムの更新の機会に二要素認証を行うことを意識して、令和 3 年度からから令和 9 年度までに二要素認証の実装を促してきた。しかし、本調査では、1要素認証と回答した施設がサーバ、端末 PC、ネットワーク機器のいずれでも 8 割を超えていた。二要素認証を必ず実装する、実装を検討する(実装の可能性が高い)と回答した施設は、サーバが 35.1%、端末 PC が 53.2%、ネットワーク機器が 24.9%であり、特にサーバ、ネットワーク機器の二要素認証の普及は施設側の意識が低く、時間だけでは解決しないと考えられた。

【USB ストレージ等の外部記録媒体や情報機器に対して接続を制限している。(令和 7 年度 2-⑨)】

サーバへの USB 接続を制限している施設は多かったが、端末 PC や部門システム端末では一定数が自由接続可能であった。また、システム制御ではなく運用ルールで制限している施設も多く、利用者教育の重要性が示された。

【3. インシデント発生に備えた対応】

連絡体制図を整備している施設は 9 割超であったが、定期見直しを行う施設は 67.3%であった。バックアップについては、全システムを対象とする施設が 45.1%、必要データを選定している施設が 32.9%であった。オフラインバックアップは 71.6%で実施されていたが、復旧訓練まで行う施設は 6.3%にとどまった。サイバー攻撃を想定した BCP は 84.5%が策定しており、多くが厚労省 BCP を参考としていた。

【4. 規程類の整備(令和 7 年度)】

多くの施設で規程類の策定が進んでいた。今後、定期的な見直しを行う施設を増やしてい

くことが大切と考えられた。

2. チェックリストへの対応状況の施設インタビュー調査

組織体制・セキュリティ人材

医療機関におけるサイバーセキュリティ対策において、専門人材の確保と組織体制の整備が共通課題として挙げられていた。C 病院では、副院長を CSIRT 委員長とし、グループ企業本社の CISO 体制と連携することで、経営層を巻き込んだガバナンスを構築していた。D 病院では、情報処理安全確保支援士および上級医療情報技師の資格を持つ責任者が中心となり、高度な専門性を内製化していた。

一方、B 病院や E 病院では、放射線技師や検査技師などのコメディカル職員を医療情報部門へ兼務配置し、現場と情報部門をつなぐ役割を担わせていた。これにより、現場のニーズを反映した運用やセキュリティ意識の浸透が図られていた。また、E 病院では、インターン受入や資格取得支援など、人材育成にも取り組んでいた。

しかし、多くの施設で高度な IT 知識と医療現場理解を兼ね備えた人材の不足が指摘されていた。特に中小規模施設では、専門人材を単独で確保・維持することが難しく、外部委託や地域連携による支援体制の必要性が示されていた。また、F 病院では、長年システム運用を担ってきた職員への依存が大きく、経験知の属人化が課題とされていた。

資産管理

資産管理については、多くの施設で Excel 台帳に加え、資産管理ツールを併用していた。B 病院では、CAD 図面上に端末配置をマッピングし、物理的配置を視覚的に把握できるようにしていた。D 病院では、資産管理ソフトを用いた全数棚卸を毎年定例化していた。

F 病院では、Excel と SS1 を併用し、今後 ARMIS による情報収集を予定していたが、ネットワーク未接続機器や旧機器、部門管理機器の把握に課題があるとされていた。また、資産管理ツールを用いることで、台帳管理だけでなく、ログ取得や外部記録媒体制御にも活用している事例がみられた。

外部接続点管理

外部接続点管理では、リモートメンテナンス回線の統制が重要課題として挙げられていた。A 病院では、セキュリティレベルを満たさない機器の導入を許可しない運用を実施していた。B 病院では、独自の「リモート規約」を全 22 ベンダーに適用し、病院側が接続の主導権を保持していた。

H 病院および I 病院では、自施設が構築したリモート接続基盤を原則利用していたが、J 病院および K 病院ではベンダーごとの接続方式を許容していた。F 病院でも、リモート接続は申請制としていたが、ポケット Wi-Fi 等による把握外接続の可能性が課題とされていた。

また、古くから設置されているネットワーク機器について、管理しきれていない可能性も指摘されており、外部接続点を含むネットワーク機器の継続的管理が必要とされていた。

MDS/SDS への対応

MDS/SDS については、ほぼ全施設で収集が実施されていた。C 病院では、「×」や空欄回答について理由を確認し、曖昧な回答を許容しない運用を行っていた。F 病院でも、リモートメンテナンス事業者に SDS 提出を求め、内容確認を行っていた。

一方で、MDS/SDS を単なる提出書類として扱うのではなく、リスク評価や導入可否判断へ活用する必要性が示されていた。また、製造元ベンダーと導入ベンダーでセキュリティ意識に差があるケースも報告されており、医療機関側がチェックシートを用いて主体的に確認する重要性が指摘されていた。

ユーザ管理

ユーザ管理では、多くの施設で退職者アカウント削除や有効期限設定が実施されていた。H 病院では、機器ごとに異なるパスワードを設定し、複雑性要件をベンダーへ求めていた。一方、他施設では、複数機器で同一パスワードを利用している事例もみられた。

F 病院では、ベンダーアカウント情報漏えいを契機に、特権管理者パスワードをランダム 13 桁へ変更し、台帳管理を実施していた。また、人事情報と連動したアカウント発行・停止や、申請書に基づく権限付与も行われていた。

特権ユーザ運用やパスワード共有は、ランサムウェア感染時の水平展開リスクを高めることから、認証情報管理の厳格化が重要とされていた。

各種ログ管理

ログ管理については、保存自体は実施されている施設が多かったが、分析・活用まで十分に行えていない実態がみられた。H 病院および I 病院では、広範囲のアクセスログ保存を実施していたが、J 病院および K 病院では電子カルテ以外のログ保存が不十分であった。

F 病院では、eventlog/syslog 収集や踏み台サーバでの操作動画記録を実施していたが、ログ相関分析は困難であり、通常時の解析は限定的とされていた。また、ログの定期確認についても人的リソース不足から継続困難との意見が挙がっていた。

セキュリティパッチ管理

セキュリティパッチ管理では、A 病院が計画停止時間を設定し、定期的にパッチ適用を行っていた。サーバへのパッチでは 3 ヶ月に 1 回、3時間のシステム停止時間枠を設けており、臨床業務への影響は少なくないと思われる。D 病院では、パッチ適用困難な機器に対し EDR を導入し、重点監視によるリスク低減策を実施していた。

一方、多くの施設では、医療機器の動作保証や保守契約上の制約から、十分なパッチ適用が困難であった。F 病院でも、WSUS による定期適用を行っていたが、アプリケーションやミドルウェアではベンダー依存が残っていた。また、モダリティ機器などでは、ベンダー側から安定稼働を理由にパッチ適用が認められないケースも報告されていた。

二要素認証への対応

二要素認証については、A 病院で IC タグと顔認証を組み合わせた低コスト運用が行われていた。F 病院では、一部部門でアプリケーションを利用し、電子カルテ端末への導入を予定していた。I 病院では電子カルテ端末は IC カードとパスワードの二要素認証を、ユーザのなりすまし防止を目的に導入をしていた。

外部記憶媒体管理

外部記憶媒体管理では、F 病院において SS1 によるシリアル番号制御と物理 USB ストッパーによる制限が行われていた。また、資産管理ツールを用いた接続制御も複数施設で実施されていた。USB メモリ等の利用については、

完全禁止ではなく、接続制御や申請運用による管理が実施されていた。

I 病院では電子カルテ端末はシステム制限により許可された USB メモリのみ接続できる設定となっていたが、電子カルテと別調達の部門システムワークステーションは USB メモリの接続制御ができなかったため、USB ポートガードを使用することで不適切な USB メモリ接続を防止する努力を行っていた。

システムバックアップ運用管理

バックアップについては、多くの施設でオフラインバックアップや複数世代管理が実施されていた。A 病院では、Azure クラウド上で 24 時間以内復旧の実証を行っていた。D 病院では、Veeam によるバックアップ運用が行われており、OS レベルからのリストア訓練を実施し、異なる仮想化基盤間での復旧も検証していた。

H 病院でも復旧訓練が行われていた一方、J 病院では復旧手順の十分な確認ができていないとされていた。F 病院では、Rubrik によるイミュータブルバックアップを導入していた。

オフラインバックアップや複数世代管理はチェックリストへの掲載で医療機関での対応が進んでいるが、インタビュー調査を行った施設では復旧訓練を行っている施設も複数あることは印象的であった。

IT-BCP の策定と訓練

IT-BCP については、全施設で策定自体は進められていた。C 病院では、100 名規模による紙カルテ訓練を実施していた。D 病院では、異常検知連絡訓練や現場スタッフを含めた IT-BCP マニュアル共同策定を行っていた。

B 病院では、机上訓練を通じて人的リソース不足などの課題抽出を行っていた。F 病院でも、年 1 回の机上訓練を開始していた。

その他

全体を通じて、インタビューを行った医療機関のサイバーセキュリティ対策は、「侵入を完全防止する」考え方から、「早期検知と迅速復旧を重視するレジリエンス型対策」へ移行していることが示されていた。

また、セキュリティ対策は、単なるチェックリスト対応ではなく、実効性を伴う運用が重要であると認識されていた。特に、バックアップ復旧訓練、紙カルテ訓練、ログ監査など、実際に「動かして確認する」取り組みが先進事例として挙げられていた。

一方、ベンダー依存の課題も多く報告されており、医療機関側が要件定義力を持ち、保守契約や調達仕様にセキュリティ要件を明記する重要性が示されていた。地域単位での情報共有や支援体制の構築も、現実的な対応策として必要性が指摘された。

3. チェックリストへの対応状況のベンダーインタビュー調査

全体として、インタビュー調査した各ベンダーとも昨今のサイバーセキュリティインシデントを受けて対策意識は高まっており、一定の対応方針や改善の方向性は示されていた。一方で、実効性のある対策を継続的に行うためには、ベンダー個別の努力だけでは限界があり、調達範囲、責任分界、費用負担、医療機関側の体制整備を含めて整理すべき課題が残されていると考えられた。特に、仕様にどこまで含めるか、部門ベンダーまで含めてどのようにガバナンスを及ぼすかが重要であると考えられる。

外部接続点管理

外部接続点管理については、各ベンダーとも近年のランサムウェア被害等を踏まえ、VPN 装置やリモート保守経路を重要なリスクポイントとして認識していた。A 社および B 社では、専用線や閉域網、自社ゲートウェイ等を用いて接続点を集約し、できる限り外部接続箇所を限定する方向で構成管理を進めていた。A 社では部門システムベンダーも含めた集約型リモート保守環境を整備し、B 社では大規模病院を中心にデータセンター経由の閉域構成を採用していた。一方、C 社では二要素認証や踏み台サーバ利用等の推奨方針は示されていたものの、ネットワーク自体を自社で統制するケースは限定的であり、施設や他ベンダーに依存する側面が大きかった。

この違いの背景には、インフラ領域を誰が調達・構築するかという責任分界の差が存在する。A 社・B 社はネットワークを含めた統合提案を行うことが多く、一定のセキュリティガバナンスを及ぼしやすい一方、別調達となるケースでは統制が及びにくくなる。実際、A 社・B 社でも中小規模施設では別のシステム企業が導入を担う事例があり、その場合には C 社と同様の課題が生じていた。

サイバー攻撃の多くが VPN 装置等を侵入口としている現状を踏まえると、医療機関側が全ての外部接続点を把握し、ベンダー横断的な管理基準を定めることが極めて重要と考えられる。

MDS/SDS への対応

MDS/SDS 対応については、いずれのベンダーでも、本社でパッケージに応じた MDS/SDS のひな型を整備・提出する運用が中心であった。主にひな型をベースとし、現地要件に応じて修正する運用としていた。

ユーザ管理

ユーザ管理では、各ベンダーとも特権付与を最小限に抑える方向性を示していた。A 社ではクライアント端末に原則として管理者権限を付与しない方針を明確にしており、必要時には端末限定やネットワーク分離を行う運用を採用していた。B 社でも新規システムでは特権なし運用が可能となっている一方、旧システムでは保守や設定変更に特権が必要となる場合が残されていた。C 社では顧客要件に応じて権限設計を行っていたが、システム制約から固定 ID や広範な権限運用が残存するケースもみられた。各ベンダーともに影響範囲の大きさから現システムについて権限の変更などを行うことは難しいことが明らかとなった。

医療機関においては、自施設のシステムの更新時期などを確認した後、ベンダーに調査依頼を行い、実態が明らかになった場合、外部接続をより強固なものにする、エンドポイントセキュリティの製品の導入など別の手段でセキュリティ対策を高めるのが望ましいと考えられた。

セキュリティパッチ管理

セキュリティパッチ管理では、A 社・B 社は社内評価・検証体制を持ち、脆弱性情報の確認や検証を定期的に実施していた。しかし、部門ベンダーとの調整やシステム停止を伴う作業が大きな制約となっていた。特にサーバーパッチでは、診療停止リスクとのバランスを考慮すると、施設ごとの個別協議が必要となるケースが多かった。一方、C 社では脆弱性確認やテスト環境適用までは実施していたものの、最終的な適用判断や動作確認は医療機関側に委ねられる部分が大きかった。

中小規模の医療機関では、十分な担当者

を確保することが難しく、本来であれば継続的な支援が望ましいが、現実にはそのための費用を確保しにくいという難しさがある。その結果、パッチ適用やネットワークのガバナンスが後回しとなり、脆弱性が生じやすい構造が継続していると考えられた。

二要素認証への対応

二要素認証については、端末側では概ね導入が進んでいたが、サーバ側では十分な実装が進んでいない実態が明らかとなった。特にサーバ側の認証については、ガイドラインで求められる水準との間に乖離があり、たとえ医療機関側が対応を求めたとしても、現行システムや構成上の制約から直ちに実装することが困難な場合があることが明らかになった。

サーバ二要素認証について、研究代表者がある電子カルテメーカにさらに確認したところ、技術的な観点からは、Windows Server の基本機能である Active Directory ドメインサービス（AD DS)と、その証明書を発行する機能である Active Directory 証明書サービス（AD CS)を組み合わせることで、追加の有料ライセンスなしで、スマートカード認証は構築できるとの回答であった。Windows Server の標準機能（グループポリシー、またはユーザー属性）を使えば、「この管理者アカウントは、スマートカードを挿さないと絶対にログオンできない（パスワード入力を受け付けない）」という強制設定も可能とのことであった。本設定で、想定される運用は、以下の通りとなる。

① サーバの目の前でログオンする場合（コンソールログオン）

(1) サーバ機に USB などで「スマートカードリーダー」を接続。
(2) サーバのログオン画面で、管理者のスマートカードを挿入。 ＃一要素
(3) 画面に PIN（暗号番号）の入力が求められるので、PIN を入力。＃二要素
(4) サーバ内の Active Directory 機能がカード内の証明書を検証し、ログオンが許可。

② 自分の席からサーバを操作する場合（リモートデスクトップログオン）

(1) 手元の PC にスマートカードリーダーを接続し、カードを挿入。＃一要素
(2) リモートデスクトップ（RDP）でサーバに接続。
(3) 接続画面で PIN を入力すると、手元の PC に挿してあるスマート＃二要素
カードの情報をネットワーク越しにサーバに転送し、サーバ側で認証を実施。

一方、スマートカード認証では証明書を使い、AD 証明書サービスの構築・運用、証明書テンプレート設計、スマートカードへの証明書書き込み、有効期限管理を個別に行う必要がある。現行システムや構築する次期システムで実行できるかと言われるとかなり難しい。現状では、ガイドライン 7.0 版(案)に示されるように VPN 装置や踏み台サーバ等、外部接続経路における二要素認証や EDR による振る舞い検知を優先的に実装することが現実的な対策と考えられる、とのことであった。

4. チェックリスト対応困難項目の主な困難要因と実施可能とするための解決策

以上を踏まえ、チェックリストのうち対応が困難な項目を、主な困難要因、実施できていた病

院の対応例、実施可能にするための解決策を取りまとめた（別添資料4）。本調査で明らかとなったチェックリストの実施状況に従い、(1) 二要素認証を実装している。または令和 9 年度までに実装予定である。（2-⑩）、(2) セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。（2-⑥）、(3) サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。（2-①）、(4) リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。（2-②）、(5) インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。（3-②）、(6) アクセスログを管理している。（2-⑪）、(7) 医療情報システム安全管理責任者を設置している。（1-①）、(8) 事業者から製造業者／サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。（2-③）、(9) 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。※管理者権限対象者の明確化を行っている（2-④）、をリストアップした。

D. 考察

アンケート調査では、「医療機関におけるサイバーセキュリティチェックリスト」が医療機関のサイバーセキュリティ対策の方向性を示し、各医療機関がその方向に向かって対策が進んでいることが明らかになった。一方、チェックリストは yes/no の二択での回答であり、yes と回答する判断基準は施設によって異なる。また、チェックリストは保健所の立ち入り調査で使用されるため、医療機関は no と回答することに抵抗がある。この結果、チェックリストは yes の多い回答となり、その甘い自己評価が当該施設のサイバーセキュリティ対策を遅らせることが懸念される。また、他施設でも yes と回答する傾向があることを医療機関は感じており、他施設と自施設との状況比較ができないことにつながっている。本アンケート調査では、チェックリストの各項目に対し、具体的な対策状況を把握できる回答項目を作成した。この結果、チェックリストで yes と回答している場合でも、対策の進捗状況は医療機関ごとにかなり異なることが明らかになった。また、本アンケート調査は匿名で、立ち入り検査などで使用されることもないため、チェックリスト項目によっては多くの医療機関で対策が進んでいない状況が明らかになった。

一方、研究班でインタビュー調査ではチェックリストに対して積極的に対策を進める医療機関を中心に選定を行った。これらの医療機関のいくつかの施設では、医療機関におけるセキュリティ対策は、単なるツールの導入フェーズから、組織的なレジリエンス（回復力）の検証というフェーズへ移行しており、チェックリスト記載事項を超える対策を進めていた。

ベンダーへのインタビュー調査では、各ベンダーとも昨今のサイバーセキュリティインシデントを受けて対策意識は高まっており、一定の対応方針や改善の方向性は示されていた。一方、ユーザ管理などは、影響範囲の大きさから現行システムについて権限の変更などを行うことは難しい見解が示された。現行システムへの対応が困難な事項については、サイバーセキュリティを最低限担保できる対策を取りながら、次期システムで適切なサイバーセキュリティ対策を仕様に含める必要があると考えられた。

サイバーセキュリティ対策はベンダーにとっても作業コストやハードウェアコストが必要となる。サイバーセキュリティ対策への対応が困難とベンダーが回答する事例として、仕様書に医療機関が求めるサイバーセキュリティ対策が記載

されておらず、サイバーセキュリティ対策に必要な作業費用が保守料金に十分含まれていないケースがあると考えられた。

また、ベンダー側にも特に中小医療機関や地方の医療機関を中心に、サイバーセキュリティ対策の知識を持つ作業者の確保が難しいことが示された。ベンダーが医療機関に適切なサイバーセキュリティ対策を提供する体制は以前より整ってきているが、ベンダーに任せていては十分なサイバーセキュリティ対策を取ることはできない。医療機関側はサイバーセキュリティ対策に知識を持つ人材を確保し、ベンダーと良好なコミュニケーションをとり、責任分界点を決めていくことが、サイバーセキュリティ対策に重要と考えられた。

本考察では、アンケート調査、施設インタビュー調査、ベンダーインタビュー調査で明らかになった課題と今後、検討すべき対策について、令和7年度版チェックリストの項目ごとに取りまとめる。別添資料5は分担研究者である鳥飼幸太がチェックリストへの対応を、Cybersecurity and Infrastructure Security Agency（CISA）が推進する Continuous Diagnostics and Mitigation（CDM）Program に従い、Data Protection Management、Network Security Management、Identity and Access Management、Asset Management の視点で取りまとめたものである。

1. 体制構築

【医療情報システム安全管理責任者を設置している。(1-①)】

チェックリストや診療報酬への記載により、医療情報システム安全管理責任者を設置する医療機関は増加した。アンケート調査の選択バイアスがあるかもしれないが、医療情報システム管理部門を設置する医療機関を多く認めた。一方、サイバーセキュリティに関する専門知識を十分に保有していない安全管理責任者が多いことも明らかになった。情報処理推進機構（IPA）の資格保有、試験合格者の割合も高くなかった。

組織インタビュー調査においても、医療情報システム管理部門の設置、CISOや安全管理責任者の配置、サイバーセキュリティ人材の育成や雇用など、組織体制の整備や人材配置が組織のサイバーセキュリティ対策を進める上で重要であることは間違いない。体制構築、人材配置ができていない医療機関は対応を進めることが望まれる。

サイバーセキュリティ人材の育成と配置については、令和5年度、6年度の厚生労働省科学研究「安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究（課題番号：23IA2007、研究代表者：武田理宏）」を受け、日本医療情報学会（2026 年現在、研究代表者が副代表理事）と IPA は協定を締結し、教育コンテンツの開発や外部人材の活用について検討を進めている。サイバーセキュリティに関する専門知識を十分に保有していない安全管理責任者やサイバーセキュリティ担当者はサイバーセキュリティに関する教育を受けることから始める必要がある。教育を受けることで知識を取得できれば、資格試験に対する心理的なハードルが下がる。獲得した知識の整理や網羅的な知識の獲得、さらなる知識獲得を目指すこと、外部から知識習得に対する評価を受けることを考えると資格取得や試験合格は大切となる。

医療機関においては、情報セキュリティ責任者（CISO）と安全管理責任者、サイバーセキュリティ担当者の役割分担が必要となる。CISO と安全管理責任者は別人物である場合や同一

人物が兼務する場合が想定される。

サイバーセキュリティ対策には投資が必要となる。適切な投資がなければ、適切なサイバーセキュリティ対策は得られない。対策を講じれば講じるほど安全性は高まるが、そこには膨大な費用が発生する。一方、どこまで対策をとっても完全な安全が担保されるわけではない。このため、インタビュー調査対象の医療機関のように「侵入を完全防止する」考え方から、「早期検知と迅速復旧を重視するレジリエンス型対策」に向かっていく必要がある。

サイバーセキュリティ対策には将来的なビジョンを持った上で、適切な投資と人材育成、人材雇用を進めていく必要があり、これは CISO の重要な役割となる。CISOは少なくとも「一定の専門知識を有しているが、対策には情報セキュリティ人材のサポートが必要である」以上の知識を持つ必要がある。単独で対策を進める専門知識が十分でない場合、「一定の専門知識を有しているおり、単独でも対策を進めることができる」知識を有する医安全管理責任者またはサイバーセキュリティ担当者と連携を取る必要がある。医療機関の規模や役割によっては、外部のサイバーセキュリティ人材と適切な契約を結ぶことも想定される。その場合、外部人材は医療情報システムが抱える課題を十分に理解している人材を選定する必要がある。

医療機関はサイバーセキュリティ対策をベンダーに任せきりになってはいけない。安全管理責任者は医療情報システム保守事業者やネットワーク保守事業者と良好なコミュニケーションを取りながら、現行システムに対して講じるべきサイバーセキュリティ対策、次期システムに導入すべきサイバーセキュリティ対策を検討し、医療機関と保守事業者と役割分担、責任分界点を明確にしながら、サイバーセキュリティ対策を講じる必要がある。さらに、組織的なレジリエンスを高めるために、IT-BCP の策定や IT-BCP に基づく災害訓練、データ復旧訓練など、セイバーセキュリティインシデント発生を想定した対策についても、保守事業者と連携しながら進める必要がある。

2 医療情報システムの管理・運用

【サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。(2-①)】

資産管理は情報セキュリティ対策の基本である。アンケート調査で多くの医療機関が台帳管理を行っていたが、漏れなく把握していると回答した施設の割合は高くなく、特にネットワーク機器の台帳管理では 48.2%にとどまった。今後、各医療機関で台帳管理の精度を上げることが求められる。

台帳管理では 8 割程度の施設はエクセル等に汎用ソフトを使用しており、専用ソフトを使用する施設の割合は高くなかった。専用の資産管理ツールは資産台帳の管理のみならず、サーバや端末 PC の操作ログ取得と管理、外部記録媒体の接続制御にも活用できる。また、昨今の医療機器に対するセキュリティ対策を意識して、情報資産危険性自動評価技術も選択のひとつとなる。情報資産危険性自動評価技術は機器の網羅的な把握やリスク評価に用いることが可能である。また、専用ソフトを用いることで、医療情報システム管理者の管理コストを軽減することが可能である。

資産管理ツールや情報資産危険性自動評価技術を導入するためには費用対効果の議論を避けることができない。先行する導入事例を作り、費用対効果の検証を行い、公表する取り組みが有効と考える。システム更新のタイミングでは専用ソフトの導入を議論のテーブルに乗

せる必要があると考える。

適切なネットワーク機器の管理を考えると、外部から医療情報システムに接続している回線数を減らす努力が必要となる。外部から医療情報システムに接続している回線を全て把握していると回答した医療機関は、回線数の減らす努力をしていると回答した割合が多く、外部回線の把握と回線数を減らす努力は表裏一体である。適切に管理できる回線数は医療機関ごとに意見が分かれたが、9 割以上が 10 回線以下と回答しており、まずは 10 回線まで外部回線を減らす努力を行うのが適切と考えられた。

【リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。(2-②)】

ランサムウェアの水平感染のリスクを考えると、リモートメンテナンス回線の適切な管理が重要となる。医療機関は、自施設でリモートメンテナンス環境の構築を行い、可能な限り例外は認めず、自施設のリモートメンテナンス環境を使った保守契約を結ぶことが大切となる。医療機関は「リモートメンテナンスに関する規約」を策定し、リモートメンテナンス環境を利用する保守事業者に遵守させる必要がある。

一方、保守事業者のセキュリティ基準を理由に用意したリモートメンテナンス環境を利用できない保守事業者が一定数存在する。このような場合に保守事業者が用意するリモートメンテナンス環境の利用を許可するか否かは医療機関の責任となる。「リモートメンテナンスに関する規約」では、保守事業者が用意するリモートメンテナンス環境の利用を許可する基準を策定し、接続の主導権を医療機関側で保持する必要がある。

【事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。(2-③)】

医療情報セキュリティ開示書（MDS/SDS）は医療機関が適切なサイバーセキュリティ対策を講じるために有用な文書となる。内容の理解には、一定のサイバーセキュリティ専門知識が必要となるが、医療機関は MDS/SDS の確認を必ず行う必要がある。MDS/SDS に曖昧な点や理解できない点がある場合、放置をせず、必ずベンダーに確認を行うことが大切と考えらえる。MDS/SDS を起点とするベンダーとのコミュニケーションにより医療機関はベンダーのセキュリティに対する考え方を知ることができ、その先の適切なサイバーセキュリティ対策につながると考える。

事業者確認用に「医療機関に製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出した。(2-③)」とあること、医療機関での確認作業を明確に表現することを考えると、医療機関確認用の表現は、「事業者から提出を受ける製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を確認する」と表現したほうが良いかもしれない。

【利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。※管理者権限対象者の明確化を行っている(2-④)】

administrator 権限のみ設定し、全ての機器群で同じパスワードを設定していると回答した施設の割合はサーバで 18.9%、ネットワーク機器で 23.1%、administrator 権限のみ設定し、機器群ごとに異なるパスワードを設定していると回答した施設はサーバで 34.9%、ネットワーク機器で 34.2%と半数以上の施設が administrator 権限のみ設定となっていた。端末 PC も 17.5%の施設が OS は administrator 権限で自動ログ

インを行う設定となっていた。一方、ベンダーインタビューでは、各ベンダーとも特権付与を最小限に抑える方向性を示していた。現行システムで権限設定を変えることは負荷が少なくない。次期システムに更新するタイミングで適切なアクセス利用権限を設定できるよう、医療機関は仕様を考える必要がある。

現行システムでまずできることはパスワード管理である。パスワードは英数字、記号が混在した 13 文字以上とする、ロックアウトを設定するなど、パスワード総当たり攻撃に対する対策を取る必要がある。全ての機器群で同じパスワードを設定している場合、サイバーインシデントが発生した場合に、被害が広がることになる。機器群ごとに異なるパスワードを設定することが望まれる。

【退職者や使用していないアカウント等、不要なアカウントを削除または無効化している。(2-⑤)】

不正アクセスを防ぐため、不要なアカウントを削除または無効化することは重要である。アンケート調査ではサーバ、端末 PC ともに、一部のアカウントが削除または無効化できていない施設やリアルタイムに削除または無効化できていない施設が明らかになった。

エンドユーザは、退職後は物理的に医療情報システムにアクセスすることが困難となることが多い。この場合、可能な限り、リアルタイムでアカウントを削除することを前提に、年に1回など定期的に棚卸作業を行い、不要なアカウントが残っていないか確認作業を行う必要がある。リモート環境で医療情報システムにアクセスできる場合、退職後、速やかにリモートアクセス権限の削除を行う必要がある。

サーバに対するアカウント管理は、管理ユーザ数は限定されるため、より厳密な管理が必要となる。リモートアクセス権限を持たないユーザは、病院スタッフエリアの入館管理、サーバ室への入室管理と合わせて、退職後速やかにサーバ機器を触れない状況を作ることが大切である。リモートアクセス権限を持つユーザは速やかにリモートアクセス権限を削除する必要がある。サーバに対してユーザごとに ID、利用権限を設定している施設は 16.8%にとどまった。このため、サーバ室へのアクセス権限、リモートアクセス権限のはく奪は重要である。保守事業者に対しては、保守事業者の職員管理が必要となるが、医療機関から見るとブラックボックスになる可能性がある。医療機関は保守事業者のリモートアクセス権限の管理がどうなっているか把握をし、適切なリモートアクセス権限の削除を指示する必要がある。

【セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-⑥)】

サーバ、端末 PC へのセキュリティパッチの適用は、「システムの動作保証」や「システム停止を伴う」といった可用性とセキュリティのトレードオフが最大の障壁となる。「システムの動作保証」を考えると保守事業者の検証作業が必要となるが、その作業コストも課題となる。以上のような理由で、医療者側と 保守事業者側がともにセキュリティパッチの適用に消極的になっていたのが、医療情報システムに対するセキュリティパッチ適用率の低さにつながっていたと考えられる。一方、昨今のサイバーインシデントに伴い、ベンダーのセキュリティパッチに適用に対する考え方は変わってきていることが、ベンダーインタビューで確認された。保守事業者の作業費用が確保できれば、セキュリティパッチの適用は進む可能性が高い。

サーバへのセキュリティパッチの適用には、システム停止が必要となる。特に急性期診療を担う医療機関では、夜間であってもシステム停止が診療に与える影響が大きい。システムの動作保証のためには、保守事業者の動作検証が必要となる。動作検証には時間と作業コストが必要となる。以上を踏まえ、医療機関は適切なセキュリティパッチを適用するタイミングを決定する必要がある。必要性の高いセキュリティパッチを可能な限り早く適用することは必須となる。定期的にセキュリティパッチを当てるか否かは、医療機関ごとの判断になるが、少なくとも1年に1回はセキュリティパッチを適用するなどの対応は必要と思われる。

端末 PC へのセキュリティパッチの適用は、研究代表者の医療機関では、期限日を設け、期限日まではエンドユーザが任意のタイミングでセキュリティパッチの適用を行い、期限日までにセキュリティパッチを適用しなかった端末 PC は期限日以降の再起動でセキュリティパッチを適用する運用を行っている。このような運用を行うことで、端末 PC へのセキュリティパッチの適用の診療への影響は最小化することができる。一方、システム動作保証については、基幹システムだけでなく、全ての部門システムに対して実施する必要がある。研究代表者の医療機関では、医療情報システム操作室に検証端末を設置し、各部門システムの SE が動作確認を行っている。診療停止という観点では、端末 PC はサーバよりセキュリティパッチの適用は容易だが、部門システムを含めた検証作業コストを考慮に入れて、セキュリティパッチ適用タイミングを決定する必要がある。

以上を踏まえ、医療機関はサーバ、端末 PC ごとに、必要性の高いセキュリティパッチの適用は当然として、定期的なセキュリティパッチの適用を行うか、定期的な適用を行う場合はその頻度を、可用性とセキュリティ、作業コストを考え、決定する必要がある。確実なセキュリティパッチ適用のためには、システム導入時の仕様にセキュリティパッチを適用する対象、タイミングを記載する必要がある。これらの作業コストは適用回数に応じて保守費に反映されることになると考えられるため、医療者側のコスト負担も課題となる。

ネットワーク機器へのセキュリティパッチの適用では、医療情報システムの動作検証やシステム停止の診療への影響は限定的である一方、サイバーセキュリティ対策への重要性は高い。このため、医療機関は保守事業者の協力のもと、セキュリティパッチを適用すべきネットワーク機器を把握し、適切なタイミングで適用を行う必要がある。アンケート結果から、ネットワーク機器へのセキュリティパッチの適用では、台帳管理から漏れているネットワーク機器の存在が最初の課題となる。ネットワーク保守事業者の協力のもと、院内に設置されるネットワーク機器を確実にリストアップし、適切なタイミングでセキュリティパッチ適用を実行する努力が求められる。

【パスワードは英数字、記号が混在した 8 文字以上とし、定期的に変更している。※二要素認証、または 13 文字以上の場合は定期的な変更は不要(2-⑦)】

【パスワードの使いまわしを禁止している(令和 7 年度 2-⑧)】

【二要素認証を実装している。または令和9年度までに実装予定である。(令和 7 年度 2-⑩)】

端末 PC のパスワード管理については、医療情報システムの真正性担保（内部の職員や保守事業者のなりすまし防止）と外部の攻撃者に対する乗っ取り防止を分けて議論をする必要が

ある。

真正性担保の観点では、業務効率を優先してパスワードを他者に教えるエンドユーザの存在の問題があり、これはパスワードの桁数を増やすことで解決はできず、二要素認証の導入が効果的である。パスワードの桁数を増やすこと、パスワードの定期的な変更を求めること、パスワードの使いまわしを禁止することは、エンドユーザの作業コストを増やすだけでなく、パスワードのメモ書きなど、かえってパスワード漏洩のリスクを高める可能性もある。外部の攻撃者に対しては、端末 PC では OS の権限管理で administrator 権限を安易に付与しないこと、administrator 権限のパスワード管理が大切である。

端末 PC の二要素認証導入については、医療情報システムの安全管理に関するガイドラインで古くから対応が求められていた。しかし、アンケート調査では一要素認証の医療機関の割合は 80%を超えており、また、今後の導入を積極的に検討している医療機関も半数程度であった。ベンダーインタビュー調査や施設インタビュー調査では端末二要素認証の技術的な課題はクリアされていると考えられる。一方、物理認証や生体認証には認証機器の導入が必要となる。認証機器は全ての端末 PC に設置する必要があり、導入コストが課題になる。また、二要素認証導入に対する業務負荷を課題とする医療機関があるかもしれない。研究代表者施設では職員カードによる物理認証とパスワードによる記憶認証の二要素認証を導入しているが、職員 ID の入力負荷が減ることにより、二要素認証に対する業務負荷は生じていない。また、カード認証機器は、電子処方箋の HPKI カード認証でも使用しており、費用対効果の点で貢献をしている。

サーバに対するパスワード管理では、内部の職員や保守事業者に対しては、ユーザごとに ID と利用者権限を付与することが求められるが、実施しているのは、アンケート回答施設の 16.8%であった。保守事業者では、夜間休日の障害対応などを想定すると、どこまで ID を発行するかが課題となる。夜間休日対応用に非常時 ID を用意し、使用された場合はパスワードを変更して ID を使いまわすという対策などが考えられる。

外部の攻撃者への対応では、パスワードを英数字、記号が混在した 13 文字以上とすることに加え、パスワードの使いまわしの禁止（機器群ごとに異なるパスワードを設定すること）が大切と考えらえる。機器群ごとに異なるパスワードを設定している施設の割合は 67.2%であったが、ユーザごとに ID を設定し、機器群ごとに異なるパスワードを使用している施設の割合は 11.3%にとどまった。外部からの攻撃者からの対応を考えると機器群ごとに異なるパスワードを設定することの優先度が高いと考えられる。

サーバに対する二要素認証については、アンケート回答施設の 1.6%にとどまった。ベンダーインタビュー調査でも、サーバの二要素認証対応の検討はほとんど進んでいない状況であり、今すぐのサーバに対する二要素認証対応は容易でないと考えられた。

サーバの現地作業では、サーバ室の入退室管理を物理認証、サーバへのログインを記憶認証として疑似的に二要素認証とすることが想定される。サーバ室内への防犯カメラを適切に設置すれば、サーバに対して個別の ID を発行しなくても、作業者を同定することも可能となる。一方、サーバ室の入退室管理は用紙記録による入退室者の把握を施設や、物理鍵による入退室管理では貸出記録の保管を行っていない

施設も多く認めた。また、防犯カメラによる監視を行っている施設の割合も高くなかった。ユーザごとに ID 管理を行っていない施設は、特に厳密なサーバ室の入退室管理や防犯カメラによる作業監視を検討する必要があると考えられた。

サーバへのリモートアクセス時の二要素認証については、外部攻撃者からの対応を考えると重要である。前述の通り、サーバに対する二要素認証は技術的には可能であっても、今すぐの導入は難しい状況である。このため、医療情報システムの安全管理に関するガイドライン第 7.0 版(案)に記載のあるとおり、サーバ群へのアクセスを、別ドメインに設置された踏み台端末からの RDP、SSH 等による接続に限定し、踏み台端末の OS ログイン時に二要素認証を実装するか、踏み台端末の EDR(Endpoint Detection and Response)機能による振る舞い検知を実装することが、現実的な代替策として求められると考えらえれた。

医療情報システムの安全管理に関するガイドライン第 7.0 版(案)
サーバ OS については以下①②いずれか、またはそれと同等以上の措置が施されていれば、二要素認証を実装できているものとみなす。
①以下 2 つを満たすもの • 医療情報システムのサーバ群(以下、サーバ群と呼ぶ)へのアクセスを別ドメインに設置された踏み台端末からの RDP や SSH 等による接続のみに限定する。 • 踏み台端末の OS ログイン時に二要素認証を実装する。
②以下3つを満たすもの
• サーバ群へのアクセスを、別ドメインに設置された踏み台端末からの RDP、SSH 等による接続に限定する。 • 踏み台端末には EDR(Endpoint Detection and Response)機能を具備し、運用上想定されない振る舞いを検知可能とする。(必ずしも EDR 製品を要せず、例えば Windows 標準機能等によってふるまい検知が可能であればよい。) • 医療機関等の外部からの接続は VPN を経由し、踏み台端末への RDP、SSH 等による接続に限定する。

サーバについて、以下を実施している。
【アクセスログを管理している。(2-⑪)】

多くの施設が全て、あるいは一部のアクセスログを保存していたが、定期的にアクセスログを確認している施設は多くなかった。アクセスログの保存期間を把握していない医療機関も少なくなかった。アクセスログを管理する必要性を感じながらコストがかかるため保管をすることができない施設が一定数(13.0%)認めるように、アクセスログの保存には費用が発生している。チェックリストはアクセスログの「保存」ではなく「管理」を求めている。アクセスログを漫然と保管している医療機関は保存の対象や保存後の取扱いについて、保守事業者と議論をする機会を持つことが必要と考えられた。

サーバについて、以下を実施している。
端末PCについて、以下を実施している。
【バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-⑫)】

不要ソフトウェアやサービスの停止は約 9 割の施設で実施されていたが、多くは導入時確

認のみで、定期点検は少なかった。アンケート調査では不要ソフトウェアの判別が困難との意見があったが、医療情報システム導入時に本件についてベンダーとコミュニケーションを取ることが大切と考えられる。また、システム稼働後はバックグランドで想定をしていないソフトウェアやサービスが動作していないか、定期的に確認を行う運用を行う必要がある。

端末PCについては、想定外のソフトウェアがインストールされることを防止することが大切である。エンドユーザが自由にソフトウェアをインストールできる医療機関はわずか(3.5%)であったが、システム設定でインストールを制御している医療機関の割合は 67.1%にとどまっていた。端末 PC は様々なユーザが操作することを考えると、端末 PC へのソフトウェアのインストールはシステムで制御を行うことは必要と考えられた。

ネットワーク機器について、以下を実施している。

【接続元制限を実施している。(2-⑬)】

アンケート調査では、約8割の施設がネットワーク機器の接続元制限の実施をしていた。管理設定や監視を行っているのは、病院とネットワーク事業者が協力して行う施設が多く、次いでネットワーク事業者に任せているという施設が多かった。ネットワーク事業者に任せている施設は、管理設定を医療機関でも把握すること、監視状況の定期報告を受けることなど、ネットワーク事業者に任せきりにならない取り組みが必要となる。

3 インシデント発生に備えた対応

【インシデント発生時における組織内と外部関係機関(事業者、厚生労働省、警察等)への連絡体制図がある。(3-①)】

アンケート調査で多くの施設で整備が行われていたが、定期的に見直しを実施していない施設も 25.1%認めた。頻回に変更される情報ではないかと考えるが、万が一、非常時に活用できないといけないので、定期的に見直しを行う体制を構築する必要がある。

【インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。(3-②)】

医療機関はデータやシステムのバックアップの対象を検討し、診療継続に必要なデータは確実にバックアップを取る必要がある。サイバーインシデントを考えるとオフラインバックアップが必要なことは広く知られているところであり、データ復旧を見据えたバックアップのタイミングや世代バックアップの在り方を検討しなければならない。インタビュー調査を行った施設では、バックアップデータからの復旧訓練を行っている施設があった。組織的なレジリエンスを高めるため、バックアップ体制を整備した医療機関は復旧訓練の実施の検討を行うべきである。復旧訓練が難しい場合でも、保守事業者と復旧手順の確認は行う必要があると考えられた。

【サイバー攻撃を想定した事業継続計画(BCP)を策定している。(3-③)】

チェックリストへの掲載により、多くの施設で BCP の策定が進んでいた。まだ策定できていない施設も 15.5%認めていたが、厚生労働省が作成した BCP を参考にして、自施設の BCP 策定を急ぐ必要がある。

策定した BCP が想定通りに機能するかは、サイバーインシデントを想定した災害訓練が必要となる。定期的な災害訓練を通じて、BCP の

改訂を行う必要がある。

地震などに対する災害訓練は病院全体で取り組むことが多いが、サイバーインシデントに対する災害訓練はサイバーセキュリティ担当者や事務組織に参加者が限定されることも少なくない。研究代表者施設では、医療情報システム障害対策を医療安全対策ととらえ、医療安全講習会のテーマとして取り扱った。多くの医療機関で電子カルテ運用が始まり 10 年以上が経過し、用紙運用を知る医療スタッフは減少している。用紙運用に関する学習コンテンツの整備や日頃から用紙運用で使用する帳票の保管場所の確認などが必要で、そのためにも病院全体での災害訓練が必要と考える。

4 規程類の整備

【上記 1-3 のすべての項目について、具体的な実施方法を運用管理規程等に定めている。(4-①)】

チェックリストに掲載されることで、多くの施設で規定等を定めていた。

医療機関におけるサイバーセキュリティインシデントの発生や、厚生労働省をはじめとする関係機関・団体による各種施策の推進を背景として、医療機関およびベンダー双方において、医療情報システムに対するサイバーセキュリティ対策の重要性に対する認識は着実に高まっている。本アンケート調査の結果、多くの施設において、チェックリスト項目への対応が進んでいることが確認された。

一方で、一部のチェックリスト項目については、医療機関間で対応状況にばらつきが認められた。特に対応が困難とされた項目では、稼働中システムへの適用に伴う作業負荷の大きさや、システムの安定稼働への影響が課題として挙げられた。このような項目については、システム更新のタイミングに合わせて、計画的かつ確実に対応を進める必要がある。

また、サイバーセキュリティ対策が十分に進まない要因の一つとして、対策に要する費用負担の問題が示唆された。サイバーセキュリティ対策は、患者情報を取り扱う医療機関にとって重要な責務であり、継続的な投資が求められる事項である。しかしながら、医療機関における情報基盤への投資可能額は、病院収益に対する一定割合として制約を受けることが多い。近年では、人件費や医療材料費の高騰に加え、ハードウェア価格やシステムエンジニアリング費用の上昇により、医療情報システム関連費用は従来の 1.5～2 倍程度に増加しているとの指摘もある。

さらに、サイバーセキュリティ対策は予防的投資としての側面が強く、必要十分な対策水準を定量的に判断することが難しい。このため、厳しい経営環境下にある医療機関において、十分なセキュリティ投資を行う経営判断は容易ではない。アンケート調査結果からも、コスト面を理由としてサイバーセキュリティ対策の実施が遅延している実態が示された。

今後、医療機関におけるサイバーセキュリティ対策への投資や、専門的なセキュリティ人材の配置・育成を適切に評価し、その体制整備に対して診療報酬等を通じた支援が行われることで、医療機関全体のサイバーセキュリティ対策のさらなる推進につながることが期待される。

E. 結論

本研究により、医療機関におけるサイバーセキュリティ対策は、厚生労働省のチェックリスト導入等を背景に一定程度進展していることが明らかとなった。一方で、セキュリティパッチ適用、二要素認証、資産管理、ログ分析など、実

運用面では多くの課題が残されていた。特に、医療情報システムでは「安定稼働」と「セキュリティ確保」の両立が大きな障壁となっており、専門人材不足やベンダー依存も対策推進を困難にしていた。

先進的な医療機関では、侵入防止のみを目的とするのではなく、早期検知・迅速復旧を重視した「レジリエンス型対策」への転換が進んでいた。今後は、医療機関が主体的にセキュリティ要件を定義し、ベンダーとの責任分界点を明確化するとともに、継続的な人材育成、復旧訓練、IT-BCP 運用を進めることが重要である。また、サイバーセキュリティ対策への投資を適切に評価し、制度的・財政的支援を行うことが、医療分野全体の安全性向上につながると考えられた。

F. 健康危険情報

なし

G. 研究発表

1. 論文発表

なし

2. 学会発表

(1)武田理宏、医療機関における情報セキュリティ人材の育成と配置に向けて、関西健康・医療創生会議オンラインセミナー、2025 年 6 月

(2)武田理宏、医療機関における情報セキュリティ人材の育成と配置に向けて、全国自治体病院協議会富山県支部講演会、2025 年 6 月、富山

(3)武田理宏、医療機関における情報セキュリティ人材の育成と配置に向けて、第 122 回近畿病歴管理セミナー、2025 年 6 月、大阪

(4)鳥飼幸太、医療分野のサイバーセキュリティ対策の現状や最新の取り組み、大会企画シンポジウム、サイバーセキュリティ人材育成の最前線、第 29 回日本医療情報学春季学術大会、2025 年 7 月、仙台

(5)武田理宏、情報セキュリティ人材の育成と適正配置、大会企画シンポジウム、サイバーセキュリティ人材育成の最前線、第 29 回日本医療情報学春季学術大会、2025 年 7 月、仙台

(6)武田理宏、医療機関における情報セキュリティ人材の育成と配置に向けて、第 8 回 メディカルジャパン東京(医療・介護・薬局 Week 東京)、2025 年 10 月、幕張

(7)橋本智広、マルチプラットフォームとデータ保護戦略による信頼性強化～医療情報システムにおける強靭化とレジリエンスの両立を考える～、第 45 回医療情報学連合大会,、2025 年 11 月、姫路

(8)橋本智広、IT-BCP 実践アプローチとサイバーレジリエンス強化に向けて ～アクションカード整備の重要性とサーバ仮想化基盤の分散管理による可用性確保～、第 45 回医療情報学連合大会、2025 年 11 月、姫路

(9)橋本智広、医療機関における IT-BCP に基づくインシデント発生時の初動対応、第 45 回医療情報学連合大会、2025 年 11 月、姫路

(10)橋本智広、現場目線で考える、医療機関の今すべき情報セキュリティ対策、第 12 回 メディカルジャパン大阪(医療・介護・薬局 Week 大阪)、2026 年 3 月、大阪

H. 知的財産権の出願・登録状況

(予定を含む。)

1. 特許取得

なし

2. 実用新案登録

なし

3.その他

なし