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

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課題調査と解決策の検討

（令和）７年度　総括･分担研究報告書

研究代表者　武田　理宏

（令和）８（２０２６）年　５月

目　　次

Ⅰ．総括研究報告
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課題調査と解決策の検討
―――――――――――――――― 1
武田　理宏
（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
（資料）２．施設訪問インタビューシート
（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」への対応状況調査項目結果
（資料）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
（資料）５．医療機関のチェックリスト充足具体化リスト

II．分担研究報告
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」への対応状況調査結果 ―――――――――――――――― 70
武田理宏、鳥飼幸太、猪飼宏、橋本智広、三上聡司、杉本賢人

２．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課題調査と解決策の検討（AからD施設インタビュー調査） ―――――――――――――――― 82
橋本智広
（資料）６．施設訪問インタビューシート（AからD施設）

３．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課題調査と解決策の検討（EからG施設インタビュー調査） ―――――――――――――――― 95
鳥飼幸太
（資料）なし

４．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課題調査と解決策の検討（HからK施設インタビュー調査） ―――――――――――――――― 100
杉本賢人、三上聡司
（資料）７．施設訪問インタビューシート（HからK施設）

５．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課題調査と解決策の検討（L施設インタビュー調査） ―――――――――――――――― 106
猪飼宏
（資料）なし

６．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課題調査と解決策の検討（ベンダーインタビュー調査） ―――――――――――――――― 109
杉本賢人
（資料）なし

III．研究成果の刊行に関する一覧表 ―――――――――――――――― 115

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

「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

本調査は、令和 7 年度厚生労働行政推進調査事業「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課題調査と解決策の検討（25IA2012）」（研究代表者：武田理宏（大阪大学）」で実施するものです。
本調査は、最初に各医療機関のサイバーセキュリティ人材の配置状況を確認したのち、令和 6 年度版の「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」に沿って対応状況をご回答いただきます。
あわせて、令和 7 年度版で追加される事項についてもお尋ねいたします。
【 】内は、質問に対応するチェックリストの項目を記載しています。
参考） 令和 6 年度版の「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」
https://www.mhlw.go.jp/content/10808000/001262036.pdf
令和 7 年度版の「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」
https://www.mhlw.go.jp/content/10808000/001450189.pdf
https://www.mhlw.go.jp/content/10808000/001490741.pdf

セクション 1 貴施設についておしえてください。

1.**所在地（都道府県）についてお教えください。**【必須】【単一選択】
[ ]

2.**貴施設に該当するものをお選びください。**【必須】【単一選択】
※ 公的な医療機関とは、次に掲げる者が開設する医療機関を指します。
国、都道府県、市町村、地方公共団体の組合、国民健康保険団体連合会及び国民健康保険組合、日本赤十字社、社会福祉法人恩賜財団済生会、厚生農業協同組合連合会、社会福祉法人北海道社会事業協会
※ 国立病院機構等も公的な医療機関としてご回答ください。
○ 国公立大学病院
○ 公的な医療機関（大学病院を除く）
○ 私立大学病院
○ 私立の医療機関

3.**貴施設の認定、指定についてお教えください**【必須】【複数選択】
□ 特定機能病院
□ 地域医療支援病院
□ 災害拠点病院（基幹）
□ 災害拠点病院（地域）
□ 第三次救急医療機関
□ 第二次救急医療機関
□ 総合周産期母子医療センター
□ 地域周産期母子医療センター
□ 小児中核病院
□ 小児地域医療センター
□ 小児地域支援病院
□ 上記の認定、指定は受けていない

4.**許可病床数についてお教えください。**【必須】【単一選択】

- ○ 1000 床以上
- ○ 800 床以上 1000 床未満
- ○ 600 床以上 800 床未満
- ○ 400 床以上 600 床未満
- ○ 300 床以上 400 床未満
- ○ 200 床以上 300 床未満
- ○ 100 床以上 200 床未満
- ○ 100 床未満

5.**診療録管理体制加算の算定状況をお聞かせください。**【必須】【単一選択】

- ○ 加算1
- ○ 加算2
- ○ 加算3
- ○ 算定していない

6.**医療情報システムを管理する部門を設置していますか。**【必須】【単一選択】

- ○ はい
- ○ いいえ

7.**専門知識を有する情報セキュリティ人材を配置していますか。**【必須】【単一選択】

※ IPA IT スキル標準レベル 4 は、「プロフェッショナルとしてスキルの専門分野が確立し、自らのスキルを活用することによって、独力で業務上の課題の発見と解決をリードするレベル。社内において、プロフェッショナルとして求められる経験の知識化とその応用（後進育成）に貢献しており、ハイレベルのプレーヤとして認められます。スキル開発においても自らのスキルの研鑽を継続することが求められます。」と定義され、サイバーセキュリティ領域では情報処理安全確保支援士試験が相当します。
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/index.html

- ○ 高度な専門知識（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
- ○ 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
- ○ 配置していない

8.診療録を電子的に管理していますか（電子カルテを導入していますか）。【必須】.【単一選択】.

- ○ はい
- ○ いいえ

セクション 2【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))】

9.**情報セキュリティ責任者（CISO:　Chief Information Security Officer）を配置していますか。**
【必須】【単一選択】

※ 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 版では、「サイバー攻撃に対しては情報セキュリティ責任者（CISO（Chief Information Security Officer））の配置や、CSIRT（Computer Security Incident Response Team）の構築が有効とされており、企画管理者はこれらの整備の要否や、必要な場合にはその構成や非常時の対応内容などについて検討し、経営層の承認を得ることが求められる。」と記載されています。

※ 情報セキュリティ責任者（CISO）に相当する役割（呼称は各施設で異なって問題ありません）の設置の有無をお答えください。

- ○ 配置している（医療情報システム安全管理責任者とは別の人物）　→ **設問 10 に**
  ※例）副院長が CISO、医療情報部長が医療情報システム安全管理責任者など
- ○ 配置している（医療情報システム安全管理責任者を配置と同一人物）　→ **設問 15 に**
- ○ 配置していない　→ **設問 14 に**

10.**情報セキュリティ責任者（CISO）はサイバーセキュリティに対する知識をどの程度保有していますか。**
【必須】【単一選択】

- ○ 高度な専門知識（IPA IT スキル標準レベル 4 以上相当）を有しており、単独でも対策を進めることができる
- ○ 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
- ○ 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
- ○ ほとんど知識を有していない
- ○ 全く知識を有していない

11.**情報セキュリティ責任者（CISO）の職位をお答えください。**【必須】【単一選択】

※ 兼任等されている場合、上位の職位をお答えください。

- ○ 医療機関の責任者（院長など）
- ○ 院長を補佐する立場（副院長、院長補佐など）
- ○ 医療情報システム管理部門の長
- ○ 医療情報システム管理部門（部門長以外）
- ○ 事務部門の長、　○事務部門（部門長以外）
- ○ 上記以外の部門の長
- ○ 上記以外の部門（部門長以外）
- ○ その他（　　）

12.**情報セキュリティ責任者（CISO）が保有する医療系資格についてお答えください。**
【必須】【複数選択】

- ☐ 医師・歯科医師
- ☐ 看護師・助産師・保健師
- ☐ 薬剤師
- ☐ 診療放射線技師
- ☐ 臨床検査技師
- ☐ 臨床工学技士
- ☐ 医学物理士
- ☐ 医療情報技師（上級医療情報技師を含む）
- ☐ 診療情報管理士
- ☐ リストにある医療系資格を保持していない

13.**情報セキュリティ責任者（CISO）が保有する情報処理推進機構（IPA）が認定する資格・試験についてお答えください。**【必須】【複数選択】

- ☐ 情報処理安全確保支援士（登録情報セキュリティスペシャリスト）
- ☐ 情報処理安全確保支援士（試験に合格のみ）
- ☐ 応用情報技術者試験
- ☐ 基本情報技術者試験
- ☐ 情報セキュリティマネジメント試験
- ☐ IT パスポート試験
- ☐ リストされる資格・試験は保持していない

14.**医療情報システム安全管理責任者を配置していますか。**【必須】【単一選択】

- ○ 配置している（情報セキュリティ責任者（CISO）とは別の人物） → **設問 15 に**
- ○ 配置していない → **設問 19 に**

15.**医療情報システム安全管理責任者はサイバーセキュリティに対する知識をどの程度保有していますか。**【必須】【単一選択】

- ○ 高度な専門知識（IPA IT スキル標準レベル 4 以上相当）を有しており、単独でも対策を進めることができる
- ○ 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
- ○ 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
- ○ ほとんど知識を有していない
- ○ 全く知識を有していない

16.**医療情報システム安全管理責任者の職位をお答えください。**【必須】【単一選択】
※兼任等されている場合、上位の職位をお答えください。

- ○ 医療機関の責任者（院長など）
- ○ 院長を補佐する立場（副院長、院長補佐など）
- ○ 医療情報システム管理部門の長
- ○ 医療情報システム管理部門（部門長以外）
- ○ 事務部門の長
- ○ 事務部門（部門長以外）
- ○ 上記以外の部門の長、
- ○ 上記以外の部門（部門長以外）
- ○ その他（ ）

17.**医療情報システム安全管理責任者が保有する医療系資格についてお答えください。**
【必須】【複数選択】

- □ 医師・歯科医師
- □ 看護師・助産師・保健師
- □ 薬剤師
- □ 診療放射線技師
- □ 臨床検査技師
- □ 臨床工学技士
- □ 医学物理士、
- □ 医療情報技師（上級医療情報技師を含む）
- □ 診療情報管理士
- □ リストにある医療系資格を保持していない

18.**医療情報システム安全管理責任者が保有する情報処理推進機構（IPA）が認定する資格・試験についてお答えください。**【必須】【複数選択】 **→ 設問 20 に**

- □ 情報処理安全確保支援士（登録情報セキュリティスペシャリスト）
- □ 情報処理安全確保支援士（試験に合格のみ）
- □ 応用情報技術者試験
- □ 基本情報技術者試験
- □ 情報セキュリティマネジメント試験、
- □ IT パスポート試験
- □ リストされる資格・試験は保持していない

19.**情報セキュリティ責任者（CISO）や医療情報システム安全管理責任者を設置しない理由を教えてください。**【必須】【複数選択】

- □ 許可病床数が 200 床以上であるが、医療情報システム安全管理責任者の設置の必要性を感じない（診療録管理体制加算の算定を行わない）から
- □ 許可病床数が 200 床以上であるが、医療情報システム安全管理責任者に適任な人材がいないから
- □ 許可病床数が 200 床未満で、医療情報システム安全管理責任者の設置の必要性を感じないから
- □ 許可病床数が 200 床未満で、医療情報システム安全管理責任者に適任な人材がいないから
- □ その他（ ）

20.**貴院のサイバーセキュリティ対策の方針を決定する際に関わる情報セキュリティ人材を選択してください。**【必須】【複数選択】

- □ 情報セキュリティ責任者（CISO）
- □ 医療情報システム安全管理責任者
- □ 院内に配置する高度な専門知識（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
- □ 院内に配置する専門知識を有する情報セキュリティ人材
- □ 同一法人等の中央組織に配置する高度な専門知識（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
- □ 同一法人等の中央組織に配置する専門知識を有する情報セキュリティ人材
- □ 同一法人等の他医療機関に配置する高度な専門知識（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
- □ 同一法人等の他医療機関に配置する専門知識を有する情報セキュリティ人材
- □ 保守契約を結ぶ医療情報システムベンダー（情報セキュリティの知識を有することを確認している）
- □ 保守契約を結ぶ医療情報システムベンダー（情報セキュリティの知識を有することを確認できていない）
- □ 情報セキュリティ対策を専門とする企業等（医療情報システムベンダー以外）の情報セキュリティ人材
- □ その他

21.**「その他」を選ばれた場合、貴院のサイバーセキュリティ対策の方針を決定する際に関わるその他の情報セキュリティ人材についてご記載ください**【テキスト入力】

[ ]

セクション 3【2. 医療情報システムの管理・運用】

【医療情報システム全般について、以下を実施している。】

【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))】

22.**医療情報システムに接続するサーバ、端末 PC、ネットワーク機器の台帳管理を行っていますか。**
【必須】【単一選択】

- ○ サーバ、端末 PC、ネットワーク機器、全てで台帳管理をしている → **設問 23 に**
- ○ サーバ、端末 PC、ネットワーク機器、いずれかで台帳管理をしている → **設問 23 に**
- ○ 台帳管理を行っていない → **設問 27 に**

23.**台帳管理を行っている医療情報システムに接続するサーバ、端末 PC、ネットワーク機器について**
【必須】

	全ての機器を把握している	全ての機器を把握していると思うが、漏れがあるかもしれない	全ての機器を把握できていない	ほとんどの機器を把握できていない	台帳管理を行っていない
サーバ	○	○	○	○	○
端末 PC	○	○	○	○	○
ネットワーク機器	○	○	○	○	○

24.**医療情報システムに接続するサーバ、端末 PC、ネットワーク機器の台帳管理を行っているのは誰ですか。**【必須】

	自施設の職員	機器を導入した事業者（保守契約など）	導入事業者以外の事業者	その他	台帳管理を行っていない
サーバ	○	○	○	○	○
端末 PC	○	○	○	○	○
ネットワーク機器	○	○	○	○	○

25.**医療情報システムに接続するサーバ、端末 PC、ネットワーク機器の台帳管理の方法をお答えください。**【必須】

	用紙運用	エクセル等の汎用ソフトを使用	専用ソフトを使用	その他	台帳管理を行っていない
サーバ	○	○	○	○	○
端末 PC	○	○	○	○	○
ネットワーク機器	○	○	○	○	○

26.**医療情報システムに接続するサーバ、端末 PC、ネットワーク機器の台帳管理に専用ソフトを使っている場合、メーカとソフト名をご記載ください。**【テキスト入力】

[ ]

27.**外部から医療情報システムネットワークに接続している回線を把握していますか。**
【必須】【単一選択】
- ○ 全て把握している → **設問 28 に**
- ○ 一部のみ把握している → **設問 28 に**
- ○ 把握していない → **設問 29 に**

28.**外部から医療情報システムネットワークに接続していることを把握している回線数を記載してください。**【必須】【数字入力】
[ ]

29.**外部から医療情報システムネットワークに接続している回線数を減らす努力をしていますか。**
【必須】【単一選択】
- ○ 努力をしている
- ○ 回線数を減らす必要性は感じているが、努力はできていない
- ○ 回線数を減らす必要性は感じていない

30.**貴施設が、外部から医療情報システムネットワークに接続している回線を、全数把握し、管理する場合、何回線以下であれば適切に管理できますか。**【必須】【数値入力】
※「適切な管理」とは、「それぞれの回線の機器に対し最新のセキュリティパッチを当てたり、リスクアセスメント（異常な通信の増加を検知し、適切な対策を取るなど）を実施したりすることなど」を想定し、貴施設が適切に管理できると考える回線数をご記入ください。
※ 貴施設で回線を管理することができない場合、管理すべきでないとお考えの場合は、「0」と入力してください。
※ ご意見、お考えがない場合は、「9999」と入力してください。
[ ]

【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))】
31.**リモートメンテナンス（保守）の病院情報システムネットワークへの接続方法についてお答えください。**
【必須】【単一選択】
- ○ 自施設が設置するリモート接続の仕組みを使った接続のみ許可している
- ○ 自施設が設置するリモート接続の仕組みを使った接続を原則とするが、ベンダー側の理由で例外を認めている（接続する全てのリモートメンテナンス回線を把握している）
- ○ 自施設が設置するリモート接続の仕組みを使った接続を原則とするが、ベンダー側の理由で例外を認めている（接続する全てのリモートメンテナンス回線を把握できていない）
- ○ 自施設でリモート接続の仕組みを有さず、ベンダー個々の接続方法で接続を許可している（接続する全てのリモートメンテナンス回線を把握している）
- ○ 自施設でリモート接続の仕組みを有さず、ベンダー個々の接続方法で接続を許可している（接続する全てのリモートメンテナンス回線を把握できていない）
- ○ リモート接続はベンダーに任せており、リモート接続の許可を行っていない（接続する全てのリモートメンテナンス回線の把握はできている）
- ○ リモート接続はベンダーに任せており、リモート接続の許可を行っていない（接続する全てのリモートメンテナンス回線の把握ができていない）
- ○ リモートメンテナンス（保守）は行っていない

【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))】

32.**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）の提出を受けていますか。**【必須】【単一選択】

- ○ 提出を受け、内容を確認し、必要があれば具体的な対応を行っている → **設問 33 に**
- ○ 提出を受け、内容を確認しているが、具体的な対応までは行っていない → **設問 34 に**
- ○ 提出を受けているが、内容は十分に確認していない → **設問 34 に**
- ○ 提出を受けていない（必要性を感じていない） → **設問 34 に**
- ○ 提出を受けていない（事業者が対応してくれない） → **設問 34 に**
- ○ 事業者と契約していない → **設問 34 に**

33.**医療情報セキュリティ開示書（MDS/SDS）の内容を確認した結果、具体的な対応事例があれば、ご記載ください。**【テキスト入力】

[ ]

セクション 4 【医療情報システムの管理・運用】

【サーバ、端末 PC、ネットワーク機器について、以下を実施している。】
【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))】
【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。(令和 7 年度 2-④)】

34.**サーバ、ネットワーク機器に対するアクセス権限の付与方法について、教えてください。**【必須】

	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	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	組織ごと（病院やベンダー）にユーザ ID と利用権限を設定し、ユーザパスワードは全ての機器群で同じである	組織ごと（病院やベンダー）にユーザ ID と利用権限を設定し、ユーザパスワードは機器群ごとに異なっている	ユーザごとに ID と利用権限を設定し、ユーザパスワードは全ての機器群で同じである	ユーザごとに ID と利用権限を設定し、ユーザパスワードは機器群ごとに異なっている
サーバ	○	○	○	○	○	○
ネットワーク機器	○	○	○	○	○	○

35.**端末 PC のエンドユーザに対するユーザ認証について、教えてください。**【必須】【単一選択】

- ○ OS のユーザ認証を活用したユーザ認証を行っている
- ○ OS のユーザ認証とソフトウェアでユーザ認証を組み合わせたユーザ認証を行っている
- ○ OS は administrator 権限で自動ログインを行い、ソフトウェアでユーザ認証を行っている
- ○ OS は administrator 以外の同一ユーザで自動ログインを行い、ソフトウェアでユーザ認証を行っている
- ○ その他（ ）

36.**端末 PC のエンドユーザに対するアクセス利用権限について教えてください。**【必須】【単一選択】

- ○ すべてのユーザに対して個別のユーザ ID を発行し、アクセス利用権限を設定している（複数のユーザで使いまわしをしているユーザ ID はない）
- ○ すべてのユーザに対して個別のユーザ ID を発行し、アクセス利用権限を設定することを原則とするが、一部、運用等の理由で、複数のユーザで使いまわしをしているユーザ ID がある（管理者権限の ID 使いまわしはない）
- ○ すべてのユーザに対して個別のユーザ ID を発行し、アクセス利用権限を設定することを原則とするが、一部、運用等の理由で、複数のユーザで使いまわしをしているユーザ ID がある（管理者権限の ID 使いまわしがある）
- ○ すべてのユーザに対して個別のユーザ ID を発行し、アクセス利用権限を設定することを原則とするが、一部、運用等の理由で、複数のユーザで使いまわしをしているユーザ ID がある（管理者権限の ID 使いまわしがあるか否かは把握できていない）
- ○ 必要に応じて、ユーザごとの ID 付与と、組織、グループごと（外部委託業者など）の ID 付与を使い分けている
- ○ その他（ ）

【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))】

37.**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ますか。**【必須】

	全て、削除または無効化できている	一部、削除または無効化できていない	全て、削除または無効化できていない
サーバ	○	○	○
端末 PC	○	○	○

38.**不要なアカウントを削除または無効化するタイミングをお答えください。**【必須】

	退職日を有効期限に設定するなどリアルタイムでアカウントを削除または無効化している	年に 1 回など棚卸作業を行い、不要なアカウントを削除または無効化している（退職後にアカウントが有効な期間が存在する）	削除または無効化できていない
サーバ	○	○	○
端末 PC	○	○	○

【アクセスログを管理している。(2-(6))】

39.**サーバ、端末 PC のアクセスログを残していますか。**【必須】【単一選択】

○ サーバ、PC 端末、いずれかのアクセスログを残している → **設問 40 に**

○ アクセスログを残していない → **設問 43 に**

40.**アクセスログを残している範囲をお答えください。**【必須】

	全ての機器のアクセスログを残している	一部の機器のアクセスログを残している	アクセスログを残していない
サーバ	○	○	○
端末 PC	○	○	○

41.**アクセスログを確認していますか。**【必須】

	病院職員がアクセスログを定期的に確認している	保守事業者がアクセスログを定期的に確認している	アクセスログを定期的に確認していないが、必要があれば病院職員が確認をすることが可能である	アクセスログを定期的に確認していないが、必要があれば保守事業者が確認をすることが可能である	アクセスログを残しているが、確認方法は把握していない	アクセスログを残していない
サーバ	○	○	○	○	○	○
端末 PC	○	○	○	○	○	○

42.**アクセスログの保管期間を把握していますか**【必須】

	医療機関がアクセスログの保管期間を指定している	保守事業者が定めたアクセスログの保管期間を医療機関として把握している	アクセスログの保管期間を把握していない	アクセスログを残していない
サーバ	○	○	○	○
端末 PC	○	○	○	○

43.**≪アクセスログを残していない場合にお答えください≫**
アクセスログを残していない理由は何ですか。【単一選択】

○ 医療機関としてアクセスログを残す必要性を感じていない
○ 医療機関としてアクセスログを残す必要性を感じているが、コストがかかるため残すことができない
○ 医療機関としてアクセスログを残す必要性を感じているが、保守事業者が対応してくれない
○ その他（ ）

【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))】
44.**サーバ、端末 PC、ネットワーク機器に対し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）を適用していますか。**【必須】【単一選択】

○ サーバ、端末 PC、ネットワーク機器のいずれかに対し、セキュリティパッチを適用している
→ 設問 45 に
○ セキュリティパッチを適用していない
→ 設問 49 に

45. サーバ、端末 PC、ネットワーク**機器に対し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）を適用していますか。**【必須】

	全ての機器に対して適用している	一部の機器に対して適用している	適用していない
サーバ	○	○	○
端末 PC	○	○	○
ネットワーク機器	○	○	○

46. サーバ、端末 PC、ネットワーク機器に対し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）を適用するタイミングを教えてください。【必須】

	セキュリティパッチごとにリアルタイムで（システム検証は行わない）	セキュリティパッチごとにできるだけ早いタイミングで（システム検証を行った後）	定期的に（○ヶ月に 1 回など時期を決めて）、セキュリティパッチをまとめて適用を行う	適用が必要なセキュリティパッチが出てきた時に、保守事業者と打ち合わせを行った上、適用時期を決める	その他	セキュリティパッチを適用していない
サーバ	○	○	○	○	○	○
端末 PC	○	○	○	○	○	○
ネットワーク機器	○	○	○	○	○	○

47. **サーバ、端末 PC、ネットワーク機器に適用す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）はどのように選択していますか。【必須】**

	全てのセキュリティパッチを適応している	医療機関が必要と判断したセキュリティパッチと保守事業者が推奨するセキュリティパッチを適用している	医療機関が必要と判断したセキュリティパッチを適用している	保守事業者が推奨するセキュリティパッチを適用している	その他	セキュリティパッチを適用していない
サーバ	○	○	○	○	○	○
端末 PC	○	○	○	○	○	○
ネットワーク機器	○	○	○	○	○	○

48.**≪セキュリティパッチを適用している場合にお答えください≫**
サーバ、端末 PC、ネットワーク機器に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）を適用する費用についてお答えください。【必須】

	保守費用に含まれる	随時、作業費用を支払っている	セキュリティパッチを適用していない
サーバ	○	○	○
端末 PC	○	○	○
ネットワーク機器	○	○	○

49.**≪セキュリティパッチを適用していない場合にお答えください≫**
セキュリティパッチを適用しない理由についてお答えください。【単一選択】

○ 医療機関として必要性を感じていない
○ 医療機関として必要性を感じているが、事業者が対応をしてくれない
○ 医療機関として必要性を感じているが、作業費用の捻出が困難である
○ その他（ ）

50.**セキュリティパッチの適用について、ご意見があればご記載ください。【テキスト入力】**
[ ]

【接続元制限を実施している。(2-(8))】

51.**ネットワーク機器の接続元制限を実施していますか。【必須】【単一選択】**
※ 接続元制限とは、特定の IP アドレスからのみサービスへのアクセスを許可する、または拒否するセキュリティ対策ことを言います。

○ はい → **設問 52 に**
○ いいえ → **設問 54 に**

52.**ネットワーク機器の接続元の管理設定は誰が行っていますか。**【必須】【単一選択】

- ○ 病院
- ○ 病院とネットワーク事業者が協力して
- ○ ネットワーク事業者に任せている
- ○ その他（ ）

53.**ネットワーク機器の接続元の監視は誰が行っていますか。**【必須】【単一選択】

- ○ 病院
- ○ 病院とネットワーク事業者が協力して
- ○ ネットワーク事業者に任せている
- ○ その他（ ）

【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))】

54.**バックグラ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ますか。**【必須】

	はい（システム導入時に確認したのみ）	はい（定期的に確認している）	いいえ
サーバ			
端末 PC			

55.**≪前問で「いいえ」を選択した場合にお答えください≫**
バックグラ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ない理由を教えてください。
【テキスト入力】
[ ]

56.**端末 PC にエンドユーザが希望するソフトウェアをインストールすることが可能ですか。**
【必須】【単一選択】

- ○ ソフトウェアを端末 PC にインストールすることは、システム設定で禁止している。エンドユーザの希望による端末インストールは行わない
- ○ ソフトウェアを端末 PC にインストールすることは、システム設定で禁止している。ソフトウェアのインストールを病院に申請し、許可を受けたソフトウェアのみシステム管理者がインストールを行う
- ○ ソフトウェアを端末 PC にインストールすることは、運用で禁止している（システム設定で制限はかけていない）。エンドユーザの希望による端末インストールは行わない
- ○ ソフトウェアを端末 PC にインストールすることは、運用で禁止している（システム設定で制限はかけていない）。ソフトウェアのインストールを病院に申請し、許可を受けたソフトウェアのみシステム管理者がインストールを行う
- ○ ソフトウェアを端末 PC にインストールすることは、運用で禁止している（システム設定で制限はかけていない）。ソフトウェアのインストールを病院に申請し、許可を受けたソフトウェアのみエンドユーザがインストールを行う
- ○ エンドユーザが自由にソフトウェアを端末 PC にインストールできる

セクション 5【医療情報システムの管理・運用(令和 7 年度)】

【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)】

57.**機器に対するパスワード管理について、教えてください。**【必須】

	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	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	左記を実現できていない
サーバ	○	○	○
端末 PC	○	○	○
ネットワーク機器	○	○	○

58.**サーバ室の入退室管理について、お答えください。**【必須】【複数選択】

- □ 用紙記録による入退室者の把握
- □ 防犯カメラのよる監視(出入口付近)
- □ 防犯カメラによる監視(サーバ室内)
- □ 物理鍵による入退室管理(貸出記録を保管)
- □ 物理鍵による入退室管理(貸出記録の保管は行わない)
- □ 知識認証(ID とパスワードなど)による入退室管理(入退室者の記録が残る)
- □ 知識認証(パスワードのみ)による入退室管理(入退室者の記録は残らない)
- □ 物理認証(カード認証など)による入退室管理(入退室者の記録が残る)
- □ 物理認証(カード認証など)による入退室管理(入退室者の記録が残らない)
- □ 生体認証(指紋認証、静脈認証、顔認証など)による入退室管理(入退室者の記録が残る)
- □ 生体認証(指紋認証、静脈認証、顔認証など)による入退室管理(入退室者の記録が残らない)
- □ サーバ室は設置していない

59.**サーバに対する二要素認証の有無について教えてください。**【必須】【単一選択】

※ 二要素認証とは、知識認証(パスワードなど)、所有物認証(ID カードなど)、生体認証(例、顔認証、指紋認証、静脈認証、虹彩認証など)の三要素のうちの二要素を認証に用いることを言います。

- ○ 一要素認証である → **設問 60 に**
- ○ 二要素認証(物理認証あるいは生体認証によるサーバ室への入退室管理とサーバに対する一要素(パスワード)認証。ただし、リモート接続では一要素認証となっている) → **設問 62 に**
- ○ 二要素認証(物理認証あるいは生体認証によるサーバ室への入退室管理とサーバに対する一要素(パスワード)認証。リモート接続でも二要素認証を実現している) → **設問 62 に**
- ○ サーバに対する二要素認証を実装している(リモート接続では一要素認証となっている) → **設問 62 に**
- ○ サーバに対する二要素認証を実装している(リモート接続でも二要素認証を実現している) → **設問 62 に**
- ○ その他 (　　) → **設問 62 に**

60.**サーバに対する二要素認証を令和 9 年度までに実装予定である。**【必須】【単一選択】

- ○ 必ず実装する → **設問 62 に**
- ○ 実装を検討中（実装の可能性が高い） → **設問 62 に**
- ○ 実装を検討中（実装の可能性が低い） → **設問 62 に**
- ○ 実装を行わない → **設問 61 に**

61.**サーバに対する二要素認証の実装を行わない理由をおしえてください。**【テキスト入力】

[ ]

62.**端末 PC に対する二要素認証の有無について教えてください。**【必須】【単一選択】

※ 二要素認証とは、知識認証（パスワードなど）、所有物認証（ID カードなど）、生体認証（例、顔認証、指紋認証、静脈認証、虹彩認証など）の三要素のうちの二要素を認証に用いることを言います。

- ○ 一要素認証である → **設問 63 に**
- ○ 端末 PC は二要素認証を導入しているが、医療情報システムネットワークに接続する部門システム端末（ワークステーション等）は一要素認証の端末がある → **設問 65 に**
- ○ 医療情報システムに接続する端末は全て二要素認証を導入している → **設問 65 に**
- ○ その他（ ） → **設問 65 に**

63.**端末 PC に対する二要素認証を令和 9 年度までに実装予定である。**【必須】【単一選択】

- ○ 必ず実装する → **設問 65 に**
- ○ 実装を検討中（実装の可能性が高い） → **設問 65 に**
- ○ 実装を検討中（実装の可能性が低い） → **設問 65 に**
- ○ 実装を行わない → **設問 64 に**

64.**端末 PC に対する二要素認証を実装しない理由を教えてください。**【テキスト入力】

[ ]

65.**ネットワーク機器に対する二要素認証の有無について教えてください。**【必須】【単一選択】

※ 二要素認証とは、知識認証（パスワードなど）、所有物認証（ID カードなど）、生体認証（例、顔認証、指紋認証、静脈認証、虹彩認証など）の三要素のうちの二要素を認証に用いることを言います。

- ○ 一要素認証である → **設問 66 に**
- ○ 二要素認証（物理認証あるいは生体認証によるサーバ室等への入退室管理とネットワーク機器に対するパスワード認証。ただし、リモート接続では一要素認証となっている） → **設問 68 に**
- ○ 二要素認証（物理認証あるいは生体認証によるサーバ室等への入退室管理とネットワーク機器に対するパスワード認証。リモート接続でも二要素認証を実現している） → **設問 68 に**
- ○ ネットワーク機器に対する二要素認証を実装している（リモート接続では一要素認証となっている） → **設問 68 に**
- ○ ネットワーク機器に対する二要素認証を実装している（リモート接続でも二要素認証を実現している） → **設問 68 に**
- ○ その他（ ） → **設問 68 に**

66.**ネットワーク機器に対する二要素認証を令和 9 年度までに実装予定である。**【必須】【単一選択】

- ○ 必ず実装する → **設問 68 に**
- ○ 実装を検討中（実装の可能性が高い） → **設問 68 に**
- ○ 実装を検討中（実装の可能性が低い） → **設問 68 に**
- ○ 実装しない → **設問 67 に**

67.**ネットワーク機器に対する二要素認証を実装しない理由を教えてください。**【テキスト入力】
[ ]

【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)】
68.**USB ストレージ等の外部記録媒体や情報機器に対してサーバへの接続を制限している。**
【必須】【単一選択】
- ○ 外部記録媒体や情報機器を接続しても、サーバが認識できないシステム設定となっている
- ○ 許可された外部記録媒体や情報機器だけが、サーバが認識できるシステム設定なっている
- ○ 外部記録媒体や情報機器を認識するが、接続は運用で禁止されている
- ○ 外部記録媒体や情報機器を認識するが、許可された外部記録媒体や情報機器のみ、サーバに接続する運用となっている（運用での制限）
- ○ 外部記録媒体や情報機器のサーバへの接続を制限していない
- ○ その他（ ）

69.**端末 PC に対する USB ストレージ等の外部記録媒体や情報機器の接続についてお答えください。**
【必須】【単一選択】
- ○ 外部記録媒体や情報機器の接続を許可していない（システム設定による接続制御）
- ○ 外部記録媒体や情報機器の接続を許可していない（システム設定ではなく、運用による接続制御）
- ○ 外部記録媒体や情報機器の接続は医療情報システム管理部門に依頼を行う（システム設定による接続制御）
- ○ 外部記録媒体や情報機器の接続は医療情報システム管理部門に依頼を行う（システム設定ではなく、運用による接続制御）
- ○ 病院に申請し許可された外部記録媒体や情報機器のみ端末 PC に接続することができる（システム設定による接続制御）
- ○ 病院に申請し許可された外部記録媒体や情報機器のみ端末 PC に接続することができる（システム設定ではなく、運用による接続制御）
- ○ 外部記録媒体や情報機器を自由に接続できる
- ○ その他（ ）

70.**部門システム管理者が使用する部門システム端末（医療情報システムネットワークに接続）に対する USB ストレージ等の外部記録媒体や情報機器の接続についてお答えください。**【必須】【単一選択】
- ○ 外部記録媒体や情報機器の接続を許可していない（システム設定による接続制御）
- ○ 外部記録媒体や情報機器の接続を許可していない（システム設定ではなく、運用による接続制御）
- ○ 外部記録媒体や情報機器の接続は医療情報システム管理部門に依頼を行う（システム設定による接続制御）
- ○ 外部記録媒体や情報機器の接続は医療情報システム管理部門に依頼を行う（システム設定ではなく、運用による接続制御）
- ○ 病院に申請し許可された外部記録媒体や情報機器のみ端末 PC に接続することができる（システム設定による接続制御）
- ○ 病院に申請し許可された外部記録媒体や情報機器のみ端末 PC に接続することができる（システム設定ではなく、運用による接続制御）
- ○ 外部記録媒体や情報機器を自由に接続できる。
- ○ その他（ ）

71.**エンドユーザが使用するワークステーション等の部門システム端末（医療情報システムネットワークに接続）に対する USB ストレージ等の外部記録媒体や情報機器の接続についてお答えください。**
【必須】【単一選択】

- ○ 外部記録媒体や情報機器の接続を許可していない（システム設定による接続制御）
- ○ 外部記録媒体や情報機器の接続を許可していない（システム設定ではなく、運用による接続制御）
- ○ 外部記録媒体や情報機器の接続は医療情報システム管理部門に依頼を行う（システム設定による接続制御）
- ○ 外部記録媒体や情報機器の接続は医療情報システム管理部門に依頼を行う（システム設定ではなく、運用による接続制御）
- ○ 病院に申請し許可された外部記録媒体や情報機器のみ端末 PC に接続することができる（システム設定による接続制御）
- ○ 病院に申請し許可された外部記録媒体や情報機器のみ端末 PC に接続することができる（システム設定ではなく、運用による接続制御）
- ○ 外部記録媒体や情報機器を自由に接続できる。
- ○ その他（　　）

セクション 6【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))】

72.**インシデント発生時における組織内の連絡体制図が整備されていますか。**【必須】【単一選択】

- ○ 整備しており定期的な見直しを実施している
- ○ 整備しているが定期的な見直しは実施していない
- ○ 整備を計画している
- ○ 整備する計画はない

73.**【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))】**
データやシステムのバックアップの対象を検討していますか。【必須】【単一選択】

- ○ すべての医療情報システムのデータはバックアップが取れている → **設問 74 に**
- ○ 診療を継続するために必要な情報を検討し、必要と判断したデータはバックアップが取れている → **設問 74 に**
- ○ 診療を継続するために必要な情報を検討しているが、バックアップが取れているのは、必要と判断した情報の一部である → **設問 74 に**
- ○ 診療を継続するために必要な情報を検討しておらず、ベンダーが提案したデータのバックアップを取っている → **設問 74 に**
- ○ データのバックアップを取っていない → **設問 79 に**

74.データやシステムのオフラインバックアップを実施していますか。【必須】【単一選択】

- ○ オフラインバックアップを実施している → **設問 75 に**
- ○ オフラインバックアップを実施できていない → **設問 76 に**

75.**データやシステムのオフラインバックアップの状況についてお答えください。**【必須】【複数選択】

- ○ テープバックアップ等によるオフラインバックアップ
- ○ イミュータブルバックアップによるオフラインバックアップ
- ○ クラウド保存でのオフラインバックアップ

76.**サイバーセキュリティ対策を想定したデータやシステムのバックアップのタイミングをお答えください。**【必須】【単一選択】

- ○ 日次
- ○ 2 日に 1 回
- ○ 3 日に 1 回
- ○ 4 日から 7 日に 1 回
- ○ 8 日から 14 日に 1 回
- ○ 15 日以上

77.**サイバーセキュリティ対策を想定したデータやシステムのバックアップは何世代行っていますか**
【必須】【単一選択】
- ○ 1 世代
- ○ 2 世代
- ○ 3 世代
- ○ 4 世代
- ○ 5 世代
- ○ 6 世代以上

78.**データバックアップの復旧手順の確認についてお答えください。**【必須】【単一選択】
- ○ データバックアップの復旧手順を確認し、復旧の実証訓練を行っている
- ○ データバックアップの復旧手順を確認しているが、復旧の実証訓練は実施していない
- ○ データバックアップの復旧は保守事業者に一任しており、医療機関として復旧手順の確認は行っていない
- ○ その他（ ）

【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))】

79.**サイバー攻撃を想定した事業継続計画（BCP）を策定していますか。**【必須】【単一選択】
- ○ 厚生労働省が作成した医療情報システム部門事業継続計画（BCP）を参考に策定した
  → 設問 80 に
- ○ 他院が作成した医療情報システム部門事業継続計画（BCP）を参考に策定した
  → 設問 80 に
- ○ 自施設で独自に策定した **→ 設問 80 に**
- ○ 策定していない **→ 設問 81 に**

80.**サイバー攻撃を想定した事業継続計画（BCP）を定期的に見直していますか。**【必須】【単一選択】
- ○ はい
- ○ いいえ

セクション 7【4. 規程類の整備（令和 7 年度）】

【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。(令和 7 年度 4-①)】

81.**体制構築について、具体的な実施方法を運用管理規程等に定めていますか。**【必須】【単一選択】

○ はい（定期的に見直している）
○ はい（定期的な見直しはできていない）
○ いいえ

82.**医療情報システムの管理・運用について、具体的な実施方法を運用管理規程等に定めていますか。**【必須】【単一選択】

○ はい（定期的に見直している）
○ はい（定期的な見直しはできていない）
○ いいえ

83.**インシデント発生に備えた対応について、具体的な実施方法（サイバー攻撃を想定した事業継続計画（BCP））を運用管理規程等に定めていますか。**【必須】【単一選択】

※ サイバー攻撃を想定した事業継続計画（BCP）が医療情報システム管理部門だけでなく、医療機関として承認され、共有されているかをご回答ください。

○ はい
○ いいえ

セクション 8　インタビュー調査へのご協力

本研究班では、本調査にご協力をいただいた医療機関のうち、いくつかの医療機関を選定し、インタビュー調査を行うことが求められています。
インタビュー調査をご協力いただく医療機関は研究班で選ばせていただきます。

84.**インタビュー調査にご協力いただけますか。**【必須】【単一選択】

※ オンラインで 60 分程度のインタビューを予定しています。
※ サイバーセキュリティ対策の責任者と実務担当者からのインタビューを想定しています。
※ 貴院でのサイバーセキュリティ対策をお聞かせいただいた後、サイバーセキュリティ対策について意見交換を行わせていただきます。

○ はい　→ **設問 85 に**
○ いいえ　→ **回答終了**

85.**研究班がご連絡をさせていただく連絡先をご記載ください。**
医療機関名【必須】【テキスト入力】
[　　]

86.ご担当部署【必須】【テキスト入力】
[　　]

87.ご担当者名【必須】【テキスト入力】
[　　]

88.ご連絡先（電話番号）【必須】【テキスト入力】
[　　]

89.ご連絡先（メールアドレス）【必須】【テキスト入力】
[　　]

別添１

令和6年度版
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

医療機関確認用

	チェック項目	確認結果（日付）	備考
医療情報システムの有無	医療情報システムを導入、運用している。 （「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ （　/　）	

*以下項目は令和6年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*1回目の確認で「いいえ」の場合、令和6年度中の対応目標日を記入してください。立入検査時、本チェックリストを確認します。

	チェック項目	確認結果（日付）			備考	R5年度項目
		1回目	目標日	2回目		
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))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**					
	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))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
	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)) ※事業者と契約していない場合には、記入不要	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
	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)) ※事業者と契約していない場合には、記入不要	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
	サーバについて、以下を実施している。					
	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))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
	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))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
	アクセスログを管理している。(2-(6))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
	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)	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		
	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))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		
	端末PCについて、以下を実施している。					
	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))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		
	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))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		
	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))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		
	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))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		
	ネットワーク機器について、以下を実施している。					
	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-(7))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
	接続元制限を実施している。(2-(8))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
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))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
	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))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		
	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))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		

- 各項目の考え方や確認方法等については、「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マニュアル～医療機関・事業者向け～」をご覧ください。
- 各チェック項目に記載された番号はチェックリストマニュアルのアウトラインに対応しています。
- R5年度項目欄（※）：「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（令和５年６月版）」において令和 5 年度中に対応することを目標として掲げた項目

令和6年度
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

事業者確認用

*以下項目は令和6年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*1回目の確認で「いいえ」の場合、令和6年度中の対応目標日を記入してください。立入検査時、本チェックリストを確認します。

	チェック項目	確認結果（日付）			備考	R5年度項目
		1回目	目標日	2回目		
1 体制構築	事業者内に、医療情報システム等の提供に係る管理責任者を設置している。(1-(1))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**					
	リモートメンテナンス（保守）している機器の有無を確認した。(2-(2))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	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))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	サーバについて、以下を実施している。					
	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))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	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))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	アクセスログを管理している。(2-(6))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	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))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	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))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	端末PCについて、以下を実施している。					
	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))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	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))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	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))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	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))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	ネットワーク機器について、以下を実施している。					
	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-(7))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	接続元制限を実施している。(2-(8))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※

事業者名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

- 各項目の考え方や確認方法等については、「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マニュアル～医療機関・事業者向け～」をご覧ください。
- 各チェック項目に記載された番号はチェックリストマニュアルのアウトラインに対応しています。
- R5年度項目欄（※）：「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（令和５年６月版）」において令和 5 年度中に対応することを目標として掲げた項目

令和７年度版
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

医療機関確認用

*立入検査時、本チェックリストを確認します。令和7年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*「いいえ」の場合、令和7年度中の対応目標日を記入してください。

	チェック項目	確認日	目標日	備考
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)	はい・いいえ (/)	(/)	
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**			
	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)	はい・いいえ (/)	(/)	
	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) ※事業者と契約していない場合には、記入不要	はい・いいえ (/)	(/)	
	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) ※事業者と契約していない場合には、記入不要	はい・いいえ (/)	(/)	
	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)	はい・いいえ (/)	(/)	
	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)	はい・いいえ (/)	(/)	
	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)	はい・いいえ (/)	(/)	
	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)	はい・いいえ (/)	(/)	
	パスワードの使い回しを禁止している。(2-⑧)	はい・いいえ (/)	(/)	
	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。 (2-⑨)	はい・いいえ (/)	(/)	
	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)	はい・いいえ (/)	(/)	
	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)	はい・いいえ (/)	(/)	
	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)	はい・いいえ (/)	(/)	
	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)	はい・いいえ (/)	(/)	
	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)	はい・いいえ (/)	(/)	
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)	はい・いいえ (/)	(/)	
	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)	はい・いいえ (/)	(/)	
	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)	はい・いいえ (/)	(/)	
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)	はい・いいえ (/)	(/)	

- 各項目の考え方や確認方法等については、「医療機関等におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関等・事業者向け～」をご覧ください。
- 各チェック項目に記載された番号はチェックリストマニュアルのアウトラインに対応しています。

令和７年度
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

事業者確認用

*以下項目は令和7年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*「いいえ」の場合、令和7年度中の対応目標日を記入してください。

	チェック項目	（日付）		備考
		確認日	目標日	
1 体制構築	事業者内に、医療情報システム等の提供に係る管理責任者を設置している。(1-①)	はい・いいえ（ / ）	（ / ）	
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**			
	リモートメンテナンス（保守）している機器の有無を確認した。(2-②)	はい・いいえ（ / ）	（ / ）	
	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)	はい・いいえ（ / ）	（ / ）	
	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)	はい・いいえ（ / ）	（ / ）	
	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)	はい・いいえ（ / ）	（ / ）	
	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)	はい・いいえ（ / ）	（ / ）	
	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)	はい・いいえ（ / ）	（ / ）	
	パスワードの使い回しを禁止している。(2-⑧)	はい・いいえ（ / ）	（ / ）	
	USBストレージ等の外部接続機器や情報機器に対して接続を制限している。 (2-⑨)	はい・いいえ（ / ）	（ / ）	
	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)	はい・いいえ（ / ）	（ / ）	
	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)	はい・いいえ（ / ）	（ / ）	
	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)	はい・いいえ（ / ）	（ / ）	
	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)	はい・いいえ（ / ）	（ / ）	
	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)	はい・いいえ（ / ）	（ / ）	

事業者名：

- 各項目の考え方や確認方法等については、「医療機関等におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関等・事業者向け～」をご覧ください。
- 各チェック項目に記載された番号はチェックリストマニュアルのアウトラインに対応しています。

厚生労働行政推進調査事業「医療機関におけるサイバーセキュリティ対策向上に 向けた課題調査と解決策の検討（25IA2012）」
施設訪問インタビューシート（Ver6. 2026.02.04）

A. 基本情報

No	大分類	小分類	調査結果
A-1	病院情報	病院名	
		所在地	
		病床数	
		病院区分	
		医療情報部門の有無、人数	
A-2	電子カルテベンダー、構築ベンダー	電子カルテシステムベンダーについて教えてください。 あわせて、実際に構築したベンダーが電子カルテシステムベンダーでない場合は、そのベンダーを教えてください。	製品名およびベンダー名： 構築ベンダー：
A-3	ネットワーク機器ベンダー、構築ベンダー	ネットワーク機器ベンダーについて教えてください。 あわせて、ネットワーク構築ベンダーについても教えてください。	製品名： 構築ベンダー：
A-4	セキュリティベンダー	セキュリティ対策について最もやり取りのある（相談する）ベンダーについて教えてください。	
A-5	主要ベンダー	医療情報システム関連で最もやり取りのある（相談する）ベンダーについて教えてください。	

B. 調査項目

No	大分類	調査の視点	調査結果	該当チェックリスト／調査項目	ヒアリングポイント
B-1	セキュリティ人材	・セキュリティ立案に関与する職員（立場、経験値、人数） ・セキュリティ運用に関与する職員（立場、経験値、人数） ・人材が確保できない要因、確保に向けて取り組んでいることは何かあるか。 ・医療情報技師（上級医療情報技師）の役割、どのように活動しているか。 ・IPA資格取得者の役割、どのように活動しているか。		【医療情報システム安全管理責任者を設置している。(1-(1))】 情報セキュリティ責任者（CISO: Chief Information Security Officer）を配置していますか。 ※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版では、「サイバー攻撃に対しては情報セキュリティ責任者（CISO（Chief Information Security Officer））の配置や、情報セキュリティ責任者（CISO）はサイバーセキュリティに対する知識をどの程度保有していますか。	・どの程度のエフォートか（ほぼ専任？） ・情報セキュリティに関する定期的なWGの有無など ・セキュリティ人材の教育などの課題 ・経営層（院長レベル）のセキュリティへの人・金の投資への理解など
B-2	資産管理	・実際にどのような手段（方法）で台帳管理しているか。 ・棚卸のタイミング、棚卸に要する工数はどうか。 ・問題点と対応にはどのようなものがあるか。		【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))】 医療情報システムに接続するサーバ、端末PC、ネットワーク機器の台帳管理を行っていますか。	・部門（診療科）が管理する機器などの把握
B-3	外部接続点管理	・外部接続点の把握方法 ・どのように調査、整理整頓を行い、棚卸を実施するか ・リモート接続時の運用ルールについて ・外部接続点における課題、運用がうまくいかない理由は何か。		【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))】 リモートメンテナンス（保守）の病院情報システムネットワークへの接続方法についてお答えください。	・外部接続の主な用途 ・外部接続の方法（施設主導の接続／ベンダー提案の接続） ・すべての外部接続点（FW）を把握・管理できているか ・部門が管理する機器の外部接続点の有無 ・外部接続の希望があった場合の対応フローが施設で整理されているか
B-4	MDS／SDSへの対応	・MDS/SDSからどのようなアクションをとったか。 ・現在の活用状況、また将来的にどう活用しようとしているか？		【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))】 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）の提出を受けていますか。	
B-5	ユーザー管理	・システムの利用者管理についてどのように運用しているか。 ・アプリの利用者管理はどのように行なっているか（新規追加から削除停止までのフロー、権限変更手順） ・OS、ミドル、ネットワークの利用者管理はどうしているか？ ・ロックアウト設定、パスワード変更タイミング、MFA対応などは実施できているか。またその範囲はどうか。		【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))】 【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。(令和7年度2-④)】 サーバ、ネットワーク機器に対するアクセス権限の付与方法について、教えてください。 【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))】 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ますか。	
B-6	各種ログ管理	・各種ログ管理について（電子カルテなど部門システムの利用ログでない） ・各種ログの収集方法 ・各種ログの確認タイミング ・各種ログの解析は誰がいつ、どのくらいの時間をかけて行なっているか。 ・ログ管理がうまくいかない理由はなにか？		【アクセスログを管理している。(2-(6))】 サーバ、端末PCのアクセスログを残していますか。	
B-7	セキュリティパッチ管理	・セキュリティパッチの実態について ・セキュリティパッチの適用方法と対応タイミング（情報認知から実施までの手順） ・対応範囲（アプリ、ミドル、OS） ・対応している中での課題（ベンダー、院内との意識） ・ベンダー等との契約はどのようになっているか？仕様書への記載文言はどのような内容か？ ・セキュリティパッチの対応がうまくいかない理由は何か？		【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、端末PC、ネットワーク機器に対し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）を適用していますか。	
B-8	二要素認証への対応	・機器に対する二要素認証の有無について ・一要素認証の場合の進められない課題、対応予定など		【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))】 サーバ、端末PC、ネットワーク機器に対する二要素認証の実装状況について。	
B-9	外部記憶媒体管理	・接続制限はどのように行っているのか？技術的対策？組織的対策？ ・その他ルールは何か？		【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)】 USBストレージ等の外部記録媒体や情報機器に対してサーバへの接続を制限している。	
B-10	システムバックアップ運用管理	・バックアップの取得方法、どのシステムで取得しているか？ ・取得したバックアップの管理方法はどうか？オンライン？オフライン？		【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))】 データやシステムのバックアップの対象を検討していますか。	
B-11	IT-BCPの策定と訓練	・IT-BCPで厚労省提示のものから追記した項目はあるか。 ・自然災害を想定したBCPとどこまで融合させているか。 ・誰が、どのくらいの期間で構築したか。 ・見直しを定期的に実施しているか。 ・IT-BCPに基づく訓練はどう対応しているか。 ・IT-BCPの対応がうまくいかない理由はなにか？		【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)) 】 サイバー攻撃を想定した事業継続計画（BCP）を策定していますか。	
B-12	その他	・セキュリティ対策に対して伝えたいこと、今後期待すること等			・セキュリティソフトの導入・保守は規模によって数百～数千の場合もある ・医療機器と違って診療報酬に結びつかず、導入のハードルは高い ・導入したからとって対策が完了する訳ではなく、運用できる人材が不可欠 ・施設の創意工夫に依存するか、何かトップダウンの施策が望ましいか

施設、組織体制

別添資料 3.

都道府県	施設数	都道府県	施設数	都道府県	施設数	都道府県	施設数
北海道	26	東京都	34	滋賀県	9	香川県	7
青森県	6	神奈川県	25	京都府	7	愛媛県	9
岩手県	6	新潟県	11	大阪府	45	高知県	5
宮城県	6	富山県	9	兵庫県	16	福岡県	26
秋田県	6	石川県	6	奈良県	9	佐賀県	2
山形県	5	福井県	5	和歌山県	10	長崎県	11
福島県	6	山梨県	7	鳥取県	3	熊本県	24
茨城県	12	長野県	11	島根県	5	大分県	6
栃木県	9	岐阜県	11	岡山県	10	宮崎県	5
群馬県	9	静岡県	15	広島県	13	鹿児島県	8
埼玉県	17	愛知県	29	山口県	9	沖縄県	7
千葉県	21	三重県	11	徳島県	1	合計	550

	施設数	割合
国公立大学病院	25	4.5%
公的な医療機関（大学病院を除く）	216	39.3%
私立大学病院	13	2.4%
私立の医療機関	296	53.8%

	施設数	割合
特定機能病院	35	6.4%
地域医療支援病院	154	28.0%
災害拠点病院（基幹）	41	7.5%
災害拠点病院（地域）	132	24.0%
第三次救急医療機関	87	15.8%
第二次救急医療機関	259	47.1%
総合周産期母子医療センター	30	5.5%
地域周産期母子医療センター	57	10.4%
小児中核病院	17	3.1%
小児地域医療センター	13	2.4%
小児地域支援病院	6	1.1%
上記の認定、指定は受けていない	185	33.6%

病床数	施設数	割合
1000床以上	6	1.1%
800床以上1000床未満	20	3.6%
600床以上800床未満	39	7.1%
400床以上600床未満	84	15.3%
300床以上400床未満	67	12.2%
200床以上300床未満	87	15.8%
100床以上200床未満	170	30.9%
100床未満	77	14.0%

診療録管理体制加算	施設数	割合
加算1	185	33.6%
加算2	127	23.1%
加算3	199	36.2%
算定していない	39	7.1%

医療情報部門の設置	施設数	割合
はい	440	80.0%
いいえ	110	20.0%

専門知識を有する情報セキュリティ人材	施設数	割合
高度な専門知識（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	29	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	209	38.0%
配置していない	312	56.7%

診療録の電子的保管	施設数	割合
はい	502	91.3%
いいえ	48	8.7%

【医療情報システム安全管理責任者を設置している。(1-(1))】

情報セキュリティ責任者（CISO: Chief Information Security Officer）、医療情報システム安全管理責任者の配置	施設数	割合
① 情報セキュリティ責任者（CISO）と医療情報システム安全管理責任者を配置（別の人物）	190	34.5%
② 情報セキュリティ責任者（CISO）のみ配置（医療情報システム安全管理責任者は配置せず）	11	2.0%
③ 情報セキュリティ責任者（CISO）・医療情報システム安全管理責任者（同一人物）を配置	212	38.5%
④ 医療情報システム安全管理責任者を配置（情報セキュリティ責任者（CISO）は配置せず）	102	18.5%
⑤ 配置していない	35	6.4%

知識	①CISO		①管理責任者		②CISO		③管理責任者		④管理責任者	
高度な専門知識（IPA ITスキル標準レベル4以上相当）を有しており、単独でも対策を進めることができる	4	2.1%	8	4.2%	0		6	2.8%	0	
一定の専門知識を有しており、単独でも対策を進めることができる	21	11.1%	35	18.4%	0		32	15.1%	4	3.9%
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	77	40.5%	90	47.4%	6	54.5%	129	60.8%	57	55.9%
ほとんど知識を有していない	76	40.0%	53	27.9%	5	45.5%	40	18.9%	31	30.4%
全く知識を有していない	12	6.3%	4	2.1%	0		5	2.4%	10	9.8%

職位	①CISO		①管理責任者		②CISO		③管理責任者		④管理責任者	
上部組織の理事など	12	6.3%	0		0		0		0	
医療機関の責任者（院長など）	83	43.7%	29	15.3%	4	36.4%	55	25.9%	27	26.5%
院長を補佐する立場（副院長、院長補佐など）	17	8.9%	25	13.2%	1	9.1%	20	9.4%	11	10.8%
医療情報システム管理部門の長	18	9.5%	60	31.6%	2	18.2%	60	28.3%	25	24.5%
医療情報システム管理部門（部門長以外）	3	1.6%	17	8.9%	0		8	3.8%	7	6.9%
事務部門の長	41	21.6%	32	16.8%	2	18.2%	39	18.4%	14	13.7%
事務部門（部門長以外）	6	3.2%	16	8.4%	1	9.1%	17	8.0%	7	6.9%
上記以外の部門の長	7	3.7%	7	3.7%	0		6	2.8%	7	6.9%
上記以外の部門（部門長以外）	3	1.6%	4	2.1%	1	9.1%	7	3.3%	4	3.9%

医療系資格	①CISO		①管理責任者		②CISO		③管理責任者		④管理責任者	
医師・歯科医師	105	55.3%	75	39.5%	5	45.5%	80	37.7%	46	45.1%
看護師・助産師・保健師	0		1	0.5%	0		0		1	1.0%
薬剤師	0		0		0		2	0.9%	2	2.0%
診療放射線技師	2	1.1%	7	3.7%	1	9.1%	8	3.8%	1	1.0%
臨床検査技師	0		3	1.6%	0		2	0.9%	0	
臨床工学技士	0		2	1.1%	0		1	0.5%	0	
医学物理士	0		0		0		0		0	
医療情報技師（上級医療情報技師を含む）	9	4.7%	29	15.3%	1	9.1%	35	16.5%	10	9.8%
診療情報管理士	10	5.3%	16	8.4%	2	18.2%	14	6.6%	9	8.8%
リストされる医療系資格を保持していない	69	36.3%	76	40.0%	3	27.3%	80	37.7%	37	36.3%

IPA資格	①CISO		①管理責任者		②CISO		③管理責任者		④管理責任者	
情報処理安全確保支援士（登録情報セキスペ）	0		2	1.1%	0		0		0	
情報処理安全確保支援士（資格試験合格のみ）	0		1	0.5%	0		1	0.5%	0	
応用技術者試験	3	1.6%	3	1.6%	0		3	1.4%	2	2.0%
基本情報技術者試験	7	3.7%	13	6.8%	0		22	10.4%	7	6.9%
情報セキュリティマネジメント試験	1	0.5%	9	4.7%	0		8	3.8%	0	
ITパスポート試験	9	4.7%	9	4.7%	0		9	4.2%	3	2.9%
リストされる資格・試験は保持していない	178	93.7%	162	85.3%	11	100.0%	178	84.0%	92	90.2%

CISO、安全管理責任者を配置しない理由	施設数	割合
許可病床数が200床以上であるが、医療情報システム安全管理責任者に適任な人材がいないから	7	20.0%
許可病床数が200床未満で、医療情報システム安全管理責任者に適任な人材がいないから	21	60.0%
許可病床数が200床未満で、医療情報システム安全管理責任者の設置の必要性を感じないから	3	8.6%
電子カルテが未導入（現状診療録が紙カルテ）	2	5.7%
その他	2	5.7%

サイバーセキュリティ対策の方針を決定する際に関わる情報セキュリティ人材	施設数	割合
情報セキュリティ責任者（CISO）	248	45.1%
医療情報システム安全管理責任者	404	73.5%
院内に配置する高度な専門知識（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	23	4.2%
院内に配置する専門知識を有する情報セキュリティ人材	151	27.5%
同一法人等の中央組織に配置する高度な専門知識（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	27	4.9%
同一法人等の中央組織に配置する専門知識を有する情報セキュリティ人材	79	14.4%
同一法人等の他医療機関に配置する高度な専門知識（ 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	9	1.6%
同一法人等の他医療機関に配置する専門知識を有する情報セキュリティ人材	17	3.1%
保守契約を結ぶ医療情報システムベンダー（情報セキュリティの知識を有することを確認している）	186	33.8%
保守契約を結ぶ医療情報システムベンダー（情報セキュリティの知識を有することを確認できていない）	94	17.1%
情報セキュリティ対策を専門とする企業等（医療情報システムベンダー以外）の情報セキュリティ人材	56	10.2%
その他	59	10.7%

【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))

サーバーの台帳管理	施設数	割合
全ての機器を把握している	389	70.7%
全ての機器を把握していると思うが、漏れがあるかもしれない	136	24.7%
全ての機器を把握できていない	10	1.8%
ほとんどの機器を把握できていない	0	0.0%
台帳管理を行っていない	15	2.7%

サーバーの台帳管理者	施設数	割合
自施設の職員	414	77.4%
機器を導入した事業者（保守契約など）	101	18.9%
導入事業者以外の事業者	15	2.8%
その他	5	0.9%
合計	535	

サーバの台帳管理方法	施設数	割合
用紙運用	22	4.1%
エクセル等の汎用ソフトを使用	448	83.7%
専用のソフトを使用	51	9.5%
その他	14	2.6%
合計	535	

端末PCの台帳管理	施設数	割合
全ての機器を把握している	341	62.0%
全ての機器を把握していると思うが、漏れがあるかもしれない	181	32.9%
全ての機器を把握できていない	17	3.1%
ほとんどの機器を把握できていない	0	
台帳管理を行っていない	11	2.0%

端末PCの台帳管理者	施設数	割合
自施設の職員	469	87.0%
機器を導入した事業者（保守契約など）	47	8.7%
導入事業者以外の事業者	20	3.7%
その他	3	0.6%
合計	539	

端末PCの台帳管理方法	施設数	割合
用紙運用	18	3.3%
エクセル等の汎用ソフトを使用	427	79.2%
専用のソフトを使用	85	15.8%
その他	9	1.7%
合計	539	

ネットワーク機器の台帳管理	施設数	割合
全ての機器を把握している	265	48.2%
全ての機器を把握していると思うが、漏れがあるかもしれない	214	38.9%
全ての機器を把握できていない	41	7.5%
ほとんどの機器を把握できていない	4	0.7%
台帳管理を行っていない	26	4.7%

ネットワーク機器の台帳管理者	施設数	割合
自施設の職員	369	70.4%
機器を導入した事業者（保守契約など）	138	26.3%
導入事業者以外の事業者	14	2.7%
その他	3	0.6%
合計	524	

ネットワーク機器の台帳管理方法	施設数	割合
用紙運用	36	6.9%
エクセル等の汎用ソフトを使用	427	81.5%
専用のソフトを使用	45	8.6%
その他	16	3.1%
合計	524	

外部から医療情報システムに接続している回線

外部から医療情報システムネットワークに接続している回線の把握

	施設数	割合
全て把握している	388	70.5%
一部のみ把握している	134	24.4%
把握していない	28	5.1%

外部から医療情報システムネットワークに接続している回線数

回線数	全て把握	一部のみ把握	合計	回線数	全て把握	一部のみ把握	合計	回線数	全て把握	一部のみ把握	合計
0	11		11								
1	33	10	43	16	7	1	8	31		1	1
2	35	13	48	17	6	2	8	32		2	2
3	43	15	58	18	5		5	33	2		2
4	30	14	44	19	1	1	2	34		1	1
5	36	14	50	20	7	5	12	35		2	2
6	23	6	29	21	1	2	3	36	1		1
7	27	3	30	22	2	1	3	38		1	1
8	10	5	15	23	2		2	40	1		1
9	13	4	17	24	1		1	43	1		1
10	19	10	29	25	2	1	3	45	2		2
11	9	2	11	26	2	2	4	48	1		1
12	12	3	15	27	2	1	3	51	1		1
13	9	2	11	28	1	1	2	80	1		1
14	7	4	11	29	4		4	89	1		1
15	8	2	10	30	6	1	7	無回答	3	2	5
						回線数の平均			8.9	9.4	9.1
						11回線以上の割合			27.3%	28.8%	27.7%

外部から医療情報システムネットワークに接続している回線を減らす努力

	全て把握		一部のみ把握		把握していない		合計	
努力をしている	199	51.3%	49	36.6%	10	35.7%	258	46.9%
回線数を減らす必要性は感じているが、努力はできていない	114	29.4%	53	39.6%	13	46.4%	180	32.7%
回線数を減らす必要性は感じていない	75	19.3%	32	23.9%	5	17.9%	112	20.4%

適切に管理できる回線数

	回線数の把握			
回線数	全て把握	一部のみ把握	把握していない	総計
0	42	18	3	63
1	41	10	1	52
2	13	4		17
3	37	7	1	45
4	5	3		8
5	31	18		49
6	4	1		5
7	2			2
8	4			4
9	1			1
10	39	18	1	58
20	8	2		10
24	1			1
25	2			2
30	3	5		8
43	1			1
合計	234	86	6	326
回線数の平均	5.1	6.0	2.3	5.3

適切に管理できる回線数

	回線数を減らす努力			
回線数	努力をしている	努力できていない	必要性を感じない	総計
0	25	25	13	63
1	36	9	7	52
2	6	5	6	17
3	21	17	7	45
4	4	4		8
5	23	18	8	49
6	2	3		5
7	1		1	2
8	3	1		4
9	1			1
10	33	16	9	58
20	6	4		10
24		1		1
25		1	1	2
30	5		3	8
43		1		1
合計	166	105	55	326
回線数の平均	5.4	5.1	5.3	5.3

【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))】

リモートメンテナンス（保守）の病院情報システムネットワークへの接続方法	施設数	割合	施設数	割合
自施設が設置するリモート接続の仕組みを持っている			346	62.9%
自施設が設置するリモート接続の仕組みを使った接続のみ許可している	100	18.2%		
自施設が設置するリモート接続の仕組みを使った接続を原則とするが、ベンダー側の理由で例外を認めている（接続する全てのリモートメンテナンス回線を把握している）	196	35.6%		
自施設が設置するリモート接続の仕組みを使った接続を原則とするが、ベンダー側の理由で例外を認めている（接続する全てのリモートメンテナンス回線を把握できていない）	50	9.1%		
自施設でリモート接続の仕組みを有さず、ベンダー個々の接続方法で接続を許可している			152	27.6%
（接続する全てのリモートメンテナンス回線を把握している）	114	20.7%		
（接続する全てのリモートメンテナンス回線を把握できていない）	38	6.9%		
リモート接続はベンダーに任せており、リモート接続の許可を行っていない			46	8.4%
（接続する全てのリモートメンテナンス回線の把握はできている）	35	6.4%		
（接続する全てのリモートメンテナンス回線の把握ができていない）	11	2.0%		
リモートメンテナンス（保守）は行っていない	6	1.1%	6	1.1%

【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))】

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）の提出を受けている				
	施設数	割合	施設数	割合
提出を受けている			514	93.5%
提出を受け、内容を確認し、必要があれば具体的な対応を行っている	140	25.5%		
提出を受け、内容を確認しているが、具体的な対応までは行っていない	261	47.5%		
提出を受けているが、内容は十分に確認していない	113	20.5%		
提出を受けていない			26	4.7%
提出を受けていない（必要性を感じていない）	19	3.5%		
提出を受けていない（事業者が対応してくれない）	7	1.3%		
事業者と契約していない	10	1.8%	10	1.8%

医療情報セキュリティ開示書（MDS/SDS）への具体的な対応事例

無回答項目への内容確認、記載依頼	3
2要素認証対応について	3
事業者が利用しているルータやファイアウォールのファームウェアバージョンアップの指示やできない場合の対応についての確認	2
同一パスワードの変更依頼、管理台帳などへの反映	1
WindowsUpdateに代表される更新プログラムの適用状況を確認し、適用が可能な内容であれば適切に対応いただいている。	1
システムのリモート対応の手段・仕組みを確認、パスワードの変更可否の確認、デバイス制御をした際のシステムの影響確認	1
セキュリティパッチの確認をし、ネットワークの切断が関係する場合は適用するスケジュールの調整など	1
ネットワーク機器のセキュリティパッチ適用	1
ベンダーで利用するリモート接続保守作業用端末を1台に限定していただき、病院側に提示していただく	1
ベンダーに対し改善依頼を行い、改善状況に応じ報告を求める。	1
扱う情報のリストの提示依頼を行った。	1
医療情報セキリティ開示書の内容確認して、設定に必要な事項があれば、申請書の提出を依頼し、規定に基づき運用を行っている。	1
管理用アカウントのパスワードが簡易なものだったため、複雑なものへの変更を指示した。	1
業者が用意したリモート接続ソフトウェアではなく、自施設が用意したリモート接続ソフトウェアの利用を依頼している	1
更新等があれば提出するように常に依頼している。	1
接続許可は、本部情報システム課が行っている。	1
対応できていない箇所について、理由及び対応可能になる時期の説明を要求している。	1
対応不十分な項目に対する対応見積の要請及び対応実施	1
単純な記入漏れがないか、「いいえ」や「対象外」、「非該当」を選択の場合、備考に理由や説明が記載してあるかを確認しています。また、記載内容に疑問があれば、問い合わせをしています。	1
部門システム更新時に、次のような対応を実施。病院での対応を依頼する表現や「指示があれば対応可能（院内タイムサーバーへの接続、資産管理ソフト導入など）」「必要に応じて病院と取り決める」「運用でカバーしてください」といった、対応が不十分な事項については、仕様書への記載や部署を交えた運用決定などの対応を実施した。	1
未対応項目についてはベンダーと交渉している	1

【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))】

アクセス権限の付与方法	サーバ		ネットワーク機器	
	施設数	割合	施設数	割合
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	104	18.9%	127	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	192	34.9%	188	34.2%
組織ごと(病院やベンダー)にユーザIDと利用権限を設定し、ユーザパスワードは全ての機器群で同じである	46	8.4%	45	8.2%
組織ごと(病院やベンダー)にユーザIDと利用権限を設定し、ユーザパスワードは機器群ごとに異なっている	116	21.1%	96	17.5%
ユーザごとにIDと利用権限を設定し、ユーザパスワードは全ての機器群で同じである	30	5.5%	38	6.9%
ユーザごとにIDと利用権限を設定し、ユーザパスワードは機器群ごとに異なっている	62	11.3%	56	10.2%

端末PCのエンドユーザに対するユーザ認証について	施設数	割合
OSのユーザ認証を活用したユーザ認証を行っている	98	17.8%
OSのユーザ認証とソフトウェアでユーザ認証を組み合わせたユーザ認証を行っている	78	14.2%
OSはadministrator権限で自動ログインを行い、ソフトウェアでユーザ認証を行っている	96	17.5%
OSはadministrator以外の同一ユーザで自動ログインを行い、ソフトウェアでユーザ認証を行っている	252	45.8%
その他	26	4.7%

- ActiverDirectory認証
- OSはadministrator以外の個別ユーザで自動ログインを行い、ソフトウェアでユーザ認証を行っている
- OSはadministrator以外の端末固有ユーザで自動ログインを行い、ソフトウェアでユーザ認証を行っている
- OSはadministrator以外の同一ユーザでパスワードなし手動ログインを行い、ソフトウェアでユーザ認証を行っている
- OSはadministrator以外の同一ユーザでパスワードによるログインを行い、ソフトウェアでユーザ認証を行っている。
- OSはadministrator以外の同一ユーザでログインを行い、ソフトウェアでユーザ認証を行っている
- OSはadministrator権限で自動ログイン、ユーザ認証は行っていない。
- OSはadministrator権限で手動ログインを行い、ソフトウェアでユーザ認証を行っている
- OSは自動ログイン(admin権限なし)、ソフトウェアでユーザー認証
- OSは端末個別ユーザーとPWでログインし、ソフトウェア(電子カルテ)でユーザー認証を行っている
- OSは端末毎のユーザー(端末名)でログインし、ソフトウェアでユーザー認証を行っている。
- OSユーザー認証はしていない、ソフトウエアでの認証もしていない
- OSユーザ認証とエンドユーザの静脈認証
- SQLサーバ使用
- 各システム、各ベンダーで異なる
- ドメインユーザー認証
- ローカル端末はadministrator以外の同一ユーザで自動ログインを行い、ソフトウェアでユーザ認証を実施、VDI側はシングルサインオンにてOSのユーザ認証を行う
- 個人用の端末には個人のIDを設定し、部署用の端末には部署のIDを設定している

端末PCのエンドユーザに対するアクセス利用権限	施設数	割合
すべてのユーザに対して個別のユーザIDを発行し、アクセス利用権限を設定している (複数のユーザで使いまわしをしているユーザIDはない)	274	49.8%
すべてのユーザに対して個別のユーザIDを発行し、アクセス利用権限を設定することを原則とするが、一部、運用等の理由で、複数のユーザで使いまわしをしているユーザIDがある		
(管理者権限のID使いまわしはない)	138	25.1%
(管理者権限のID使いまわしがある)	44	8.0%
(管理者権限のID使いまわしがあるか否かは把握できていない)	8	1.5%
必要に応じて、ユーザごとのID付与と、組織、グループごと(外部委託業者など)のID付与を使い分けている	56	10.2%
その他	30	5.5%

- O/Sレベルではローカルadmin権限を有するが、UI上で機能制限をかけている。また、アプリレベルではすべてのユーザに対して個別のユーザIDを発行しているが、一部のアプリで使いまわしをしている。
- OSでは全てのユーザに対してIDは共通である。ソフトウェアのIDはユーザごとに個別に発行し、アクセス利用権限を設定している。
- OSのユーザは端末毎に個別のユーザIDを発行し複数のユーザで使い回しをしている場合がある
- OSは基本同一ユーザでログインし、ソフトウェアは全てのユーザに対して個別のIDを発行している
- OSは自動ログイン(admin権限なし)、ソフトウェアでユーザー認証及び利用権限を設定
- OSユーザー認証はしていない、ソフトウエアでの認証もしていない
- OSレベルのログインは非特権の単一のIDパスワードを使用している。このOSIDに対しては、端末上でアプリケーションを使用するために最小の権限を設定している。アプリケーションレベルは個別のユーザIDにより　、アプリケーション内のアクセス利用権限を設定している。
- WindowsLogInは全て共用、ソフトウェアログイン時に個別ユーザー、パスワードを入力
- すべてadministratorを利用しアクセス利用権限は設定されていない
- すべてのユーザーに対して個別のIDを発行し、アクセス権限を設定している。電子カルテメンテナンス業者については、専用IDを発行し、ID利用者を台帳管理している
- すべての端末は固定IDで運用されている。利用者権限のみで利用されている。
- すべて共通ユーザで使用している。各アプリケーションはユーザ個別にIDを発行しアクセス権を管理。富士通のパッケージはそうなっていると聞いています。
- ユーザではなく端末ごとにIDを生成
- 運用等の理由で、共通ユーザIDを使用
- 各システム、各ベンダーで異なる
- 管理者権限と、同一ユーザIDで使い分けている
- 機器ごとのIDI・パスワードを使用
- 制限なし
- 全てのユーザーに対して個別のIDを発行し、アクセス権限を設定している。電子カルテメンテナンス業者については、専用IDを発行しID利用者を台帳管理している。
- 端末IDは1つだが、システムは個別IDで対応
- 端末PCのエンドユーザーは端末毎のユーザー(端末名)で、標準ユーザーである。端末PCの管理者ユーザーは、システム管理者のみ利用可能。(管理者ユーザーは全端末で共通)　ソフトウェアのユーザーIDでアクセス利用権限を設定している。
- 端末ごとにユーザIDを作成し、複数ユーザで使いまわしている。このIDにはローカル管理者権限を付与している
- 端末は共有IDを使用しているが、電子カルテへのアクセスは個別IDにてアクセスしている
- 端末レベルでは自動ログイン、アプリケーションレベルで個別ユーザID発行
- 同一ID
- 同一ユーザで自動ログイン
- 部門毎の設定で複数のユーザで使いまわしをしている

【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している。(2-(5))】

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	サーバ		端末PC	
	施設数	割合	合計	割合
全て、削除または無効化できている	404	73.5%	391	71.1%
一部、削除または無効化できていない	114	20.7%	133	24.2%
全て、削除または無効化できていない	32	5.8%	26	4.7%

不要なアカウントを削除または無効化するタイミング	サーバ		端末PC	
	施設数	割合	合計	割合
退職日を有効期限に設定するなどリアルタイムでアカウントを削除または無効化している	347	63.1%	345	62.7%
年に1回など棚卸作業を行い、不要なアカウントを削除または無効化している （退職後にアカウントが有効な期間が存在する）	157	28.5%	167	30.4%
削除または無効化できていない	46	8.4%	38	6.9%

【アクセスログを管理している。(2-(6))】

アクセスログの残している範囲	サーバ		端末PC	
	施設数	割合	施設数	割合
全ての機器のアクセスログを残している	308	56.0%	285	51.8%
一部の機器のアクセスログを残している	183	33.3%	165	30.0%
アクセスログを残していない	59	10.7%	100	18.2%

アクセスログを確認しているか	サーバ		端末PC	
	施設数	割合	施設数	割合
病院職員がアクセスログを定期的に確認している	57	11.6%	63	14.0%
保守事業者がアクセスログを定期的に確認している	46	9.4%	19	4.2%
アクセスログを定期的に確認していないが、必要があれば病院職員が確認をすることが可能である	177	36.0%	238	52.9%
アクセスログを定期的に確認していないが、必要があれば保守事業者が確認をすることが可能である	179	36.5%	110	24.4%
アクセスログを残しているが、確認方法は把握していない	32	6.5%	20	4.4%

アクセスログの保管期間	サーバ		端末PC	
	施設数	割合	施設数	割合
医療機関がサーバのアクセスログの保管期間を指定している	102	20.8%	115	25.6%
保守事業者が定めたアクセスログの保管期間を医療機関として把握している	164	33.4%	147	32.7%
アクセスログの保管期間を把握していない	225	45.8%	188	41.8%

アクセスログを残さない理由	施設数
医療機関としてアクセスログを残す必要性を感じていない	12
医療機関としてアクセスログを残す必要性を感じているが、コストがかかるため残すことができない	72
医療機関としてアクセスログを残す必要性を感じているが、保守事業者が対応してくれない	18
その他	24

- オーダリングソフトに機能がない
- システムの仕様をベンダーが握っており、全体を統一して管理できないため。
- システム管理が兼務のためログの管理まで手が回らない
- ソフトウェアのログオンにてアクセス確認している。
- ソフトウェアの利用ログはサーバー上にログが残る。クライアントログは取っていない。
- ドメイン管理をしていないため
- ベンダーが管理しているかもしれないが病院で把握できていない
- 一度選択したら外せないのでここに記載
- 各システム、各ベンダーで対応が異なるため
- 残していると回答
- 実施を検討中
- 主要な機器は残しているが、部門機器などよくわからないものがある
- 他の業務が優先されて対応できていない
- 端末PC：アクセスログの管理はないが、NDR、EPPにより保護されている
- 端末PC上に医療情報は保管せず、サーバー上で保管されているため。サーバーへのアクセスログのみ管理している。
- 端末からシステムにログインすることで当該システムのサーバーにアクセスログが残るため端末には残していない。また、端末自体は不特定多数の職員が使用するため自動ログインするため。
- 端末には共通IDでログインしているので、残しても利用できない。
- 端末のアクセスログを残す費用は無い
- 端末自体はほとんど何もできないユーザーでログインしているため。電子カルテログイン後はアプリケーション側のログを取得している
- 電子カルテ等個人情報に係るネットワークが未導入の為
- 電子カルテ用PCは複数が使用するため端末PCにアクセスログは設定していない
- 必要性は感じているが、未対応
- 不明
- 方法が分からない

【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))】

セキュリティパッチの適用	サーバ		端末PC		ネットワーク	
	施設数	割合	施設数	割合	施設数	割合
全ての機器に対して適用している	138	25.1%	137	24.9%	173	31.5%
一部の機器に対して適用している	149	27.1%	117	21.3%	187	34.0%
適用していない	263	47.8%	296	53.8%	190	34.5%

セキュリティパッチを当てるタイミング	サーバ		端末PC		ネットワーク	
	施設数	割合	施設数	割合	施設数	割合
セキュリティパッチごとにリアルタイムで（システム検証は行わない）	40	13.9%	55	21.7%	42	11.7%
セキュリティパッチごとにできるだけ早いタイミングで（システム検証を行った後）	44	15.3%	39	15.4%	56	15.6%
定期的に（〇ヶ月に1回など時期を決めて）、セキュリティパッチをまとめて適用を行う	26	9.1%	29	11.4%	31	8.6%
適用が必要なセキュリティパッチが出てきた時に、保守事業者と打ち合わせを行った上、適用時期を決める	165	57.5%	115	45.3%	219	60.8%
その他	12	4.2%	16	6.3%	12	3.3%

セキュリティパッチを当てる範囲	サーバ		端末PC		ネットワーク	
	施設数	割合	施設数	割合	施設数	割合
全てのセキュリティパッチを適応している	47	16.4%	61	24.0%	51	14.2%
医療機関が必要と判断したセキュリティパッチと保守事業者が推奨するセキュリティパッチを適用している	73	25.4%	68	26.8%	107	29.7%
医療機関が必要と判断したセキュリティパッチを適用している	15	5.2%	24	9.4%	18	5.0%
保守事業者が推奨するセキュリティパッチを適用している	149	51.9%	95	37.4%	174	48.3%
その他	3	1.0%	6	2.4%	10	2.8%

セキュリティパッチを当てる費用	サーバ		端末PC		ネットワーク	
	施設数	割合	施設数	割合	施設数	割合
保守費用に含まれる	233	81.2%	206	81.1%	269	74.7%
随時、作業費用を支払っている	54	18.8%	48	18.9%	91	25.3%

セキュリティパッチを適用しない理由	施設数	割合
医療機関として必要性を感じていない	18	6.3%
医療機関として必要性を感じているが、事業者が対応をしてくれない	68	23.6%
医療機関として必要性を感じているが、作業費用の捻出が困難である	102	35.4%
その他	100	34.7%

【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))】

セキュリティパッチを適用しない理由(その他)

- 外部インターネットに接続していないクローズドシステムため
- Closed Netwokで端末は未適用
- HISソフトの動作安定優先
- HIS系ネットワーク（保守ベンダーリモート接続のみ）のため、Windows Updateに対応できていない。一部、ソフトウェアでアップデート対応ができないため時期システム更改時にしか対応できない状況です。
- OSは更新プログラムを適応していないが、ウイルス対策ソフトにて対応している
- VDIとなっていて、すべての部門システムが「相乗り」になっていて、医療機関内で検証ができない
- windows のアップデートは適用していないが、ウイルスソフト「ESET」の更新を実施している
- アプリケーションがセキュリティパッチの更新に対応できない。
- アプリケーションの動作可否の確認と作業時間などの捻出が難しい。
- アプリの関係で適用できない
- インターネットから分離していることと、稼働中のシステムへの影響が懸念されることから、セキュリパッチの適用が難しい環境にある。そのため、インターネットからの分離と、外部記憶媒体の接続制限による代替対応を実施している。代替対応については、医療情報システム安全管理に関するガイドラインQ&Aを参照した。
- インターネットに接続していないため
- インターネットに接続していない前提。又、パッチ適用後の不具合等でシステムに影響させないため
- イントラネットはインターネットに接続していない為
- イントラネットワークをインターネット接続できないようにしているため
- オフアインのため適用が困難
- オフラインの為、適用できない、ウィルス対策ソフトはパッチ適用している
- オフライン運用なので
- オフライン運用の為
- オフライン運用をしている
- オンプレであり、電子カルテ系統はネット接続していない
- オンプレ環境のため、また、テスト環境がないため
- カルテ端末はカルテ以外にもシステムが相乗りしているため、全てのシステムで検証を行わないと動作に不安がある。また、当院ではカルテ端末はネット不可のためWSUSなど更新に必要な仕組みを構築する必要がある。よって端末は外部記憶装置使用の制限やセキュリティソフトで対応している。
- クローズシステムの為
- クローズド運用であること、パッチを当てることによる動作不良等が発生する問題があることと、作業費用の捻出が難しいため適応は難しい。
- クローズド環境のため、セキュリティ更新環境を構築していない。また、システムベンダー側で都度のOSセキュリティ更新におけるシステム動作検証に対応していないため、セキュリティ更新環境を整えてもOSセキュリティ更新を行えないのが実態である
- クローズなので更新が困難
- サーバ、端末PCについては業務システムへの影響を考慮してベンダーへ対応方針を確認中です
- サーバ、端末に関してはクローズドネットワークのため適用していない
- サーバー以外はアップデート済
- システムが稼働しなくなる可能性があるため
- システムが対応していない
- システムによってはセキュリティパッチを適用することで動作に不具合が生じるシステムが存在するため
- システムの仕様をベンダーが握っており、全体を統一して管理できないため。
- システムへの影響が大きい為適用が困難と聞いている
- システム運用上の制限がある
- セキュリティパッチの適用によりシステムの運用障害発生の可能性があるのでクローズネットワーク内のサーバ、PCには適用しない
- セキュリティパッチを適用している
- ソフトウェアの動作保証が確認できない
- ネットに繋げていない
- パッチを適用することによりその影響でシステムが停止（動作不良）の可能性があり、診療継続できない恐れがあるため。
- パッチを適用すると電子カルテが正常動作しない
- パッチ適用による予期せぬ動作不具合のリスクを回避できない可能性があるため
- パッチ適用後の動作検証ができていない
- ベンダーから医療機関の端末PCにおいてセキュリティパッチを適用している機関はほぼないと聞いている
- ベンダーと相談し必要に応じ適用することとしているため
- メーカーの意向
- レセコン単独使用環境
- 医療機関として必要性を感じているが、作業費用の捻出や電子カルテシステムや部門システムの動作検証が困難である。
- 医療情報システムの正常動作への懸念
- 医療情報ネットワークはクローズのため
- 影響が大きいセキュリティパッチのみ保守業者の申告により適用している
- 可能なものは適応している。オフライン環境であり、医療情報システムの運用上未適応のものがある。
- 回線都合
- 外部接続は保守業者のVPNのみであるため。
- 外部接続負荷/クローズの状況で使用しているため
- 各システム、ベンダーで対応が異なる
- 完全な必要性の場合、検討する。
- 機器更新を行って間もないため
- 検証が取れていない
- 検証上適応できないものもあるため
- 原則閉域網であるHIS系機器へのセキュリティパッチを適用が困難。各種システムの動作への影響を懸念
- 古いOSの端末がたくさんあり個々の対応が必要であるが、設定するスタッフがいない
- 作業費用および作業人員の捻出が困難
- 事業者、作業費用の両面で困難である。
- 事業者が拒否している為
- 実施している
- 脆弱性該当機器のみパッチ適用
- 端末PCには不要
- 端末PCのbっ氏hs、パッチ適用による動作不能のリスクがあるため
- 摘要できる環境にない
- 適用させると部門システム含め最新のOSやブラウザに対応していない場合、システムが動作しなくなる可能性があるため。
- 適用することでシステムの稼働が不安定にならないかが心配である
- 電カル関係はパッチ適用による動作保証がない
- 電子カルテシステム・OSに制限がある為
- 電子カルテへ影響する可能性がある場合
- 電子カルテメーカーがインターネッと接続を認めない
- 電子カルテ端末はセキュリティパッチを適用すると動作及び保守対象外となる、または高額な費用を請求されるため適用していない
- 動作の保証がない
- 動作を保証できないため
- 動作確認の保証に関わるから
- 特定の機器・サーバを特定（決済・オン資）FWで接続を制御、リモートメンテもリモート先から外部への接続無し。次期システムでパッチ適用を開始する。
- 費用ももちろんですが、電子カルテ側が最新のパッチに適応されていないため困難
- 費用面から業者が行うのではなく安全管理責任者が行う。またセキュリティパッチの適用自体を禁止にしているベンダーもいる
- 必ずしも最新にはしておらず脆弱性がある場合のみ
- 必要性は感じています
- 必要性は感じているが、各システムが正常に動作することを確認できないため。
- 必要性は感じており、検討中で
- 必要性は理解できるが、オフラインのネットワーク環境でのパッチ適用作業が現実的ではない
- 必要性を感じているが、現在はWSUS等の環境がなく次期更新で検討
- 病院内のみの医療情報システムであり、外部接続は原則ないため。
- 不明
- 負荷
- 部分的に必要に応じて適用しているが、全体としては作業費用の捻出が困難である
- 複数のシステムと連携しているため
- 閉じたLANであり、パッチの適用が難しい
- 閉域網であり、保守事業所の判断
- 保守回線以外ではインターネット接続不可の為
- 保守用の回線のみでダウロードするインターネット接続口がない
- 有償で対応可能だが、他部門システムとの動作確認ができていない為
- 「一律に全台/全パッチ適用」ではなく、リスクに応じた機器選定が現実的になるので、チェックシートでもそのような記載にしてほしい。
- ベンダーが言うようにパッチ適用によることによって出るかもしれない不具合が心配。パッチ適用がある意味リスク。
- パッチ適用を促すのであれば、医療機関へ対応を求めるのではなく、医療情報システムを提供しているベンダーへの義務化をするべき。・利用している医療機関は立場が弱い、できないと言われたり、動作保証できないと言われたり、費用が掛かったりで厳しい。
- その他、パッチ適用に限らず、セキュリティチェックリストで求められていることは、ベンダーへ対応求めるようにしないと解決できない。
- CTやMRI、超音波機器などのモダリティ機器へのセキュリティパッチ適用は、機器の安定稼働の面から適用できないと言われています。ですが、セキュリティ対策チェックリストでは「必要」となっています。現状との解離が生じていますが、この辺りの見解をお聞かせ願います。
- DMZにある機器に対しては、セキュリティパッチを適用している。通常の電子カルテ端末は、多くのシステムが相乗りしており、全パッケージベンダーが対応できないとパッチが当てられない。セキュリティパッチ適用の見積もりを取得すると、高額な見積もりになる（正確にはパッチ適用後に発生する可能性に対する費用は別途になる）医療情報を扱うソフトウェアに対して、セキュリティ順守度を確認する制度ができないか？と考えます。

【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))】

セキュリティパッチに対する意見 (1)

- HISベンダー側でアプリケーション側のセキュリティパッチ対応の開発が進まない。一般的な汎用システムに比較して医療ベンダーの認識が低く大変困っている。
- OSバージョン固定が大半の医療システム仕様条件となっているため、パッチ適用は補償範囲外となり適用できない。
- PC、サーバは基本的にクローズネットワーク上の配置なのでWindowsUpdateなどの更新は行えない。セキュリティアプリ（シマンテック）は毎日更新しています。
- アプリケーションがセキュリティパッチによる動作保証ができないのであれば、Webアプリケーション化やコンテナ化など、ローカルのカーネルに依存しない作りにする方向で開発して欲しい
- アプリケーションが止まることがあり、この足を踏んでしまう
- あらゆるベンダーの動作検証が必要で、期間は数か月を要し、さらに費用面においても懸念がある。持続的なパッチ更新はほぼ困難。
- いずれのベンダーとの保守契約にもセキュリティパッチの適用は含まれていません。理由は稼働に問題が出た場合に対処ができないとの回答。これは厚労省の規約で記載があっても現状はこのような状況です。
- ウイルスソフト等のパターン更新は可能であるが、OS等の更新プログラム適用は各施設での個別対応は不可能であり、事業者への依頼となると莫大な費用が掛かる。理想ではあるが現実的でない項目であるため解決策が見つからない。
- ウイルス対策ソフトのパターンファイルのみ更新を行うようにしているが、Windows のセキュリティパッチは対応できていないです。また、一部ソフトウェアにおいてWindows Updateで不具合がでるため更新不可との回答があり、費用や運用面において次期リプレイスまでは使い続けるしかない状況です。
- オフライン（インターネット非接続）のサーバーや端末の運用はオンラインの機器とは切り離して考えていただきたい
- オフラインで運用しているとアップデート作業が非常に手間である
- オフライン環境で既存で動いているシステムやプログラムの影響を考慮しながら常にセキュリティーパッチを適用していくのは困難
- オフライン環境下でのパッチ適用作業が現実的ではない。windowsが以前あったSP(サービスパック)方式ではなくなったので、アップデート作業自体非常に手間と時間がかかる。
- オンプレの状況で、セキュリティパッチがどこまで必要か検討しあぐねている
- オンプレミス環境ではサーバーや端末PCへの適用はできてもルーターのファームウェアは実施が難しい
- オンプレ製品を利用している場合、閉鎖空間にあるためパッチ適用が困難であること、また、医療情報システムが正常に動作しなくなる懸念があり適用できない
- カルテ端末はカルテ以外にもシステムが相乗りしているため、全てのシステムで検証を行わないと適用できない。また、当院ではカルテ端末はネット不可のためWSUSなど更新に必要な仕組みを構築する必要がある。よって端末は外部記憶装置使用の制限やセキュリティソフトで対応している。
- クライアントにWindowsを使用している医療機関が多いと思うがマイクロソフトがインターネット接続を実質的に必須としているためオフラインでの運用が非常に困難である。WSUSサーバにおいても廃止予定であり、導入費用もそれなりに高額であるため今更導入は出来ない。そのため安全管理責任者が夜間に手動で当てているが毎月全台数を当てることは難しい。またベンダーもそういう相談には乗ってもらえない。パッチをこちらが当てること自体を禁止しているベンダーもいる。（そういうことを想定していないのではと感じることもある）
- クライアント端末への適用が出来ているが、サーバに関してはベンダー側から許可が下りず対応できていない。また、対応が出来たとしても適用毎に作業費が発生するため、全てのサーバに適用しようとすると多額の費用が掛かる
- クラサバを一定の基準で構築しており、セキュリティパッチの適用により、その関係性を阻害され、サービスの安定的提供ができないおそれがあるため、セキュリティパッチの適用は行いたいという希望はあるが、サービスの安定的提供を優先し、積極的なパッチ適用はベンダーとの了解のもと、行っていない。
- クローズドネットワークでの運用のため、適切なアップデート方法が分からない
- クローズなので更新が困難
- クローン環境を構築しパッチ適用テストを行わないと、実環境への適用は難しいと思います。そうなると、非現実的な環境構築費用を捻出する必要があり、収益の乏しい施設では事実上不可能と判断します。
- サーバ、クライアントのwindowsパッチを適用すると動作保証できず、対応できないと全てのアプリケーションベンダーから言われています。この考えが大多数でないでしょうか。最大手の電子カルテベンダー、最大シェアの各部門システムも同様の姿勢です。
- 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動作の検証等に高額な費用がかかるため困難である。
- サーバーPCや端末PCに最新のファームウェアを適用する際にはインターネット接続が必要と考えています。作業のために接続することが逆にウイルス感染のリスクを高めると思っておりますが如何なものでしょう？
- サーバーや端末PCもOSセキュリティパッチ適用については大病院ほど実質不可能であり、ネットワーク機器と同列にするのは無理がある。（システムが動かなくなる可能性がある。特に部門システム）
- サーバとネットワーク機器につては、VPNでクラウドのサーバと法人内施設にだけ接続しているが、リモート用回線が業者と接続されている。院内ネットワークに入るには、リモート用回線からしか接続できない為、まったく外部からの侵入は考えていない。その為、クライアントはバージョンアップを行っていない。今後はAIの利用を考えるのなら、インターネットに接続できる院内ネットワークが必要になるが、それによりセキュリティが下がる可能性がある。
- サーバと端末PCのパッチ適用には数多ある全システムベンダーによる医療情報システムの動作検証が必要であり、その都度適用する労力と費用を考えると、NDRやEDR等セキュリティ対策用のシステムで画一的に対策する方が現実的であると考える。
- システムの安定動作が担保されるか疑問
- システムの仕様上対応が難しいと言われるケースもある
- システムベンダーから自己責任で適用するように言われているため、医療機関として対応する時間が取れない
- システムベンダー側がオフラインだからという姿勢を崩さないため、実現ができない。適用したいと伝えても、対応したことがないとの回答になる。適用後の動作検証もベンダーでは行わないため、万が一不具合が出た場合に対応してもらえないので、医療機関側の判断だけで行うこともできない。セキュリティパッチだけではなく、バージョンアップも同じ理由で断られる。地方の病院では各々の部門で選択できるシステムベンダーが少ないため、対応ができないのであればシステムを導入しないといった強気の姿勢をとるのは難しい。医療機関にベンダーと協議するようにとの指導ではなく、ベンダーに直接指導を行っていただきたい。
- システムベンダー側で、構築時のOSの状態以外は動作保証しないという姿勢を改めてほしい
- システム停止を伴う作業のため、対応が難しい。
- システム導入契約時のパッチに合わせてベンダが設計構築を行っているため、稼働後のパッチ適用によって生じる不具合・障害が発生するリスクが高い。このような影響を受けない製品の販売開始が待たれるところ。
- セキュリティパッチの重要性や必要性は感じているが、適用後にシステム障害が発生する可能性を考えると適用に躊躇する。また、システムベンダーも適用前後の検証に前向きではなく、病院単独では実施できない。
- セキュリティパッチの対象（OS、アプリケーション、ファームウェア等）や、アプリケーションの動作に必要なソフトウェア（ミドルウェア等）の脆弱性を把握したうえで適切な対応ができていない。優先度が高いもの（例えばファイアウォール）については対応しているものの、それ以外の対応ができていない。SBOMも今後意識しなければならいと理解していますが、当院では今後、対象の洗い出しと、それにおけるリスク、さらに優先順位をまず整理する必要があると認識しています。限られた人的リソースで円滑にパッチ適用が運用できている医療機関を参考にできればと思います。
- セキュリティパッチの適用については、ベンダーに過去20年実施を求めているが、サーバについては検討するとの回答をベンダーが繰り返され適切な実施が遅延されている。
- セキュリティパッチの適用については、作業費用の負担を含め、機器の設置、システムを構築した事業者側の義務としてほしい。特に、PC端末については、複数の事業者のシステムが相乗りした状態で運用しているため、パッチ適用による動作保証ができないと回答する事業者が1つでもあるといつまでも適用できない状態が続くことになる
- セキュリティパッチの適用は必須であると考えるが、システム体制はパッチ適用を前提としていないため、不具合が発生した場合業務停止のリスクがある。ベンダー体制もこれまで閉鎖環境で、稼働率重視で環境を変えない事を前提として設計されているため、設計思想から変更する必要があるため、容易にセキュリティパッチ適用を行う事が難しい。また医療システムは高額である為、容易にシステム更新が出来ないため、EOLを迎えたシステムで稼働していたとしても更新が困難である為、これらの医療施設固有の問題を踏まえ、現実的なセキュリティ対策のガイドラインを示していただく（ネットワーク振る舞い検知型の対策）、セキュリティシステムを継続利用出来るための補助金などの制度を検討していただきたい
- セキュリティパッチの適用後、システムへの影響がどこまであるのか不明なため、テストや状況判断に多くの時間がかかる。
- セキュリティパッチの適用前の確認に時間を要するので、即時適用ができない。
- セキュリティパッチの必要性は感じているが、医療情報システムへの影響がわからないということで医療情報システムベンダーが対応していません。
- セキュリティパッチをあてていても侵入される可能性もあり、可用性の関係や費用を考慮すると非現実的な対策と考える
- セキュリティパッチをサーバや端末に適応させると、部門システムが動かなくなる。ただ、セキュリティ上不安がある
- セキュリティパッチを適用してもこれまでどおり正常に稼働するかの事前検証が難しい
- セキュリティパッチを適用の課題について、システムベンダー側がどう対応を進め取り組んでいるか見えません。状況を定期的に周知してもらえると良いです。
- セキュリティパッチを当てる事で不具合が起こった事もあり、判断が難しい。
- セキュリティパッチ適用はシステムベンダーの検証が済まないと対応できないと考えています。一部システムについては、最新パッチを当てて良いとしているベンダーがありできる範囲での対応を行っている。検証結果を得られないベンダーやベンダーに依頼する必要がある場合、高額になることから対応できていない部分がある。

【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-(7))】

セキュリティパッチに対する意見 (2)

- セキュリティパッチ適用義務を医療ベンダに国として義務化してほしい
- セキュリティパンチの適用意識がベンダーに欠けている。もっと指導して欲しい。
- セキュリティ上重大な問題がある場合のみ検証済みパッチのみ適用、普段のWindows Updateなどは当たっていない
- ゼロデイリスクは認識していうが、ネットワークなどをセキュリティアップにともなう不具合による、医療情報システムのエラー、不具合対応に不安がある。アップデートタイミングが難しい
- ソフトウェアとの親和性を確認してからの適用なので手間である。
- ソフト等の影響により更新が難しい場合が多々ある
- そもそもの設計に根本の問題がある限り、かけるコストに無駄が多すぎる。セキュリティbyデザインに移行することに、補助金を出し、旧式のデザイン哲学を変えるべき。
- どこまでのことを指すのかが不明。端末PCにファームウェアやWindowsUpdateは適用不可。セキュリティ対策ソフトは該当？
- なし
- パッケージ製品の動作保証（検証）をユーザー側では行えないため、本項を求められる場合は商法上の取扱いについて解決策を提示して欲しい。
- パッチの適用は医療機関側では対応できることではない。電子カルテ業者が不具合の可能性と言うことで対応してくれないため、事業者にパッチの適用を求めるべきである。
- パッチの動作確認には相当な時間と労力もしくは費用が必要となるが、それだけの人材の確保すること若しくは費用に対して理解は得られない。
- パッチの内容にもよる　重大なセキュリティホール等のケースは優先的に実施するが、軽微なもの、利用サービス対象外の機能であれば様子をみる場合もあるが、例えば電子カルテ端末等はメーカがアップデートは対応できないなど、その場合ハードウェア事更新が必要であったりするケースもあるが、一概にパッチを適応していないという文言だけの判断は危険と考えます
- パッチを当てただけで電子カルテがストップする可能性もあり実質適応不可能
- パッチを当てると電子カルテシステムが正常に動作しなくなる
- パッチ適用できるものは適用するようにしているが、ほとんどのシステムがパッチ適用での動作保証をしていないのでは？特にクローズド環境の電子カルテや部門システムについてはほぼ非対応と思われる。実環境と指針があっていないと感じる。
- パッチ適用によるシステムトラブル。ベンダーの保証が得られないため適用できない。
- パッチ適用による不具合リスクがある為、動作優先となる。
- パッチ適用の重要性は十分に理解しているが、1つの端末PCに多くのシステムが稼働しており、セキュリティパッチを適用するたびに各システムベンダーを招集し評価を実施するためには、かなりの費用や時間が必要となる点が一番の課題であると感じている。
- パッチ適用後に障害が発生した場合、問題の切り分け（復旧）対応に関する保証内容が明確になっていない
- パッチ等は安定稼働の問題上、適用が難しく当てていない。
- ベンダーから、セキュリティパッチを適用すると、業務システムの動作保証できないと言われている。
- ベンダーが指定したOSバージョンとは異なる環境下でのアプリケーションの不具合を懸念する
- ベンダーの保守料金内にセキュリティパッチの適用を含めて欲しい
- ベンダーやソフトウェアメーカーの対応が遅い。
- ベンダ側の動作検証がとられていないため、最新に上げることができない。また、作業費用が保守費用以外に発生し病院経営を圧迫してしまう。
- メーカーが動作保証を行えない以上、病院の独断でセキュリティパッチを適用させて、別のリスクを発生させる訳にはいかない。
- リスクや作業量を考慮すると中小病院では外注せざるを得ないが、費用がない。
- 医療機関としては適用していきたいが、電子カルテなどの基幹システムの挙動に影響があると業務に支障をきたすので、医療機関の判断だけでは適用ができない。ベンダー側は動作保証ができないと適用に難色を示すことがある。さらに端末に部門ベンダーのシステムが相乗りしていると全てのベンダーのシステムで動作保証ができない。
- 医療機関は、診療機能を維持し、恒常的に提供できる体制を保つことが主目的であり、セキュリティを向上することはそのための手段に過ぎない。一方、電子カルテベンダは医療機関が診療機能を維持し、恒常的に診療を提供できる体制を保てるように補助することがベンダが果たすべき役割であり、本来であれば、ベンダ側の責任の下、セキュリティパッチ適用後の電子カルテシステム等の動作検証の実施と、セキュリティパッチの適用を担うべきである。特にサーバに関しては、セキュリティパッチ適用によるアプリケーションへの影響を推し量ることは病院の担当者では不可能であり、開発元が責任を以て検証をし、医療機関へ対応すべきである。
- 医療機器は　医療機関の判断で　セキュリティパッチを当てることができない。メーカーマターとなる。
- 医療系のシステムはオフラインの運用が主流であるため、オフラインセキュリティパッチに対応しているシステム業者がそもそも少ない。
- 医療情報システムは、保守用回線以外の外部ネットワークに接続していないクローズドな環境であることが多く、また、稼働中のシステムへの影響も懸念されるため、セキュリティパッチの適用は難しい。そのため、インターネットからの分離と外部記憶媒体の接続制限による代替対応が現実的だと考える。その場合、保守用回線のVPN装置等のファームウェアアップデートが重要になるが、現状、医療機関側からベンダーに確認しないと対応が進まない。保守用回線を導入する場合、医療機関とベンダーの双方が互いに確認し合うような仕組み作りが必要と考える。
- 医療情報システム事業者への義務化が必要です。パッチを適用する場合、適用に要する費用及びシステム不具合が出た場合の費用は医療機関負担となるうえ、不具合の責任は負いませんがそれでも実施しますか？と言われるケースが大多数であり、実質的にセキュリティパッチが適用できません。
- 一部システムや保守事業者では、セキュリティパッチの適応自体が不可能との回答を行う場合があり、実際セキュリティパッチの適用によりシステム障害となることもあるため、セキュリティホールをそのままにして利用を継続しなければならない事態となることがあり、悩ましい。
- 一部はできているが、基幹システムに関しては、パッチ適用後の不具合リスクが大きいため、セキュリティ対策ソフトでカバーしているものもある
- 院内の電子カルテネットワークは完全にイントラネットとなっており、クライアントにはセキュリティパッチを適用していない。
- 開発環境がない施設は、テストが出来ないためアプリケーション動作リスクが伴う可能性がある
- 外部との接続は専用回線で行っており、その他は外部接続は物理的に不可能である
- 各システムの動作検証および、適用するにあたり病院業務の停止が発生する
- 各システムベンダーは、ソフトウェアの動作保証を持ち出してセキュリティパッチの適用に消極的だが、それはベンダーの技術力不足・怠慢だと考えます。
- 各システムメーカーが前提としていないので、大変難しいです。
- 基幹の電子カルテシステムに関わらず、システムにより何かしら業務停止を伴うため、以前より現場の拒否感が強い。
- 規模の小さいベンダーのソフトウェアの製品において、セキュリティパッチの適応に対応していない、または対応に時間がかかることがあり、別途費用が発生する。随時セキュリティパッチが適用できない大きな要因となっている。
- 業務システムにおいては動作検証が必要で難しい部分がある
- 原則閉域網であるHIS系機器へセキュリティパッチやOS等の更新の必要性と仮に行った場合の各種システム正常動作とのリスクが計れない。
- 現実的にすべての機器を対象にパッチ適用することは不可だと考えております。レガシーOSで動かす必要がある端末がぞんざい下り、多々ある種類の機器類の知識を得て判断することは厳しいと思います。
- 古い部門サーバーは移行もできていないため、OSのサポートが切れている。データ移行の費用もねん出できない。
- 互換性の問題で常時最新にはできない。セキュリティパッチを最新にすることを病院に強要するより、ベンダーにセキュリティパッチが最新にできない医療情報システム製品を販売することを禁じてほしい。最低でも追加費用なしで8年間の最新のセキュリティパッチ更新、OSの更新への対応ができることを前提とした厚労省の認定制で販売してほしい。
- 国側で各ベンダーに適用像できるように指示が必要
- 最低限の備えとしてセキュリティパッチは重要と認識しているが、これまでの無事故を理由に対応をしないという方針が事業者から示されています。対象システムはオンプレミスで、約6年間パッチ更新が行われていないレガシーシステムであり、事業者からは技術的、または人員的な理由で現在の状態からのセキュリティパッチ対応は不可能との回答を得ています。事業者から代替案としてセキュリティソフトの配布サーバ新設が提案されました。しかし、この提案はOSの脆弱性を突く攻撃に対する根本的な対策ではなく、単なるアンチウイルス対策に留まるため、根本的な回避策になっていないと回答しました。この対応不可能な状態は、サイバー攻撃に対する重大な脆弱性を継続的に放置していることであり、事業継続性に関わる深刻なリスクとして認識しています。
- 作業費用およびリスクがおおきいため、サーバ、端末など全ての機器に適用するのは困難最低限対応すべきパッチの内容、および対象などの指針を出してほしい
- 事業者からは、「影響が不明であるため適用できない」「適用には高額な検証費用が必要となる」といった回答があります。さらに、いまだに「外部と接続していないため不要と考える」という事業者も存在します。このような状況から、医療機関が単独で対応を進めることは困難。国として事業者対応の実施を働きかけるとともに、必要となる費用の支援をご検討いただきたい。
- 次期システム2029年1月予定で対応
- 次期システム更新時に要件としてパッチ適応を要求していく
- 次年にはベンダー主導にてパッチ適応が行える環境に移行予定
- 手動アップデートは可能であるため、検討中
- 重要性は理解しているが費用が高額であり、連携システムとの兼ね合いで全てに適用するのは難しい。
- 重要度の高い、緊急度が高い項目については、セキュリティパッチの適用を行うよう対応している。しかし、システム停止が伴うため、救外など確認を行い、夜間に対応することになる。
- 助成金が欲しい（適応範囲の拡充、増額）

【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))】

セキュリティパッチに対する意見 (3)

- 上記の理由により当院ではパッチ適用を実施していないが、実際にやっている病院があればどのように実施しているかご教示いただけますと幸いです。
- 常に最新のセキュリティパッチを適用するには、相当高額な費用と適用前のテストなどの準備が必要となり、対応したくても現実的に難しい現状がある。
- 情報管理部門としては必要性を理解しているが、病院管理者が不同意。
- 新たな脆弱性は増加の一途、本来は迅速に適用すべきだが、検証・費用がかかるため、必ずしも迅速に適用できていません。また、ベンダによってはセキュリティ対策に前向きでないケースも散見されます。公的な機関から、実運用が可能なレベルでの必須度や緊急度のガイドライン提示や、ベンダへの対応必須化を指導していただけることを希望します。
- 診療報酬や補助金等による十分な補填がなければ実施困難である。
- 数百のサーバ及び百数十のシステム（オンプレ、Saas含む）に対し、まずパッチの対象かどうか、各ベンダに適用の可否を確認、そして適用作業立会いと適用後の変更・構成管理のサイクルを最低でも月1で行うことは、SBOMを使用しても情報システム部門のマンパワーが足りず難しいと苦慮している。またパッチ当てを行うことを保守契約に追加する、もしくはスポットで依頼すると大幅に費用増となるため、予算計上が難しくなる
- 素人なのでセキュリティパッチを適用して不具合が起こった場合、元に戻す手立てがわからない。
- 多種多様な構成のシステムを運用しており、セキュリティパッチの適応でシステム自体の動作に影響が発生する場合がある。もちろん可能なものは最新のパッチを適応しているが一律に最新のパッチを適応するにはならない。
- 端末・サーバへのセキュリティパッチは動作不良を起こす可能性があるので、全国的な課題であると考えます。
- 端末PCについて、Windowsの最新のセキュリティパッチの適用が場合によって使用している電子カルテ等の互換性の確認がされておらず不具合が発生する場合があり業者に確認を要する。また、イントラ環境下の端末PCについて自動的に最新のパッチ適用ができず現実的に対応はできていない。（現状実施する場合は、1台ずつインターネットに接続して適応を繰り返すことになる）
- 適用するには、メーカーによる影響調査及び作業（有償）が発生するため、金額的に難しい
- 適用による動作保証が取れず、ほぼ適用できない状況です。大きな障害になる事が予想される不具合に対するパッチのみ適用しています。
- 適用による不具合が懸念される
- 電子カルテシステムのクライアント端末などの複数台に対して、適用することは難しいと考えております。
- 電子カルテなどのソフトウェアとの競合を理由になかなか更新を行えない状況
- 電子カルテベンダーがwindowsのパッチに対応するのが遅い（国内ベンダーに検証する要員が少ない）
- 電子カルテベンダーより、最新パッチを適用した場合にソフトウェアが動かなくなるとの連絡があるため。またバンドル版OSなどの場合、オフラインでの最新パッチの適用が非常に手間である。WSUSも検討したが、費用がかかる。各端末に直接インストールは現実的ではない。よい手段があれば開示してほしい。
- 電子カルテベンダより対応不可と言及
- 電子カルテ関連のサーバーや端末について、当院は電子カルテでは富士通製を利用しており、その他の部門システムと連携していますがセキュリティパッチの適用は、現行の電子カルテシステムとの互換性に関わるため、富士通や部門システムベンダーの専任事項になっています。そのため、一般に公開されたタイミングでのセキュリティパッチ適用ができない状況です。電子カルテや部門システムベンダーには一般に公開されたタイミングになるべく合わせてセキュリティパッチの検証を実施し、病院側でパッチ適用ができるように運用していただきたい。
- 電子カルテ端末だけでも、複数のシステムが相乗りしており動作検証などの作業負荷や費用面の負担が大きいと感じる。医療機器等を含めてすべからずと言われると、現実的にはかなり厳しいイメージ。医療機器業者からは薬機法のため適用不可と言われることが多い。
- 電子カルテ端末のパッチ適用は理解できますが、これが医療機器も情報端末の一部と規定された場合、医療機器ということもあり不具合が出る可能性があるので対応が難しいです。
- 当院ではまず電子カルテベンダーが対応しないため、施設内でパッチ適用を試みたが動作不良が発生したりと継続できない状況また、たとえ電子カルテベンダーが対応したとしても相乗りの部門ベンダーが対応しなければ意味がないすべてのベンダーがセキュリティ対策への共通認識を持ってほしい
- 当院としてはWindowsUpdateの最新化は必要性を感じているが、システムベンダーのポリシーとして対応が難しい。最新化後の都度のシステム健全性の確認など
- 当院と契約がある業者は、必要がある場合に業者で自動適用(契約内)してくれるか、必要な場合には有償で対応となる場合が多い。最新版のセキュリティパッチを常に適用するのが望ましいのは理解できるが、ソフトの動作や機器の動作といった面、費用面でとても現実的でない。
- 当院のネットワーク構成と業務への影響を鑑み、一般的な緊急性とコスト（発生時）を統合的に判断が必要。
- 動きがおかしくなることがあり　パッチは当てていない　逆にウイルスが入らないように努力している
- 動作の保証ができないといって、特に部門ベンダが積極的にWindowsUpdateをやりたがらない。チェックリストに記載があるのならば、厚生省からベンダに積極的に働きかけるべきである。
- 動作保証されるもの、ベンダーより情報があったものは適応する。また、FWのパッチは全て当てているが、スイッチ類はメモリーリークなど大きな障害になるもの以外は適応していません。
- 導入されている全システムでの検証が必要であり、費用もかかるが、多くのベンダーが対応してくれない。現時点では、非現実的と感ぜらるる。
- 特になし
- 特に端末に関しては電子カルテの動作安定性を優先する関係上、一律でのパッチ適用は困難であり、業者からも推奨はされていないため、中々実施できない。
- 年に1回程度のパッチ適用を行っているが、本来は月1回程度は実施すべき。しかしパッチ適用による運用アプリへの影響を考慮すると現実は年2回程度と考える。運用には専従の院内システム担当者または、保守業者との契約が必要と考えるが、現実的には予算確保が難しい。
- 費用、人的に公的な支援が不可欠である
- 非常にコストがかかり厳しい
- 病院側も最新のセキュリティパッチの内容を把握する努力が必要
- 富士通の電子カルテは、OSのパッチをあてると、動作しなくなり、その都度動作確認と改修が必要になる。時間と費用が必要になる。
- 部門システムでIE11を使用している。実施出来たとしても全サーバ・端末へ対応は台数が多いため、コスト（費用と時間）が確保できるか不明
- 部門システム等の仕様によりパッチ適用ができないケースがある。
- 複数のシステム会社のアプリケーションが混在する医療システムPCにおいて、常にOSの最新セキュリティパッチを適用していくことはシステム動作保証の観点から非現実的であると思われます。つまりは最新のOSバージョンもリリースの度に不具合が発生しており、さらにOSバージョンアップリリースの度にその動作検証を10数社ある相乗りアプリケーションのすべてを動作検証することは現状の保守契約では実現不可であり保守契約費用の高騰が考えられ、費用面から病院システム運用継続も難しくなることが想定されます。 ガイダンスにあるとおり常に最新のOS環境で運用している病院情報システムが存在するでしょうか？存在するのであればモデルケースとして是非公開して頂きたいと思います。
- 閉じているから大丈夫の神話が長引いたため、セキュリティパッチを当てて最新化するという文化がなく、パッチを当てたことによるシステムへの影響が予測・対応する体制がとられていないためベンダーの担当者自体を、医療の世界以外のインターネット接続当たり前の世界を担当していたSEなどに切り替えないと、変わっていけないと思います。
- 閉域で運用中の電子カルテサーバ、端末へのセキュリティパッチ適用は、システム不具合発生リスク、作業コスト等を考慮してあまり現実的ではない。
- 閉域網でのセキュリティパッチを充てる必要があるかどうか。また、それにかかる費用は誰が負担するか？
- 閉域網での運用でセキュリティパッチの適用に関して重要性を低くとらえる文化が医療機関・ベンダー双方にあり、ガイドライン改定後もそれに関する提案などは少なく、機運が盛り上がらないでいる。最低限行うべきラインについて、具体的な製品名と標準的な設定などで示された方が上層部には理解しやすく、導入の判断を促すために、それに対する公的な助成が行われることが望ましい。
- 閉域網の医療情報システム端末について、保守業者にセキュリティパッチを適用したいと提案すると、「動作保証対象外」、「保守対象外」、「保守費とは別に作業費とさらなる保守費の上乗せ」と回答されます。中小規模病院では大規模病院と比較し、①立場が弱く強く出れない（保守業者に撤退されたりするとシステム更新時等に更新希望業者不在となるリスク）のと②経営が厳しいため追加費用の捻出が難しいという現実的な問題があります。セキュリティパッチ適用後の動作保証等は他業界では当たり前に行われており、特に医療関係の業者はセキュリティパッチ適用という現代の常識が無いように感じています。国や都道府県より、医療システム業者やメーカに対し強く、ユーザ側に対し追加費用が生じることなくセキュリティパッチ適用することを業界標準としてできるよう動いてもらいたいです。
- 保守業者が行わず院内システム管理者が適応を行っている。
- 保守契約にパッチ適用が含まれないので、都度予算調整が必要になる。このため、予算面から不可になるケースや速やかな対応が困難であるケースがある。また、業務システムへの影響が不透明であり、業務影響への懸念からパッチ適用が難しい。管理部署が異なる機器への統制が困難である。
- 保守事業者ごとに保守範囲が異なるため、択一式のアンケートでは回答が難しい。
- 本当に必要なパッチは適用する必要があると感じているが、動作保証や作業時間の確保などで対応することは難しい。
- 問39、自院で対応している。
- 問41に回答選択を追加していただきたいです。医療機関側で実施するため費用なし。

【接続元制限を実施している。(2-(8))】

ネットワーク機器の接続元制限の実施		
	施設数	割合
はい	439	79.8%
いいえ	111	20.2%

ネットワーク機器の接続元の管理設定と監視	管理設定		監視	
	施設数	割合	施設数	割合
病院	61	13.9%	81	18.5%
病院とネットワーク事業者が協力して	252	57.4%	182	41.5%
ネットワーク事業者に任せている	114	26.0%	152	34.6%
その他	12	2.7%	24	5.5%

管理設定(その他)
- システムベンダー
- ネットワーク事業者とシステムベンダー
- メーカー
- 機器による。運用委託事業者等。低機能のハブは制限していない。
- 上部組織(機構本部)
- 中央組織の職員
- 同一法人の中央組織および病院
- 保守事業者
- 保守用回線を導入しているシステムベンダー
- 本庁とネットワーク事業者に任せている
- 本部
- 本部中央管理

監視(その他)
- インターネットからのアクセスはすべて認めず、必要なメンテナンス回線は閉域網に限定している。
- システムベンダー
- ネットワーク事業者とシステムベンダー
- メーカー
- 監視していない
- 監視はしていない
- 監視はそれぞれの事業者任せ
- 監視は出来ていない
- 監視までにはいたっていない
- 期限を設けているため監視していない
- 機器による。運用委託事業者等。低機能のハブは制限していない。
- 上部組織(機構本部)
- 常時はネットワーク事業者に任せ、任意タイミングで病院が接続実績のみ確認。
- 常時監視はしていない
- 常時監視は行っていない
- 全てのネットワークの監視を実施できてはいない。
- 中央組織の職員
- 同一法人の中央組織および病院
- 病院でやれと言われたが、方法は提示されなかった。
- 保守事業者
- 保守用回線を導入しているシステムベンダー
- 本部
- 本部中央管理

【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))】

バックグランドで動作している不要なソフトウェア及びサービスの停止	サーバ		端末PC	
	施設数	割合	施設数	割合
はい(定期的に確認している)	75	13.6%	78	14.2%
はい(システム導入時に確認したのみ)	420	76.4%	411	74.7%
いいえ	55	10.0%	61	11.1%

端末PCにエンドユーザが希望するソフトウェアをインストールすることが可能ですか。	施設数	割合
ソフトウェアを端末PCにインストールすることは、システム設定で禁止している。 エンドユーザの希望による端末インストールは行わない	126	22.9%
ソフトウェアを端末PCにインストールすることは、システム設定で禁止している。 ソフトウェアのインストールを病院に申請し、許可を受けたソフトウェアのみシステム管理者がインストールを行う	243	44.2%
ソフトウェアを端末PCにインストールすることは、運用で禁止している(システム設定で制限はかけていない)。 エンドユーザの希望による端末インストールは行わない	38	6.9%
ソフトウェアを端末PCにインストールすることは、運用で禁止している(システム設定で制限はかけていない)。 ソフトウェアのインストールを病院に申請し、許可を受けたソフトウェアのみシステム管理者がインストールを行う	93	16.9%
ソフトウェアを端末PCにインストールすることは、運用で禁止している(システム設定で制限はかけていない)。 ソフトウェアのインストールを病院に申請し、許可を受けたソフトウェアのみエンドユーザがインストールを行う	31	5.6%
エンドユーザが自由にソフトウェアを端末PCにインストールできる	19	3.5%

バックグラ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ない理由

- Word、Excel、Acrobat等、業務に必要であるため。
- カルテ端末はカルテ以外にもシステムが相乗りしているため、判断が難しい。
- ゲームソフト以外のソフトウェアに関して、バックグランドでどのように動作しているかわからないため削除後の不具合も考え削除していない。
- コスト
- これまで医療情報システムの管理は主に病院(医事課)が行っており、設問にある不要なものを停止するという知識が無かった。
- サーバーのインストールはシステム業者に一任のため、こちらではインストールされているアプリに関与していない。
- サーバや端末のすべてのソフトウェア、サービスを把握しないと不要なものの判断がつかないと思いますが、一般的なOSが動作している端末のサービスは約200ぐらい項目があり、実行中のサービスは40程度はあると思いますがそのすべてを把握することが困難で、その為不要と判断することができないサービスは停止できないと回答せざるをえないと思うのですが、本件はもっとアバウトに考えてもよいのでしょうか？
- サーバを職員が常に監視しておらず、定期的に確認を行ったとしても不要なソフトウェアかどうかの判断が難しい。
- サービス停止の影響を把握出来ない、また、サービス停止の方法が複雑なため、職員が対応できない。
- システム導入時の役務に含まれていなかった。慣例的に明らかに不要なソフトウェアやサービスの一部を停止している。
- バックグラウンド動作している不要なソフトウェアの判断が病院職員では難しいため。
- バックグランドで動作している不要なソフトウェア及びサービスが何か判断できない
- ベンダーがサーバーについては対応してもらえない
- ベンダーによる動作確認作業が必要な為
- ベンダーに任せているため
- ベンダー自身が不要なサービスを把握できていない。
- メーカー製PCを端末として使っているならば、不必要なソフトウェアとサービスは外しているつもりでも、OSとドライバーだけがインストールされた製品はないので、全てのソフトとサービスを把握ができるわけがなく、バックグランドで動作しているものすべてが止められるわけもなく、不要かどうかがわかるわけがないので。不要なソフトとサービスをすべて止めることができたと思っているのがおかしいと思う。
- 意図していない不要なソフトを検知するためにセキュリティーソフトを導入している。
- 一部完全に不要なサービスは止めているが、全て止めているわけではないため、いいえとしている。
- 何が不要かわからない。
- 何が不要なソフトウェアか判断がつかない為。
- 稼働時よりインターネトに接続している端末はなく、USBも院内で1台のみ接続が可能で、その端末を管理している者の許可が必要で、ウィルスチェック後に接続ができるようになる為。
- 各システム、各ベンダーでの対応が異なるため。
- 管理コスト、工数不足
- 管理端末数が600台強あり、全端末の管理は出来ない
- 基本的に必要なものしかインストールしていない理解であり、バックグラウンドで意図しないソフトウェアおよびサービスは動いていない認識である。さらに、ポート制限を徹底して行っており、意図しないバックグラウンドのソフトウェア、サービスがあってもネットワーク越しの通信自体ができないようにしているから。
- 機器による。特に医療機器は製造販売事業者からの情報開示がほぼ無い。
- 手が回らない。スキル不足。
- 専門知識が無い為、そういう確認作業に困難がある
- 全ての端末で不要なソフトの有無などを確認しきれていないため
- 全ての不要なサービスを停止しているかの確認はできていません。具体的に不要であれば起動していないことが望ましいプロセスを提示して頂けると、それに沿った確認は可能かと思います。
- 対応する知識を有していないから
- 端末においては、複数メーカーソフトが相乗りしており、停止することでの影響を考慮し、ベンダーと必要に応じて調整することとしているため。
- 端末一台一台把握することが難しいため
- 知識、技術不足
- 知識を持つ職員が少なく、体系的な管理ができていない
- 導入当時にシステムベンダにて不要と判断されたサービスは停止しているが、システム導入から7年経過し見直す必要性があると思うが人的リソースが足りず実施できていない。
- 必要な知識を有していない
- 必要性が不明
- 不要なソフトウェア、不要なサービスを調べる手間がかかる。停止した場合の動作トラブルの懸念。
- 不要なソフトウエア・サービスの判断がつかない
- 不要なソフトウェアかどうかの判断がつかない
- 不要なソフトウェアをインストールしていない。また確認できる人数も少ないため確認が出来ない。
- 不要なソフトウェア及びサービスの利用は停止している
- 不要なソフトウェア及びサービスを導入していないため
- 不要なソフトウェア及びサービスを把握していない。
- 不要なソフトの定義が曖昧でベンダーの理解が得られない。ベンダーですらOS標準は全て必要なソフトだと思っている。
- 不要なものがない
- 不要の判断がつかないため
- 複数のベンダがあり、電子カルテのサーバや端末PCは導入初期や定期的に対応できているが、一部のベンダが対応できていない。対応できていない理由は、作業分担面や費用面などの調整ができなかったため。
- 明らかに不要なものは停止しているが、何が不要なものか判断できないものもあるため100%停止しているかどうか判断がつかない

【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)】

機器に対するパスワード管理	サーバ		端末PC		ネットワーク	
	施設数	割合	施設数	割合	施設数	割合
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	135	24.5%	65	11.8%	128	23.3%
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	155	35.3%	257	58.5%	155	35.3%
左記を実現できていない	260	59.2%	228	51.9%	267	60.8%

サーバ室の入退室管理	施設数	割合
用紙記録による入退室者の把握	305	55.5%
防犯カメラのよる監視		
出入口付近	111	20.2%
サーバ室内	66	12.0%
物理鍵による入退室管理		
貸出記録を保管	121	22.0%
貸出記録の保管は行わない	150	27.3%
知識認証(IDとパスワードなど)による入退室管理		
入退室者の記録が残る	16	2.9%
入退室者の記録は残らない	29	5.3%
物理認証(カード認証など)による入退室管理		
入退室者の記録が残る	128	23.3%
入退室者の記録が残らない	16	2.9%
生体認証(指紋認証、静脈認証、顔認証など)による入退室管理		
入退室者の記録が残る	33	6.0%
入退室者の記録が残らない	1	0.2%
サーバ室は設置していない	34	6.2%

サーバに対する二要素認証の有無	施設数	割合	施設数	割合
一要素認証である	465	84.5%	465	84.5%
二要素認証(物理認証あるいは生体認証によるサーバ室への入退室管理とサーバに対する一要素(パスワード)認証)			70	12.7%
リモート接続では一要素認証となっている	55	10.0%		
リモート接続でも二要素認証を実現している	15	2.7%		
サーバに対する二要素認証を実装している			9	1.6%
リモート接続では一要素認証となっている	5	0.9%		
リモート接続でも二要素認証を実現し	3	0.5%		
その他	7	1.3%	7	1.3%

サーバの二要素認証の実現	施設数	割合
必ず実装する	20	4.3%
実装を検討中		
実装の可能性が高い	143	30.8%
実装の可能性が低い	229	49.2%
実装を行わない	73	15.7%

サーバに対する二要素認証の実装を行わない理由

- 今までコストが発生していないものなので事務長等の上司への理解が非常に難しい。
- IT知識不足のため
- オフライン運用なので
- ガイドライン上二要素認証の適用範囲が不明瞭であり、サーバ群まで適用が必要か不明のため
- クラウド型の電子カルテへ更改する予定のため。
- コスト
- コストが高いため
- コストを抽出できない。病院建て替え時にしか検討できない
- サーバOSに対するログインに二要素認証が義務付けられると考えていなかった
- サーバー室内に設置しているため。
- サーバに接続できるIPアドレスを制限することでサーバのセキュリティを強化する方向である。
- サーバ設置場所が施錠された室内であり操作者が限定されるため
- システムが未対応
- システムの更新時に2要素認証を検討する予定
- システムベンダーに現在のところその機能が無い
- システムベンダより推奨提案を受けていない為
- システム更新の予定がない
- システム導入にコストがかかるため
- そもそも金銭コスト・人的コスト上オンプレミスを持つべきではなく、Saasへの積極的移行とオンプレミスの廃止を目標と考えるため
- どのように実施するか実現方法なども特に検討していないため。
- ベンダーからの提案もなく、独自に価格を調べたが、高額であり実現不可能
- ベンダーが対応できない
- ベンダーとは話題になっていない(クライアント側はある)
- ベンダーメンテナンス上の問題。
- まだ検討していない。
- リモート保守時に対応ができないため
- リモート保守時に対応できないため
- 医療システム更新を令和10年度に予定しているため。
- 医療情報システム完治部門のみメンテナンス等で対応する運用のため
- 運用上の問題が懸念される事や、改修費用の負担が大きいため。
- 各種システムサーバーは、原則、保守業者のみの取り扱いのため
- 管理者として導入するメリットがない
- 関連費用の捻出
- 業務の煩雑化にしかならない。医療システム全体が多岐に渡ることに対して、管理をミクロ化しすぎることは望ましくない。
- 経営層からの承認がおりない。費用がない。
- 警備されているサーバー室内で、施錠されているサーバーラックに設置されているため。
- 現在更新の予定がない為。
- 現時点では対応検討の話もでていない
- 現時点では対応検討の話も出ていない
- 現時点で検討していなかったため、メーカーに対しても確認していないため。
- 現実的でない費用
- 後付けで設定するのは費用が高く、院内の理解が得られない。また、サーバごとにベンダーが異なるので実装方法にも違いが出て管理も困難。
- 構築ベンダーとも検討しておりますが、具体的な解決にまで至っておりません。
- 今年サーバーを入れ替えたばかりで早期実装は難しい
- 次期サーバ更新時に対応予定
- 次期システム2029年1月対応
- 設問34のとおり、サーバは管理者権限の使いまわしを行っており、現状では二要素認証の実装が不可能であるため。
- 対応の煩雑さと費用的な理由になります
- 費用がかかる、またシステム更新が近くなるので余分な出費となる
- 費用的な問題と、システムベンダーが対応不可(更新が必要)という理由※稼働済システムは努力義務と言う認識です
- 費用捻出が難しい
- 費用の面から実装を行わない。令和11年度に 医療情報システムの更改を行うときに導入する予定である。
- 必要な知識を有していないから
- 必要性を感じないため
- 病院情報管理システムの次回更新(令和12年1月)に併せ実装予定のため
- 物理的手段(鍵・入室許可)を講じている。論理的には令和7年度中に接続デバイスが実装予定。
- 毎年の予算申請に導入申請をしても通らず、却下される為
- 予算がないため
- 予算が出ない
- 令和10年度に医療情報システムを更新予定であるため
- 令和8年3月末にて閉院のため
- 令和9年度までに対応は事業者が不可能と回答

【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)】

端末PCに対する二要素認証の有無	施設数	割合
一要素認証である	449	81.6%
端末PCは二要素認証を導入しているが、医療情報システムネットワークに接続する部門システム端末(ワークステーション等)は一要素認証の端末がある	62	11.3%
医療情報システムに接続する端末は全て二要素認証を導入している	20	3.6%
その他	19	3.5%

端末PCの二要素認証の実現	施設数	割合
必ず実装する	67	14.9%
実装を検討中		
実装の可能性が高い	172	38.3%
実装の可能性が低い	165	36.7%
実装を行わない	45	10.0%

ネットワーク機器に対する二要素認証	施設数	割合	施設数	割合
一要素認証である	483	87.8%	483	87.8%
二要素認証(物理認証あるいは生体認証によるサーバ室等への入退室管理とネットワーク機器に対するパスワード認証)			48	8.7%
リモート接続では一要素認証となっている	37	6.7%		
リモート接続でも二要素認証を実現している	11	2.0%		
ネットワーク機器に対する二要素認証を実装している			8	1.5%
リモート接続では一要素認証となっている	2	0.4%		
リモート接続でも二要素認証を実現している	6	1.1%		
その他	11	2.0%	11	2.0%

ネットワーク機器の二要素認証の実現	施設数	割合
必ず実装する	10	2.1%
実装を検討中		
実装の可能性が高い	110	22.8%
実装の可能性が低い	266	55.1%
実装を行わない	97	20.1%

二要素認証を実装しない理由

端末PC

- アプリケーションで二要素認証を実装しているため
- オフライン運用なので
- コスト
- システムで二要素認証を実装する為。
- システムベンダーに現在のところその機能が無い
- システム更新の予定がない
- システム導入にコストがかかるため
- どのように実施するか実現方法なども特に検討していないため。
- 医療システム更新を令和10年度に予定しているため。
- 運用上の問題が懸念される事や、改修費用の負担が大きいため。
- 運用上の理由から現時点では検討していない。
- 外部への接続が不能であること。パスワードを半年ごとに変更していること
- 看護業務に差し支える
- 関連費用の捻出
- 業務効率の低下とコスト増
- 経営層からの承認がおりない。費用がない。
- 現時点で検討していなかったため
- 現実的でない費用
- 個々に任せているため
- 今までコストが発生していないものなので事務長等の上司への理解が非常に難しい。
- 次期システム2029年1月対応
- 実装を検討したが予算の都合により対象をアプリケーションのログイン時とした。
- 対応の煩雑さと費用的な理由になります
- 端末PCのログインユーザは共通としているため、ソフト側での二要素認証対応を予定している。
- 費用
- 費用がかかる、またシステム更新が近くなるので余分な出費となる
- 費用的な問題と、システムベンダーが対応不可(更新が必要)という理由※稼働済システムは努力義務と言う認識です
- 費用捻出が難しい
- 費用面
- 費用の面から実装を行わない。令和11年度に 医療情報システムの更改を行うときに導入する予定である。
- 必要な知識を有していないから
- 不便
- 不要。
- 本庁担当職員とベンダーとの協議等で必要な場合に取り入れると思われるが、現時点では計画の予定がないため
- 毎年の予算申請に導入申請をしても通らず、却下される為
- 予算がないため
- 予算が出ない
- 令和10年度に医療情報システムを更新予定であるため
- 令和8年3月末にて閉院のため

ネットワーク機器

- DHCPでなく、固定IPを使用。また、WI-FIはステルス型で認証を必要とし、システム管理者以外の接続が難しいと考えるため。
- ID/パスワードの2段階認証を実装できているため
- IT知識不足のため
- ガイドライン上二要素認証の適用範囲が不明瞭であり、NW機器まで適用が必要か不明のため
- コスト
- コスト。
- コストがかかりすぎる
- コストが高くなるため
- コストの関係
- コストの捻出が難しい
- サーバ・端末PCについては前述の通りだが、ネットワーク機器については二要素認証を考えていなかった為
- サーバーと同じ理由です。
- サーバー同様
- システムの複雑化
- システムベンダによる設定情報がないとログイン不可のため
- システム導入にコストがかかるため
- どのように実施するか実現方法なども特に検討していないため。
- ネットワーク機器が二要素認証に対応しておらず、改修費用の負担が大きいため。
- ネットワーク機器が二要素認証未対応
- ネットワーク機器についての二要素認証はガイドラインで定められていないため。
- ネットワーク機器にも二要素認証が必要との情報を知らなかったため
- ネットワーク機器に対して要件がないため
- ネットワーク機器に対する二要素認証の必要性を把握していませんでした。
- ネットワーク機器に二要素認証が義務付けられると考えていなかった
- ネットワーク機器の管理がベンダーの提示したものをそのまま利用している為
- ネットワーク機器の管理を保守業者に委託しているため
- ネットワーク機器は関係者しか扱うことができないため。
- ベンダーからの提案もなく、独自に価格を調べたが、高額であり実現不可能
- ベンダーで対応できない
- ベンダーとは話題になっていない
- ベンダーメンテナンス上の問題。
- ベンダー等保守業者のみの取り扱いのため
- 医療システム更新を令和10年度に予定しているため。
- 医療情報システム管理部門のみメンテナンス等対応する運用のため
- 一般職員が操作できる場所にない為、1要素認証で充分と考えている
- 一般的なネットワーク機器における二要素認証は、Azureなどの外部認証サーバを使用した二要素認証であることが多く、これが医療情報システムの安全管理に関するガイドラインに準拠しているか不明であることと、通常は外部との通信を遮断していることから外部認証事体も使用が困難であることが理由となります。
- 該当機器なし
- 管理機能に接続できるIPアドレスを制限することでセキュリティを強化する方向である。
- 管理者として導入するメリットがない
- 関連費用の捻出
- 機器が機能を実装していない。
- 機器が対応していない
- 機器が対応できない
- 機器更新の予定がない
- 機器仕様上二要素認証に対応できるとは限らず、現在採用している機器では二要素認証が導入不可。機器更新が発生する際は再検討とする。
- 機器上実装が困難
- 業者が対応していない。また出来るようになっても更新時しか検討できない
- 経営層からの承認がおりない。費用がない。
- 現時点では対応検討の話もでていない
- 現時点では対応検討の話も出ていない
- 構築ベンダーとも検討しておりますが、具体的な解決にまで至っておりません。
- 今までコストが発生していないものなので事務長等の上司への理解が非常に難しい。
- 今後検討は行うが、令和9年度までの実装は未定。
- 施錠されているシャフト内で、施錠されているHUB BOXに設置しているため。
- 次期システム2029年1月対応
- 次期ネトワーク更新時に検討する。
- 実装方法を把握できていないため、また各機器において個別に設定することは現実的に不可と思われるため
- 接続する管理コンソールで実施を検討
- 対応していない機器を導入している
- 対応の煩雑さと費用的な理由になります
- 対応機器を導入していない。
- 導入費用が捻出できない
- 二要素認証がないため
- 二要素方法がないため
- 費用
- 費用捻出が難しい・実現自体が難しい
- 費用の面から実装を行わない。令和11年度に 医療情報システムの更改を行うときに導入する予定である。
- 必要な知識を有していないから
- 必要性を感じていないため
- 必要性を感じない
- 必要性を感じないため
- 不要。
- 物理的手段(鍵・入室許可)を講じている。論理的には令和7年度中に接続デバイスが実装予定。
- 無理なので。ネットワーク機器がサーバー室だけにあるわけがないし、設置した箇所全部を2要素認証にするほどの予算が出るわけがない。
- 予算がないため
- 予算が出ない
- 予算都合があわない。サーバー機のため、設置は保守ベンダーとなるため。
- 利便性が低下する
- 利用上の理由
- 令和10年度に医療情報システムを更新予定であるため
- 令和8年3月末にて閉院のため
- 令和9年度までに対応は事業者が不可能と回答

【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)】

サーバに対するUSBメモリの使用	施設数	割合
外部記録媒体や情報機器を接続しても、サーバが認識できないシステム設定となっている	94	17.1%
許可された外部記録媒体や情報機器だけが、サーバが認識できるシステム設定なっている	122	22.2%
外部記録媒体や情報機器を認識する		
接続は運用で禁止されている	134	24.4%
許可された外部記録媒体や情報機器のみ、サーバに接続する運用となっている(運用での制限)	100	18.2%
外部記録媒体や情報機器のサーバへの接続を制限していない	92	16.7%
その他	8	1.5%

端末PCに対するUSBメモリの使用	端末PC				部門システム管理者が使用する部門システム端末				エンドユーザが使用する部門システム端末			
	施設数	割合	施設数	割合	施設数	割合	施設数	割合	施設数	割合	施設数	割合
外部記録媒体や情報機器の接続を許可していない												
システム設定による接続制御	149	27.1%	167	30.4%	91	16.5%	152	27.6%	131	23.8%	202	36.7%
システム設定ではなく、運用による接続制御	18	3.3%			61	11.1%			71	12.9%		
外部記録媒体や情報機器の接続は医療情報システム管理部門に依頼を行う												
システム設定による接続制御	103	18.7%	113	20.5%	67	12.2%	101	18.4%	49	8.9%	77	14.0%
システム設定ではなく、運用による接続制御	10	1.8%			34	6.2%			28	5.1%		
病院に申請し許可された外部記録媒体や情報機器のみ端末PCに接続することができる												
システム設定による接続制御	204	37.1%	223	40.5%	138	25.1%	204	37.1%	117	21.3%	185	33.6%
システム設定ではなく、運用による接続制御	29	5.3%			66	12.0%			68	12.4%		
外部記録媒体や情報機器を自由に接続できる	24	4.4%	24	4.4%	63	11.5%	63	11.5%	53	9.6%	53	9.6%
その他	13	2.4%	13	2.4%	30	5.5%	39	7.1%	33	6.0%	33	6.0%

【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の連絡体制図の整備	施設数	割合
整備しており定期的な見直しを実施している	370	67.3%
整備しているが定期的な見直しは実施していない	138	25.1%
整備を計画している	33	6.0%
整備する計画はない	9	1.6%

データやシステムのバックアップの対象の検討	施設数	割合
すべての医療情報システムのデータはバックアップが取れている	248	45.1%
診療を継続するために必要な情報を検討している		
必要と判断したデータはバックアップが取れている	181	32.9%
バックアップが取れているのは、必要と判断した情報の一部である	52	9.5%
診療を継続するために必要な情報を検討しておらず、ベンダーが提案したデータのバックアップを取っている	60	10.9%
データのバックアップを取っていない	9	1.6%

データやシステムのオフラインバックアップ	施設数	割合
オフラインバックアップを実施している	394	72.8%
オフラインバックアップを実施できていない	147	27.2%

バックアップの手法				
テープバックアップ	イミュータブルバックアップ	クラウド保存	施設数	割合
●			230	58.4%
	●		57	14.5%
		●	51	12.9%
●	●		15	3.8%
●		●	26	6.6%
	●	●	9	2.3%
●	●	●	6	1.5%

バックアップのタイミング	施設数	割合
日次	476	88.0%
2日に1回	6	1.1%
3日に1回	8	1.5%
4日から7日に1回	33	6.1%
8日から14日に1回	3	0.6%
15日以上	15	2.8%

バックアップは何世代行っているか	施設数	割合
1世代	71	13.1%
2世代	60	11.1%
3世代	172	31.8%
4世代	19	3.5%
5世代	42	7.8%
6世代以上	177	32.7%

データバックアップの復旧手順の確認	施設数	割合
データバックアップの復旧手順を確認し、復旧の実証訓練を行っている	34	6.3%
データバックアップの復旧手順を確認しているが、復旧の実証訓練は実施していない	214	39.6%
データバックアップの復旧は保守事業者に一任しており、医療機関として復旧手順の確認は行っていない	285	52.7%
その他	8	1.5%

サイバー攻撃を想定した事業継続計画(BCP)の策定	施設数	割合	施設数	割合
策定している				
厚生労働省が作成したBCPを参考	326	59.3%	465	84.5%
他院が作成したBCPを参考	75	13.6%		
自施設で独自に策定した	64	11.6%		
策定していない	85	15.5%	85	15.5%

事業継続計画(BCP)の定期的な見直し	施設数	割合
はい	319	68.6%
いいえ	146	31.4%

【4. 規程類の整備（令和7年度）】

体制構築について、具体的な実施方法を運用管理規程等に定めていますか。		
	施設数	割合
はい（定期的に見直している）	285	51.8%
はい（定期的な見直しはできていない）	216	39.3%
いいえ	49	8.9%

医療情報システムの管理・運用について、具体的な実施方法を運用管理規程等に定めていますか。		
	施設数	割合
はい（定期的に見直している）	287	52.2%
はい（定期的な見直しはできていない）	224	40.7%
いいえ	39	7.1%

インシデント発生に備えた対応について、具体的な実施方法（サイバー攻撃を想定した事業継続計画（BCP））を運用管理規程等に定めていますか。		
	施設数	割合
はい	356	64.7%
いいえ	194	35.3%

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

順位	チェックリスト項目	CL相当の実施状況	研究で把握した実効性指標	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
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）	実装済みまたは実装予定は、ネットワーク機器24.9%、サーバ35.1%、端末PC53.2%。(p9, L1-8)	実装済みは、ネットワーク機器1.5%、サーバ1.6%、医療情報システム接続端末全体3.6%。(p65, L29-36; p66, L4-18)	機器・システム未対応、費用、実装方法不明、保守業者管理、業務負荷、既存システム改修の困難さ。(p20, L4-18; p66, L29-66)	A病院は電子カルテ端末にICタグ＋顔認証、F病院は一部部門でアプリケーション、I病院は電子カルテ端末にICカード＋パスワードを導入。ネットワーク機器では病院配布証明書による所持認証を併用する例もある。(p11, L7-13; p94, L59-64)	全機器への一斉導入が困難な場合、VPN、踏み台サーバ、管理GUI、リモート保守経路など外部接続・管理操作部分から二要素認証を先行導入する。サーバOSログインへの直接実装が困難な場合は、別ドメイン踏み台端末にアクセスを限定する。(p20, L4-18; p21, L1-18) システム更新のタイミングで二要素認証あるいは代替策の予算確保と仕様への追加を確実に行う。
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）	適用済みは、端末PC46.2%、サーバ52.2%、ネットワーク機器65.5%。(p8, L20-23; p74, L26-32)	「全機器に適用」に限ると、端末PC24.9%、サーバ25.1%にとどまる。(p74, L26-32)	医療情報システムの安定稼働、ベンダー検証、システム停止、SE人件費、保守費用の問題が障壁。(p8, L20-36; p79, L1-14)	A病院は3か月に1回、3時間の計画停止枠を設けてサーバパッチを適用。D病院はパッチ適用困難な機器にEDRを導入し重点監視。F病院はWSUSによる定期適用を実施。(p11, L24-36; p88, L16-18; p96, L16-21)	システム導入時・更新時に、パッチ適用の頻度、対象範囲、検証方法、停止時間、費用負担を保守契約に含める。パッチ適用困難な機器にはEDR、接続制限、重点監視などの代替的リスク低減策を講じる。(p8, L17-22; p103, L1-6)
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）	全機器を把握している施設は、ネットワーク機器48.2%、端末PC62.0%、サーバ70.7%。(p6, L31-43)	台帳管理自体はほとんどの施設で実施されているが、網羅性に差がある。(p6, L31-43)	特にネットワーク機器は、古い機器、部門管理機器、外部接続機器、保守事業者管理機器が漏れやすい。資産管理ツール導入にはコストが必要。(p6, L31-43)	B病院はCAD図面上に端末配置をマッピングし、物理配置を可視化。D病院は資産管理ソフトを用いた全数棚卸を毎年定例化。F病院はExcelとSS1を併用。(p10, L16-29)	Excel台帳だけでなく、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る。外部接続点の棚卸とセットで実施し、好事例を示して費用対効果を説明する。(p6, L37-43)
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）	全てのリモートメンテナンス回線を把握できていない施設が18%存在。逆に、把握できている、またはリモートメンテナンスを行っていない施設は約82%。(p7, L14-22)	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%、その仕組みのみを許可している施設は18.2%。(p7, L14-22)	自施設管理の仕組みはあっても、ベンダー側の理由で例外を認めざるを得ない。ベンダー依存により全容把握が難しい。(p7, L16-22)	B病院は独自の「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。H病院・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。(p10, L31-36; p10, L1-8; p87, L30-34)	病院側が管理するリモート接続基盤に集約する。例外接続を認める場合も、接続元・接続先・認証方式・接続回線・責任分界を台帳化し、管理対象に含める。(p7, L23-27)
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）	復旧手順を確認している施設は45.9%：実証訓練あり6.3%＋実証訓練なし39.6%。(p67, L61-70)	オフラインバックアップは72.8%で実施。復旧の実証訓練まで行っている施設は6.3%。(p67, L61-70)	バックアップ取得は進んでいても、実際に復旧できるかを確認していない施設が多い。復旧を保守事業者に一任し、医療機関として復旧手順を確認していない施設が52.7%。(p67, L65-70)	A病院はAzureクラウド上で24時間以内復旧を実証。D病院はVeeamによるバックアップ運用とOSレベルからのリストア訓練を実施。F病院はRubrikによるイミュータブルバックアップを導入。(p11, L34-36; p12, L1-5; p96, L27-30)	保守事業者と共同で復旧手順を確認し、リストア訓練・机上訓練を行う。復旧対象、優先順位、RTO/RPOを定め、バックアップ取得だけでなく「戻せること」を確認する。(p22, L31-36)
6	**アクセスログを管理している。**（2-⑪）	多くの施設が全て、または一部のアクセスログを残している。(p8, L9-16)	病院職員または保守事業者が定期的に確認している割合は、端末PC14.9%、サーバ18.7%。(p74, L7-18)	ログ保存自体は行っていても、定期確認・分析・相関分析まで人手が回らない。アクセスログの保管期間を把握していない施設も少なくない。(p8, L9-16)	H病院・I病院は広範囲のアクセスログ保存を実施。F病院は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るが、ログ相関分析は困難。(p11, L10-22)	重要サーバ、電子カルテ、踏み台サーバなど対象を絞って、確認頻度・担当者・異常時対応を定める。保守事業者と、ログの保存範囲、保管期間、確認方法、異常時対応を協議する。(p8, L14-16; p21, L40-57)
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）	CISOまたは医療情報システム安全管理責任者を配置していない施設は6.4%にとどまり、設置自体は93.6%。(p6, L1-8)	IPA ITスキル標準レベル4以上相当の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の配置は38.0%。(p6, L17-20)	形式的な責任者設置は進んでいるが、実務を担える専門知識・経験が不足している。(p6, L21-25)	D病院では情報処理安全確保支援士・上級医療情報技師の資格を持つ責任者が中心となり専門性を内製化。B病院・E病院では放射線技師・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。(p9, L31-35; p10, L1-6)	CL上の「設置」を形式面で終わらせず、サイバーセキュリティ教育、IPA資格・試験取得奨励、院内人材育成、外部専門人材活用、地域連携により、実効性ある体制にする。(p6, L21-25; p13, L28-36; p14, L1-18)
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）	MDS/SDSの提出を受けている施設は93.5%。(p7, L29-36)	MDS/SDSの内容を確認し、具体的対策まで実施している施設は25.5%。(p7, L29-36)	提出を受けるだけで、内容確認やリスク評価、導入可否判断、具体的対策への反映に至っていない。(p7, L32-36)	C病院は「×」や空欄回答の理由を確認し、曖昧な回答を許容しない運用を実施。F病院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る。(p10, L14-27; p88, L15-18)	MDS/SDSを単なる提出書類にせず、リスク評価、導入可否判断、二要素認証・パッチ適用・外部接続管理・バックアップ等の要求事項に反映する。調達・保守契約時の確認資料として活用する。(p10, L21-27)
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）	CL相当の単純な「アクセス権限設定」の実施率は、本文要約部分では明確な単一割合として整理されていない。	ユーザごとにID・権限を設定し、機器群ごとに異なるパスワードとしている施設は、ネットワーク機器10.2%、サーバ11.3%。一方、機器群ごとに異なるパスワード設定は、サーバ67.3%、ネットワーク機器61.8%。(p7, L6-18)	共有ID・共通パスワード、管理者権限IDの使い回し、ベンダー共通ID、旧システム制約が残りやすい。(p7, L6-30)	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に求めていた。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。(p10, L30-36; p11, L1-4)	外部攻撃対策として機器群ごとに異なるパスワード、内部対策としてユーザごとのID・権限設定を進める。管理者IDの個人別化、特権ID棚卸、作業申請制、保守事業者アカウント管理を行う。(p7, L9-18; p20, L19-28)

CISA-CDM	1: Data Protection Management	2: Network Security Management		3: Identity and Access Management		4: Asset Management				
チェック項目／病院情報システム構成要素	バックアップ/復旧基盤	ネットワーク/境界	外部接続/保守/事業者	ID/権限基盤	権限管理	電子カルテ	端末PC/VDI	医療機器/IoT	検体検査・放射線・薬剤等部門(RMF-High)	サーバ/仮想基盤
1-① 安全管理責任者設置	復旧統括者・担当者明確化	NW責任者・連絡先明確化	事業者窓口・連絡先明確化	権限承認者・連絡先定義	責任者・代行・委員会・連絡先設置	システム責任者・連絡先選出	端末管理責任部門選出・連絡先明確化	機器管理責任者選出・連絡先明確化	各部門で責任者を選出・連絡先明確化	基盤(ハードウェア)オーナー明確化・連絡先明確化
2-① 資産台帳管理	バックアップ対象・RTO/RPO台帳	IP・FW・アクセス制御リスト台帳	回線・接続元・契約台帳	ID・特権ID台帳	CMDB・棚卸周期	版数・DB・連携先台帳	所属・権限・EDR台帳	IP/MAC・保守形態台帳	装置・接続先台帳	機種・OS・EOL・XDR
2-② リモート保守有無確認	緊急遮断手順	閉域/VPN・送信元制限	全台数把握・作業画面・環境録画・作業許可制	保守ID分離・MFA(多要素認証)	承認制・申請台帳	対象機能明確化	常時許可禁止	装置別可否・手順化	対象機能明確化	Jump経由・時間制限
2-③ MDS/SDS提出	復旧支援範囲明確化	暗号・管理IF仕様確認	提出義務・更新通知条項	認証方式の明示	調達要件化・改版時再提出	MDS/SDS受領	端末制約確認	同・保守条件確認	MDS/SDS受領	OS/脆弱性対応仕様確認
2-④ 職種/業務別権限設定	非常時権限付与手順	NW管理権限分離	保守権限最小化	職務ベースアクセス制御・特権管理・定期棚卸	権限基準・職務分掌	職種別権限・緊急閲覧統制	ローカル管理者禁止	操作/設定権限分離	技師/医師/保守分離	管理者権限分離
2-⑤ 不要アカウント削除/無効化	緊急失効手順	共有ID廃止	契約終了時停止	アカウントライフサイクル管理自動化	入退職連動型サービス品質保証(SLA)	退職者ID即時停止	休眠端末ID停止	保守ID失効	退職者ID即時停止	孤立ID・共有ID棚卸
2-⑥ パッチ適用	パッチ起因障害の復旧手順	FW/SW/無線更新	SLA・緊急連絡体制	認証情報管理システム/アクティブディレクトリ更新	パッチ方針・例外管理	アプリ/DB/OS更新計画	OS/EDR/アプリ更新	ファーム更新・代替策	ベンダ協調更新	OS/ミドル/DB更新
2-⑦ パスワード強度/更新	非常時保管手順	機器秘密情報管理	保守IDへ強制適用	長パス・辞書禁止・MFA	パスワード標準強度設定	個人ID徹底・共有禁止	LAPS等で端末PW分離	既定PW変更	個人ID徹底・共有禁止	サービスアカウント管理
2-⑧ パスワード使い回し禁止	緊急PWも一意化	機器ごと別PW	事業者共通PW禁止	シングルサインオン(SO)・秘密情報管理庫	禁止規程	個人認証徹底	端末ローカルPW個別化	装置既定PW個別化	個人認証徹底	共通管理PW廃止
2-⑨ USB等外部媒体制限	災害時代替媒体手順	NAC/ポート制御	持込媒体申請・消毒手順	例外申請者限定	媒体持込規程・例外承認	データ書出し制御	Device Control・暗号化	FW更新媒体の許可制	装置取込の例外管理	USB無効
2-⑩ 二要素認証	緊急代替認証手順	VPN/管理GUIで必須	保守接続で必須	IdP/FIDO2/OTP	MFA方針・対象定義	院外利用・管理操作で必須	VDI/端末管理で必須	可能機種は管理面で必須	管理機能で必須	管理者・遠隔接続で必須
2-⑪ アクセスログ管理	復旧/演習ログ保全	Syslog/NetFlow	保守セッション録画	認証/特権操作ログ	保管基準・監査体制	参照・更新監査証跡	EDR/OS操作ログ	設定変更・操作ログ	検査/画像操作ログ	OS/DB/Sysmon/SIEM連携
2-⑫ 不要ソフト/サービス停止	復旧後の再無効化	未使用管理IF停止	不要保守口閉鎖	不要連携停止	ハードニング基準	不要モジュール停止	不要アプリ削除	未使用ポート/サービス停止	不要機能停止	不要サービス停止・allowlist
2-⑬ 接続元制限	非常時暫定許可手順	VLAN/ACL/セグメンテーション	固定IP・Jump host	管理系接続元限定	通信許可基準	AP-DB間など通信最小化	管理接続元限定	医療機器専用セグメント・物理キー	装置-部門鯖間限定	Host FW・allowlist
3-① インシデント時連絡体制	指揮命令系統の作成と組織合意	NW当番体制	24時間窓口・警察/厚労省連携	認証基盤障害連絡先制定	CSIRT(サイバー初動対応者)・連絡網・報告順序の制定	EHR責任者・ベンダ連絡先	HD/現場支援窓口設置	ME/機器業者連絡先連絡先決定	部門責任者連絡先決定	基盤当番体制決定
3-② バックアップと復旧手順確認	Offline/Immutable保有・復旧訓練	機器設定backup	復旧支援SLA	ディレクトリ/秘密復旧	優先復旧順序定義	DB/帳票/IF復旧手順	Gold image・予備機	設定export・再設定手順	検査/画像データ復旧	仮想環境イメージ/DB/設定backup
3-③ サイバー攻撃想定BCP	RTO/RPO・訓練・演習	分断/迂回設計	保守停止/緊急接続統制	代替認証・停止判断	Cyber BCP・ダウンタイム運用手順・実施指示権限制定	紙カルテ・ダウンタイム運用	代替端末・紙運用	スタンドアロン運用	検査依頼紙運用	隔離/再構築手順
4-① 1-3を規程化	Backup/復旧/BCP台帳・手順文書	FW/ACL/分離手順	リモート保守規程・契約条項	ID管理手順書	運用管理規程・委託契約取り交わし	権限/監査/変更管理規程	端末管理基準	医療機器接続基準	装置別運用手順	構築/ハードニング手順
鳥飼追加:サイバー攻撃検知(CSF-Detection能力チェック)	負荷トレンド異常監視	IPS/NDRによる異常トラフィック量・経路検知	異常検知時に速やかに連絡照会	異常振る舞いアカウントの検知・管理者通知	管理者権限アカウントの監視	XDRなどによる攻撃予兆検知	挙動監視・なりすまし監視	設定(流量など)の適性値監視	挙動監視・なりすまし監視	挙動監視・なりすまし監視
鳥飼追加:サイバー攻撃対処(CSF-Response能力チェック)	バックアップ経路即時遮断	アタックサーフェス経路即時遮断	サイバー攻撃状態での安全な異常確認・設定セキュア化作業実施	異常検知アカウントの権限停止	管理者権限アカウントの異常時停止	カルテ隔離後参照系自動切換えなど保護手段実施	異常端末をネットワーク自己隔離やネットワークスイッチ連動隔離	異常設定値時に医療安全側に動作モードが遷移する(フェイルセーフ)	異常サーバをネットワーク自己隔離やネットワークスイッチ連動隔離 紙運用一斉同報・切り替え	異常サーバをネットワーク自己隔離やネットワークスイッチ連動隔離 幹事社に異常自動通知

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)
分担研究報告書

テーマ:「医療機関におけるサイバーセキュリティ対策チェックリスト」への対応状況調査結果

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
研究分担者　鳥飼幸太　群馬大学医学部附属病院　システム統合センター　准教授
研究分担者　猪飼宏　京都府立医科大学附属病院　医療情報部　准教授
研究分担者　橋本智広　大津赤十字病院　事務部　医療情報課　課長
研究分担者　三上聡司　社会医療法人三上会　東香里病院　院長
研究分担者　杉本賢人　大阪大学大学院医学系研究科　医療情報学　特任助教

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実態を詳細に把握することを目的として実施した。近年、医療機関を標的としたサイバー攻撃が増加し、診療停止などにより地域医療に重大な影響を及ぼす事例が発生している。一方、既存の「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」は「はい／いいえ」の二択回答であり、実態把握には限界があった。そこで本研究では、チェックリスト各項目を具体化した 89 問の Web アンケートを作成し、全国の医療機関 550 施設から回答を得た。

調査の結果、多くの施設で CISO や医療情報システム安全管理責任者の配置、BCP 策定、バックアップ取得、アクセス制御など一定の対策は進んでいた。一方で、高度な専門知識を持つ情報セキュリティ人材は少なく、IPA 資格保有者も限定的であり、人材不足が明らかとなった。また、ネットワーク機器の台帳管理や外部接続回線の把握が不十分な施設が一定数存在し、特にネットワーク機器管理の難しさが示された。

リモートメンテナンスでは、ベンダー側の接続経路を完全に把握できていない施設が多く、管理の不十分さが課題であった。MDS/SDS の提出は多くの施設で受けていたが、内容を具体的な対策へ結びつけている施設は少数であった。アクセス権限管理では、管理者 ID やパスワードの使い回し、個別 ID 未整備など脆弱な運用が残存していた。

アクセスログ管理や不要アカウント削除は一定程度進んでいたものの、ログ確認やリアルタイム対応は限定的であった。セキュリティパッチ適用率は十分ではなく、費用負担やシステム停止リスク、ベンダー依存が大きな障壁となっていた。さらに、二要素認証の導入率は低く、令和 9 年度までの実装目標に対して対応の遅れが顕著であった。

バックアップや BCP は比較的整備されていたが、復旧訓練の実施施設は少なく、規程類も策定後の定期見直しが不十分であった。以上より、医療機関のサイバーセキュリティ対策は一定程度進展している一方、専門人材育成、ネットワーク管理、認証強化、パッチ運用、復旧訓練などに大きな課題が残されていることが明らかとなった。

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」としてまとめている。各医療機関の「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」への対応状況については、チェックリストは「はい」、「いいえ」の二択の回答となっていること、保健所の立入検査で確認される性質上、立入検査や厚生労働省の医療機関等情報支援システム（G-MIS）の調査では実態が十分に明らかにならないことが想定される。

そこで、本研究では、「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」に挙げられる具体的な項目に対して、「はい」、「いいえ」ではなくより具体的な質問項目を作成し、各医療機関へのアンケート調査を実施することで、各医療機関におけるサイバーセキュリティ対策の実施状況を明らかにすることである。

B. 研究方法

Microsoft Office 365 の Form を用いて Web アンケート調査を行った。

「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（令和6年度版）」の質問項目それぞれに対し、研究代表者、研究分担者で質問内容を議論し、作成を行った。質問内容はできるだけ具体的に記載することで、医療機関側が正しく理解をしたうえで回答できるように工夫を行った。次に、「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（令和 7 年度版）」で追加された質問項目についても、質問内容を設定した。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。セクション 1 は「貴施設についておしえてください」で質問項目は 8 問、セクション 2 は【1. 体制構築】で質問項目は 13 問、セクション 3 は【2. 医療情報システムの管理・運用】で質問項目は 12 問、セクション 4 は【医療情報システムの管理・運用】で質問項目 23 問、セクション 5 は【医療情報システムの管理・運用(令和 7 年度)】で質問項目は 15 問、セクション 6 は【3. インシデント発生に備えた対応】で質問項目は 9 問、セクション 7 は【4. 規程類の整備（令和 7 年度）】で質問項目は 3 問であった。最後にセクション 8 で、本アンケート調査後に予定されるインタビュー調査への協力の有無を確認した。質問項目は 6 問であった。具体的な質問内容は別添資料 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」への対応状況調査に示す。

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、各施設にメーリングリスト等を用いて調査協力をしてくださるように依頼を行った。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、インタビュー調査に協力いただける医療機関を除き、収集しなかった。

（倫理面への配慮）

アンケート調査は匿名を原則とした。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、本研究では施設情報は削除し、匿名の状態で解析を行った。

C. 研究結果

550 施設から回答を得た。アンケート結果は別添資料 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。

1.【医療情報システム安全管理責任者を設置している。(1-(1))】

550 施設のうち、①情報セキュリティ責任者(CISO)と医療情報システム安全管理責任者に別の人物を配置する施設が190施設(34.5%)、②CISO のみ配置する施設が 11 施設(2.0%)、③CISO と医療情報システム安全管理責任者を同一人物で配置する施設が 212 施設(38.5%)、④医療情報システム安全管理責任者のみを配置する施設が 102 施設(18.5%)、⑤CISO、医療情報システム安全管理責任者をともに配置しない施設が 35 施設(6.4%)であった。

①CISO と安全管理責任者を別におく施設では、上部組織の理事を含め組織の長が務め、安全管理責任者は医療情報システム管理部門長が 31.6%となるなど、役割分担が意識されていた。

CISO、安全管理責任者のうち、高度な専門知識(IPA IT スキル標準レベル 4 以上相当)を有しており、単独でも対策を進めることができると回答したのは 18 名(2.6%)、一定の専門知識を有しており、単独でも対策を進めることができると回答したのは92名(13.0%)、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と回答したのは 359 名(50.9%)、ほとんど知識を有していないと回答したのは 205 名(29.1%)、全く知識を有していないと回答したのは 31 名(4.4%)であった。医療情報技師(上級医療情報技師を含む)の資格保有者は 84 名(11.9%)、情報処理推進機構(IPA)の資格、試験として、情報処理安全確保支援士(登録情報セキュリティスペシャリスト)が 2 名(0.3%)、情報処理安全確保支援士(資格試験合格のみ)が 2 名(0.3%)、応用技術者試験が 11 名(1.6%)、基本情報技術者試験が49名(7.0%)、情報セキュリティマネジメント試験が 18 名(2.6%)、IT パスポート試験が 30 名(4.3%)であり、621 名(88.1%)はリストした IPA の資格・試験は保持していなかった。

2.【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))】

全ての機器を把握していると回答したのは、サーバ 389 施設(70.7%)、端末 PC341 施設(62.0%)、ネットワーク機器 265 施設(48.2%)でネットワーク機器はサーバ、端末 PC に比較して低かった。また、ネットワーク機器は台帳管理を行っていないと回答した施設が 26 施設(4.7%)あった。台帳の管理者は自施設の職員が多かったが、機器を導入した事業者の割合はネットワーク機器がサーバ、端末 PC に比べ高かった。ネットワーク機器の管理はサイバーセキュリティ対策を考えると重要であるが、全てのネットワーク機器の管理は容易でないことが明らかになった。台帳の管理方法はエクセル等の汎用ソフトを使用するケースが多く、専用のソフトウェアの使用頻度は高くなかった。

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のは 388 施設(70.5%)、一部のみ把握していると回答したのが 134 施設(24.4%)、把握していないと回答

したのは 28 施設（5.1%）であった。接続回線数の平均は、全て把握と回答した施設が 8.9 回線、一部のみ把握と回答した施設が 9.4 回線であったが、全て把握していると回答した施設で 40 回線以上の具体的な回線数を答える施設が 8 施設あった。

外部からの回線数を減らす必要性は 438 施設（79.6%）であった。実施に努力をしているのは 258 施設（46.9%）で、回線を全て把握していると回答した施設では 51.3%、一部のみ把握していると回答した施設（36.6%）、把握していないと回答した施設（35.7%）を大きく上回った。適切に管理できる回線数については、10回線以内が 304 施設（93.2%）を占めた。

3.【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))】

リモートメンテナンス（保守）の病院情報システムネットワークへの接続方法については、自施設が設置するリモートメンテナンスの仕組みを持っている医療機関が 346 施設（62.9%）であったが、自施設のリモートメンテナンスを使った接続のみ許可しているのは 100 施設(18.2%)であった。ベンダー側の理由で例外を認めている医療機関のうち 50 施設は全てのリモートメンテナンスを把握できていないと回答があった。リモートメンテナンスを行っている医療機関のうち 99 施設（18%）は全てのリモートメンテナンスを把握できていないと回答していた。

4.【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）の提出を受けている医療機関は 514 施設（93.5%）であった。内容を確認し必要があれば具体的な対策を行っている施設が 140 施設（25.5%）、具体的な対策を行っていない施設が 261 施設（47.5%）、内容を十分に確認していない施設が 113 施設（20.5%）であり、多くの施設は提出を受けるにとどまっていた。医療情報セキュリティ開示書（MDS/SDS）への具体的な対応については、二要素認証対応やセキュリティパッチへの対応など、チェックリストへの未対応事項への対応を求めるなど、医療情報セキュリティ開示書（MDS/SDS）を有効に活用している事例が報告された。

5.【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))】

アクセス権限についてユーザごとに ID と利用権限を設定し、ユーザパスワードは機器群ごとに異なっている施設はサーバで 62 施設（11.3%）、ネットワーク機器で 56 施設（10.2%）にとどまった。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施設はサーバで 104 施設（18.9%）、ネットワーク機器で 127 施設（23.1%）認めた。

端末 PC のエンドユーザに対するユーザ認証については、OS は administrator 以外の同一ユーザで自動ログインを行い、ソフトウェアでユーザ認証を行っている施設が最も多く 252 施設（45.8%）であった。エンドユーザに対するアクセス利用権限については、全てのユーザに対して個別のユーザ ID を発行し、アクセス利用権限を設定している（複数のユーザで使いまわしをしているユーザ ID はない）と回答した施設が 274 施設（49.8%）であった。

6.【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

たのはサーバが 404 施設（73.5%）、端末 PC が 391 施設（71.1%）であった。リアルタイムでアカウントを削除または無効化していると回答したのはサーバが 347 施設（63.1%）、端末 PC が 345 施設（62.7%）にとどまった。

7.【アクセスログを管理している。(2-(6))】

全ての機器のアクセスログを残している施設はサーバが 308 施設（56.0%）、端末 PC が 285 施設（51.8%）、一部の機器のアクセスログを残していると回答したのは、サーバが 183 施設（33.3%）、端末 PC が 165 施設（30.0%）であった。病院職員、または保守事業者がアクセスログを定期的に確認しているのはサーバが 103 施設（18.7%）、端末 PC が 82 施設（14.9%）であった。

アクセスログを残さない施設のうち、アクセスログを残す必要性を感じていない施設は 12 施設にとどまり、アクセスログを残す必要性を感じているが、コストがかかるため残すことができない施設が 72 施設、保守事業者が対応してくれない施設が 18 施設あった。

8.【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))】

全ての機器に対してセキュリティパッチを適用していると回答したのは、サーバが 138 施設（25.1%）、端末 PC が 137 施設（24.9%）、ネットワーク機器が 173 施設（31.5%）、一部の機器に対してセキュリティパッチを適用していると回答したのは、サーバが 149 施設（27.1%）、端末 PC が 117 施設（21.3%）、ネットワーク機器が 187 施設（34.0%）であり、ネットワーク機器は他に比べてやや高い傾向を示したものの、セキュリティパッチを適用していない施設が多く見られた。

セキュリティパッチを適用するタイミングについては、適用が必要なセキュリティパッチが出てきたときに、保守事業者と打ち合わせを行った上、適用時期を決めると回答した施設が多く、定期的にセキュリティパッチを適用している施設は多くなかった。セキュリティパッチを適用する範囲については、保守事業者が推奨するセキュリティパッチを適用する施設の割合が多かった。セキュリティパッチを適用する費用については約 80％の施設が保守費用に含まれると回答したが、随時、作業費用を支払っている施設も少なくなかった。

セキュリティパッチを適用しない理由については、医療機関として必要性を感じていないと回答した施設は 18 施設（6.3%）にとどまり、必要性は感じているが事業者が対応してくれない 68 施設（23.6%）、作業費用の捻出が困難である 102 施設（35.4%）、その他 100 施設（34.7%）であった。その他では、システム動作が保証できないといった理由や、外部インターネットに接続していないといった理由など、多くの理由が挙げられた。セキュリティパッチに対する意見についても、非常に多くのコメントが得られたが、各施設のセキュリティパッチ対応に向けた対応の難しさを記載したものが多かった。

9.【接続元制限を実施している。(2-(8))】

ネットワーク機器の接続元制限の実施をしていると回答した施設は 439 施設（79.8%）であった。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。

10.【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))】

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施設はサーバ、端末 PC ともに 90%前後の対応状況であったが、多くの施設はシステム導入時に確認したのみで、定期的な確認は行っていなかった。端末 PC へのエンドユーザが希望するソフトウェアのインストールについては、システム設定で禁止している施設が多く、許可を受けたソフトウェアのみシステム管理者がインストールを行う対応を取っている施設が多かった。

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ない理由として、不要なソフトウェアやサービスの判別が難しいといった意見も認められた。

11.【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では 260 施設（59.2%）、端末 PC では 228 施設（51.9%）、ネットワーク機器では 267 施設（60.8%）認めた。

認証については、1要素認証と回答した施設がサーバでは 465 施設（84.5%）、端末 PC では 449 施設（81.6%）、ネットワーク機器では 483 施設（87.8%）と、ほとんどの施設が二要素認証に対応していない状況であった。

12.【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)】

サーバに対する USB メモリの使用については外部記録媒体や情報機器のサーバへの接続を制限していないと回答した施設は 92 施設（16.7%）にとどまった。端末 PC に対する USB メモリの使用については、外部記録媒体や情報機器を自由に接続できると回答したのは端末 PC が 24 施設（4.4%）、部門システム管理者が使用する部門システム端末では 63 施設（11.5%）、エンドユーザが使用する部門システム端末では 53 施設（9.6%）であった。USB メモリの接続を許可していない、制限していると回答した施設でも、システム設定でなく運用による接続制御と回答した施設が端末 PC では 57 施設（10.4%）、部門システム管理者が使用する部門システム端末では 161 施設（29.3%）、エンドユーザが使用する部門システム端末では 167 施設（30.4%）であり、利用者に対する運用徹底が重要と考えられた。

13.【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の連絡体制図の整備では、整備しており定期的な見直しを実施している施設が 370 施設（67.3%）、整備しているが定期的な見直しは実施していない施設が 138 施設（25.1%）であった。

データやシステムのバックアップの対象の検討については、全ての医療情報システムのデータはバックアップが取れていると回答した施設が 248 施設（45.1%）、診療を継続するために必要な情報を検討しており、必要と判断したデータはバックアップが取れていると回答した施設が 181 施設（32.9%）であり、バックアップのタイミングは日次が最も多かった。3 世代と 6 世代以上のバックアップと回答した施設が多かった。

データのオフラインバックアップを実施している施設は 394 施設で全施設の 71.6%、バックアップを取っている施設の 72.8%であった。バックアップの方法としてはテープバックアップが最も多く、複数のバックアップ手法を用いている施設が 56 施設（14.2%）認めた。

データバックアップの復旧手順の確認については、34 施設（6.3%）が復旧の実証訓練まで行っていた。一方、バックアップの復旧は保守事業者に一任しており、医療機関として復旧手順の確認は行っていないと回答した施設は 285 施設（52.7%）認めた。

サイバー攻撃を想定した BCP は 465 施設（84.5%）が策定を行っており、その多くが厚生労働省が作成した BCP を参考にしていた（326 施設（59.3%））。BCP の定期的な見直しを行っている施設は 319 施設（68.6%）であった。

14.【4. 規程類の整備（令和 7 年度）】

体制構築について、具体的な実施方法を運用管理規程等に定めている施設は 501 施設で、うち 285 施設は定期的な見直しをしていた。

医療情報システムの管理・運用について、具体的な実施方法を運用管理規程等に定めている施設は 511 施設で、うち 287 施設は定期的な見直しをしていた。

インシデント発生に備えた対応について、具体的な実施方法（BCP）を運用管理規程等に定めている施設は 356 施設であった。

D. 考察

回答のあった 550 施設の所在地は 47 都道府県にまたがり、様々な性格を持った医療機関からの回答が得られた。医療情報部門を設置する医療機関が 440 施設（80%）と高い割合を示しており、アンケートを自由回答とした性質上、医療情報部門を設置する医療機関から多く回答が得られた選択バイアスが生じている可能性がある。一方、高度な専門知識（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 29 施設（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 209 施設（38.0%）であり、専門知識を有する情報セキュリティ人材を配置していない施設からも多く回答が得られた（312 施設（56.7%））。

1.【医療情報システム安全管理責任者を設置している。(1-(1))】

情報セキュリティ責任者（CISO: Chief Information Security Officer）、医療情報システム安全管理責任者を配置していない施設は 35 施設（6.4%）にとどまり、人材配置は順調に進んでいることが確認できた。CISO は医師・歯科医師の割合が多く、IPA の資格保有や試験合格の人材は多くなかった。医療情報システム安全管理責任者は診療放射線技師、医療情報技師（上級医療情報技師）、診療情報管理士などの医療系の資格を持つ人材が一定数見られた。IPA の資格保有者や試験合格者の割合は決して高くなかった。今後、医療機関が配置した情報セキュリティ人材の資格取得をいかに支援するかが課題と考えられた。

2.【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))

ほとんどの医療機関で台帳管理が行われていたが、ネットワーク機器の台帳管理では全ての機器を管理できていないと回答した施設が多く、ネットワーク機器の漏れのない台帳管理の難しさを示していた。一部の施設（サーバ：51 施設、端末 PC：85 施設、ネットワーク機器:45 施

設）は IT 資産管理ツールなど専用のソフトウェアを使用していたが、多くの施設はエクセル等の汎用ソフトを用いた管理となっており、費用対効果が見込みづらい領域への投資の難しさを表していると考えられた。

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のは 388 施設（70.5%）であったが、これは回答した医療機関自身の評価であることは注意が必要である。全て把握の施設と一部のみ把握の施設で、接続する回線数の平均に大きな違いは認めなかったが、全て把握と回答した施設には、40 回線以上の具体的な回線数を答える施設が 8 施設あった。

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。適切に管理できる回線数は 3 回線以下（54.3%）、5 回線（71.8%）、10 回線以下（93.2%）と回答があり、多く見積もっても 10 回線以下に回線数を減らす努力が必要と考えられた。

3.【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))】

リモートメンテナンス（保守）の病院情報システムネットワークへの接続方法については、自施設が設置するリモートメンテナンス回線を持っている医療機関が 346 施設（62.9%）と半数を超える医療機関が独自のリモートメンテナンスの仕組みを持っていた。このうち、自施設のリモートメンテナンスの仕組みのみ許可している施設は 100 施設にとどまり、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。

今後、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。

4.【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))】

多くの施設が、医療情報セキュリティ開示書（MDS/SDS）の提出を受けて、内容確認を行っていた。具体的な対応まで行っている施設は 25.5%であったが、「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」への対応を考えた確認作業など、MDS/SDS の確認の有用性を示すものであった。提出を受けた MDS/SDS の内容を十分に確認していない施設は 20.5%、提出を受けていない施設は 4.7%あり、まずは内容を確認することを始めるべきと考えられた。

5.【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。また、システム導入時や更新時のタイミングにおいては、ベンダーに対してユニークなパスワード設定とID管理へのアプローチが必要と考える。

6.【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いか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。

7.【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。アクセスログの保管が不要と考える医療機関は少なかったが、導入費用の問題で保管できない医療機関をある程度の数認めた。

アクセスログの管理は費用がかかるものであり、必ず保管すべきアクセスログは何か、定期的に確認すべきアクセスログは何か、有事のために保管すべきアクセスログは何で、その期間はどの程度かなど、アクセスログの取扱いについて、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。

8.【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病院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、これらの施設で病院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り、業務継続への影響が生じる可能性がある。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。

これらを踏まえると、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、最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。

セキュリティパッチ適用の必要性を感じていない医療機関はほとんどなく、必要性は感じているが事業者が対応してくれない施設の割合が 23.6%、作業費用の捻出が困難である施設の割合が 35.4%であった。前者の場合も、医療機関側の費用捻出が困難なことが、事業者が対応してくれない理由となっている可能性も高い。適切なサイバーセキュリティ対策には費用が必要となることは、病院長や CISO が理解をする必要がある。一方、必要性を感じていても費用の捻出が困難な医療機関も少なくないと考えられ、診療報酬での対応など、何らかの対応を国として考える必要はあると考えられた。

9.【接続元制限を実施している。(2-(8))】

約 8 割の施設がネットワーク機器の接続元の制限を実施していた。管理設定や監視に医療機関が関わっているのは管理設定で約 7 割、監視で約 6 割であった。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。

10.【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))】

約 9 割の施設がサーバ、端末 PC で、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たが、定期的に確認をしている施設は多くなかった。

エンドユーザが希望するソフトウェアの端末 PC へのインストールはシステム設定で自由にインストールできないようにしている施設が 67.1%であった。運用で制限をしているがシステム設定で制限をかけていない施設が約 3 割みられ、ユーザ教育でどこまで対応できるか課題があると感じた。どのソフトウェアやサービスが不要か、判断ができないと回答する施設も多かったが、まずは保守事業者と議論を行い、施設として管理できる体制を構築することが大切と思われた。

11.【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、病院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、以前から令和 9 年度までに二要素認証の導入を求めている。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。

12.【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)】

USB ストレージ等の外部記録媒体のサーバへの接続については、入退室管理が行われているサーバ室に設置されているサーバについては、システム管理者等、限定した利用者が想定され、ルールによるガバナンスが効きやすい。一方、端末 PC は多数の病院職員が使用するためルールによるガバナンスは効きづらい状況になる。システム設定により USB ストレージなどの外部媒体の接続を制御している施設の割合は、サーバで 39.3%、端末 PC で 82.9%であり、適切な対象に優先して費用投資がされていた。一方、端末 PC でも、部門システム管理者がし使用する部門システム端末のシステム制御は 53.8%、エンドユーザが使用する部門システム端末は 54.0%で、これらの端末に対するシステム制御を進めていく必要があると考えられた。

13.【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の連絡体制図は 9 割を超える施設で整備されており、今後、定期的な見直しの実施率を上げることが課題と考えられた。

システムのバックアップは多くの施設で取られていたが、バックアップが取れているのは、必要と判断した情報の一部である（9.5%）、診療を継続するために必要な情報を検討しておらず、ベンダーが提案したデータのバックアップを取っている（10.9%）、データのバックアップを取っていない（1.6%）となっていた。オフラインバックアップがとられている施設の割合は 72.8%にとどまった。

データバックアップの復旧手順を確認し、復旧の実証訓練を行っていると回答した施設は 34 施設あり、他施設も実証訓練実施の検討を行うべきだと考えられた。

サイバー攻撃を想定した事業継続計画（BCP）は多くの医療機関で策定が進んでいた。厚生労働省が作成した BCP を参考にしている施設の割合が 59.3%と高く、見本を示すことで対策が進む好事例になっていると考えられた。BCP の定期的な見直しを行っている施設は 68.6%にとどまり、今後、定期的な見直しを行う施設の割合を増やすことが大切と考えられた。

14.【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。

E. 結論

全国 550 施設を対象とした調査により、医療機関におけるサイバーセキュリティ対策は、責任者配置、BCP 策定、バックアップ整備など基礎的対策は一定程度進展していることが確認された。一方で、高度な専門知識を有する情報セキュリティ人材の不足、ネットワーク機器管理や外部接続回線把握の不十分さ、二要素認証導入の遅れ、セキュリティパッチ運用の困難さなど、多くの課題が明らかとなった。特に、ベンダー依存の高い運用体制や、復旧訓練・規程

見直しの不足は、インシデント発生時の対応力低下につながる可能性がある。今後は、専門人材育成、医療機関と事業者の協働、継続的な運用改善を通じて、実効性あるセキュリティ体制の構築が求められる。

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

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）
分担研究報告書

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課題調査と解決策の検討

研究分担者　橋本　智広　　大津赤十字病院　事務部　医療情報課

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実効性を明らかにすることを目的に、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（厚生労働省）に基づき、全国の病院を対象としたアンケート調査および訪問インタビュー調査、電子カルテベンダー調査を実施したものである。その結果、ウイルス対策やアクセス制御、バックアップ等の基本的対策は一定程度普及している一方、専門人材の不足やベンダー依存により、運用面の実効性に課題が認められた。特に、ログの活用不足、セキュリティパッチ未適用、リカバリ訓練の未実施などが顕著であった。先進的な医療機関では、経営層の関与や現場職員の参画、復旧検証の実施等を通じてレジリエンスの向上が図られていた。今後は、好事例の共有とチェックリストの実装性向上を通じ、現場実態に即した持続的な対策推進が求められる。

A. 研究目的

近年、医療機関に対するサイバー攻撃の増加を受け、診療停止や患者の個人情報漏えいといった深刻な被害事案が確認されている。こうした状況を踏まえ、令和 5 年 4 月 1 日に医療法施行規則が改正され、病院、診療所及び助産所の管理者は、「医療の提供に著しい支障を及ぼすおそれがないよう、サイバーセキュリティを確保するために必要な措置を講じること」が法令上求められることとなった。同改正においては、管理者が講ずべき「必要な措置」の具体的内容について、最新の「医療情報システムの安全管理に関するガイドライン（厚生労働省）」を参照することが示されており、あわせて、医療機関が優先的に取り組むべき事項を整理した「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（厚生労働省）」（以下、チェックリストと略す）が策定され、毎年その内容が改版され周知されている。　この状況下で、医療機関におけるサイバーセキュリティ対策は、法令により管理者責務として明確に位置付けられたものの、その具体的な実装については、ガイドラインおよびチェックリストを参考としつつ、各医療機関の実情に応じた対応が求められている。

一方、医療法に基づく立入検査では、このチェックリストを基に医療機関の対応状況を確認されるものの、医療機関の実態は多様であり、その違いによりチェックリストに含まれる項目への対応が十分でないケースもあると想定される。同時に、当該項目はチェックリストの改版に伴い見直しが行われることから、医療機関はその対応に向けて速やかな検討に着手する必要となる。

本研究は、チェックリスト（令和 6 年版、令和 7 年版）に着目し、チェックリストに含まれる各項目について、医療現場においてその趣旨や考え方が正しく理解された上で実践されているかを把握・分析することを目的とする。これにより、単なるセキュリティ対策の実施有無にとどまらず、チェックリストが現場において実効的なツールとして機能しているかを検証し、今後の制度運用や見直しに資する知見を提供することにつなげ

る。

B. 研究方法

本研究は、6名の研究者（研究代表者 1 名、研究分担者 5 名）により構成される。次に示す 2 種類の調査を段階的に実施し、実態把握と参考事案の抽出、さらには課題抽出から対応策の検討を行った。

1. アンケート調査の実施

厚生労働省が提示するチェックリスト（令和 6 年版、令和 7 年版）の項目ごとに質問項目を設定し、当該項目への対応状況について調査した。調査の詳細は次のとおりである。回答結果については、項目ごとの実施状況や傾向を整理し、チェックリストの趣旨と現場実態との乖離の有無を分析した。

・調査期間：2025 年 10 月 15 日～11 月 30 日
・調査対象：国内の医療機関（病院を対象）
・調査方法：オンライン形式（Microsoft Forms を使用）
・調査項目：チェックリストに含まれる各項目に対して①から④について調査する。
①各項目の理解度　②実施状況　③運用面での工夫や課題　④その他

2. 訪問インタビュー調査の実施

アンケート調査の結果を踏まえ、チェックリストに基づく対応が積極的に実施されている医療機関を抽出し、当該医療機関を訪問してインタビュー調査を実施した。対象施設は〇施設であり、うち筆者が担当した対象施設は 4 施設であった。当該調査は、別添 2 に示すインタビューシートを作成し、これに含まれる項目について調査した。具体的には、チェックリストの全項目から、アンケート調査の結果から医療機関の対策が十分でないと判断した 12 項目を選出した。当該項目に対してインタビューする観点を事前に設定し、インタビュー調査の精度向上を目指した。

・筆者が担当した対象施設および調査日：
A 病院：800 床クラス、独立行政法人
（調査日：令和 8 年 2 月 10 日）
B 病院：600 床クラス、自治体
（調査日：令和 8 年 2 月 20 日）
C 病院：500 床クラス、企業
（調査日：令和 8 年 2 月 24 日）
D 病院：600 床クラス、公的
（調査日：令和 8 年 3 月 10 日）
・インタビュー時間：各施設 4 時間
・調査シートに含まれる調査内容：
A. 基本情報
A-1　病院情報
A-2　電子カルテﾍﾞﾝﾀﾞｰと構築ﾍﾞﾝﾀﾞｰ
A-3　ネットワーク機器ﾍﾞﾝﾀﾞｰと構築ﾍﾞﾝﾀﾞｰ
A-4　セキュリティベンダー
A-5　主要ベンダー
B. 調査項目
表1に示す 12 項目(B1-B12)について調査。

3. システムベンダーに対するインタビュー調査

医療機関に対して実施した訪問インタビュー調査内容を踏まえて、電子カルテベンダーに対してオンライン形式でインタビュー調査を実施した。対象ベンダーは、大規模医療機関に対する導入実績がある3社とした。

・調査期間：2026 年 3 月 17 日～3 月 25 日
・調査対象：電子カルテベンダー（日本 IBM、日本電気株式会社、富士通 Japan 株式会社）
・調査方法：オンライン形式
・調査項目：訪問インタビュー調査シートに基づく。

表 1：訪問インタビュー調査項目

No	大分類	チェックリスト 該当項目
B-1	セキュリティ人材	【 1-①】医療情報システム安全管理責任者を設置している。
B-2	資産管理	【 2-①】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。
B-3	外部接続点管理	【 2-②】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。
B-4	MDS／SDSへの対応	【 2-③】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。
B-5	ユーザー管理	【 2-④】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。
B-6	各種ログ管理	【 2-⑪】アクセスログを管理している。
B-7	セキュリティパッチ管理	【 2-⑥】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。
B-8	二要素認証への対応	【 2-⑩】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。
B-9	外部記憶媒体管理	【 2-⑨】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。
B-10	システムバックアップ運用管理	【 3-②】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。
B-11	IT-BCPの策定と訓練	【 3-③】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。
B-12	その他	なし

※項目番号は令和7年版に準ずる

（倫理面への配慮）

本研究においては、アンケートおよびインタビューはいずれも任意参加とし、研究目的および取り扱い方針を事前に説明した上で同意を得た。また、収集した情報は本研究目的以外には使用せず、適切に管理した。

C. 研究結果

1. アンケート調査結果

1−1. 回答施設に関する情報

アンケートは医療機関の 550 施設からの回答が得られた。回答施設の傾向としては、経営形態としては私立の医療機関が 296 施設（53.8%）と過半数を占めており、次いで公的な医療機関（大学病院を除く）が 216 施設（39.3%）であった。医療機関の機能別では、二次救急医療機関が 259 施設（47.1%）と最も多く、地域医療支援病院が 154 施設（28.0%）、災害拠点病院（基幹・地域）が 173 施設（31.5%）と、地域医療の基幹を担う施設が多く含まれていた。病床規模に関しては、100 床以上 200 床未満の施設が 170 施設（30.9%）と多く、次いで 200 床以上 300 床未満が 87 施設（15.8%）、400 床以上 600 床未満が 84 施設（15.3%）、100 床未満が 77 施設（14.0%）と続いている。診療報酬における診療録管理体制加算の算定状況は、加算 3 が 199 施設（36.2%）、加算 1 が 185 施設（33.6%）、加算 2 が 127 施設（23.1%）となっている。

また、回答施設の 502 施設（91.3%）が電子カルテ等の「診療録の電子的保管」を導入済みであった。さらに、440 施設（80.0%）が医療情報部門を設置しており、電子カルテを含む情報システムの医療現場への展開とともに、その運用管理の必要性が組織として理解されていると想像される。以上のことから、本アンケート調査は電子カルテを導入している小中規模から大規模までの幅広い基幹的病院の現状を反映したものといえる。

1−2. 情報セキュリティ人材の現状

医療機関における情報セキュリティ人材の配置状況は極めて厳しい実態にある。具体的には、セキュリティに関する専門知識を有する人材を「配置していない」と回答した施設は 312 施設（56.7%）にのぼり、半数以上の医療機関で専門人材が不

在となっている。IPA の IT スキル標準レベル 4 以上相当の「高度専門人材」を配置できている施設は、わずか 29 施設（5.3%）という極めて限定的な状況にある。また、情報セキュリティ責任者（CISO）や医療情報システム安全管理責任者は、組織によっては、同一法人内で統一的な運用ルールが策定されており、その中に当該責任者をどの職に設定するか定めているケースもあるため、必ずしも専門知識を有することが当該責任者の条件になっていない。一方、専門人材を配置できない理由としては、「適任な人材がいない」ことが最大の要因として挙げられており、病床数に関係なく同様の回答が見受けられる。セキュリティ対策の方針決定にあたっては、医療情報システム安全管理責任者（404 施設）や CISO（248 施設）のほか、「保守契約を結ぶ医療情報システムベンダー」に依存している施設が合計で280施設（知識確認済み 186、未確認 94）に達しており、外部の知見に頼らざるを得ないという体制面の課題が浮き彫りとなった。

1−3．チェックシートにおけるカテゴリ別の現状と分析

1−3−1．組織体制と人材の現状

医療機関における CISO（情報セキュリティ責任者）や医療情報システム安全管理責任者の設置は形式上進んでいるが、実働を担う専門人材の不足が顕著であることが明らかとなった。高度な専門知識（IPA レベル 4 相当以上）を持つ人材を配置できているのはわずか 5.3%に留まり、56.7%の施設が専門人材を配置できていないため、多くが「適任者がいない」ことを理由に外部ベンダーへ依存せざるを得ない状況になっている。

1−3−2．資産・回線・リモート管理

サーバの台帳管理は 389 施設（70.7%）の施設で「全ての機器を把握している」と回答されているが、端末 PC の把握率は 341 施設（62.0%）、ネットワーク機器の把握率は 265 施設（48.2%）に留まっている。管理手法はエクセル等の汎用ソフトが448施設（83.7%）であり、資産管理ソフトを導入施設はまだ少ないと判断できる。外部回線の把握は、全て把握できているとされる施設は 388 施設（70.5%）で進んでいるものの、リモートメンテナンスにおいては自施設の仕組みを持ちつつも、ベンダー側の都合による例外接続を認めているケースが多く、管理の主導権を完全には握りきれていない実態がある。

1−3−3. MDS/SDS の活用とアカウント管理

MDS/SDS の提出を受けている施設は514施設（93.5%）と非常に高いものの、その内容を確認して具体的な対策（パスワード変更や設定変更）に繋げているのは 140 施設（25.5%）に過ぎない。アカウント管理では退職者の削除は 404 施設（73.5%）と進んでいるものの、端末ログイン時の ID 使い回しや自動ログインが約 40%あり、個人が特定できる管理の徹底に課題がある。

1−3−4．ログ管理・セキュリティパッチ適用・ソフトウェア管理

サーバのアクセスログの取得は、全ての機器のログを残している施設は 308 施設（56.0%）で実施されており、病院職員が定期的な確認を行っているのは、何らかのログを残していると回答された施設において 57 施設（11.6%）に留まっている。端末 PC のアクセスログの取得は、全ての機器のログを残している施設は 285 施設（51.8%）で実施されており、病院職員が定期的な確認を行っているのは、何らかのログを残していると回答された施設において 63 施設（14.0%）に留まっている。

セキュリティパッチの適用については、サーバ

への未適用が 263 施設（47.8%）、端末 PC への未適用が 296 施設（53.8%）、ネットワーク機器への未適用が 190 施設（34.5%）に達しており、「システムの動作保証がない」「診療停止を伴う」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っている。ソフトウェア管理では、端末へのインストール制限は対応されることが広がっている一方、不要なバックグラウンドサービスの停止は「知識不足」や「ベンダー任せ」により困難な状況にあると考える。

1−3−5. サーバー・端末・ネットワーク機器の認証

サーバー室の物理的な入退室管理は、用紙記録等で広く行われている。一方、サーバ・端末 PC・ネットワーク機器に対する認証方法として、二要素認証の実装は、いずれも 10%程度と極めて少数であった。当該認証の実装には導入コストや業務の煩雑化が理由とされ、現時点でも一要素認証（パスワードのみ）で運用されている施設が多い。その中で、パスワードの定期変更すら行えていない施設が 228 施設（41.4%）存在した。

1−3−6. 外部ストレージ・バックアップ

外部ストレージの制限は端末 PC で先行しているが、サーバー側では十分に対応できていない傾向が見受けられる。バックアップについて、本項目には 541 施設が回答を得ており、394 施設（72.8%）がオフラインバックアップを実現しているが、復旧の実証訓練を行っているのはわずか 34 施設（6.2%）に留まっている。中でも、手順の確認方法についてもベンダーに一任している施設が過半数となっている。

1−3−7. IT-BCP

IT-BCP の策定においては厚生労働省が作成した医療情報システム部門事業継続計画（BCP）を参考にした施設は 326 施設（59.2%）であった。IT-BCP は策定済みであるが、訓練による実効性の確認が今後の課題と考える。

1−4. アンケート調査結果のまとめ

本アンケート調査結果から、ウイルス対策ソフトの導入、アクセス制御の実施、バックアップの取得等、比較的基本的な技術的対策については、多くの医療機関で一定水準の対応がなされていることが確認されたが、「形式的な体制整備」に留まるケースもあり、「実効的な運用を想定した体制整備」が必要になると考える。例えば、厚生労働省のガイドラインや BCP ひな形の浸透により、責任者の設置や規定の策定、バックアップの取得といった基本的な枠組みは多くの施設で整備に向けて取り組まれている状況にある。一方、組織全体における責任体制の明確化や定期的な教育・訓練の実施、さらにインシデント発生時を想定した具体的な対応手順の整備と訓練が行われるべきである。ただし、医療機関に所属する人材として、これらの牽引役となる専門人材は不足していることが明らかとなった。高度専門人材の配置は 5.3%に留まり、その結果として、取得した MDS/SDS をリスク評価に活用できない、膨大なログを放置せざるを得ない、あるいは可用性への懸念からパッチ適用を断念するといった「受動的な対策」に留まっている実態が浮き彫りとなった。特に、「備え（バックアップや規定）」はあるが「検証（復旧訓練や見直し）」が進んでいないと考える。復旧訓練の実施率の低さは、有事の際の実効性に大きく影響を与えるものである。今後は、「今あるリソース」を活かしつつ、現場の医療職を巻き込んだ訓練やベンダーとの具体的な対策協議を通じて、組織全体の「対応力」を底上げしていくことが求められる。

２．訪問インタビュー調査結果

訪問インタビュー調査結果の要約を別添資料 6 に示す。

２−１．施設別結果

各病院のインタビュー調査結果に基づき、他施設の参考となる具体的な取り組みを 5 項目ずつ抽出した。

２−１−１．病院 A

①「セキュリティなき導入」を許さない厳格な統制

インシデントの経験から、独自チェックリストでセキュリティレベルを事前審査し、基準を満たさない機器は現場のニーズがあっても導入を許可しない強いガバナンスを確立している。

②クラウドを活用した 24 時間以内の復旧検証

電子カルテデータを Azure クラウドへバックアップし、実際に参照系サーバを 22 時間 16 分で構築できることを実証実験によって確認している。

③診療停止を伴う計画的なセキュリティパッチ適用作業の実施

端末 PC は月 1 回、サーバは 3 ヶ月に 1 回、あらかじめ設定した「平日 20 時〜23 時」のシステム停止時間枠で計画的にセキュリティパッチを適用している。

④Microsoft Teams を活用したデータ出力の申請フロー

二次利用等のためのデータ持ち出しが必要な際、Microsoft Teams を用いたデジタル申請・承認フローを構築し、証跡管理と効率化を図っている。

⑤コストを抑えた二要素認証の工夫

高価な IC カードの代わりに安価な IC タグと顔認証を組み合わせることで、委託業者を含む全利用者への展開し、全体のコストを抑制している。

２−１−２．病院 B

①現場と医療情報室を繋ぐ「コメディカル兼務」体制

診療放射線技師等の医療職 7 名を医療情報室兼務とし、「医療情報室と現場とのパイプ役」として午前は臨床、午後はシステム保守を担うことで現場感覚を運用に反映している。

②CAD 図面を用いた IT 資産の視覚的配置管理

端末 PC の設置場所をエクセル台帳だけでなく CAD（図面）上でマッピングし、物理的な所在を直感的に把握できるように整えている。

③独自規約による複数ベンダーのリモート管理

医療情報室が作成した「リモート規約」の遵守を全 22 ベンダーに義務付け、接続の主導権を病院側で保持している。

④脆弱性情報の能動的な収集体制

特定のベンダーからの連絡を待つだけでなく、IPA、JPCERT/CC 等のサイトから自ら情報を入手し、脆弱性への対策を検討する習慣が定着している。

⑤課題抽出のための机上訓練

IT-BCP の訓練を通じ、「現場と医療情報室を仲介する人員の不足」といった具体的なリソースの限界を事前に洗い出し、対策に活かす取り組みを実施している。

2−1−3．病院 C

①経営層が主導する病院内 CSIRT

医師でもある副院長を CSIRT 委員長に据え、グループ企業本社の CISO 体制と密に連携することで、経営と医療の両面からセキュリティを統制している。

②MDS/SDS における「曖昧回答」の徹底追及

ベンダーからの回答で「×」や「空欄」がある場合、必ずその理由を確認し、回答の曖昧性を排除した上でリスク評価を行っている。

③グループ企業本社基準による月次の脆弱性監査

グループ企業本社の基準に基づき、毎月のサーバセキュリティ監査を実施し、リスクの高さに応じて対策期限を厳格に管理している。

④全職種参加型「紙カルテ訓練」の実施

医療情報システムが停止したことを想定し、実際に医師や看護師ら 100 名が参加して紙カルテによる診療継続をシミュレートする訓練を実施した。

⑤カルテ不適切閲覧監査

「職員が入院した際の診療外閲覧」など、具体的なシナリオに基づいてカルテ監査を 6 ヶ月ごとに実施し、抑止力を高めている。

2−1−4．病院 D

①高度有資格者による組織的統治

情報処理安全確保支援士（登録セキスペ）かつ上級医療情報技師の資格を持つ責任者が実務を主導し、専門性の高い判断を院内で行える体制を構築している。セキュリティ対策に関する経営層への働きかけも積極的に行なっている。

②OS レベルからの実機リストア訓練の完遂

バックアップを取得するだけでなく、2025 年に OS レベルからの復元訓練（リストア）を実施し、実際にシステムを戻せることを技術的に確認した。具体的には、2 種類の仮想化基盤（VMWare、Nutanix AHV）において、稼働する VM（OS レベル）を Veeam Backup & Reprication にてバックアップし、そのバックアップデータを用いて同一基盤への復旧と異なる基盤への復旧が実現できるかを訓練した。

③セキュリティパッチ適用不能機器への「EDR」による補完

動作保証等の理由でセキュリティパッチが適用できないレガシー機器に対し、EDR を導入して常時監視を行うことで、リスクを許容範囲内に収める現実的な解決策を講じている。

④現場スタッフとの IT-BCP マニュアル共同策定

医療情報課員だけでなく各現場のスタッフを含めた複数名で IT-BCP マニュアルを作成することで、臨床現場で機能する実効性の高いマニュアルを整備している。

⑤本社報告フローと連動した資産の全数棚卸の定例化

毎年にグループ本社への IT 資産報告を行うタイミングに合わせ、資産管理ソフトを用いた全数棚卸を業務ルーチンとして完全に定着させている。

3．訪問インタビュー調査対象の 4 病院の取り組みに関する相互チェックと分析

各病院の対策を比較・検証すると、「100%の防御」という考え方から、「いかに早期に検知し、いかに迅速に復旧するか」というレジリエンスを意識した取り組みとなっていることが確認された。具体的には次の 5 点について示す。

（1）体制と人材の多様性

病院 C はグループ全体としての組織力を背景に、本社の CISO 体制と連携した非常に強固

なガバナンスが構築されていた。一方で、病院Bのような自治体病院では、行政職の人事サイクルという制約の中で、現場を熟知したコメディカル職員を兼務させることで「知識の橋渡し」を行っている点は組織を設計する上で参考になると考える。病院 D は、上級医療情報技師や情報処理安全確保支援士（登録セキスペ）といった高度な資格を持つ職員を核として、限られた体制の中でも専門性を担保している。

（2）「水際」でのガバナンス強化

病院 A は、過去のインシデント経験から「セキュリティレベルが低い機器は導入を許可しない」という非常に強い拒否権を医療情報部門が持っている。病院 B も同様に、物品管理担当部署と連携して「医療情報部門の許可なしには機器を購入できない」という仕組みを構築しており、組織的な管理体制整備が共通の有効手段となっている。

（3）バックアップと復旧の実効性

病院 A がクラウド環境上で参照系サーバを 24 時間以内に復旧させる検証を行っている点と、病院 D が OS レベルからのリストア訓練を実際に行っている点は、他施設においても参考とされたい事例となる。多くの施設が「バックアップの取得」に取り組む中、この 2 施設は、バックアップからの復元検証が実現できている。

（4）「形」から「質」への移行

厚労省のガイドラインに沿った体制（CISO の設置や IT-BCP の策定）は整備されつつあるが、その体制が実際の有事発生時に実行できるかが重要となる。策定した組織体制やマニュアルは、定期的に自施設の環境に合わせて見直す必要がある。実際には、訓練を通してマニュアルを見直すきっかけとすることができる。

（5）専門人材不足への「現実的な解」の提示

高度な専門人材を即座に採用することは困難であるが、病院 B のように「現場の知恵（コメディカル）」と「管理の知恵（行政・情報職）」を融合させることで、自立した管理が可能になると考える。

4．具体的な対策事例とその効果

訪問インタビュー調査結果から、医療機関において参考になる具体的な対策事例について示す。特に、必ずしも多額の予算を必要とせず、「運用のルール化」や「既存の人的資源の再配置」などによって比較的実現可能なものをまとめた。自施設の規模や実態に合わせて、自施設の取り組みを振り返り、さらなるセキュリティ対策に向けて参考にされたい。

（1）【人的リソースの工夫】 コメディカル兼務制度（病院 B）

○具体策：放射線技師や臨床検査技師、ME などを情報部門の兼務とし、自部署のシステムメンテナンスやトラブル対応の「窓口」とする。

○効果：情報部門に現場のニーズが正確に届くようになり、同時に現場側へのセキュリティ意識の浸透（啓蒙）がスムーズになる。

（2）【ガバナンスの工夫】 購入前チェックリストの徹底（病院 A・B）

○具体策：医療機器の導入時、契約書に判を突く前に、情報部門が作成した「セキュリティ要求事項」にベンダーが回答し、それを満たさない限り導入させない運用にする。

○効果：把握不可能な外部接続ポイントの発生を防止し、管理可能なアタックサーフェスを維持することができる。

（3）【実効性の工夫】 OS レベルのリストア訓練（病院 D）

○具体策：データのバックアップだけでなく、バックアップ管理ツールを用いて、OS や設定

情報を含めて丸ごと復旧させる訓練を定期的（年１回程度）に行う。
○効果：有事の際、「手順書はあるが実行できない」という最悪の事態を防ぎ、復旧までに必要な作業や正確な時間を経営層に報告できるようになる。
（４）【訓練の工夫】 100 名規模の全職種参加訓練（病院 C）、異常検知連絡訓練（病院 D）
○具体策：紙カルテを用いた診療継続訓練を、医師・看護師だけでなく事務部門も含む大規模なものとして実施する。また、現場で異常を検知した際に、マニュアルに従い初動対応ができるかを訓練する。
○効果：システム停止が「情報部門の問題」ではなく「病院全体の診療継続の問題」であるという共通認識が生まれ、インシデント発生時にすべきことを確認できる。
（５）【資産配置場所の把握】 資産配置場所のマッピング（病院 B・C）
○具体策：エクセル台帳だけでなく、CAD 図面（フロア図）上に端末 PC の配置場所を視覚的にプロットする。
○効果：インシデント発生時（特定の端末が通信遮断の対象になった際など）、その端末が「物理的にどこにあるか」を即座に特定でき、初動対応を加速させることにつながる。
（６）【資産管理ツールの活用】 専用の資産管理ツールの導入（病院 B・C・D）
○具体策：資産管理ツールを導入することで、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。
○効果：ひとつのツールで複数のセキュリティ対策に寄与できる。医療情報部門の管理工数削減にも期待できる。

５．医療情報セキュリティ対策の深化と「病院 D モデル」の意義

訪問インタビュー調査対象の 4 病院の調査結果を俯瞰すると、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いると考える。その中でも特に病院 D の取り組みは、多くの医療機関が直面する課題に対する「標準的な対策事例」として示される。

まず、「専門性の内製化」が重要な成功要因となっている。病院 D では、情報処理安全確保支援士と上級医療情報技師を保持する責任者が指揮を執り、外部ベンダーに依存しすぎない自立した意思決定を行なっている。これは、病院 B がコメディカルを巻き込んで知識を共有している事例と同様に、「現場を理解した専門家」が院内にいることの強みを象徴している。次に特筆すべきは、病院 D と病院 A に共通してみられる「検証の文化」である。多くの施設がアンケート調査結果等で「バックアップは取っているが復旧訓練は未実施」という課題を抱える中、病院 D は実際に OS レベルからのリストア訓練を成功させている。さらに、セキュリティパッチの適用に向けて取り組む必要性は理解できるものの、実際には適用に至っていない医療機関が多い。全ての機器にセキュリティパッチを適用することは重要であるが、医療現場ではアプリケーションの動作保証がされない等、様々な要因により困難な場合が多い。これに対し病院 D は、セキュリティパッチ未適用の機器にも EDR で重点監視するというリスクベースのアプローチを採用している。これは病院 A の「ネットワーク隔離」や病院 C の

「MDS/SDS の徹底査読」と並び、リソースが限られた中で最大の効果を上げるため戦略のひとつといえる。セキュリティパッチを適用する場合は、パッチが提供された際に、その重要度を確認し、適用タイミングを調整することが重要である。パッチ適用においてシステム停止が伴うケースもあり、複数のパッチをまとめて適用するようなスケジュールも検討されたい。

最後に、「現場の巻き込み」が形骸化を防ぐことにつながると考える。病院 D が IT-BCP 策定に向けた作業を医療情報課員に加え、現場スタッフを参画させたことは、セキュリティを「医療情報部門だけの問題」から「病院全体の診療継続の問題」へと意識改革の一つになったと想像する。総じて、訪問インタビュー調査結果から、これらの先進事例から学べるのは、高度な専門知識に裏打ちされた「実効性の証明」と、現場・経営層を巻き込んだ「組織的な合意形成」を両立させることの重要性であると考える。これらの知見は、専門人材の確保に悩む多くの医療機関にとって、既存のリソースをいかに再配置し、実戦的な体制を築くべきかという具体的な参考事例になるといえる。

6.システムベンダーに対するインタビュー調査

医療機関に対して実施した訪問インタビュー調査内容を踏まえて、電子カルテベンダーに対してオンライン形式でインタビュー調査を実施した。本調査から認識したこと、また課題とされることについて次に列挙する。

・セキュリティ対策として、医療機関側の要求に応じて対応しているベンダーがあった。

・製造元ベンダー、導入ベンダーが異なる場合は、導入ベンダー側でセキュリティ対策に関する方針が提示されるケースもある。

・電子カルテベンダーからの積極的なセキュリティパッチ情報の提供がない。

・システム稼働後に OS やミドルウェア等のパスワード変更等が医療機関から要求された場合、作業を担当する人材が不足しているために対応が困難となるケースがある。技術的な問題よりも、工数（リソース、コスト）の捻出が問題となる。

・ベンダーによっては医療機関側からの働きかけがなければセキュリティ対策の提案が十分に及んでいないケースもある。

得に、電子カルテ導入においては、製品の製造元ベンダーと導入を担当するベンダーが異なる場合も多く、両者間でサイバーセキュリティ対策への意識が異なるケースがあることが明らかとなった。各医療機関においては、これらの乖離についても着目した上で、システム導入作業を行うべきである。両者に乖離が生じた場合は、チェックシートを基に取り組むべき対策について医療機関からも提示した上で、ベンダー関係者内でもその理解を深め、医療機関とベンダーの相互理解に取り組む必要がある。

D. 考察

本研究から、医療情報システムのサイバーセキュリティ対策においては、チェックリストが「対策の方向性を示す有効な指針」である一方、現場の実情に合わせた理解と運用のためには、具体的な取り組み案を提示することが不可欠であることが示唆された。

特に、形式的な対応にとどまらず、具体的にチェックリストの項目が求めていることを明示し、担当者によってその解釈が異なることがないように示すことが必要と認識した。なぜその対策が必要なのかという考え方の共有や医療業務の特性を踏まえた実践的な運用設計が、継

続的な対策実施において必要な要素になると考える。また、積極的に取り組みを行っている医療機関の事例は、他の医療機関にとって有用な参考情報となり得ることから、今後は事例共有の仕組みづくりも重要な課題である。その一つとして、地域の医療機関同士で日頃からセキュリティ対策に対して共有できる組織を構築することも検討されたい。滋賀県では「滋賀県病院医療情報システム担当者の集い」が 2024 年から年 3 回実施されている。事務局は大津赤十字病院が務め、企画運営の中心を担っている。日頃から医療機関の担当者同士が交流することで、共助できる関係性の構築が可能となり、万が一サイバーインシデントが県内の医療機関で発生した際にも支え合うことのできる関係性が構築できると考える。

また、医療機関の多くはセキュリティ対策の必要性は理解されており、調達仕様に含めるべきであるとの考えは今後も必要となる。一方、セキュリティ対策を行うことは、調達全体のコストが高くなるという懸念も生じる。その中で、ベンダー側も費用を明確にしたうえで、標準提案として、セキュリティ対策レベルを厚労省ガイドラインやチェックリストが求めるレベルにまで引き上げ、その上で対応することが必要と考える。また、現在製品として提案されるシステムの多くは、標準機能にセキュリティ対策が含まれていないケースもあり、対策を加えるたびにコストが増加し、セキュリティ対策を投資として捉えることができない状況になるのではないか。実際には、標準機能にセキュリティ対策があらかじめ含まれたかたちで調達範求められる。今後は、医療機関の実態を踏まえた取り組み事例の共有や、チェックリスト自体の継続的な見直しを通じて、現場に即した形で実効性のあるサイバーセキュリティ対策が実囲の検討を開始し、不要とされる対策をその範囲から除外する等の流れにすること必要と考える。ベンダー側が「提案できる」のであれば、できることを適切に提案し、そこから施設の実情によって対策を検討できるような提案方式が実現されることを期待したい。電子カルテパッケージにセキュリティパッケージとしての適用を標準として展開されることを提案したい。

E. 結論

本研究では、「医療情報システムのサイバーセキュリティチェックリスト」に基づく医療機関の取り組み状況を、アンケート調査およびインタビュー調査により把握・分析した。

その結果、チェックリストは一定の対策水準を担保するための有効な枠組みである一方、運用面においては医療現場の実態との間に課題が存在することが明らかとなった。医療機関における対策の方向性を示す上で有効な指針である一方、その趣旨や考え方が十分に共有されていない場合、形式的な対応にとどまる可能性があることが示唆された。特に、医療機関においては、診療業務の特性や人的資源の制約を踏まえた運用が不可欠であり、チェックリストの各項目について「求められる背景・目的」を理解した上で、各施設の実情に応じた実装が重要であると考えられる。

今後は、医療機関の実情を踏まえた好事例の共有や、現場に即した形で実践可能なチェックリストの改善を通じて、医療機関における実効性の高いサイバーセキュリティ対策の推進が施される環境づくりが求められる。

積極的に取り組みを実施している医療機関においては、経営層の関与のもとで体制整備が行われていること、また医療現場の負担を考慮

した現実的な運用ルールの工夫がなされていることが確認された。一方、人材・時間・予算の制約、チェックリストの解釈の難しさといった課題も見受けられたことから、各医療機関は、「人員と予算の制約」という課題を抱えながらも、チェックリストを最低限取り組むべきセキュリティ対策として捉えて、運用ルールの徹底や既存資産の有効活用によって、実効性のある対策を模索し続ける必要がある。今後も時代に応じたチェックリストへの改版と、それに対して具現化して取り組むことができるかを検証しながら取り組む必要がある。

また、積極的に取り組みを行っている医療機関の事例は、他の医療機関にとって有用な参考となることから、こうした事例を共有する仕組みの整備や、チェックリストの分かりやすさ・実装容易性を高める工夫も検討すべき課題である。

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

・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.

・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ー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.

・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.

・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.

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

別添資料4：訪問インタビュー調査結果の要約

該当チェックリスト／調査項目	病院A	病院B	病院C	病院D
病院区分	地方独立行政法人	自治体	企業	公的
インタビュー実施日	2026年2月10日	2026年2月20日	2026年2月24日	2026年3月1日
医療情報部門の体制	医療情報部（部長は医師）の下に情報企画室があり、常勤5名、非常勤2名、委託ヘルプデスク6名で構成される。診療情報管理室なども含め、組織全体で専門実務を分担している。	医療情報室。室長（医師）、行政・医療職の副室長等に加え、情報システム係5名（行政職4名、臨床工学技士1名）が所属。さらに、現場と兼務するコメディカル7名が実務を支援する体制である。	事務統括室 経営支援・デジタル変革G 情報管理T。兼任1名、専任6名に加え、常駐委託8名が実務を分担。グループ本社のCISO体制および病院内CSIRT（副院長が委員長）と連携した重層的な組織構造である。	事務部 医療情報課（課長は事務職）。48名体制（情報システム係12名、診療情報管理係11名、診療支援係25名）。システム運用・セキュリティに関与する実務メンバーは、情報システム係の常勤・委託職員が中心となる。
【医療情報システム安全管理責任者を設置している。(1-①)】	インシデント経験からセキュリティ意識は非常に高いが、対策費用の捻出には理事長や機構本部の理解・承認を要するプロセスとなっている。情報処理安全確保支援士の資格を持つ責任者を配置。	情報処理安全確保支援士の有資格者を配置しているが、行政職の人事は本庁主導であり、継続的な人材育成や専門性の維持が組織上の課題となっている。	医療情報システム安全管理責任者を設置し、実務レベルでは高度な専門知識を持つ兼務職員（主幹級）が、具体的な立案や運用を主導している。	医療情報システム安全管理責任者は情報処理安全確保支援士（登録セキスペ）および上級医療情報技師の資格を持つ。主な実務担当者4名が有資格者と密に連携して対応にあたっている。
【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)】	エクセルで管理。電子カルテ関連機器はリース契約に基づき把握されている。	資産管理ソフト「SKYSEA」で電子カルテネットワークを管理。IoMT管理システムにより、IPアドレスだけでは不明な機器の可視化も実現している。	グループ本社の資産管理システムに加え、エクセルや専用ツールで管理。年1回、約50時間をかけて全数棚卸を実施。	資産管理ソフト「SS1」にて管理。日本赤十字社本社への報告のため、毎年9月頃に全数棚卸を実施している。情報資産危険性自動評価技術「xDome」を採用し、院内ネットワークに接続される機器を可視化する。
【リモートメンテナンスを利用している機器の有無を確認した。(2-②)】	13回線の外部接続点を把握。独自チェックリストでセキュリティレベルを確認し、基準に満たない場合は導入を許可しない運用を徹底。	16回線、22ベンダーのリモート接続を把握。独自作成のリモート規約遵守とチェックリストによる対策確認を全ベンダーに実施している。	推奨環境（Tunaclo等）を整備し、約30社が利用。個別回線も一覧表で管理し、保健所の立ち入り検査に合わせて棚卸を予定している。	独自回線と集約回線を併用。リモート接続時は医療情報課に連携する運用としているが、病院側の意向が反映されにくい点は課題としている。
【医療情報セキュリティ開示書（MDS/SDS）を提出してもらっている。(2-③)】	現状はシステムベンダーからのみ取得。立入検査時に提示するに留まっており、内容を確認した上での具体的なアクションには至っていない。	取得はしているが、その後の具体的なアクションは未実施。新規契約時には、自治体作成の約款や特記事項による合意形成を重視している。	MDS/SDSの回答で「○」以外がある場合はベンダーに理由を確認。回答の曖昧性を排除し、効率的なフォローを行っている。	関係性のあるベンダーからは毎年取得している。ただし、内容を詳細にレビューして協議を行う等の取り組みまではできていない。
【職種・業務別のアクセス利用権限設定／不要アカウントの削除。(2-④、2-⑤)】	電子カルテやM365のユーザー管理を情報企画室で一括実施。OSログインのロックアウト設定は全台対応済みである。	電子カルテの標準設定に準拠。部門システムについては、各部門のシステム担当者が管理を行っている。	職種・担当業務別に権限を設定。人事部門からの連絡に基づきIDを停止。未使用IDの停止についても検討中である。	職種別に権限を設定し、人事情報をベースに適宜削除・無効化を実施。デフォルトパスワードから独自パスワードへの変更を推進している。
【アクセスログを管理している。(2-⑥)】	syslogサーバで全サーバログ（1年間）を管理。SKYSEAも導入済みだが、日常的なチェックまでは手が回っていない。	SKYSEAで端末操作ログを収集。ネットワークにはsyslogサーバを設置しているが、障害時以外に参照することはない。	電子カルテ標準機能で収集。6ヶ月ごとに不適切利用監査を実施し、セキュリティ管理者が分析を行っている。	資産管理ソフトSS1で端末ログを管理。サーバOSログの毎日チェックを試みたが、業務負担は大きい。
【セキュリティパッチを適用している。(2-⑦)】	端末は月1回、サーバは3ヶ月に1回、システムを停止して適用。事前にテスト環境で検証を行っている。	現状は未対応。次期更新時にベンダーのパッチ管理ソリューションを採用し、自動または半自動での運用を検討中。	年1回のサーバセキュリティ監査で脆弱性を検査し対策。グループ本社の合格基準を満たす必要がある。	ベンダーからの提案に基づき実施。外部接続用のネットワーク機器は、情報を認知後速やかにアップデートを行う運用である。
【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。(2-⑩)】	電子カルテ端末に顔認証＋ICタグを導入済み。サーバやネットワーク機器については今後検討予定としている。	端末PCについては次期システム更新で対応予定。ネットワーク機器では病院配布の証明書を用いた所持認証を併用している。	現状は1要素だが、2027年の更新時に端末PCの二要素化（顔認証＋ID/PW）を計画。	救急時閲覧端末には実装済み。その他の端末やサーバについては、基幹システムの更新時に順次実施する予定である。
【USBストレージ等の外部記録媒体の接続を制限している。(2-⑨)】	資産管理ツール「SKYSEA」で制御し、電子カルテ端末は原則不可。データの出力が必要な際はTeamsでの申請制としている。	デバイス管理ツール「ポートシャッター」および物理的なUSBキャップで制限。利用時はソフトウェアで期限付き許可を与える申請運用を実施。	事務用PCは「秘文」、電子カルテPCは専用ツールで制御。持出しが必要な際は、情報管理担当が作業を代行する。	資産管理ツール「SS1」の機能を活用し、電子カルテおよび部門システムの端末・サーバ日体して導入し。技術的な接続制限を実施している。
【バックアップの実施と復旧手順の確認。(3-②)】	テープとクラウドで管理。クラウド上で参照系を24時間以内に復旧させる検証を実施済みである。	今後はデータセンターへのバックアップ（クラウド＋オンプレ）に移行予定。イミュータブルなバックアップも作成する。	多重管理（DB内、LTO、遠隔地DC等）を実施。サイバー攻撃対策としての新たなバックアップ整備も検討中である。	2021年から統合バックアップ基盤「Veeam」を構築。2025年にはOSレベルでのリストア訓練を実施し、復旧可能性を確認済み。仮想化基盤は2種類の基盤で稼働させており、有事を想定して意図的に別の基盤アプリケーションとした
【サイバー攻撃を想定したBCPを策定している。(3-③)】	IT-BCPと自然災害BCPの両方を整備している。	厚労省のひな形を活用して策定。机上訓練を実施したが、現場との仲介人員不足が課題として浮き彫りになった。	グループ本社の体制と連携し1年かけて策定。紙カルテを用いた100名規模の訓練やシステム訓練を実施している。	厚労省のひな形をベースに独自マニュアルを整備。毎年訓練を実施し、その結果をマニュアルに反映させている。特に「異常検知連絡訓練」では、マニュアルに示される内容に準じて職員が行動できるかを訓練する。

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)
分担研究報告書

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

研究分担者　鳥飼　幸太　群馬大学医学部附属病院システム統合センター　准教授

研究要旨
本分担研究では、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対応の実効性を検討するため、E 病院および F 病院に対して、情報システム管理体制、マンパワー、チェック方法、ベンダー対応、IT-BCP 等に関するヒアリングを行った。E 病院では、専任職員と委託・派遣職員を組み合わせた体制のもと、資産管理、外部接続点管理、SDS 確認、特権アカウント管理、外部記憶媒体制御、イミュータブルバックアップ等の対策が進められていた。一方、長期にわたり病院情報システムの監修・保守・更新を担ってきた職員の経験知を、後進にどのように移転するかが課題として認識された。F 病院では、臨床検査技師としての現場経験を起点に病院情報システム管理へ職域を拡張した人材が中心となり、組織的な医療情報部体制の整備、人材確保、ベンダーへの具体的指示、費用制約下での重点的対策が進められていた。両施設の結果から、チェックリスト対応は単なる項目充足ではなく、医療情報システムの運用知識、ベンダー調整能力、後継者育成、診療報酬・補助制度を含む資源配分の設計と一体で評価する必要があることが示された。

A. 研究目的

医療機関では、電子カルテ、オーダリング、部門システム、ネットワーク、外部保守接続、医療機器接続が診療機能の基盤となっている。サイバー攻撃やシステム障害により医療情報システムが利用困難となった場合、患者情報の閲覧、指示伝達、検査・処方・会計等の業務が制約され、医療安全と診療継続に影響する。厚生労働省の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、各医療機関が優先的に取り組むべき項目を示す一方、実装可能性は病院規模、既存システム構成、人材配置、ベンダーとの責任分界、予算制約に左右される。本分担研究の目的は、チェックリストへの対応が進む医療機関へのヒアリングを通じて、項目充足を支える組織能力、運用上の制約、後継者育成と知識移転に関する課題を整理し、持続可能な医療サイバーセキュリティ対策の実装条件を明確化することである。

B. 研究方法

令和 8 年 2 月 19 日に E 病院、令和 8 年 2 月 20 日に F 病院を対象として、現地または Web 会議を併用した半構造化ヒアリングを実施した。E 病院では、病院情報システム部門の担当者から、医療情報部門の体制、電子カルテ・ネットワーク・セキュリティ関連ベンダー、資産管理、外部接続点、MDS/SDS、利用者管理、ログ管理、パッチ管理、二要素認証、外部記憶媒体、バックアップ、IT-BCP に関する回答を得た。F 病院では、医療情報部門の形成過程、人材確保、資格取得、インターン受入、ベンダー調整、費用制約と診療報酬制度に関する課題について聞き取りを行った。調査では患者個人を識別

する情報を収集せず、施設の組織体制、運用方法、情報システム管理上の課題を対象とした。倫理面への配慮として、報告書では個別患者情報および機微な設定情報を記載せず、医療機関の実務改善に資する範囲で結果を整理した。

（倫理面への配慮）

本研究の施設へのインタビュー調査結果は具体的な施設が特定できないよう仮名化したうえで報告する。

C. 研究結果

E 病院は 950 床の特定機能病院であり、医療情報部門は専任 7 名、兼務 7 名、嘱託 3 名、委託・派遣 3 名から構成されていた。電子カルテは HOPE EGMAIN-GX で、構築ベンダーは富士通 Japan、ネットワーク機器は Cisco、ネットワーク構築は住友電設、セキュリティ対策ではセイコーソリューションズとのやり取りが多いとの回答であった。

1. E 病院における体制と運用

同院では、資産管理について Excel と SS1 を併用し、今後は ARMIS による収集を予定していた。ネットワークに接続していない機器や旧機器の網羅性には課題があり、部門管理機器を含めた資産把握が継続的な検討対象であった。外部接続点についてはルータおよびファイアウォールを管理し、リモートメンテナンス事業者を Excel で把握していた。リモート接続は申請制とし、SDS を用いてセキュリティ対応状況を確認していたが、ポケット Wi-Fi 等による把握外接続の可能性が課題として認識されていた。MDS/SDS は立入検査対応として収集が進められており、リモートメンテナンス事業者には SDS 提出と内容確認を求めていた。

利用者管理では、委託先ベンダーのアカウント情報漏えいを契機に特権管理者のパスワードをランダム生成の 13 桁へ変更し、台帳管理を行っていた。人事情報と連動したアカウント発行・停止、出向時の職種変更、申請書に基づく権限付与が実施されていた。OS のパスワード管理はシステム部で行う場合が多い一方、ミドルウェアやネットワーク機器の利用者設定は各ベンダーに依存する部分が残っていた。ログ管理ではサーバの eventlog/syslog、ネットワーク機器の syslog 集約、踏み台サーバにおける操作動画記録が実施または導入途中であったが、ログ相関分析は困難であり、通常時の解析は限定的であった。

セキュリティパッチについては、WSUS を用いて適用可能なサーバ群に半年に一度を基本として対応し、緊急度の高い脆弱性では IPA の情報等を参照しながら随時対応していた。アプリケーションやミドルウェアについてはベンダー側の製品サポートや運用設計が制約となり、閉域網前提の運用感覚からの移行が課題であった。二要素認証は一部部門でアプリケーションを利用し、令和 9 年 1 月に電子カルテ端末での適用を予定していた。外部記憶媒体は SS1 によるシリアル番号制御と物理的な USB ストッパーにより制限されていた。バックアップは Rubrik によりイミュータブルなバックアップを取得し、IT-BCP はシステム部で約 3 か月をかけて作成し、年 1 回の机上訓練を開始していた。

ヒアリングでは、30 年にわたり病院情報システムの監修、保守、更新を担ってきた職員の経験知が、迅速な障害対応、調達段階からの介入、資源配分の判断を可能にしてきた点が確認された。一方で、その経験知が個人に蓄積されているため、定年退職後に知識と技能が現

場に適用されにくくなることが課題として示された。若手職員は後進として情報システム課に配属され、引継ぎと OJT を受けているが、情報システム立ち上げ時の段階的成長を経験していない。着任時点で高度化、複雑化、大規模化した病院情報システムと向き合う必要があり、技術的課題と心理的負担が同時に生じることが明らかとなった。

2. F 病院における体制形成と人材確保

F 病院では、K 氏にヒアリングを行った。K 氏は入職時に検体検査技師として勤務し、検体検査領域の電子化に関与する中で、電子カルテやオーダリングシステムを含む病院全体の情報システム管理へ業務範囲を拡張してきた。組織への働きかけにより医療情報部が組織され、職員が加わることで現在の体制に至った。K 氏は上級医療情報技師の資格を取得し、T 大学医療情報学科からのインターン生を受け入れるなど、専門知識を有する人材の確保に取り組んでいた。

同院では、公的・準公的な病院組織に共通する人事枠の制約の中で、急速に拡大するサイバーセキュリティ要求に対応する人材登用が容易ではないとの認識が示された。電子カルテを担当する富士通 JAPAN 株式会社をはじめ、IT ベンダーの対応品質は担当者のスキルにより差が生じるとのコメントがあり、医療機関側が十分な知識を持ち、ベンダーに対して具体的な指示を出せる能力が重要であることが確認された。保険収載の枠組みの中で医療を提供する医療機関にとって、近年新たに求められるサイバーセキュリティ対策は、診療録管理体制加算等の制度的支援の拡充とともに、人材拡充を必要とする領域であった。

3. G 病院における体制形成と人材確保

G 病院では K 氏にヒアリングを行った。事務部門である医事課医療情報係によって資産管理が行われている。サイバーセキュリティ強度確保のため、固定 IP アドレスと MAC アドレスの紐づけを行い、任意の端末/サーバを院内 LAN に接続しても動作しない運用となっている。2025 年までは中央放射線部で検査機器のローカルアドレス運用を行っており、2026 年度の PACS 更新によってアドレスの一意化を行う予定であることが確認された。各診療科や診療支援部門からの端末要求は文書により行われ、週次定例の場にて払い出し/修理持ち込みの件数が把握されている。G 病院では 2011 年 3 月に東日本大震災で計画停電に見舞われたこと、夏季に落雷が多く停電が頻発する地域であることから、2013 年に非常用発電機を 200kW 追加し、停電時にはうち 1000kW を電子カルテが設置されている外来棟に給電する運用規定を定めている。

利用者管理として、8 桁 ID 化とパスワード有効期限 60 日の運用を行っている。最短パスワード長の制限、シンクライアント端末における IC カード認証ドライバの適用に課題が生じている。セキュリティパッチについては、適用可能なサーバ群に対応し、緊急度の高い脆弱性では IPA の情報等を参照しながら随時対応していた。EDR/XDR(Trend Micro 社)のアップデートにはオンライン接続によるパターンファイルのダウンロードを随時行うことで対応している。EDR には機械学習型挙動監視が有効化されており、端末の操作ログ確認の代わりに、不審な操作（許可されていないソフトウエアのインストールなど）を行うと検知されネットワーク隔離が自動で行われる。EDR/XDR のスキャン範囲は攻撃されやすい temp ファイルを含めていることが確認され、

動作障害を起こしやすい SQL を多用するプログラムに対しては EDR から証明書を発行し、検知除外を行いつつプログラムの真正性を担保するようにしていた。外部記憶媒体は管理側ソフトウエアにより、許可された USB のみを運用可能な方法としていた。バックアップは電子カルテ本体(PureStorage)によるイミュータブルなバックアップ、NEC 製 IStorage によるイミュータブル相当機能のバックアップ、参照系システムによるバックアップ、大学病院情報システムバックアップ(Gemini)により取得していた。IT-BCP はシステム部で 2024 年 11 月に作成され、内閣府が主催する分野横断型演習、全分野演習に対し、病院長、情報基盤センター長、CSIRT、電子カルテベンダー、PACS ベンダー、ネットワークベンダー、サーバベンダーのサプライチェーンが合わせて参加し、年 1 回の机上訓練を継続していた。人材確保については、大学教員側 3 名、事務職員側 7 名の 11 名体制で行われている。大学教員と電子カルテベンダー、ネットワーク/セキュリティベンダー、サーバベンダーが月 1 回保守会議を行い、1 か月内でのトラブル対応、アップデート対応などの報告受け、ならびにシステム全体に関係する調整事項の検討とアクション化を行っている。この方法では、運用年数の増加によりベンダー側にも保守スキルが蓄積することから、大学職員側が入れ替わった場合においても、ベンダー側からのスキル情報提供を継続できる。事務職員側で異動が生じるが、部署で専門職員として登用された職員が技術の維持やスキル伝達を行っている。またローテーションが医事課で行われることが多く、10 年程度で再び同じ部課に戻ることもあることから、現状では大きなスキル損失に至っていない。併せて、常駐ベンダーによる保守の中にセキュリティ監視を契約として含めることでマンパワーの充足をはかっている。今後の課題として、災害発生時における院内 BCP とのより整合の取れたアクションマニュアルの整備、急増する検査システム等の外部ネットワーク接続状況の把握、継続的な資産管理の維持が挙げられる。

D. 考察

3 施設の結果から、医療機関におけるサイバーセキュリティ対策は、チェックリスト項目の実施有無だけで評価するよりも、医療情報システムの構成理解、運用手順、ベンダー調整、権限管理、ログ確認、バックアップ、BCP 訓練を継続的に実行できる組織能力として評価する必要がある。E 病院の事例は、高度な実務経験を持つ職員が病院全体の情報システムを長期に把握することで、複雑なシステム変更や障害対応を統合的に判断できることを示す。同時に、その能力が個人依存となる場合、退職、異動、体調不良により組織としての対応能力が低下するリスクが生じる。F 病院の事例は、医療専門職が現場業務の電子化を契機に医療情報システム管理へ発展し、資格取得、教育、インターン受入を通じて人材基盤を形成する実装経路を示す。

後継者育成では、完成した巨大な病院情報システムを一度に理解させる方法ではなく、資産、ネットワーク、認証、外部接続、バックアップ、BCP、部門システム連携といった単位に分解し、変更管理、障害対応、リスク評価を小さな実務単位として経験させる教育設計が有効と考えられる。Group A、Group B、Group C のような人材層別化は、大学病院・特定機能病院等が地域の指導的役割を担い、中規模病院が自施設の防御力を高め、小規模医療機関が外部支援を受けながら最低限の対策を実施する構造を設

計するうえで有用である。ベンダー対応のばらつきに対しては、医療機関側の要件定義力、SDS/MDS の読み取り、保守契約条件へのセキュリティ要件明記、パッチ適用と検証の責任分界の明確化が実務上の要件となる。

E. 結論

E 病院、F 病院、G 病院へのヒアリングから、医療機関のサイバーセキュリティ対策は、情報システム部門の人数、専門性、長期経験、後継者育成、ベンダー調整能力、財政制度と密接に関連することが確認された。チェックリスト対応を持続的に実行するためには、項目ごとの技術対策に加え、医療情報システムの構成を継続的に理解する人材の配置、経験知の文書化、OJT の段階設計、地域内での実地研修、診療報酬・補助金・資格評価を含む人材確保策が必要となる。今後は、ヒアリングで得られた知見を、チェックリスト項目の実装難度、必要人材、ベンダー責任分界、医療安全上の優先度に対応づけ、医療機関が実行可能な対策パッケージとして整理することが課題である。

F. 健康危険情報

分担研究報告書に該当する健康危険情報は認められない。

G. 研究発表

1. 論文発表

該当なし

2. 学会発表

該当なし

H. 知的財産権の出願・登録状況

（予定を含む。）

1. 特許取得

該当なし

2. 実用新案登録

該当なし

3.その他

該当なし

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）
分担研究報告書

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課題調査と解決策の検討

研究分担者　杉本賢人　大阪大学大学院医学系研究科 医療情報学　特任助教（常勤）
研究分担者　三上聡司　社会医療法人三上会東香里病院　院長

研究要旨
本研究では、厚生労働省の「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」をもとに、実際に医療機関へのインタビュー調査をもとに対応困難な項目とその要因を明らかにし、改善方針を示すことを目指す。
全国の医療機関を対象とした Web アンケートから、研究代表者、研究分担者が所属する医療機関を含めて 13 医療機関を選定し、インタビュー調査を実施した。本報告書では、そのうち、4 施設（大規模 2 施設、中小規模 2 施設）の回答結果について報告する。
いずれの医療機関もチェックリストを意識した対策を講じていたが、その程度は差があり、特に外部接続管理、アクセス権限・ログ管理、セキュリティパッチ適用などにおいて施設間で差異が認められた。大規模な医療機関では、予算をかけてセキュリティ対策を実施しているものの、どこまで対策するべきかといった費用対効果の判断が難しいという課題が示唆された。また、中小規模施設では専門人材の不足やコスト負担が大きな課題であり、十分なセキュリティ対策を講じるための運用面での課題もいくつか明らかになった。

A. 研究目的

本研究の目的は、厚生労働省が示す「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」について、それらの内容を元にしたアンケート調査を医療機関に行い、実際の医療現場で対応が難しい項目やその背景にある課題などを明らかにし、改善するための方針を提示することである。近年、医療分野では DX の推進とともにサイバー攻撃被害が増加し、実際に診療停止など地域医療に深刻な影響を及ぼす事案も生じている。しかし、既存のチェックリストには一部の医療機関で十分に対応できていない項目があり、そのままでは対策の遅れが継続するおそれがある。そこで本研究では、全国の医療機関への Web アンケート、対応できている医療機関へのインタビュー調査などを通じて、対応困難な項目とその要因を整理する。さらに、具体的な解決策などを検討し、全国の医療機関が活用しやすい、より実効性の高いチェックリストの整備を目指す。

B. 研究方法

まず、Web アンケートにより、「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」の各項目の対応状況と、未対応項目に対応できていない理由を全国の医療機関に調査する。さらに、アンケート結果を踏まえ、その結果から、複数の医療機関にインタビュー調査を実施する。

（倫理面への配慮）

本研究の医療機関へのインタビュー調査結果は具体的な医療機関が特定できないよう仮名化したうえで報告する。

C. 研究結果

インタビューに対応頂けるとの回答のあった医療機関のうち、本報告書では、4 医療機関（H 病院、I 病院、J 病院、K 病院）に実際にヒアリングを行い、対応状況の調査を実施した結果について報告する。

尚、H 病院、I 病院病院は病床数 600 以上の国公立大学病院であり、特定機能病院として地域の中核を担っている医療機関である。J 病院、K 病院は病床数 200 床程度の私立の医療機関である。それぞれの選定基準としては、病床数、規模が異なる医療機関に調査を行うことで、対応状況、サイバーセキュリティに関する考え方など異なる視点で調査する目的にある。

まず、全体としては、いずれの医療機関でも、対応可否の項目のレベルはあったものの、チェックリストを意識して対応を取っていることが分かった。

体制・人材については、いずれの医療機関でも、医療情報システム安全管理責任者（CISO）を配置しているとの回答を得た。H 病院、I 病院、K 病院では、CISO に医療情報システム、サイバーセキュリティに関する知識を有する人材を配置していたが、J 病院については CISO がサイバーセキュリティに関する十分な知識を有しておらず、組織として課題に感じているとの説明があった。

外部から医療情報システムネットワークに接続する回線については、H 病院および I 病院では、原則として自施設が設置するリモート接続の仕組みを用いた接続のみを認めていたが、例外的にベンダーが提供する仕組みによる接続も許可していた。 これに対し、J 病院および K 病院では、ベンダーごとの接続方法による外部接続を許可していた。ただし、接続されるすべてのリモートメンテナンス回線は把握しているとの説明があった。

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）については、いずれの医療機関でも事業者から提出を受けていた。

アクセス権限およびパスワードポリシーについては、調査医療機関で対応に差異がみられた。H 病院では、パスワードの文字数や複雑性に関する要件をベンダー側に求めていたほか、機器ごとに異なるパスワードを設定する運用としていた。一方、残りの医療機関では、サーバ保守作業等を基本的に特権ユーザーで実施しており、また、複数の機器群で同一のパスワードを設定しているとの回答があった。

ユーザー管理については、いずれの医療機関でも、有効期限などを設定し、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との回答を得た。

アクセスログについては、H 病院および I 病院では、すべての機器のアクセスログを保存しているとの回答が得られた。一方、J 病院および K 病院では、電子カルテのログ以外は保存できておらず、今後の課題として認識していた。

セキュリティパッチについては、医療機関ごとに対応の違いがみられた。医療機関および保守事業者が必要と判断するセキュリティパッチを定期的に適用している医療機関と定期的なパッチ適用が十分できていない医療機関があった。

インシデント発生に備えた対応として、いずれの医療機関でもオフラインバックアップを実施しており、複数世代で管理することで、データ消失や改ざんが生じた場合にも復元可能な体制を整備していた。復旧手順については、H 病院ではデータバックアップの復旧手順を確認するとともに、復旧の実証訓練を実施しており、インシデント発生時に速やかにシステム復旧へ移

行できる体制を整備していた。一方、J 病院では、データバックアップの復旧手順を医療機関として十分に確認できておらず、復旧体制の整備状況に課題がみられた。

いずれの医療機関でも、サイバー攻撃を想定した事業継続計画（BCP）を策定しており、初動対応、診療継続体制の確保、復旧までの対応フローを明確化していた。一方で、計画の定期的な見直しについては、いずれの医療機関でも十分には実施できていなかった。

D. 考察

体制・人材については、CISO の配置そのものは進んでいるが、その専門性や組織的な人材体制には医療機関間で差があることが示唆された。特に中小規模の医療機関では、高度な IT 知識と経験を有する人材が限られており、セキュリティ体制を継続的に構築・運用する上で大きな課題となっていた。病院情報システムの管理には、IT スキルに加えて医療現場の業務や環境への理解も求められるため、多面的な専門性が必要であるが、医療機関の処遇の枠組みの中では必ずしも十分に位置づけることが容易ではなく、人材確保や定着の難しさにつながっている可能性があるとの認識も示された。このことから、各医療機関が単独で必要な専門人材を確保・維持することには限界があり、一定程度の外部委託や、地域・複数機関での支援体制の構築も現実的な対応策として検討する必要があると考えられる。

H 病院では、医療機関とセキュリティを担当するベンダーとの間で定期的な打ち合わせを行い、関連システムの脆弱性の有無やセキュリティインシデントに関する情報共有の場を設けていた。このような取り組みは、医療機関が主体的にセキュリティの対策を進める上で有用な取り組みの一つと言える。一方で、こうした体制は病院情報システムの保守契約に付随して実施されている側面もあり、すべての医療機関で同様の取り組みを導入できる訳では無い。また、このような取り組みは医療機関側にも高い IT 知識と経験を有する人材が必要とされるが、上述のように、各医療機関がこのような人材を単独で確保・維持することは容易ではない。このことから、費用対効果の観点も踏まえると、医療機関ごとに個別対応を行うだけでなく、地域など一定のブロック単位で情報共有や支援を行う仕組みを整備することが、現実的な対応策の一つである。

外部接続については、医療機関側で基盤を構築し、統制する方式は、安全管理の観点から有用である一方、構築・運用上の負担が課題となる。特に中小規模の医療機関では、リモート接続基盤を自前で整備することは容易ではない。また、ベンダーによっては自社方式による接続でなければ保守対応が困難である事例も認められた。外部接続のあり方については、安全性が重要課題であるものの、一律に医療機関側で基盤を構築、維持することは現実的に困難であり、規模を踏まえた対策を検討する必要があると考える。また、大規模な I 病院では、医療機関で把握できていない古くから設置されている NW 機器の存在を否定できず、また、国公立大学病院特有の人材の流動性から引き継ぎが難しく、定期的な管理体制の維持の課題が挙がった。運用面の対策として、外部接続点を含む NW 機器を管理するツールなどの導入・活用が考えられる。

アクセス権限やパスワードポリシーについては、ランサムウェア被害の拡大を防ぐためには、侵入後に特権ユーザーが奪取されないこと、また他の重要なシステムへ水平展開されないことが重要である。この点で、特権ユーザーの運用

方法やパスワードポリシーは重要な対策と考えられる。パスワードの複雑性や機器ごとの個別設定を求める運用は、認証情報の使い回しを防止する観点から有効と考えられる。昨今はサイバーセキュリティ意識の高まりにより、特権ユーザーでの運用を前提とするシステムは減少しつつあるものの、インタビューを通じて、依然としてそのような運用を前提とする部門システムも存在することが明らかになった。アクセス権限やパスワードポリシーについては、医療機関側の運用見直しだけでなく、システムを提供するベンダー側の意識も同時に高める働きかけも重要であると考えられる。

アクセスログについては、保存の有無だけでなく、保存したログを実際に確認・活用できる体制の整備が重要とされる。この点について、J病院ではログの確認は行われていたものの、確認ポイントの判断や人的リソースの制約から、継続的な監視は容易ではなかったとの課題が挙がった。チェックリスト上は「定期的な確認」が求められているものの、現場では人的リソースや業務負担の面から長期的に継続することが難しいという実態が明らかになった。残りの医療機関も、ログは保存されているが、確認まではできていいないという状況であった。ログの性質として、確実に保存しておくという証跡管理の目的と不正アクセスなどを未然に防ぐ抑止の観点があるが、チェックリストではこの観点を分けて、医療機関が「どこまで対策できているか」を確認できるようにするのが望ましいと考える。

セキュリティパッチについては、医療機関単独では不可能であり、SE 作業が発生することが多く、この場合に保守契約にパッチ適用が含まれるかどうかで判断が異なる。セキュリティパッチの適用が保守契約に含まれていない場合、対応してもらうのが困難となる。今後のシステム更新ではセキュリティパッチの定期的な適用などを保守契約に含んでいくことがサイバーセキュリティの観点からは望ましいとされるが、セキュリティを高める対策を取ることで、システム費用はより高額になるため。費用対効果としては説明が難しいとの課題についても意見があり、経済的負担との両立が重要な検討課題であることが示された。また、モダリティ機器へのセキュリティパッチ適用は、ベンダー側から機器の安定稼働の面から適用できないケースがあるとの説明があった。この実情については、定期的なパッチ適用を期待するチェックリストとの乖離が生じており、医療機器の特性を踏まえた評価や代替的なリスク低減策を併せて検討する必要があると考えられる。

インシデント発生に備えた対応として、多くの医療機関でバックアップの取得や BCP の策定は進められている一方で、復旧手順の確認や実証訓練、計画の継続的な見直しといった運用面には課題が残されていると考えられる。したがって、インシデント対応の実効性を高めるためには、計画や体制を整備するだけでなく、それらを定期的に検証・更新する仕組みをあわせて整えることが重要である。

E. 結論

サイバーセキュリティチェックリストに沿ったインタビュー調査について、施設の規模や体制が異なる複数の医療機関に対して実施した。いずれの医療機関でも、チェックリストを意識した対応が取られていたが、実現項目については、医療機関で違いが見られた。いずれの医療機関でも重要性は強く認識されていたが、人材や専門性などの観点で対応できていない項目がいくつか見られた。人材・費用対効果の点から、全ての規模の医療機関に一律のレベルを要求することは現実的に困難であり、今後は地域・

複数機関での対策、医療機関の規模に応じた施策の提案などが期待される。

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

なし

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

別添資料X：訪問インタビュー調査結果の要約

該当チェックリスト／調査項目	病院H	病院I	病院J	病院K
病院区分	国公立病院	国公立病院	一般病院	一般病院
インタビュー実施日	2026年2月16日	2026年2月16日	2026年2月16日	2026年2月16日
医療情報部門の体制	医療情報部（部長は医師）の下に情報企画室があり、セキュリティについては、主に教員6名、研究員・技術職員3名で運用している。	教員1名、事務員2名、SE4名（常駐委託含む）で運用している。	情報システム管理室（放射線科医が室長）。6人で運用している（全員が臨床と兼務）。	院長1名、副院長1名の元、情報企画室2名で運用している。
【医療情報システム安全管理責任者を設置している。(1-①)】	医療情報システム安全管理責任者を設置しており、実務レベルにおいて、高度な専門知識を持つ教員が、具体的な立案や運用を主導している。	医療情報システム安全管理責任者を設置しており、実務レベルにおいて、高度な専門知識を持つ教員が、具体的な立案や運用を主導している。	医療情報システム安全管理責任者（病院長）を設置しているが、様々な対策を行うのに十分な体制とは言えない。	医療情報システム安全管理責任者（病院長）を設置しているが、様々な対策を行うのに十分な体制とは言えない。
【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)】	Excelにて台帳管理を行っている。	資産管理ソフト「SSI」で電子カルテネットワークを管理。	Excelにて台帳管理を行っている。	Pleasnter（WEBデータベースにて管理）と電子カルテのアプリで管理。
【リモートメンテナンスを利用している機器の有無を確認した。(2-②)】	自施設が設置するリモート接続の仕組み使った接続を原則とするが、ベンダー側の理由で例外を認めている。 古い機器で管理部門が把握・管理できていない接続点もあることが懸念。	20回線のリモート接続を把握。ベンダーが希望する場合に例外的にベンダー主導の回線を許容。	ベンダー個々の接続方法で接続を許可している（接続する全てのリモートメンテナンス回線を把握している）。	セキュリティ調査時にチェックした時に全体を把握している。リモートの運用ルールについてセキュリティが担保されたものを使っているかベンダーに説明を求めている。
【医療情報セキュリティ開示書（MDS/SDS）を提出してもらっている。(2-③)】	取得しているが、現状は具体的なネクストアクションには至っていない。	取得しており、必要に応じてベンダーへのヒアリングおよび対策を行っている。	取得しているが、現状は具体的なネクストアクションには至っていない。	取得しているが、現状は具体的なネクストアクションには至っていない。
【職種・業務別のアクセス利用権限設定／不要アカウントの削除。(2-④、2-⑤)】	すべてのユーザに対して個別のユーザIDを発行し、アクセス利用権限を設定している（一部、サーバについては不要アカウントの削除はできていない）。	すべてのユーザに対して個別のユーザIDを発行し、アクセス利用権限を設定している（一部、サーバについては不要アカウントの削除はできていない）。	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	すべてのユーザに対して個別のユーザIDを発行し、アクセス利用権限を設定している。退職時に手動で不要アカウントを削除している。
【アクセスログを管理している。(2-⑥)】	端末PCについてはアクセスログを残している。サーバについても一部の機器のアクセスログを残しているが、定期的には確認できていない。	全ての機器のアクセスログを残している。サーバ・VPNは保守事業者が定期的に確認している。	電子カルテの操作ログ、サーバーについては把握できていない。NWログについては収集の仕組みを検討している。	現在電子カルテのログ以外保存できていない。復旧のため、サーバ・NWについては、今後検討する。
【セキュリティパッチを適用している。(2-⑦)】	端末PCは定期的に実施。サーバについては、ベンダーからの提案に基づき実施。外部接続用のネットワーク機器は、情報を認知後速やかにアップデートを行う運用。	端末PCは定期的に実施。サーバについては、ベンダーからの提案に基づき実施。外部接続用のネットワーク機器は、情報を認知後速やかにアップデートを行う運用。	サーバ、端末PCについては、適用できていない。NW機器については、全ての機器に対して適用している。	サーバーはパッチ適用していない。端末は手動でバージョン適用をしている。ネットワーク機器は適宜行うが、都度更新はできていない。
【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。(2-⑩)】	電子カルテ端末については二要素認証（職員カード+パスコード）を実装済み サーバ、ネットワーク機器は二要素認証までできていない。	電子カルテ端末については二要素認証（職員カード+パスコード）を実装済み サーバ、ネットワーク機器は二要素認証までできていない。	二要素認証ができていない。次期システム更新で実装する予定。	現在は導入していない。二要素認証は今後導入を前向きに検討している。
【USBストレージ等の外部記録媒体の接続を制限している。(2-⑨)】	許可されたUSBのみ接続できるようにしている。	許可されたUSBのみ接続できるようにしている。	許可されたUSBのみ接続できるようにしている。	サーバー上で各端末において外部記憶媒体の接続や起動の制限を管理している。 通常、USBは病棟や外来では起動しないが、必要な場合、適宜、可否を判断している。
【バックアップの実施と復旧手順の確認。(3-②)】	すべての医療情報システムのデータはバックアップが取れている（復旧手順については医療機関側で十分に確認できていない）。	すべての医療情報システムのデータはバックアップが取れている（復旧手順については医療機関側で十分に確認できていない）。	すべての医療情報システムのデータはバックアップが取れている（復旧手順については医療機関側で十分に確認できていない）。	バックアップサーバーにデータが保存され、ベンダーのデータセンターにもバックアップが保存されている。
【サイバー攻撃を想定したBCPを策定している。(3-③)】	自施設で独自に策定したものを運用（ただし、定期的な見直しはできていない）。	自施設で独自に策定したものを運用（ただし、定期的な見直しはできていない）。	厚労省のひな形をベースに独自マニュアルを整備。ただし、定期的な見直しはできていない。	自然もIT-BCPもどちらも対応可能な形のマニュアルにしている。

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）
分担研究報告書

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

研究分担者　研究分担者　猪飼　宏　京都府立医科大学 附属病院医療情報部 部長

研究要旨

本分担研究では、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対応の実態を明らかにすることを目的として、公立の特定機能病院であるL病院に対しヒアリング調査を行った。 医療情報部門の体制、電子カルテ・ネットワーク・セキュリティ関連ベンダとの役割分担、資産管理や外部接続点管理、ログ・パッチ・バックアップ運用、IT-BCP 策定状況等を整理し、チェックリスト項目との対応状況と課題を抽出した。 その結果、L 病院では長年の運用経験とベンダとの協働により多くの項目が概ねカバーされている一方、移動端末や部門システムの統合管理、ゼロトラストを見据えたネットワーク再設計、セキュリティ人材の育成・評価など、組織的・構造的な課題が残されていることが明らかとなった。

A. 研究目的

医療のデジタル化に伴い、電子カルテ、オーダリング、部門システム、ネットワーク、外部保守接続、医療機器など多様なシステムが統合的に運用され、院内外のシステム連携が診療機能の基盤となっている。 サイバー攻撃やシステム障害により医療情報システムが利用困難となった場合、患者情報の閲覧、指示伝達、検査・処方・会計等が制約され、医療安全および診療継続に重大な影響を及ぼす恐れがある。

厚生労働省「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、医療機関が優先的に取り組むべき対策項目を提示しているが、その実装可能性や運用の成熟度は、病院規模、既存システム構成、人材配置、ベンダとの責任分界、予算制約等に左右される。

本分担研究では、チェックリストへの対応が比較的進んでいる公立大学病院である L 病院を対象に、医療情報部門の体制やベンダとの分担、資産管理・外部接続管理・ログ管理・バックアップ・IT-BCP といった実務運用の実態を把握し、その強みと課題を明らかにすることを目的とした。 併せて、長年蓄積された病院情報システム運用の経験知をどのように継承し、組織としてセキュリティ人材を育成・評価しうるかを検討し、チェックリスト対応の実効性評価に資する知見を得ることを目指した。

B. 研究方法

本分担研究では、2026 年 1 月から 3 月にかけて、L 病院の医療情報部門職員および電子カルテ・ネットワーク・セキュリティ関連ベンダ担当者を対象にヒアリング調査を実施した。 調査では、医療情報部門の体制、電子カルテおよびネットワーク・セキュリティ関連ベンダの役割、資産管理、外部接続点、MDS/SDS、利用者管理、ログ管理、パッチ管理、二要素認証、外部記憶媒体、バックアップ、IT-BCP に関する運用状況や課題について聞き取りを行った。

ヒアリングは厚生労働省「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」に沿って実施し、各項目に対する対応状況、運用上の工夫、実装上の制約やリスク認識などを半構造化インタビュー形式で収集した。 倫理面への配慮として、報告書では個別患者情報および機微な設定情報は記載せず、医療機関の実

務改善に資する範囲で結果を整理することとした。

C. 研究結果

L 病院では、端末・サーバを IP アドレスおよび所在と一体的に資産台帳で管理しており、電子カルテ端末を含む多くの機器について網羅的な把握がなされていた。 一方で、ノート PC や検査機器など移動して利用される機器については、必要に応じて通信ログを用いて所在確認を行う場面もあり、動的な資産の管理には一定の負荷を要していた。 電子カルテ以外の部門端末におけるウイルス対策やソフトウェアアップデートは、原則として各部門ベンダの管理に委ねられており、病院側で一元的に端末管理を行うソリューションの導入も検討されていたが、費用面から導入には至っていなかった。

リモート接続については、病院として共通の仕組みを整備し、ベンダごとに接続元 IP アドレスを極力限定したうえで ID とパスワードを発行していた。 ただし、一部の医療機器では仕様上、ベンダ固有の保守用外部回線を必要とするものが存在し、その場合は商用回線の設置を届け出制により許可することで、全ての外部接続を把握する運用が取られていた。 遠隔診療やクラウドサービス利用に伴い、専用の商用回線や専用線上の VPN 接続も増加しており、サービスおよび連携先拠点数の拡大に伴う費用増大が新たな課題となっていた。 ゼロトラストを前提としたネットワーク設計への移行も検討されていたが、電子カルテベンダ・ネットワークベンダともに十分な経験を有しておらず、中長期的な検討課題として位置付けられていた。

MDS/SDS については、適時調査や特定共同指導、立入検査の機会に整備状況が確認されており、概ね全項目で遵守状況が維持されていたため、個別の課題抽出に活用した実績は乏しかった。 利用者管理に関しては、特権管理者のパスワード桁数を増やすなどの強化が行われていたが、更新はシステム更改時などに限られ、日常的な頻繁更新は実施されていなかった。 一般ユーザのアカウントは人事情報と連動して発行・凍結・権限変更が行われているものの、大学病院特有の事情として、学生や研修医の頻繁な所属変更や、出向後も診療協力医として継続勤務するケースが多く、厳密なアカウント管理には一定の困難が認識されていた。

ログ管理では、サーバおよびネットワーク機器からログ収集が行われていたものの、ログ解析の経験を有する職員は限られており、日常的・体系的なログ分析は十分には実施されていなかった。 セキュリティパッチについては、EPP（エンドポイント保護ソフト）の定義ファイル等は院内の配信サーバから定期的に配布されていた一方で、Windows Update は電子カルテおよび部門システムベンダによる動作検証に多大な労力とコストを要することから、重要度の高いものに限って不定期に適用される運用であった。

バックアップについては、いわゆる 3-2-1 ルールに沿って、LTO ドライブによる外部保管に加え、遠隔地へのオンラインミラーリングを実施し、参照系システムとしても活用していた。 システム障害時には参照系から本系への切り替えにより診療継続を図る想定であったが、データ破損や改ざん発生時におけるバックアップデータからの本格的なシステム復旧については、ベンダ側の経験も十分とは言えず、今後の課題として認識されていた。

IT-BCP については策定済みであり、年 1 回の机上訓練が実施されていたが、全てのハザードを網羅した病院全体の BCP、ならびに教

育・研究を含む大学全体の BCP との連携や整合性については、引き続き検討が必要とされていた。 組織的課題としては、公的病院として行政との間で人事異動が頻繁に生じることから、病院採用職員と行政職員とで求められるキャリアパスが異なり、情報セキュリティに関する資格取得や専門性の維持が困難になりやすいことが指摘された。

D. 考察

公立大学病院である L 病院では、約 35 年にわたり病院情報システムを整備・運用してきた実績を背景に、電子カルテおよびネットワークそれぞれのベンダと密接な連携を取りながら、サイバーセキュリティチェックリストの大部分をカバーする運用が構築されていた。 一方で、部門システムを担当するベンダ間では技術力や対応能力にばらつきがあり、そのギャップを病院職員の経験やスキルによって補完せざるを得ない場面も多く、責任の分界が曖昧になりうることが課題として示された。

また、システムの開発・構築・運用に長年携わってきた担当者であっても、情報セキュリティやネットワークに関する最新の知識を継続的にアップデートするには多大な労力を要する。現行の人事制度や評価体系では、こうした学習・研鑽が十分に評価されにくく、個人の自己研鑽に大きく依存している実態が明らかになった。

特定機能病院など高度急性期医療を担う医療機関において、組織としてセキュリティ人材育成に取り組むためには、診療報酬上の施設基準や加算要件としてセキュリティ関連資格や専任配置を位置付けることや、公的病院における人事評価の中で資格取得・維持や継続教育を評価する仕組みを整備することが有用と考えられた。

E. 結論

L 病院でのヒアリングから、大規模医療機関における医療情報システムの安全な設計・構築・運用には、病院長の理解の下での明確な組織的位置付け、専任を含む情報システム人材の確保、ベンダとの調整スキルおよび信頼関係の構築が重要な役割を果たすことが確認された。

今後、遠隔医療や地域医療連携の拡大に伴い、中核医療機関が周辺医療機関に対して情報セキュリティ面でも支援を行う役割を担うことが想定される。 そのためには、組織マネジメント（人事評価を含む）を通じたセキュリティ人材育成、資格取得・維持の体系的支援、部門システム等を担うベンダ側でのスキル向上といった課題に計画的に取り組む必要があると考えられた。

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

なし

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

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)
分担研究報告書

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課題調査と解決策の検討

研究分担者 杉本賢人 大阪大学大学院医学系研究科 医療情報学 特任助教(常勤)

研究要旨
本研究では、厚生労働省の「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」をもとに、実際に医療機関へのインタビュー調査をもとに対応困難な項目とその要因を明らかにし、改善方針を示すことを目指す。
全国の医療機関を対象とした Web アンケート結果を踏まえ、医療機関におけるシステム導入・保守に関与するベンダーを対象としてインタビュー調査を実施した。本報告書では、そのうち主要な医療情報システムの提供または運用支援を行う 3 社の回答結果について報告する。
その結果、昨今のサイバーセキュリティインシデントを受け、いずれのベンダーでも支援体制やセキュリティ対策の整備が進められていた一方で、その内容や対応範囲には差がみられた。特に、システム、ネットワークなどの管理主体が分かれる場合には、責任範囲や調整主体が不明確となり、統一的な管理が困難となる事例が明らかとなった。また、セキュリティ対策の実施には、医療機関や関係ベンダーとの調整、停止を伴う作業、費用対効果の判断が制約となることが示唆された。今後は、システム更新時の仕様書において、セキュリティ要件や責任範囲を明確化するとともに、対策に必要な費用負担のあり方についても検討することが重要である。

A. 研究目的

本研究の目的は、厚生労働省が示す「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」について、その内容をもとに医療機関を対象としたアンケート調査を行い、実際の医療現場で対応が困難な項目や、その背景にある課題を明らかにし、改善方針を提示することである。近年、医療分野では DX の推進とともにサイバー攻撃被害が増加しており、診療停止など地域医療に深刻な影響を及ぼす事案も生じている。しかし、既存のチェックリストには一部の医療機関で十分に対応できていない項目があり、その背景には、医療機関側の人材・費用・運用体制の制約だけでなく、医療情報システム等を提供・保守するベンダーとの役割分担や支援体制に関する課題も含まれると考えられる。

そこで本研究では、全国の医療機関を対象とした Web アンケート、医療機関へのインタビュー調査、さらに関連ベンダーへのインタビュー調査を通じて、対応困難な項目とその要因を多面的に整理する。本報告書では、そのうちベンダー分のインタビュー調査結果を対象として、医療情報システム等を提供・保守するベンダーの支援状況、運用上の制約、および医療機関との役割分担に関する課題を整理する。

B. 研究方法

まず、Web アンケートにより、全国の医療機関を対象として「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」の各項目に対する対応状況、および未対応項目に対応できていない理由を調査する。さらに、アンケ

ート結果を踏まえ、複数の医療機関および関連ベンダーに対してインタビュー調査を実施する。

本報告書では、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、ヒアリングを実施し、セキュリティ対策の支援状況や運用上の課題について調査した結果を報告する。

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）

本研究のベンダーへのインタビュー調査結果は具体的な企業名が特定できないよう仮名化したうえで報告する。

C. 研究結果

全体として、いずれのベンダーにおいて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、認証、接続管理、パッチ適用、バックアップなどの各領域で一定の共通する対応方針が示されていた。一方で、調達範囲やシステム構成、保守体制の違いにより、インフラ領域のガバナンス、権限管理、運用負荷、復旧訓練の実効性などにベンダーごとの課題がみられた。

まず、外部接続点については、A 社・B 社は、自社サービスを活用するなどして、外部接続点を集約・制御する方向での提案や構成管理を進めていた。A 社は、接続点を可能な限り少なくする方針のもと、部門ベンダーも含めた集約的なリモートメンテナンス環境や、専用線・ゲートウェイを活用したセキュア接続を提案しているとの報告があった。B 社は、主に大規模病院については、共通基盤やデータセンター経由の閉域的な構成を採用していたとの報告があった。一方、C 社は、望ましい接続形態として二要素認証や踏み台利用の考え方を示していたが、自社がネットワーク全体を構築・統制するケースは限定的であり、施設側や他ベンダーの方針に依存する側面が大きいとの見解であった。これらの方向性の違いは、A 社・B 社はインフラ（ネットワーク）を含めて自社で調達・構築に関与することが多く、インフラ領域まで一定のガバナンスが及んでいるケースが多い一方、ネットワークが別調達となることが多い C 社では、インフラ領域のセキュリティガバナンスが必ずしも十分に及ばず、管轄外となる場合があることが分かった。なお、B 社についても、導入する病院規模によってはパッケージを別のシステム企業が導入する事例があり、その場合には C 社と同様に、インフラ領域のガバナンスが十分に及んでいない場合があるとの課題が示された。

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。

システムのユーザー管理については、A 社・B 社は、製品（パッケージ）や運用条件によって差はあるものの、特権付与をできるだけ限定する方向で整理していた。A 社は、クライアントアプリケーションでは原則として管理者権限を持たせない方針を明確にしており、必要な場合、対象端末の限定やネットワークを分離する運用

などの対応をしていた。B 社は、新しい系統のシステムでは特権なしでも運用可能な一方、旧システムではクライアントやサーバ保守に特権が必要となる場合があるとの報告があった。一方、C 社は、要件定義に応じて必要な権限を整理し、顧客要望に応じて運用を調整する形で対応していたが、システム制約上、特権や固定的な認証運用が残る場合があった。

セキュリティパッチ管理については、A 社・B 社は、自社内での評価・検証の枠組みを持っていた。A 社は、定期的な社内評価を実施していたが、部門ベンダーとの調整や影響範囲の見極めが課題として挙げられていた。B 社は、PC については比較的定期的な適用の仕組みを整えており、自社製品についても定期的な検証を行っていたが、サーバについてはシステム停止が必要であり、施設と個別協議となる場合が多いとの説明があった。一方、C 社は、脆弱性確認、テスト環境適用、全体適用判断といった工程を自社で整理していたものの、費用対効果の観点により、全て自社で適用まですることは困難であり、実際の適用判断や動作確認は施設側に委ねられる部分が大きいとの実情が示された。

二要素認証については、いずれのベンダーでも、主に端末側は対応していたが、サーバの対応は規模が大きくなることから、検討中、もしくは必要性は理解しているが、社内で十分に議論できていないなどの実情が明らかになった。

D. 考察

全体として、インタビュー調査に協力頂け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。

外部接続点については、A 社・B 社ではインフラを含めて調達・構築に関与するケースが多く、接続点の集約や閉域的な構成を通じて、インフラ領域まで一定のセキュリティガバナンスを及ぼしやすい構造にあると考えられる。一方で、A 社・B 社であっても、病院規模や調達形態によっては、必ずしもこうした統制しやすい仕組みを導入できるとは限らず、特に中小規模の医療機関やインフラ（ネットワーク）が別調達となるケースでは、統合的な管理が及びにくい場合がある。実際に、C 社ではネットワークが別調達となることが多く、接続方式や認証方式について望ましい考え方は示されているものの、実際の統制は施設側や他ベンダーに委ねられる部分が大きいとの実態が示されていた。また、B 社でも中小規模の医療機関では別のシステム企業が導入を担う事例があり、その場合には同様にインフラ領域のガバナンスが十分に及ばない可能性がある。昨今のサイバー攻撃では、外部接続点に設置された VPN 装置等を起点とした侵入が多くみられることから、外部接続点の管理は特に重要な論点である。この観点から、A 社・B 社が有する統合基盤や閉域サービスは、接続点の集約、管理責任の明確化、設定の標準化という点で有用と考えられる。他方で、過去の事例でもみられるように、必ずしもセキュリティ意識や運用体制が十分でない部門ベンダー、A 社・B 社のような体制・人材が十分に整っていない別のシステム企業などが設置・管理するVPN 装置等が脆弱性となる場合があり、電子

カルテベンダーがこうした外部接続点にどこまでガバナンスを及ぼせるかが重要である。他方で、電子カルテベンダーが自社の調達範囲外にあるネットワークや保守接続まで十分に統制することには限界がある。したがって、これらを管轄外として扱うのではなく、医療機関側が外部接続点の全体像を主体的に把握し、必要な管理基準を定めたうえで、関係ベンダーに対して横断的に適用していくことが重要である。

ユーザー管理については、いずれのベンダーでも、特権付与をなるべく限定する方向性を示していた。一方、システム導入から 5 年以上経過している施設については、旧システムを中心に特権が必要な場面が残っているとの実態が示された。このようなケースにおいて、ベンダー側としては次のシステム更新では特権付与を最小限にする方向性を示したものの、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の難しさも明らかになった。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る。

セキュリティパッチ管理については、A 社・B 社はベンダー内で評価・検証の仕組みを持っていた一方で、部門ベンダーとの調整やシステム停止を伴う作業が実務上の大きな制約となっていた。C 社は最終的な適用判断や確認を医療機関側に委ねる割合が大きく、運用の実効性が施設側の体制に影響されやすい構造と考えられた。特に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る。

二要素認証については、端末側では概ね対応が進みつつある一方で、サーバー側では十分に実装が進んでいない実態が確認された。特にサーバー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。このため、中長期的にはベンダー側でもサーバー自体に二要素認証の仕組みを備えていくことが望ましいが、当面の現実的な対応としては、ガイドラインにも示されているように、VPN 装置から踏み台サーバーに至るリモート保守経路において確実に二要素認証を確保し、不正アクセスの起点となりやすい外部接続点での防御を優先することが重要であると考える。

全体として、いずれのベンダーにおいてもセキュリティ対策の重要性は十分に認識されており、その意識の高さはインタビューを通じて明確にうかがえた。一方で、その対策をどこまで仕様や調達要件として明示的に盛り込むかについては、実務上きわめて難しい課題がある。一般に、求めるセキュリティ水準を高めるほど、構築や運用に要する費用は増加しやすく、その結果として医療機関側の予算との折り合いがつかず、必要性が理解されていても導入に至らない場合が少なくない。したがって、今後は単に対策強化を求めるだけでなく、どの対策を最低限の必須要件とし、どの対策を段階的な拡張項目とするかを整理したうえで、仕様や調達に落とし込んでいくことが重要である。

全体として、いずれのベンダーにおいてもセ

キュリティ対策の重要性は十分に認識されており、その意識の高さはインタビューを通じて確認された。一方で、これらの対策をどの範囲まで仕様又は調達要件として具体化するかについては、実務上の難しさが大きい。一般に、求めるセキュリティ水準を高めるほど、導入時及び運用時の費用は増加するため、医療機関側の予算との調整が困難となり、実装に至らない場合がある。加えて、医療機関の規模や体制によって現実的に実施可能な対策の水準は異なることから、一律の高水準要件を求めるのみでは十分な実効性を確保できない可能性がある。このため、今後の施策として、病院規模や体制に応じて求めるべきセキュリティ対策のレベルや優先度を段階的に整理し、それぞれに対応する具体的な事例や実装例を提示することは、医療機関にとって有用な指針となり得るかもしれない。

令和 6 年度の厚生労働科学研究「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」においては、医療情報セキュリティ人材の不足が指摘されるとともに、医療機関外の人材活用や、指導的な医療機関を中心とした地域連携モデルの必要性が示されている。本報告書でも同様の方向性となるが、医療機関においては、例えば、システム更新における仕様策定時、セキュリティに精通した外部人材等の関与を得つつ、仕様及び要件を具体化し、ベンダーに対して必要な対応を着実に求めていくことが引き続き重要であると考える。

さらに、費用面については、中長期的にはセキュリティ対策に要する費用を維持できる仕組みを構築していくことが求められる。病院情報システムに関わるベンダーも必要なセキュリティ対策を講じるためには、システム構築、運用維持、人材確保に要する費用を適切に確保する必要がある。したがって、医療機関側に対策費用の必要性を求めるだけでなく、ベンダー側が必要な対応を持続的に実施できるだけの費用構造をどのように設計するかという視点も重要である。

E. 結論

本調査により、大手電子カルテベンダーでは、昨今のサイバーセキュリティインシデントを受け、チェックリストを意識した支援体制やセキュリティ対策の整備が一定程度進められていることが明らかとなった。一方で、その内容や対応範囲には差があり、特に外部接続管理、アクセス権限・ログ管理、セキュリティパッチ適用などでは、どこまでを担当ベンダーの責務とするか、システムとネットワークの管理境界をどのように整理するか、医療機関や部門システムとの調整をどのように行うかが実務上の課題となっていた。また、システム更新時の仕様書において、セキュリティ要件やベンダーの責任範囲を明確に記載することの重要性が示唆された。一方、セキュリティ対策は費用対効果の判断が難しく、ベンダーがその重要性を認識していても、医療機関側の予算や運用上の制約により、仕様書上で優先度を十分に高めにくいという課題も認められた。今後は、医療機関側の体制整備に加え、ベンダーとの責任範囲の明確化、更新時の仕様書へのセキュリティ要件の反映、対応手順の標準化、継続的な運用支援を組み合わせた実効性の高い対策が求められる。

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

なし

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

研究成果の刊行に関する一覧表

書籍　なし
雑誌　なし

令和 8 年　2 月　16 日

厚生労働大臣　　殿

機関名　国立大学法人大阪大学

所属研究機関長　職　名　医学部附属病院長

氏　名　野々村 祝夫

次の職員の令和 7 年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　　地域医療基盤開発推進研究事業

２．研究課題名　　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課題調査と解決策の検討

３．研究者名　（所属部署・職名）　　大阪大学医学部附属病院・教授

（氏名・フリガナ）　　武田　理宏・　タケダ　トシヒロ

４．倫理審査の状況

	該当性の有無	左記で該当がある場合のみ記入（※1）		
	有　無	審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること（指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査に場合は、その理由を記載すること。
（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■無 □（無の場合はその理由：　　）
当研究機関におけるＣＯＩ委員会設置の有無	有 ■無 □（無の場合は委託先機関：　　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■無 □（無の場合はその理由：　　）
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■有の場合はその内容：　　）

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。

令和8年2月25日

厚生労働大臣　　殿

機関名　国立大学法人大阪大学

所属研究機関長　職　名　大学院医学系研究科長

氏　名　石井　優

次の職員の令和 7 年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　地域医療基盤開発推進研究事業

２．研究課題名　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課題調査と解決策の検討

３．研究者名　（所属部署・職名）　大学院医学系研究科・特任助教（常勤）

（氏名・フリガナ）　杉本　賢人・スギモト　ケント

４．倫理審査の状況

	該当性の有無	左記で該当がある場合のみ記入（※1）		
	有　無	審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること（指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査に場合は、その理由を記載すること。
（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：　　）
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：　　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：　　）
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■有の場合はその内容：　　）

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。

令和８年３月６日

厚生労働大臣　　殿

機関名　国立大学法人群馬大学

所属研究機関長　職　名　学長

氏　名　石崎　泰樹

次の職員の令和 7 年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　　地域医療基盤開発推進研究事業

２．研究課題名　　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課題調査と解決策の検討

３．研究者名　（所属部署・職名）　医学部附属病院・准教授

（氏名・フリガナ）　鳥飼　幸太・トリカイ　コウタ

４．倫理審査の状況

	該当性の有無 有　無	左記で該当がある場合のみ記入（※1）		
		審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること （指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査に場合は、その理由を記載すること。
（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：　　）
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：　　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：　　）
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■（有の場合はその内容：　　）

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。

令和８年１月26日

厚生労働大臣　　殿

機関名　京都府立医科大学

所属研究機関長　職　名　学長

氏　名　夜久　均

次の職員の令和 7 年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　地域医療基盤開発推進研究事業

２．研究課題名　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課題調査と解決策の検討

３．研究者名　（所属部署・職名）京都府立医科大学　附属病院　・准教授

（氏名・フリガナ）　猪飼　宏・イカイ ヒロシ

４．倫理審査の状況

	該当性の有無 有　無	左記で該当がある場合のみ記入（※1）		
		審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること （指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査に場合は、その理由を記載すること。
（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：　　）
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：　　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：　　）
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■（有の場合はその内容：　　）

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。

２０２６年1月２６日

厚生労働大臣　　殿

機関名　大津赤十字病院

所属研究機関長　職　名　病院長

氏　名　小川　修

次の職員の令和 7 年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

1．研究事業名　地域医療基盤開発推進研究事業

2．研究課題名　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課題調査と解決策の検討

3．研究者名　（所属部署・職名）　医療情報課　課長

（氏名・フリガナ）　橋本　智広　　ハシモト　トモヒロ

4．倫理審査の状況

	該当性の有無	左記で該当がある場合のみ記入（※1）		
	有　無	審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	■　□	■	大津赤十字病院倫理委員会	□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること（指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査に場合は、その理由を記載すること。
（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

5．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　未受講 □

6．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：　　）
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：　　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：　　）
当研究に係るＣＯＩについての指導・管理の有無	有 ■　無 □（有の場合はその内容：　　）

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。

令和８年１月１６日

厚生労働大臣　　殿

機関名　社会医療法人三上会東香里病院

所属研究機関長　職　名　院長

氏　名　三上　聡司

次の職員の令和７年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　　地域医療基盤開発推進研究事業

２．研究課題名　　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課題調査と解決策の検討

３．研究者名　（所属部署・職名）　　社会医療法人三上会東香里病院　　院長

（氏名・フリガナ）　　三上　聡司・ミカミ　サトシ

４．倫理審査の状況

	該当性の有無	左記で該当がある場合のみ記入（※1）		
	有　無	審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること（指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査に場合は、その理由を記載すること。
（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有　　無 ■（無の場合はその理由：　　大阪大学　　）
当研究機関におけるＣＯＩ委員会設置の有無	有 □　無 ■（無の場合は委託先機関：　　大阪大学　　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：　　）
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■（有の場合はその内容：　　）

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。