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