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