別紙 3

厚生労働科学研究費補助金
政策科学総合研究事業（臨床研究等 ICT 基盤構築・人工知能実装研究事業）

分担研究報告書
クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言

研究分担者　尾﨑 勝彦　徳洲会インフォメーションシステム株式会社 代表取締役社長
研究協力者　福田 秀樹 徳洲会インフォメーションシステム株式会社 導入管理部 部長代理

研究要旨

医療現場における医療 AI の利活用は働き方改革にも繋がる医療従事者の業務効率化と省力化、医療レベルの高度化、患者サービスの向上、さらに専門医不在など医療資源が不足している離島やへき地で提供される医療のレベルとカバーレンジを都市部に近づけるパワーを持つ。このように大きな可能性を持つ医療 AI であるが、その多くはインターネット上のクラウドに存在し、一方病院を中心に医療機関の電子カルテ等はインターネットから分離したクローズドな環境の中にあるものが多い。本研究では医療機関の電子カルテ端末等から医療 AI をセキュアに利用するための技術や方策の検討を行うが、そのためにはまず医療機関の院内情報システム、また医療機関そのものがセキュアな環境でなければならない。徳洲会グループでは、グループの IT 部門である徳洲会インフォメーションシステム株式会社とグループ病院の院内システムエンジニア約 180 名の集合体である情報システム管理部会が協力してグループ内の病院にシステム監査（サイバーセキュリティ監査）を行ってきた。このシステム監査をより実効性のあるものにブラッシュアップし、さらにグループ外の医療機関にも適用しうる標準的な監査とすることで医療 AI の導入を進める医療機関のセキュリティレベル向上に繋げたいと考えている。R 5 年度はまず 5 月にリリースされた厚生労働省「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」に準拠したシステム監査とすること、また徳洲会グループ病院の監査からフィードバックを行って監査項目や監査方法の改善を実施し、標準化に向けた土台作りを行えたと考える。

A. 研究目的

医療現場における医療 AI の利活用は働き方改革に繋がる医療従事者の業務効率化と省力化、医療レベルの高度化、患者サービスの向上、さらに専門医不在など医療資源が不足している離島やへき地で提供される医療のレベルとカバーレンジを都市部に近づけるパワーを持つ。このように大きな可能性を持つ医療 AI であるが、その多くはインターネット上のクラウドに存在し、一方病院を中心に医療機関の電子カルテ等はインターネットから分離したクローズドな環境の中にあるものが多い。本研究では医療機関の電子カルテ端末等から医療 AI をセキュアに利用するための技術や方策の検討を行うが、そのためにはまず医療機関の院内情報システム、また医療機関そのものがセキュアな環境でなければならない。徳洲会グループでは、グループの IT 部門である徳洲会インフォメーションシステム株式会社とグループ病院の院内システムエンジニア（以下「院内 SE」）約 180 名の集合体である情報システム管理部会が協力してグループ内の病院にシステム監査（サイバーセキュリティ監査）を行ってきた。このシステム監査をより実効性のあるものにブラッシュアップし、さらにグループ外の医療機関にも適用しうる標準的な監査とすることで医療 AI の導入を進める医療機関のセキュリティレベルの向上に繋げることが目的である。

B. 研究方法

R５年５月に公表された厚生労働省「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」（以下「厚労省ガイドライン」）にもとづき徳洲会グループ「情報システム運用管理規程」（以下「運用管理規程」）を改訂、９月に第 6.0 版をリリースした。この厚労省ガイドライン・運用管理規程それぞれの第 6.0 版に準拠するよう、システム監査で用いる「システム監査チェックシート」上の監査項目の再編を行った。さらにＲ５年度に実施した徳洲会グループ３病院でのシステム監査結果のフィードバックからも監査項目や監査方法の見直しを実施した。

C. 研究結果

１．監査チェックシートの再編

① 厚労省ガイドラインの反映

厚労省ガイドラインの改定ポイント・内容を運用管理規程に反映させ、そこから特に重要と考えるものを監査チェックシートの項目として採用した。その一例を示す。

表１　システム監査チェックシート（抜粋）

	チェック内容	チェック対象資料等	資料提出	結果	監査員コメント
2	情報システム委員会が設置され各部署から委員が選出されている	①組織図 ②役務任命簿	事前	○	問題ない
11	不要な電子カルテのユーザIDの残存有無が定期的に確認されている	不要な電子カルテのユーザIDの存在有無の点検が行われたことが確認できる資料 （別紙9_ID・権限棚卸結果報告書・別紙10_ID・権限棚卸結果管理書 等）	事前	×	退職時に総務課で利用者マスタに退職チェックを入れる運用だが、定期的な棚卸しは行われていない
15	ウイルス対策ソフトは適正なライセンス数を購入し、サーバおよび端末にインストール、定義ファイルを定期的に更新している	①ウイルス対策ソフトのライセンス購入と本数が確認できる資料 ②端末管理台帳 ③ウイルス対策ソフトのパターンファイルの日付が確認できる画面	事前および当日	△	アンチウイルスのライセンス数が端末数より少ない/実際にアンチウイルスがインストールされていない端末がある
18	端末からデータを抜き出せない設定を行っている	①USBメモリ/CD等の制御設定が確認できる画面のハードコピー （ActiveDirectory ・ESET） ②USBメモリ利用許可端末の一覧等（部署名・用途が記載されたもの）	事前および当日	△	ActiveDiretoryの設定は適正だが、アンチウイルスの入っていない端末では任意のUSBメモリを差すことが可能な状態
22	ランサムウェア等のウイルスの感染が発生した際の初動対応が周知されている	①ランサムウェア感染時の初動対応が記載された資料（ランサムウェア感染時：対応チェックリスト 等） ②その周知方法が確認できる資料	事前および当日	○	各部署に『ランサムウェア感染時対応チェックリスト』が配付され、現場の職員にも周知されている

厚労省ガイドライン：災害、サイバー攻撃、システム障害等の非常時における対応や対策

監査チェックシート：項番 22『ランサムウェア等のサイバー攻撃が発生した際の初動対応が周知されている』

厚労省ガイドライン：ネットワーク境界防御型思考／ゼロトラストネットワーク型思考

監査チェックシート：項番 24『医療機器保守用回線のネットワーク機器（VPN ルータ・ファイアウォール）が一覧化され、適切に管理されている』

また厚労省から出されたチェックリストを監査でも有効活用すべく、次の項目も追加した。

監査チェックシート：項番 25『【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】は医療機関確認用と事業者確認用が作成、保管されている』

② 監査項目内容・項目数の変更

従来院内 SE の業務内容なども含めていた監査項目をサイバーセキュリティ／セーフティ関連のものに絞り、また 1 項目をより深く見て議論でき、かつ監査を効率的に実施できるよう項目数を従来の 70 → 50 とした。

③ 準備資料等の明確化

病院側の準備と監査がスムーズに行えるよう、監査で確認する書類や写真等を監査チェックシートの添付資料として具体的に提示した。

2．監査方法の見直し

① 事前のオンライン面談実施

従来は病院から事前に提出された資料等にもとづき文書監査を行い、その後現地監査を実施していた。今年度は文書監査後に監査メンバーと病院 SE で状況と課題を共有するオンライン面談を試行、これにより病院側の理解が深まり、現地監査の円滑化にも繋がった。

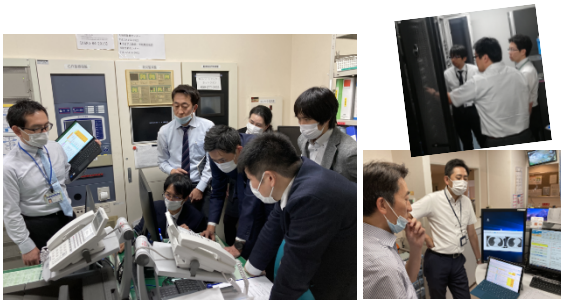

図 1　システム監査：現地監査の様子

② 監査報告提出後の改善フォロー実施

従来は現地監査後に監査報告書を送付し、病院はこれにもとづき指摘事項の改善作業を行っていた。しかし病院側の理解が不十分で改善になかなか手を付けられないなどのケースがあったため、監査報告提出後に監査メンバーと病院 SE で指摘された項目の改善方法やスケジュール、支援の方法などについてオンラインで話し合う場を持った。これにより改善作業がより円滑に開始・実行されるようになったと考える。

表 2　システム監査結果報告書（抜粋）

2．監査結果概要

監査は計 50 の項目について実施しました。カテゴリごとに『充足』『一部充足』『未充足』の 3 段階で評価（運用ルールはあるが実績がないものは『該当なし』）を行い、結果は次のとおりです。
このうち『未充足』の 3 項目と『一部充足』の 9 項目については次の 3．指摘事項 にその内容を記載しています。

監査カテゴリ／監査項目数		監査結果			
カテゴリ	項目数	充足 項目数	一部充足 項目数	未充足 項目数	該当なし 項目数
管理体制	3	2	1	0	0
個人情報保護対策	3	3	0	0	0
セキュリティ管理（管理者権限）	2	1	1	0	0
セキュリティ管理（アプリケーション）	6	4	2	0	0
セキュリティ管理（サーバ・端末）	6	5	0	0	1
セキュリティ管理（サイバー攻撃対策等）	5	4	1	0	0
パスワード管理	3	3	0	0	0
文書・マニュアル等の管理	7	5	1	1	0
サーバ運用	9	4	3	2	0
端末運用	4	4	0	0	0
システム管理室関連	2	2	0	0	0
	計 50 項目	計 37 項目	計 9 項目	計 3 項目	計 1 項目

（指摘事項：計 12 項目）

3．3　指摘事項の詳細

【未充足項目】

カテゴリ／項番	問題・課題と改善策	指摘事項の内訳
文書・マニュアル等の管理／項番 30	◆電子カルテ等院内システムがダウンした際の訓練が実施され、手順の見直しが定期的に行われている： 電子カルテ等が利用不能となったことを想定した訓練が行われておらず、有事に診療の継続等対応が適切に行えない可能性がある。 → サイバー攻撃やシステム障害に備え（また R6 年度より診療録管理体制加算 I の要件となったことも合わせ）、システムダウン時の訓練を実施し、その結果に基づく手順の見直しを行ってください。その後、訓練が実施されたこと・手順の見直しを行ったことが確認できる資料を提出してください。	①
サーバ運用／項番 38	◆サーバのバックアップは適切に取得・保管されている： 電子カルテサーバのデータバックアップは取得されているが、システム管理者がその世代管理や保管場所等を十分把握できておらず、障害時に円滑な対応ができない可能性がある。SE 部会提供の資料も参考にバックアップ運用について把握しておくことが推奨される。 → 電子カルテサーバのバックアップ運用を理解し、それを示した資料を提出してください	①
サーバ運用／項番 42	◆サーバ室は災害時に被害を受けにくい場所にある： 電子カルテサーバ等が設置されたサーバ室が地下 1 階にあり、浸水等により電子カルテが利用不能となることが考えられる。 → 現在各システムサーバの 5 階への移設が進められており、電子カルテサーバの移設も検討し移転時期やサーバラック内の設置予定場所等を示した計画書を提出してください。	①

【一部充足項目】

カテゴリ／項番	問題・課題と改善策	指摘事項の内訳
管理体制／項番 3	◆情報システム委員会は月 1 回程度開催され、機能している： コメディカル部門から新たに委員を選出し適切な体制となったが、新体制による委員会がまだ開催されていない。 → 新体制による委員会の 2 回分の議事録（必要な署名あるいは押印がされたもの：PDF）を提出してください。	③
セキュリティ管理（管理者権限）／項番 7	◆管理者 ID（サーバ OS の ID や電子カルテのスーパーユーザ等）は必要最低限の ID のみが登録されている／また不要な管理者 ID の残存有無が定期的（年 1 回程度）に確認されている： 管理者 ID（電子カルテのスーパーユーザー等）の棚卸しが行われておらず、必要のない職員に大きな権限が付与されたままになる可能性がある。 → 運用管理規程：別紙 9【ID・権限棚卸結果報告書】および 10【ID・権限棚卸結果管理表】にもとづき管理者 ID の棚卸しを行い、これらの書類（必要な署名あるいは押印がされたもの：PDF）を 1 部ずつ提出してください。	①

D．考察

「C.1．監査チェックシートの再編」においては厚労省ガイドライン第 6.0 版の内容の反映、項目内容と項目数の見直し、準備資料等の明確化を行うことでより Up to Date かつ効果的・効率的なチェックシートとすること

ができた。また「C.２．監査方法の見直し」では、事前のオンライン面談と監査報告提出後の改善フォローを通じて病院と監査員とのコミュニケーションの機会を増やしたことにより、監査をスムーズに行えるようになっただけでなく、病院がサイバーセキュリティの重要性や課題の理解を深めることにも繋がったと考える。

E. 結論

Ｒ５年度はこれまで徳洲会グループで実施してきたシステム監査について監査項目や方法の見直しを検討、見直した内容にもとづいた監査を行い、フィードバックを実施というサイクルで継続的なブラッシュアップを行った。次年度の徳洲会グループ以外の病院でのシステム監査実施、つまり標準化に向けてのファーストステップを踏むことができ、またこの取り組みに関わった監査員のレベル向上にも繋がったと評価する。

F. 健康危惧情報

総括研究報告書に記載

G. 研究発表

福田 秀樹, 江苅 孝, 藤岡 和美, 尾﨑 勝彦. グループ病院でのセキュリティ対応とその課題～システム監査を中心に～. *医療情報学*, 2024, **44(Suppl.)**, 363-367

H. 知的財産権の出願

なし

資料　システム監査グループの全体スケジュール