

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 尾崎 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がたいと考えている。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った。続く R 6 年度においては徳洲会グループ 3 病院で監査を実施して前年同様にフィードバックと改善を行うとともに、初のグループ外の 1 病院での監査を実施した。この監査では監査項目や提出資料などを大幅に見直し、また監査を通じて多くの気づきや課題を見出すことができ、目的である広く国内の医療機関に適用できる監査の標準化に向けて第一歩を踏み出すことができたと思う。

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

R 5 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 版に準拠した「システム監査チェックシート」にもとづき R 5 年度に 4 病院、R 6 年度にも次の 4 病院でシステム監査を実施し、それぞれの結果をフィードバックして監査項目や監査方法の見直しを行い、次の監査で検証とフィードバックを行う形で実施した。特に R 7 年 3 月に実施した A 病院は初の徳洲会グループ外の施設における監査であり、事前に監査チェックシートや提出資料の大幅な見直しを行うことで、医療機関に広く適用するための標準化を試みた。

【システム監査実施病院】

R 6 年度

6 月 25 日 東大阪徳洲会病院（大阪府）

12 月 19 日 宮古島徳洲会病院（沖縄県）

2 月 28 日 山川病院（鹿児島県）

3 月 7 日 A 病院（愛知県）

C. 研究結果

ここでは主に R 7 年 3 月に実施した徳洲会グループ外の A 病院での監査について、その準備と実施について記述する。

1. 監査チェックシートの見直し

監査チェックシートについては次の観点で見直しを行った。

表 1 システム監査チェックシート（抜粋）

	監査項目	チェック対象資料等	チェック対象資料等の提出方法	資料等の確認	結果
総則					
1	医療情報システム安全管理責任者・企画管理者・情報システム運用担当者・情報セキュリティ責任者（厚労省ガイドライン上のこれらの役割を担う担当者名も併記）が任命され、それぞれの役割が明文化されている	①役職者名簿（氏名・所属・院内役職が記載されたもの） ②任命書の提出が確認できる資料（規程の該当部分など）	①・②ともデータが PDF で提出ください ①は最終更新日があるもの	事前	△
2	院内の医療情報システムの安全管理やセキュリティ対策について協議・情報共有する情報システム委員会（別名称でも良い）が設置され、各部署から委員が選出されている		①・②ともデータが PDF で提出ください（いずれも最終更新日があるもの）	事前	△
3	情報システム委員会は月 1 回開催開催されて機能しており、議事内容が幹部・各部署に共有されている	①情報システム委員会議事録 ②委員会の議事内容の幹部・各部署への共有が確認できる資料（記録記録や幹部が出席する会議の議事録など）	①・②ともデータが PDF で提出ください ①は①は直近の 2 回分	事前	△
個人情報保護					
4	病院の個人情報保護方針が策定され、患者の見える場所に提示されている	①病院の個人情報保護方針 ②個人情報保護方針の提示状況（当日）	①はデータが PDF で提出ください ②は当日提示を確認します	事前 および 当日	○
5	医療情報システムから個人情報を含むデータを抜き出す際のルールが明記、適切に運用されている	①医療情報システムからのデータ抜き出しに関するルールが確認できる資料（規程の該当部分など） ②運用が確認できる資料（申請書など）	①はデータが PDF で ②は実際に使われた（記載のある）もののデータが PDF で提出ください（2 回分）	事前	○

① 運用管理規程等ルールの有無の確認

徳洲会グループには厚労省ガイドラインに準拠したルールブックである「情報システム運用

管理規程 第 6.0 版」があり、グループ病院においてはこの規程にもとづく運用が適切に行われているかについて監査をする。しかしグループ外の病院ではそもそもルールの有無が不明であるため、多くの項目で「①厚労省ガイドラインにもとづくルールがあり ②それにもとづく運用が行われているか」という観点でのチェック形式に変更した。

② 徳洲会グループ書式の書き換え

徳洲会グループ病院では運用管理規程の別紙として「ID・権限棚卸結果報告書」「外部記憶媒体貸与台帳」など計 27 種類の帳票を用いることでルールにもとづく運用を行うこととしており、監査チェックシートの「チェック対象資料等」にもこの帳票名を記載している。しかしグループ外の病院にはこの名称の帳票はないため、「電子カルテ ID の棚卸が行われたことが確認できる資料」「院外に情報機器を持ち出す際の運用が確認できる資料」といった記載に変更した。

③ 電子カルテのアプリ名等の書き換え

徳洲会グループ病院では同一メーカーの電子カルテを利用しており、監査チェックシートの「チェック対象資料等」にもそのアプリ名を記載しているものがある。これもグループ外病院の電子カルテメーカーが不明であるため、「電子カルテのアクセスログが表示された画面」「パスワードでの復帰が必要なスクリーンセーバ」などの記載に変更した。

④ 監査項目の見直し

グループ内外の病院を問わず、監査を通じて確認すべき事項としたものに加え、サイバーセキュリティに関する動向、厚労省の「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」や「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」等も参考に、監査項目の見直しを継続的に行った。

2. 監査方法の見直し

① 事前提出資料の削減

A 病院の監査では病院側の準備の負担軽減のために事前提出資料が必要な項目数を従来の 46 から 42 へ減らし、その 4 項目については現地で確認することとした。

② 監査後の改善支援

徳洲会グループ病院においては監査報告書の提出後、その改善を 3～6 ヶ月かけてフォローアップする仕組みがあるが、今回の研究ではこの部分を行わないこととした。

上記①・②以外は監査の全体スケジュール（監査通知 → 資料の事前提出 → 文書監査と結果通知 → 現地監査 → 監査報告書提出）を含めグループ病院と同様に実施した。

3. 監査の実施と結果

A 病院での監査結果とそこにあらわれた課題について記述する。

① 監査結果：全体

×（未充足）と△（一部充足）を合わせると全 50 項目中 32 項目、全体の 64%が指摘項目となった。

表 2 A 病院の監査結果（全体）

○	18 (36.0%)
△	17 (34.0%)
×	15 (30.0%)
NA	0 (0%)

○：充足 △：一部充足 ×：未充足 NA：該当なし

② 監査結果：詳細

監査項目の内容を満たしていないものをカテゴリー別に、またその一部を具体的に次に示す（いずれも現地監査当日の総評で病院へ報告したもの）。

表3 A病院の監査結果（詳細）

監査カテゴリ／項目数			監査結果			
カテゴリ	項目数	項目番号	○ 充足	△ 一部充足	× 未充足	NA 該当なし
管理体制	3	1～3	0	3	0	0
個人情報保護	2	4～5	2	0	0	0
文書類の整備	4	6～9	2	2	0	0
管理者権限の管理	3	10～12	1	0	2	0
ID・パスワード管理	8	13～20	4	1	3	0
サイバー攻撃・災害・BCP対策	9	21～29	3	3	3	0
サーバ管理	7	30～36	2	2	3	0
端末管理	8	37～44	4	2	2	0
ネットワーク管理	4	45～48	0	3	1	0
その他	2	49～50	0	1	1	0
合 計	50		18	17	15	0

×：未充足の項目（抜粋）

12 電子カルテのサーバOSのアクセスログを取得し、いつでも調査可能な状態である

14 電子カルテIDのパスワードは次のいずれかである

A：13桁以上の英数記号のパスワード（定期変更はなし）

B：8桁以上の英数記号のパスワードで最低2ヵ月に1度変更

C：二要素認証を採用

16 電子カルテIDの棚卸しが定期的に行われ、不要なIDの残存有無が確認されている

28 BCP対策で定めた対応手順にもとづく訓練が定期的に実施され、手順の見直しが行われている

39 インターネットに繋がる情報系LAN上の端末やNASに診療情報を保管していない

△：一部充足の項目（抜粋）

6 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『情報システム運用管理規程』があり、各部署にペーパーで保管されている、あるいは各部署の端末から閲覧できる

24 USBメモリの利用に関するルールがあり、適切に運用されている

26 BCP対策で定めた電子カルテ等院内システムがダウンした際の対応手順があり、各部署にペーパーで保管されている

34 サーバ室の空調機器は故障に備えて2基設置されており、サーバ室の室温異常をシステム運用担当者が把握できる

47 情報システム・医療機器の保守回線とこれに接続されたネットワーク機器（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

D. 考察

1. 初のグループ外病院監査における考察

・監査チェックシートは大幅な修正を行ったが、なお標準化に不十分だった項目がある、また類似した内容の項目が複数あるなどさらなる検討と改善が必要。

・事前の資料準備での病院負担を軽減するため、現場の状況は写真提出ではなく当日確認としたが、現場訪問のルート設定がやや曖昧でこれを明確にすればより効率的にラウンドできたと考える。

・文書監査後にその結果を送付するだけでなく、Web会議等で結果の説明、現地監査の段取りや準備等についてコミュニケーションを取ればお互いに理解を深め、より良い監査に繋がると考える。

2. 監査結果の考察

・セキュリティに配慮された運用が見られる一方、情報漏えいやウイルス感染に繋がるセキュリティリスクが存在することも確認された。

・最も大きな課題は厚労省ガイドラインにもとづく「情報システム運用管理規程」の内容が不十分であり、診療情報の電子的な取り扱いと情報システムの運用に関する安全管理のルールが確立していない点である。

・まずは運用管理規程の整備により情報システムのセーフティ／セキュリティのルールとその責任者および運用体制を明確に定めること、次にそのルールを院内に周知し、ル

ールに沿った運用を行うことが診療情報や情報システムの安全に繋がると考える。

・大規模停電やサイバー攻撃の際の備えが十分でないことも懸念される点である。システムを停止させないこと、また停止した場合の診療継続については院内で検討の上早急な対応が必要と考える。

・SEは専任1名・兼任1名、知識や経験もあり精一杯業務に取り組まれていると感じたが、いかんせん医療機関でのIT関連業務は多岐にわたり、厚労省を含め国の施策もあり増加の一途である。情報を的確につかみ対応していくこと、特に十分なセキュリティ対策を取ることは現状の体制ではかなり難しいと思われる。

E. 結論

R6年度は徳洲会グループ病院でこれまでどおりシステム監査を実施しながらその都度フィードバックとシステム監査チェックシートや監査方法の改善を行い、次の監査で試行するというサイクルで継続的なブラッシュアップを行った。R7年3月には初の徳洲会グループ以外の病院でのシステム監査を実施し、目的である監査の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。

システム監査は現状のセキュリティ上の問題点を洗い出すことが目的だが、この問題点を改善しなければ病院のセキュリティレベルは向上しない。しかし「改善を」「ルールの方策を」「関係書類の作成と適切な運用を」と言ってもSEをはじめシステム管理体制に余力がない病院においては病院外からの支援がなければ難しいことをあらためて認識した。この支援についての方法と体制についても徳洲会グループでの改善支援活動をベースにR7年度の研究課題として取り組みたい。

F. 健康危機情報

総括研究報告書に記載

G. 研究発表

福田 秀樹, 江荊 孝, 藤岡 和美, 尾崎 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

福田秀樹. 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～. *第11回日本医療安全学会学術総会*, 2025.3.15

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

	2023年度												2024年度												2025年度											
	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3			
STEP 1	(1) GL6.0版準拠の監査CSの検討 (2) (3) (4) 監査方法・報告書・改善支援内容／方法の検討 CS = チェックシート																																			
STEP 2	(1) 監査CS・方法にもとづく監査実施 (2) 監査の振り返りと修正点の洗い出し (3) 監査CS・方法等の修正 (4) 修正した監査CS・方法にもとづく監査実施																																			
STEP 3	(1) 医療機関の類型化の検討 (2) 類型ごとの監査項目・監査方法等の検討																																			
STEP 4	(1) 『推奨されるシステム監査』の提言検討 (2) システム監査体制等の提言検討																																			