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 取締役会長
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、一方医療機関、特に病院で利用される電子カルテ等はインターネットから分離され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と提言を行うが、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セキュリティ監査を行ってきた。この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、またこれまでの徳洲会グループ病院の監査結果をもとに改善を実施し、標準化に向けた土台作りを行った。続く R 6 年度・7 年度においては引き続き徳洲会グループ 6 病院で監査を実施して毎回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 2 病院での監査を実施した。このグループ外病院の監査では監査項目や提出資料、評価方法についても大幅な見直しを行った。準備から実施、振り返り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大きな一歩を踏み出すことができたと考える。また監査を通じてセキュリティレベルが高く維持されている病院、反対にハイリスクな病院それぞれにその要因は何か、さらには病院に対して真に効果的なシステムセキュリティ監査とはどんなものかについても考察し、提言とした。

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うるパワーを持つ。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、一方医療機関、特に病院の電子カルテ等は現在もインターネットから分離され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セキュリティ監査を行ってきた。この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の「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「システムセキュリティ監査チェックシート」にもとづきＲ５年度に３病院、Ｒ６年度・７年度には計８病院の監査を実施、毎回結果をフィードバックし監査項目や監査方法の見直しを行って次回の監査で検証、というサイクルにもとづく改善を継続的に行った。特にＲ７年３月のＡ病院、同８月のＢ病院は初の徳洲会グループ外の病院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、またここでもフィードバックにより多くの気づきや課題を得ることができ、これらにもとづき国内の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】

Ｒ５年度

６月 30 日　古河総合病院（茨城県）

12 月 20 日　大垣徳洲会病院（岐阜県）

３月 15 日　湘南厚木病院（神奈川県）

Ｒ６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）

Ｒ７年度

７月 30 日　野崎徳洲会病院（大阪府）

８月 29 日　Ｂ病院（千葉県）

１月 14 日　野田総合病院（千葉県）

３月 19 日　出雲徳洲会病院（島根県）

C. 研究結果

ここではＲ７年３月と８月に実施した徳洲会グループ外のＡ病院・Ｂ病院での監査について、その準備と実施および改善について記述する。

（1）A病院

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　システムセキュリティ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提出方法	資料等の確認	結果
管理体制					
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別名称の役職者でも良い）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役職者の役割が確認できる資料（規程の該当部分など）	①・②ともデータかPDFでご提出ください（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ともデータかPDFでご提出ください（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回程度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（回覧記録や幹部が出席する会議の議事録など）	①・②ともデータかPDFでご提出ください（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掲示されている	①病院の個人情報保護方針 ②個人情報保護方針の掲示状況（当日）	①はデータかPDFでご提出ください ②は当日掲示を確認します	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あり、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（申請書類など）	①はデータかPDFで ②は実際に使われた（記載のある）ものをデータかPDFでご提出ください（２部）	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行う。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 徳洲会グループ標準書式の書き換え

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

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 ヵ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

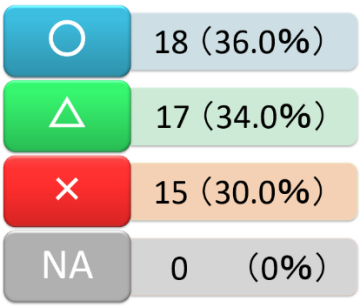
A病院での監査結果とそこにあらわれた課題について記述する。

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）



○：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。

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

（２）B病院

１．監査チェックシートの見直し

A病院での結果にもとづき、標準化として不十分と思われる部分を中心にブラッシュアップを行った。

２．監査方法の見直し

① 事前のコミュニケーションの強化

監査期間前に病院側のメンバーと監査メンバーでWebによる顔合わせおよび監査に関する説明と質疑応答の時間を設けた（約１時間）。これにより病院は比較的スムーズに監査準備に取りかかることができ、また資料準備期間のメールによる質疑応答もより活発に行われたと考える。

② 監査後のコミュニケーションの強化

監査報告書提出後に病院より報告書の内容についての詳細説明と意見交換の機会を設けることが提案された。これを受けて Web で実施し、病院は監査結果についてより深い理解を得られ、監査メンバーは病院からの率直な意見を聞くことで多くの気づきがあり、取り組むべき課題を知ることができた。非常に有意義な場となり、監査メンバーは監査後のコミュニケーションの重要性について認識した。

3．監査の実施と結果

A病院と比較すると院内のセキュリティルールや BCP 対策も整備されているなど、セキュリティレベルは高く感じられた。しかし総評で示した結果では指摘事項となる「△・×」の項目数はA病院とほとんど変わらなかった。個々の内容を確認すると「○にわずかに届かない△」が多いことが判明し、3段階評価が実態を表すには粗いものであることを実感した。そこで後日の監査報告書作成にあたり 4 段階評価（充足率で評価／A：80%以上　B：50～79%　C：20～49%　D：20%未満）を採用し、これにより監査メンバーが現地で感じたセキュリティレベルに近い結果を得ることができた。

表４　３段階 → ４段階評価への見直し

表５　B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	A	B	C	D	NA
管理体制	2	1～2	2	0	0	0	0
個人情報保護	1	3	1	0	0	0	0
文書類の整備	3	4～6	2	1	0	0	0
管理者権限の管理	4	7～10	1	1	0	2	0
ＩＤ･パスワード管理	8	11～18	2	0	4	2	0
サイバー攻撃･災害･BCP対策	10	19～28	5	3	1	1	0
サーバ管理	7	29～35	3	1	2	1	0
端末管理	8	36～43	3	1	3	0	1
ネットワーク管理	5	44～48	1	1	1	2	0
その他	2	49～50	0	1	0	1	0
合 計	50		20	9	11	9	1

D．考察

1．初のグループ外病院監査における考察

① 監査チェックシートの標準化

監査チェックシートは２度のグループ外病院の監査を通じてベースとなった徳洲会グループのものから様変わりし、なお改善の余地はあるもののより標準的な内容に書き換えることができた。

② コミュニケーションの重要性

システムセキュリティ監査の受審経験がない病院にとっては各フェーズでの綿密なコミュニケーションが想像以上に重要であることを実感した。期間前・資料準備期間中・現地監査中・総評時・監査報告書提出後、それぞれのフェーズで活発な質疑応答が行われることにより、病院は監査の意義や効果、取り組むべき課題などをより深く理解し、指摘された事項を改善するモチベーションを高めることができる。多く質問されたのはその項目について徳洲会グループでは具体的にどのような取り組みをしているかというものであったが、普段現場で対策に当たる現役の病院 SE が監査メンバーにいることで具体的な対策を示すことができ、これは病院にとって非常に有効なものであったと考える。

2．セキュリティレベルに差が生まれることに対する考察

徳洲会グループの内外を問わず、監査を行う

と病院によってセキュリティレベルに大きな差が生じていることがわかる。要因は様々考えられるが、過去の監査結果にもとづいて見ると病院の規模や病床区分、医療情報システムの規模、院内 SE の人数といったことにより明確な傾向は現れなかった。唯一要因として実感できるのは病院幹部のセキュリティに対する関心や重要性の認識の違いである。幹部がセキュリティ対策について理解のある病院（幹部が総評に出席し積極的に質問や相談を行う、指摘事項の改善の推進を院内に指示するなど）は現場の職員もセキュリティに関する意識が高く、院内 SE もセキュリティ関連業務に時間を割き、また各部門のメンバーで構成するシステム委員会が機能して病院全体でセキュリティ対策に取り組んでいるといった傾向が明らかになった。一方、病院幹部がセキュリティに対して関心を示さない病院は職員・院内 SE・システム委員会についても前述の逆の状態にあり、結果として多くのセキュリティリスクを抱えているケースが多い。

3.「求められるシステムセキュリティ監査」に関する考察

① 一般的なシステムセキュリティ監査の問題点

セキュリティベンダーやコンサル等の専門家によるシステムセキュリティ監査と改善支援は各業種で広く行われているが、これを現在の医療業界でそのまま行うには無理があると考える。現場への教育の不足も要因の一つだが、病院の SE ですら電子カルテや部門システムには強いがセキュリティは苦手とするケースが多い。ましてや病院幹部や一般職員にはセキュリティのハードルはまだまだ高い。

②「誰もが理解できるシステムセキュリティ監査」

監査を行って問題点を洗い出し、解決策を提示しても病院がその意義や内容を理解できなければ改善はできない。セキュリティ対策には少なくないコストが発生したり現場の職員に負担を強いるものもある。病院の幹部がその重要性を理解して費用を捻出し、院内 SE や現場の職員に強いメッセージを出す必要がある。「病院の誰もが理解できるシステムセキュリティ監査」が強く求められる。私たちがこの研究を通じて模索し実践してきた「医療現場を良く知る病院職員（SE）らによるシステムセキュリティ監査」の有効性を明確にできたと考える。

4．内部監査と外部監査に関する考察

徳洲会グループにおいても人的資源の制約により監査を行えるのは年 4 病院程度にとどまる。これでは監査を受けられない病院が多く、グループ全体のセキュリティレベルは思うように上がらない。そこで監査チェックシートから重要な項目を絞り、これに実施手順やチェック方法を記載した平易なマニュアルを作成、病院はこれにより定期的（年 1 回程度）に内部監査を実施する。さらに 2～4 年に 1 回程度の外部監査で専門的視点からの助言や支援を行い、病院幹部とも面談し理解を得る。このサイクルを確立することで病院のセキュリティレベルは確実に向上すると考える。

E. 結論

研究期間を通じて徳洲会グループで行ってきたシステムセキュリティ監査のブラッシュアップと標準化に、グループ内外の病院での監査を実施しながら継続的に取り組んだ。特に初の徳洲会グループ以外の 2 病院でのシステム監査が標準化に大きく寄与したと考える。また監査結果を考察することで病院のセキュリティレベルの差に病院幹部の理

解や認識が大きな影響を与えていることがわかり、病院幹部をはじめ中間管理職、現場の職員にも理解できるわかりやすいシステムセキュリティ監査が重要かつセキュリティレベルの向上に有効であることも考察できる。D.4.の内部監査と外部監査を継続的に実施することでセキュリティ対策が日常的なものとして医療スタッフの意識に、医療現場の運用に根付いていく。幹部と院内 SE、現場の医療スタッフの共通理解と協力のもと、病院のセキュリティレベルの向上が期待される。

F. 研究発表

福田 秀樹. 医療機関におけるサイバーセキュリティ対策～その現実と問題解決に向けて. *第 10 回日本医療安全学会学術総会,2024.4.13*

尾﨑 勝彦. 病院経営に大きなメリットをもたらす情報の一元化とデータの利活用. *医事業務 No.675, 2024.9.1*

福田 秀樹. 医療機関におけるサイバーセキュリティ対策～その現実と問題解決に向けて. *最新医療経営フェイズ3 Presents 医療経営セミナー<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>の有効な活用とは？, 2024.9.13*

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

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*

福田 秀樹、尾﨑 勝彦. ～医療機関のサイバーセキュリティ対策～徳洲会グループシステム監査：標準化の試み. *医療情報学*, 2025

G. 知的財産権の出願

該当なし

資料：システムセキュリティ監査チェックシート① 項番 1～19

	項　目	監査対象資料等	監査対象資料：提出方法等	厚労省GL要求事項	資料等の確認時期	結果
	管理体制					
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別名称の役務者でも良い）が任命され、それぞれの役割が明文化されている	①役務者名簿（氏名・所属・院内役職が記載されたもの） ②役務者の役割が確認できる資料（規程の該当部分など）	①・②ともデータかPDFでご提出ください（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、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名簿（氏名・所属が記載されたもの） ②情報システム委員会議事録 ③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（回覧記録や幹部が出席する会議の議事録など）	①・②・③ともデータかPDFでご提出ください（①は最終更新日があるもの／②は2回分）		事前	
	個人情報保護対策					
3	病院の個人情報保護方針は個人情報保護法が求める内容を適切に反映（個人情報の利用目的や苦情相談窓口が明記されているなど）しており、患者の見える場所に掲示されている	①病院の個人情報保護方針 ②個人情報保護方針の掲示状況（当日）	①はデータかPDFでご提出ください ②は当日掲示を確認します	○	事前および当日	
	文書類の整備					
4	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	①ガイドライン第6.0版に準拠した運用管理規程 ②①が各部署でペーパー保管されている、あるいは各部署の端末で閲覧可能なこと（当日）	①はデータかPDFでをご提出ください ②は当日任意の部署で確認します	○	事前および当日	
5	『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（MDS／SDSを含む）が保管されている	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（医療機関確認用） ②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） ③MDS/SDS	①・②・③ともデータかPDFでご提出ください（②・③は2社分）	○	事前	
6	業務委託をしている外部業者とは秘密保持について明記した契約書を締結している	秘密保持契約書あるいは秘密保持条項が含まれる業務委託契約書等	データかPDFでご提出ください（2部）	○	事前	
	管理者権限の管理					
7	管理者ID（電子カルテのサーバOSや電子カルテの）は必要最低限のものが登録されている	管理者ID（サーバOSや電子カルテの）が記載された一覧表など	データかPDF（最終更新日があるもの）でご提出ください	○	事前	
8	サーバOSの管理者IDのパスワードは同一のもの、また容易に類推可能なものを使用していない	サーバOSの管理者IDのパスワード	当日確認します	○	当日	
9	管理者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	管理者IDの棚卸しが行われたことが確認できる資料	データかPDF（棚卸し実施日があるもの）でご提出ください	○	事前	
10	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	ログイン／ログアウトおよびログインの失敗ログが確認できる画面	画面のハードコピーをご提出ください	○	事前	
	ID・パスワード管理					
11	電子カルテIDの登録・変更・削除の申請と承認に関するルールがあり、適切に運用されている	①電子カルテIDの登録・変更・削除の申請・承認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（申請書類など）	①はデータかPDFで ②は実際に使われた（記載のある）ものをデータかPDFでご提出ください（2部）	○	事前	
12	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	①電子カルテIDのパスワードの桁数・使用文字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電子カルテIDのパスワード桁数・使用文字を制限する設定情報	①はデータかPDFで ②はデータかPDFあるいは設定情報画面のハードコピーをご提出ください	○	事前	
13	電子カルテのログイン試行回数は上限が設定されている	①電子カルテのログイン試行回数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電子カルテのログイン試行回数を制限する設定情報	①はデータかPDFで ②はデータかPDFあるいは設定画面のハードコピーをご提出ください	○	事前	
14	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	電子カルテIDの棚卸しが行われたことが確認できる資料	データかPDF（棚卸実施日があるもの）でご提出ください	○	事前	
15	他の職員の電子カルテIDを利用するなどの不適切なID運用をしていない	①不適切なID運用の禁止を職員に周知する資料 ②その周知方法が確認できる資料（職員向け掲示、イントラサイト上にその情報が表示された画面、会議・研修会のレジュメや議事録など） ③職員の電子カルテID運用の認識（当日）	①はデータかPDFで ②はデータかPDFあるいは画面のハードコピーをご提出ください ③は当日任意の部署で職員の認識について確認します	○	事前および当日	
16	電子カルテの共用ID（複数の職員・実習生などが一定期間同じIDを利用するもの）に関するルールがあり、適切に運用されている	①共用IDのルールが確認できるもの（規程の該当部分など） ②共用IDの運用が確認できるもの（共用IDの管理簿など）	①はデータかPDFで ②は実際に使われた（記載のある）ものをデータかPDFでご提出ください		事前	
17	電子カルテIDごとのアクセスログを取得し、いつでも調査可能な状態にある	電子カルテのアクセスログデータあるいはアクセスログが表示された画面	データかPDFあるいは画面のハードコピーをご提出ください（1画面分程度）	○	事前	
18	電子カルテ利用者の職種・担当業務等による診療情報へのアクセス権限を設定している	電子カルテのデータアクセス権限の設定が確認できる資料（職種別権限一覧表など）	データかPDF（最終更新日があるもの）でご提出ください	○	事前	
	サイバー攻撃・災害・BCP対策					
19	すべてのサーバおよび端末にウイルス対策ソフトを導入し、最新のパターンファイルを適用している	①ウイルス対策ソフトのライセンスを購入していることが確認できる資料 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最終更新日時（当日）	①はデータかPDFで ②はデータかPDF（最終更新日があるもの）でご提出ください ③は当日電子カルテサーバと端末で定義ファイルの更新日時を確認します	○	事前および当日	

資料：システムセキュリティ監査チェックシート② 項番 20～37

	項　目	監査対象資料等	監査対象資料：提出方法等	厚労省GL要求事項	資料等の確認時期	結果
20	不審なメールの添付ファイルの開封、ウェブ利用でのウイルス感染警告アラート表示への対応方法など、インターネットに接続する端末のウイルス感染やサポート詐欺対策が周知されている	①ランサムウェアやサポート詐欺等のサイバー攻撃防止対策を職員へ周知する資料 ②その周知方法が確認できる資料（職員向け掲示、イントラサイト上にその情報が表示された画面、会議・研修会のレジュメや議事録など） ③職員のウイルス感染防止の認識（当日）	①はデータかPDFで ②はデータかPDFあるいは画面のハードコピーをご提出ください ③は当日任意の部署で職員の認識について確認します		事前および当日	
21	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ランサムウェア等ウイルス感染時の初動対応について記載された資料 ②その周知方法が確認できる資料（職員向け掲示、イントラサイト上にその情報が表示された画面、会議・研修会のレジュメや議事録など） ③職員のウイルス感染時初動対応の認識（当日）	①はデータかPDFで ②はデータかPDFあるいは画面のハードコピーをご提出ください ③は当日任意の部署で職員の認識について確認します	○	事前および当日	
22	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	①USBメモリの利用に関するルールが確認できる資料（規程の該当部分など） ②USBメモリの制御設定情報（ActiveDirectory ・ウイルス対策ソフトなどの） ③USBメモリ利用許可端末の一覧（部署名・用途が記載されたもの） ④病院から部署・職員へ貸与しているUSBメモリの一覧 ⑤端末でのUSBメモリ制御状況（当日）	①・③・④はデータかPDFで ②はデータかPDFあるいは画面のハードコピーをご提出ください ⑤は当日任意の部署の端末で設定状況を確認します	○	事前および当日	
23	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あり、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（申請書類など）	①はデータかPDFで ②は実際に使われた（記載のある）ものをデータかPDFでご提出ください（2部）	○	事前	
24	電子カルテサーバのデータ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の仕組み（データの流れ、世代数、バックアップ間隔、オンライン／オフラインの別など）が確認できる資料	データかPDFでご提出ください	○	事前	
25	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	①BCP対策で定めた対応手順が確認できる資料（院内システムダウンマニュアル等） ②院内システムがダウンした際の職員の緊急連絡網 ③院内システムがダウンした際のシステム業者連絡先一覧 ④①・②・③の部署でのペーパー保管状況（当日）	①・②・③はデータかPDFでご提出ください ④は当日任意の部署でペーパーでの保管状況を確認します	○	事前および当日	
26	BCP対策で定めた対応手順には電子カルテ復旧後の事項についても記載されている	項目26の①と同じもの	データかPDFでご提出ください		事前	
27	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	①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たことが確認できる資料（報告書・訓練記録など） ②訓練の手順見直しを行ったことが確認できる資料（議事録・検討資料・改定前と後のマニュアル等）	①・②ともデータかPDFでご提出ください	○	事前	
28	電子カルテサーバや主要なネットワーク機器は非常用電源に接続され、停電時にも電子カルテが限定された端末から利用できる	電子カルテサーバや主要なネットワーク機器の非常用電源への接続状況（当日）	当日接続状況を確認します		当日	
	サーバ管理					
29	サーバ管理台帳があり、随時最新の状態に更新されている	①サーバ管理台帳 ②①のシステム管理室での保管状況（当日）	①はデータかPDF（最終更新日のあるもの）でご提出ください ②は当日保管状況を確認します	○	事前および当日	
30	サーバの名称・機能がわかりやすく明示されている	サーバの名称・機能の明示（サーバに貼られたラベル・タグなど）状況（当日）	当日明示の状況を確認します		当日	
31	サーバの異常の有無を毎日確認している	サーバの異常の有無を記録している資料	データかPDFでご提出ください（直近1ヵ月分）		事前	
32	サーバ室は常時施錠されており、入退室管理が行われている	①サーバ室の入退室記録が確認できる資料 ②サーバ室の施錠管理状況（当日）	①はデータかPDFで提出ください（直近1ヵ月分） ②は当日施錠の状況を確認します	○	事前および当日	
33	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	①サーバ室の空調設備（当日） ②室温異常時のシステム運用担当者等への通知方法（通知システムのマニュアルや送信されたメッセージなど）（当日）	①・②とも当日状況を確認します		当日	
34	サーバ室の天井部分からの水漏れ対策を行っている	サーバ室の天井からの水漏れ対策（当日）	当日対策の状況を確認します		当日	
35	サーバ室は災害時に被害を受けにくい場所にある	病院平面図（サーバ室のあるフロアのみ、階数が確認できるもの）	データかPDFでご提出ください	○	事前	
	端末管理					
36	電子カルテ端末の管理台帳があり、随時最新の状態に更新されている	①電子カルテ端末管理台帳 ②①のシステム管理室での保管状況（当日）	①はデータかPDF（最終更新日があるもの）でご提出ください ②は当日保管状況を確認します	○	事前および当日	
37	電子カルテ端末にパスワードでの復帰が必要なスクリーンセーバを設定している	電子カルテ端末のスクリーンセーバ設定状況（当日）	当日任意の部署で端末を確認します	○	当日	

資料：システムセキュリティ監査チェックシート③ 項番 38～50

	項　目	監査対象資料等	監査対象資料：提出方法等	厚労省GL要求事項	資料等の確認時期	結果
38	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	情報系端末と共用NAS中の診療情報の有無（当日）	当日任意の部署の情報系端末と共用NASを確認します		当日	
39	院外に持ち出す情報機器（端末・記憶媒体等）の管理に関するルールがあり、適切に運用されている	①院外に情報機器を持ち出す際の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（申請書類など）	①はデータかPDFで ②は実際に使われた（記載のある）ものをデータかPDFでご提出ください（2部）	○	事前	
40	個人所有パソコンの院内ネットワークへの接続ルールがあり、適切に運用されている	①個人所有のパソコンを院内ネットワークに接続する際の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（申請書類など）	①はデータかPDFで ②は実際に使われた（記載のある）ものをデータかPDFでご提出ください（2部）	○	事前	
41	電子カルテ端末（ノート型）に盗難防止対策を施している	電子カルテ端末（ノート型）の盗難防止対策状況（当日）	当日任意の部署で端末を確認します	○	当日	
42	端末やサーバの廃棄に関するルールがあり、適切に運用されている	①端末やサーバの廃棄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業者から提出された廃棄証明書・HDD破壊の写真等	①・②ともにデータかPDFでご提出ください	○	事前	
43	端末故障時に交換する予備機が常備されている	予備機の確保状況（当日）	当日予備機の確保状況を確認します		当日	
	ネットワーク管理					
44	院内のネットワーク機器管理台帳があり、随時最新の状態に更新されている	①ネットワーク機器管理台帳 ②①のシステム管理室での保管状況（当日）	①はデータかPDF（最終更新日があるもの）でご提出ください ②は当日保管状況を確認します	○	事前および当日	
45	院内LAN配線図があり、随時最新の状態に更新されている	①院内LAN配線図 ②①のシステム管理室での保管状況（当日）	①はデータかPDF（最終更新日があるもの）でご提出ください ②は当日保管状況を確認します	○	事前および当日	
46	情報システム・医療機器の保守回線とこれに接続されたリモート保守用のネットワーク機器（VPNルータ等）が一覧化されている	情報システム・医療機器保守回線およびネットワーク機器の一覧表など	データかPDFでご提出ください	○	事前	
47	リモート保守用のネットワーク機器のファームウェアは最新のものに更新されている	46の一覧表などでファームウェアの情報が記載されているもの	データかPDFでご提出ください	○	事前	
48	診療系の無線LANのSSIDは非表示（ステルス）かつ暗号化（WPA2以上）の設定をしている	①電子カルテ用の無線LANアクセスポイントの設定情報（SSID・ステルス情報・暗号化など） ②端末でSSIDが見られないこと（当日）	①はデータかPDFあるいは画面のハードコピーをご提出ください ②は当日任意の部署で端末を確認します	○	事前および当日	
	その他					
49	ソフトウェア管理台帳（電子カルテアプリケーション・その他）があり、随時最新の状態に更新されている	①ソフトウェア管理台帳 ②①のシステム管理室での保管状況（当日）	①はデータかPDF（最終更新日があるもの）でご提出ください ②は当日保管状況を確認します	○	事前	
50	サイバーセキュリティに関する職員への研修や教育、意識啓発の取組みが行われている	①職員研修が実施されたことが確認できる資料（レジュメ・議事録など） ②研修資料や院内に共有した厚労省・関係団体等による注意喚起文書等、	①・②ともデータかPDF（実施日等がわかるもの）でご提出ください	○	事前	