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

サイバーセキュリティ対策の相互チェックの手順書の作成

研究分担者　武田　理宏　大阪大学大学院医学系研究科

研究要旨

本研究は、医療機関におけるサイバーセキュリティ対策の向上と均てん化を目的として、医療安全分野で実施されている「相互チェック」や「ピアレビュー」の仕組みを参考に、サイバーセキュリティ対策の相互チェック手順書を作成することを目的としたものである。近年、厚生労働省による「医療情報システムの安全管理に関するガイドライン」改定や「サイバーセキュリティ対策チェックリスト」の策定等により、医療機関における対策強化がはかられている。しかし、対策には投資や専門人材が必要であり、各医療機関において適切な対策レベルを判断することは容易ではない。このため、他施設との比較や優良事例の共有を可能とする相互チェック体制の必要性が高まっている。

本研究では、大阪大学医学部附属病院中央クオリティマネジメント部へのヒアリングを通じて、国立大学病院で実施されている医療安全・質向上のための相互チェックおよび特定機能病院間のピアレビューの運営実態を調査した。医療安全分野では、過去の重大医療事故を契機として全国統一のチェック体制が整備され、現在は重点項目に特化した相互訪問型のレビューへと発展している。重点項目は、最新の課題やガイドラインを踏まえて専門 WG が設定し、2 年 1 サイクルで相互訪問と改善確認を行う仕組みとなっている。また、特定機能病院間のピアレビューでは、医療法に基づき毎年の実施が義務化されており、医療安全体制や医薬品管理等について継続的な相互評価が行われている。

これらを踏まえ、本研究ではサイバーセキュリティ対策においても、毎年実施する基本項目と、最新の脅威や課題に応じた重点項目を組み合わせた相互チェック制度の導入が有効であると考察した。基本項目には厚労省チェックリストや本研究班によるセキュリティ監査項目を活用し、重点項目は専門 WG が設定して 2 年間で改善状況を確認する運用が望ましいと考えた。また、訪問ペアを毎年変更し、Group A～C 人材を含めた多層的な参加体制とすることで、人材育成や知見共有にも寄与すると考えられた。さらに、制度運営には取りまとめ医療機関と専任事務局の設置が不可欠であり、継続的な予算措置や人的支援が必要であると考えられた。

A．研究目的

医療機関におけるサイバーセキュリティ対策は、厚生労働省が中心となる「医療情報システムの安全管理に関するガイドライン」改定や「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」策定、「医療機関におけるサイバーセキュリティ確保事業」等により対策が進められている。サイバーセキュリティ対策を進めるためには医療機関による投資が必要となる。各医療機関で費用対効果を見極めながら投資を行うことになるが、どこまで対策を進めることが望ましいかの判断は簡単ではない。また、サイバーセキュリティ対策には、医療機関のサイバーセキュリティ人材だけでなく、病院執行部の意向や医療情報システムベンダーやネットワーク事業者との調整が関わるため、他医療機関がどの程度の対策を進めているか、他医療機関の良い取り組み事例の把握などが非常に参考になると考えられる。

本研究では、サイバーセキュリティ対策の相互チェックの手順書の作成を目的としている。

B．研究方法

医療安全領域では、国立大学病院間では「医療安全・質向上のための相互チェック」、特定機能病院間では「特定機能病院間相互のピアレビュー」が実施されている。これらの相互チェックは、各施設の医療安全対策の向上だけでなく、全ての施設の医療安全対策レベルの均てん化に貢献している。

そこでサイバーセキュリティ対策においても、先行する医療安全対策の取り組みを倣った相互チェック手順を構築するため、国立大学病院の相互チェックの取りまとめを行っている大阪大学医学部附属病院中央クオリティマネジメント部からヒアリング調査を実施した。

倫理的配慮

本研究はヒアリング調査であり、人を対象とする研究は含まれず、倫理的配慮は該当しない。

Ｃ．研究結果

１．「医療安全・質向上のための相互チェック」

１―１．歴史と概要

平成11年に横浜市立大学病院で患者取り違え事故等が起こり、国立大学附属病院で「医療事故防止のための安全管理体制の確立に向けて（提言）」を作成し、この提言を実施できているかを全国統一チェック項目で相互チェック（500項目）することになった。

平成19年から、国立大学病院長会議の常置委員会診療担当（医療安全管理）校である大阪大学が実施するようになり、以下のような変革が行われた。

- 「自己チェックシート（従来の500項目）」と「重点項目（最新の知見から、取り組むべき事項）」の2本立てとする
- 重点項目について詳しい専門家を全国から集めた「相互チェックWG」を設置して、重点項目に関するチェック項目を作成
- 平成24年度からは重点項目について相互訪問にて確認・意見交換する年と、その際に指摘された事項を含めて改善に取り組んだことを報告する年との2年1セットに（相互訪問は2年に1回へ）
- 令和元年頃に自己チェックシートは不要と判断し終了。重点項目のみのチェックへ。

１－２．重点項目に関する相互チェック

基本的には（国内外の）ガイドラインや提言、なすべきこととされることがある程度明確な事柄を重点項目のテーマとし、その導入を促進することを目的としている

≪これまで取り扱ってきたテーマ≫

- 手術安全チェックリストの導入
- 鎮静下処置の安全
- 入院時支援
- 画像レポート確認
- 働き方改革と医療の質・安全の担保

≪スケジュール≫

4月：

- 重点項目のテーマを決定（担当校医療安全部門が中心となって議論）
- 重点項目によりWGメンバー決定

5～6月：

- WGを対面またはオンラインで開催し、質問項目を作成
- 事務局（担当校医事課）で、確定した項目をエクセルシート化
- 訪問ペアの作成

※訪問大学と被訪問大学が異なるように、かつ直近10年以内は同じ相手にならないように、（担当校医事課）がペア表を作っている

※病院長や副病院長の日程を合わせる必要があると、日程調整に苦慮する。

※厚生労働省は、地区レベルでの訪問案や、国公立だけでなく私立大学も含めて相互訪問する案を提案（国公立だけでなく、多様な背景を有する私立大学病院まで含めると、事務局負担が過剰になることと、文化も違うことから、医療安全では国公グループと私立グループに分けている）。

7月末：

- 全国の国公立大学病院医療安全担当窓口へ送付

⇒訪問大学と被訪問大学は秋に訪問できるよう日程調整

※訪問側は医療安全担当副病院長、医療安全部門、重点項目に応じたメンバー

9～12月初旬まで：

- 相互訪問
- 訪問校は、評価結果を事務局（担当校医事課）に提出

12月末：

- 事務局（担当校医事課）が全51大学病院のシートを単純集計したシートを作成
- 担当校医療安全部門に集計結果を共有

～翌年度4月：

- 担当校医療安全部門が中心となりつつWGメンバーで報告書作成

翌年度5月頃：

- 改善状況調査の項目を作成
- （担当校医療安全部門が中心に作成し、WGはオンライン開催とすることが多い）

翌年6月：

- 国立大学病院長会議総会で報告、報告書配布

翌年7月末：

- 改善状況調査シートを全国へ送付

２．「特定機能病院間相互のピアレビュー」

群馬大学病院の腹腔鏡で死亡症例が相次いだ事案を受けて厚労省が医療法を改正し、「特定機能病院間相互のピアレビュー」を「毎年」行うことが義務化された。

- 医療法で医療安全体制（全死亡症例の把握、質モニタリング、重大事象への対応など）、医薬品安全管理、未承認新規医薬品、高難度新規医療技術、外部監査の5領域を中心に相互訪問で確認を行う規程がある。
- 調査項目は前回の調査項目を引き継ぎながら

少しずつ深掘りしている、という状況である。
- 訪問のペアは、医療安全・質向上のための相互チェックと同じペアで、訪問時に同時に調査を行う。
- 相互チェックWGでは相互チェック用と、ピアレビュー用と、2種類の質問項目と報告書を作成することとなり、相互訪問も隔年から毎年へと変更になった。
- 「相互チェック＋ピアレビュー」項目を実地調査する年と「ピアレビュー」項目を主に実地調査する年（相互チェックは書面調査）の交互
- ピアレビューが開始となり厚生労働省から予算が事務局につくようにはなったが年々減少傾向となっている。
- 年間を通じた業務負担は非常に大きい。

D．考察

1．医療機関におけるサイバーセキュリティ対策の相互チェック

毎年チェックを行う基本項目と、サイバーセキュリティインシデントの発生状況や新たなサイバーセキュリティ対策などを反映した重点項目を定め、相互チェックを行うことが好ましいと考える。

基本項目は、厚生労働省が定める医療機関等におけるサイバーセキュリティ対策チェックリストを網羅した上で、本研究班で定める「セキュリティ監査項目一覧」からリストを作る必要がある。基本項目の相互チェックを毎年行うことで集中管理機関間のサイバーセキュリティ対策状況の比較だけでなく、経年的なサイバーセキュリティ対策の向上を定量化することができる。

重点項目は、集中管理機関のGroup A人材からWGメンバーを選定し、WGで適切なテーマを決める必要がある。重点項目は医療安全と同様に2年で1つのテーマを取り扱い、1年目の相互チェックを受けた改善状況を2年目で確認することで、確実なサイバーセキュリティ対策の向上につながると考えられる。

2．医療機関におけるサイバーセキュリティ対策の相互チェックの訪問ペアと訪問者、応対者の構成

訪問ペアは訪問機関と被訪問機関を異なるように設定することで、2つの医療機関とディスカッションができることになる。また、毎年、訪問ペアを変更することで、様々な医療機関のサイバーセキュリティ対策を学ぶことができる。

訪問者は集中管理機関のGroup A人材を含んだメンバー構成とすることを想定する。応対者は情報セキュリティ責任者（CISO）と医療情報システム安全管理責任者、医療情報システム安全管理責任者と異なればGroup A人材を想定する。今後の人材育成を考えると、それぞれの施設はGroup B人材、Group C人材も訪問者、応対者に含める検討をするべきである。

3．医療機関におけるサイバーセキュリティ対策の相互チェックの取りまとめ医療機関

上記を実現するためには、取りまとめ医療機関を設置することが必須と考える。

取りまとめ医療機関の医療情報システム担当部門が中心となり、相互チェックの企画運営を行っていく必要がある。医療安全の相互チェックでは1年を通じ継続的に業務が発生しており、サイバーセキュリティ対策の相互チェックにおいても専任の教官ポストの検討などが必要と思われる。

その作業負担を考えると事務局は必須と考えられ、医療情報システム部門との連携を考えると、取りまとめ医療機関内に置くことが好ましい。

以上のように取りまとめ医療機関にはしかるべき予算配分が必要と考える。

取りまとめ医療機関以外においても、重点項目の決定やチェック項目の選定を行うWGメンバーを輩出することや、相互チェックでペア医療機関を訪問する必要があるため、取りまとめ医療機関以外においても相応の予算配分が必要と考える。

E．結論

本研究では、医療安全分野で成熟している「相互チェック」および「ピアレビュー」の仕組みを参考に、医療機関におけるサイバーセキュリティ対策の相互チェック制度構築の方向性を示した。サイバーセキュリティ対策は、各医療機関単独で進めるだけでは限界があり、他施設との比較や優良事例の共有を通じて対策レベルを向上・均てん化することが重要である。基本項目と重点項目を組み合わせた継続的な相互チェックにより、経年的な改善状況を可視化し、実効性の高い対策推進が可能になると考えられる。また、WGによる重点項目設定、人材育成を意識した訪問体制、取りまとめ医療機関と事務局の整備が制度運営の鍵となる。今後は、本調査結果を踏まえ、サイバーセキュリティ対策相互チェックの具体的手順を策定していく予定である。

G．研究発表

1．　論文発表

該当なし

2.　学会発表
該当なし

H．知的財産権の出願・登録状況
（予定を含む。）
1．特許取得
該当なし

2．実用新案登録
該当なし

3.その他
該当なし

2.　学会発表
該当なし

H．知的財産権の出願・登録状況
（予定を含む。）
1．特許取得
該当なし

2．実用新案登録
該当なし

3.その他
該当なし