厚生労働行政推進調査事業費補助金

厚生労働科学特別研究事業

医療機関におけるサイバー攻撃対応のための事業継続計画（BCP）の普及に向けた研究

令和5年度　総括研究報告書

研究代表者　鳥飼　幸太

令和６（2024）年　５月

目　　次

厚生労働行政推進調査事業費補助金（厚生労働科学特別研究事業）
（総括）研究報告書

医療機関におけるサイバー攻撃対応のための事業継続計画（BCP）の普及に向けた研究

研究代表者　鳥飼　幸太　《国立大学法人 群馬大学 医学部附属病院システム統合センター》

研究要旨

．研究目的
国内におけるサイバー攻撃の被害が増加しており、医療分野におけるサイバーセキュリティ能力の向上は医療能力の安定提供を通じ国民福祉に貢献する。これまで医療機関におけるサイバー攻撃対策ならびに同攻撃被害時における医療ITの事業継続計画(Business Continuing Plan: BCP)(以下IT-BCP)の策定ならびに実施については各医療機関における自主的な取り組みが進められてきた。一方、人為的サイバー攻撃に対し、NIST CSF(CyberSecurity Framework)における用語の意味での「検知」(Detection)や「対応」(Response)といったアクティブディフェンスを行うために際しては、サイバー攻撃対処の技能習得ならびに実施に際して高度な技術能力が必要である。このため、本研究では医療機関が基本的に備えるべき共通のIT-BCP対策の内容について調査検討し、実施可能なチェックリスト案を作成することを目標とする。

Ｂ．研究方法
本研究では、研究代表者所属機関（群馬大学医学部附属病院）、研究分担者所属機関（徳島大学医学部附属病院、大津赤十字病院）におけるサイバーセキュリティ対策のうち、IT-BCPとして捉えられる内容を調査した。次に、IT-BCP対策の参照資料である「医療情報システムにおける安全管理に関するガイドライン第6.0版」を精査し、IT-BCPが備えるべき特徴のカテゴリについて検討を行い案を作成した。作成にあたっては、米国NIST CSFならびに米国CISA CDM(Continuous Diagnostics and Mitigation)の分類を参考とした。その後、作成したIT-BCPカテゴリを参考としながらIT-BCPが備えるべき項目について検討し、実施可能な記述内容であることを確認しながらチェックリスト（IT-BCPチェックリスト）の作成を行った。

（倫理面への配慮）
本研究では患者および個人に関する情報を扱わないため、倫理面での問題は生じない。

Ｃ．研究結果
1.医療情報システムにおける安全管理に関するガイドライン6.0版におけるCSF/CDM/BCP分類の作成
本研究ではIT-BCPを検討する基礎として、今後遵守の対象となっている医療情報システムにおける安全管理に関するガイドライン第6.0版について、多角的な考察を行う目的で、CSF/CDM/BCP分類のどのカテゴリに相当した内容であるかについて調査を行った。調査の結果、図1に示すように、CSF分類としては識別/防御に関する対策が充実していることが分かった。一方、BCP対策における１次対応に相当するアクティブディフェンス能力である検知/対応については相対的に項目が少ないことがわかった。また、BCPにおいて重要な指標である復旧についても、同様に相対的に項目が少ないことがわかった。本調査項目については別添資料にて記載する。

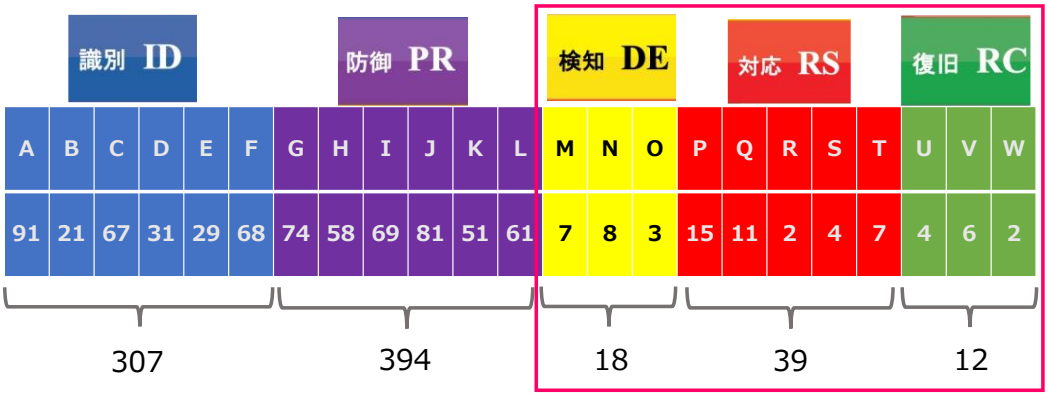

図１医療情報システムにおける安全管理に関するガイドラインのCSFカテゴリ分類

2.医療サイバーセキュリティに関するIT-BCPチェックリストの作成
研究班員はすべて自医療機関（500床以上）での病院情報システム全体更新を主導した経験を有し、またシステムトラブル対処経験を有する。過去にシステムトラブルから復旧した際に必要とした能力や知識について議論を行い、医療機関における事業継続を達成するためには、CSFに示されたサイバー攻撃のみに関する準備のみでは不十分であり、またCDMに示されたサイバー攻撃に備えた防御策のみでも不十分であるとの認識に至った。そこで、サイバー攻撃への対処の中で、システムトラブルと同様の対処が必要な内容を追加し、病院ITのBCPとしてのカテゴリとして以下の５項目を選定した。

１・通常時の備え、
２・サイバー攻撃を覚知できる能力、
３・覚知したサイバー攻撃に対し、自組織の活動停止を回避し、患者生命を保全しつつ攻撃に対処する能力、
４・攻撃の脅威から免れたのち、通常診療のレベルまで速やかに状態を復旧できる能力、
５・復旧後、インシデントに対する振り返りができ能力ならびに善後策を講じる能力

以上の項目より、細目について、CSF/CDMの各5分類からカバーすべき内容に偏りが生じないように内容を選定し記載した。本チェックリストの記載に当たっては、すべての医療機関において使用されるが、特に診療録管理体制加算が充実した200床以上の病院に対して適用できることを考慮して記載した。チェックリストの実施者としては、医療機関におけるシステム管理者のほか、サイバーセキュリティに熟達していない事務職員等においても把握できるよう記載の用語や内容について確認を行った。

D．考察
サイバーセキュリティの実装においては、これまでサイバーセキュリティの専門家のみでの監修が多く、把握すべき資料はインターネットから取得可能ではあるが分量が多いことが理解の妨げになっていたと推測される。また、サイバーセキュリティの用語については、日常用語または医療用語からかけ離れた特有の呼称が多く存在し、サイバーセキュリティの概念の独自性とあわせて理解が困難な側面が存在した。今回、医療機関でのワークフローと連成した資料を作成することにより、医療機関側でセルフチェックが可能になる様式を整備できたと考えられる。これは厚生労働省が目指す均霑化の目的に合致するものと考えられる。また、ガイドライン6.0版のCSF/CDMチェックを事前に行うことにより、各章立てに基づく内容の分割から、その効果に基づく内容の分割を検討でき、BCPとして備えるべき項目に対する根拠づけを行うことができた。

E．結論
本研究は単年度事業であり、研究成果として、医療情報システムにおける安全管理に関する

ガイドライン第6.0版を踏まえた、幅広い医療機関で活用されることを目的としたIT-BCPチェックリスト作成を実施した。

Ｆ．健康危険情報
本研究では生物由来資料、検体、医療機関における診療行為などを調査対象として含まないため、本研究に基づく健康危険は生じないと考えられる。

Ｇ．研究発表
1.　論文発表
鳥飼幸太、　医療機関におけるサイバー攻撃対応のための事業継続計画(BCP)の普及に向けた研究、第43回日本医療情報学会抄録集、2023年11月

2.　学会発表
鳥飼幸太、　サイバー攻撃に備えた医療IT-BCPの策定、第27回日本医療情報学会春季学術大会・シンポジウム（大会企画セッション3）、2023年7月
鳥飼幸太、　医療機関におけるサイバー攻撃対応のための事業継続計画(BCP)の普及に向けた研究、第43回日本医療情報学会シンポジウム、2023年11月

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