

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・分担）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

研究分担者 橋本 智広 «大津赤十字病院 事務部 医療情報課»

研究要旨

本研究では、医療機関が自機関における BCP の策定に向けて、支援するためのツールの作成を行った。具体的には、医療機関における医療情報システムの安定稼働に対する日常的な業務の経験と、前述したサイバー攻撃被害事例を踏まえて、BCP 策定に必要と考えられる要素を整理した。整理した結果を踏まえて、医療機関の BCP 策定を支援するツール（「BCP 策定のための確認表」「確認表の手引き」「ひな形」）を作成した。

A. 研究目的

近年、日本国内の医療機関に対するサイバー攻撃により、診療業務の継続が困難となり診療に多大なる影響を及ぼした事例が相次いでいる。具体的には、徳島県つるぎ町立半田病院（被害年月：令和 3 年 10 月）、大阪急性期・総合医療センター（被害年月：令和 4 年 10 月）の遭遇したランサムウェア被害は国内に広く報道された。これらの事案は、数か月にわたり通常診療の継続が困難な状況に陥った。このことから、医療機関は自施設の情報セキュリティ対策を見直す契機となったことはいままでのない。この状況下で、医療法施行規則の改定（令和 5 年 4 月 1 日施行）において、医療機関の管理者がサイバーセキュリティへの対応が求められる旨が追加された。また、「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（令和 5 年 5 月）」（以下、ガイドラインと略す）が公開されたことで、医療機関はさらなる情報セキュリティ対策が求められるようになった。さらに、医療法に基づく立入検査では、サイバーセキュリティに関する検査項目が追加され、「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」に基づく対応が求められている。各医療機関はこれまで経験したことのないサイバー攻撃による被害に対して、診療継続を含む医療サービスの提供を継続することを目的として事業継続計画（以下、BCP と略す）の策定が求められている。これまで自然災害においては災害拠点病院等を中心に BCP が作成されている現状はあるものの、サイバー攻撃を想定した BCP はその策定にセキュリティに関する知識や技術的対策に対する考慮が必要となるため必要十分な BCP が作成できないことが想像される。

本研究では、医療機関が自機関における BCP の策定に向けて、支援するためのツールの作成を行う。具体的には、医療機関における医療情報システムの安定稼働に対する日常的な業務の経験と、前述したサイバー攻撃被害事例を踏まえて、BCP 策定に必要と考えられる要素を整理する。整理した結果を踏まえて、医療機関の BCP 策定を支援するツール（「BCP 策定のための確認表」「確認表の手引き」「ひな形」）を作成する。

B. 研究方法

本研究は、3 名の研究者により役割分担した上で推進した。具体的には、研究者の所属機関を含むこれまでの教育経験、業務経験から、事実に基づく研究成果が達成できるように務めた。

1. サイバー攻撃の被害に遭遇した医療機関に対する調査および文献調査

前述したサイバー攻撃の被害に遭遇した 2 つの医療機関に対して、当該医療機関の担当者から得られた情報と、一般公開されている報告書から、BCP に必要と想定されることを検討した。具体的には、「徳島県つるぎ町立半田病院コンピュータウイルス感染事案有識者会議調査報告書 (<https://www.handa-hospital.jp/topics/2022/0616/index.html>)」「大阪急性期・総合医療センター情報セキュリティインシデント調査委員会調査報告書 (<https://www.gh.opho.jp/important/785.html>)」から情報収集を行った。

2. 調査結果に基づくガイドラインをベースとした BCP 策定に必要な要素整理

項番 1 の調査から得られた結果を踏まえて、医療機関に求められる安全管理対策が記載されているガイドラインに含まれる「遵守事項」をリストアップし、表 1 に示す分類のどれに該当するかを全ての項目に対してチェックした。なお、本分類は、「NIST-SP800 シリーズ」に記された CDM (Continuous Diagnostics and Mitigation) および「NIST」の CSF(Cybersecurity Framework)をベースに、医療サービス提供において考慮すべき事象を踏まえて設定した。

表1：分類一覧

分類番号	分類名
1	医療装置・直接
2	医療装置・間接
3	関連装置・間接
4	物理インフラ・間接
5	基幹情報サーバ・間接
6	情報サービス・間接
7	診療データ運用・間接
8	不法対策・間接
9	BCP意思決定
10	BCP必要条件

3. 医療機関の BCP 策定を支援するツールの作成

項番 2 の結果を踏まえて、医療機関が自機関で BCP 策定に向けた取り組みが実行できるように「BCP 策定のための確認表」「確認表の手引き」「ひな形」を作成した。

4. ガイドラインの遵守事項に対する不足する項目の洗い出しと追加すべき項目の検討

ガイドラインには、情報セキュリティ対策として必要最低限の対策として遵守事項が示されているが、CDM および CSF の観点と、医療機関での医療情報システムに対する実運用を踏まえて不足している点が発見された。具体的には、CSF に含まれる「検知」「復旧」のフェーズに関連する項目が不足しているとして、追加すべき項目の検討を行った。

(倫理面への配慮)

本研究においては、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として、人を直接の対象とした研究には該当しない。

C. 研究結果

ガイドラインに含まれる「遵守事項」において、表1に示す分類のどれに該当するかを全ての項目に対してチェックした結果を表2に示す。結果として、いずれの分類にも該当しないものが16件確認された。本研究で設定した分類は、医療サービス提供において考慮すべき事象を踏まえてあらかじめ設定したものであった。結果として、遵守事項にも各分類において件数に差はあるものの、比較的網羅されていることが明らかとなった。

表2：分類別の件数

分類番号	分類名	件数
1	医療装置・直接	52
2	医療装置・間接	52
3	関連装置・間接	56
4	物理インフラ・間接	141
5	基幹情報サーバ・間接	137
6	情報サービス・間接	198
7	診療データ運用・間接	121
8	不法対策・間接	168
9	BCP意思決定	54
10	BCP必要条件	135

表2の結果を踏まえて、「BCP策定のための確認表」「確認表の手引き」「ひな形」を作成した。「BCP策定のための確認表」においては、次の5項目を大項目として用意し、各項目に含まれる小項目を設定した。

- (1)平時：
平時において、非常時に備え、サイバーセキュリティの体制整備を行う。
- (2)検知：
医療情報システム等の障害が見受けられる場合は、早期に医療情報システム部門へ報告し、異常内容の事実確認を行う。
- (3)初動対応：
迅速に初動対応を進めて、サイバー攻撃による被害拡大の防止や診療への影響を最小限にする。
- (4)復旧処理：
復旧計画に基づいて、医療情報システムの事業者及びサービス事業者等と協力して復旧を行う。証拠保存の観点からバックアップデータ等を取得する。
- (5)事後対応：
復旧結果の報告を受け、再発防止に向けた検討と再発防止策の周知と実施を進める。

さらに、ガイドラインの遵守事項に対する不足する項目の洗い出しと追加すべき項目の検討として、検知（12項目）、復旧（17項目）、要検討（6項目）を新規追加案として列挙した。

D. 考察

医療機関において、診療提供体制が機関ごとに異なることから、医療情報システムや医療機器等の資産は、医療サービスの提供に必要なものを保有する現状がある。その中で、各機関は独自にBCPを作成する必要がある。医療機関の多くは、前述したとおりサイバー攻

撃の被害に遭遇した施設は多くないため、被害が発生した際の対応として必要な対策がBCPにもれなく含めることができないかもしれない。本研究の支援ツールを用いて作成されたBCPを各機関から収集することで、BCPの比較や診療提供体制ごとベンチマーク、さらには第三者による評価を行うことで、各機関に対するさらなる提言が可能になると考える。

E. 結語

本研究では、医療機関が自機関におけるBCPの策定に向けて、支援するためのツールの作成を行った。医療機関におけるサイバーセキュリティへの対応は、今後さらに高度な対策を求められると考える。その中で、医療機関がサイバー攻撃により診療業務の継続が困難になった場合、医療機関の規模問わず地域医療に与える影響は計り知れない。そのためにも、医療機関は医療サービスの提供に向けたBCPの策定が急務となる。将来的には、各機関において、策定されたBCPが適宜改版され、PDCAサイクルに基づくBCP維持が実践されることを期待する。あわせて、サイバー攻撃に対するBCPと、自然災害、感染等を目的とした既存のBCPを統合した「オールハザード型BCP」の策定が今後必要になると考える。

F. 健康危険情報

G. 研究発表

1. 論文発表

なし

2. 学会発表

- ・鳥飼幸太, 田木真和, 橋本智広. IT-BCPをどう実現するか. 第43回医療情報学連合大会, 2023年11月.
- ・鳥飼幸太, 田木真和, 橋本智広. 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回医療情報学連合大会, 2023年11月.

H. 知的財産権の出願・登録状況

1. 特許取得

なし

2. 実用新案登録

なし

3. その他

なし