令和６年度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）
「医療施設のオール・ハザード型の事業継続計画（BCP）構築に向けた体制確立のための研究」

分担研究報告書

「サイバー・インシデント対応に際し求められる BCP 項目に関する研究」

研究分担者　高橋　礼子
（愛知医科大学　災害医療研究センター　講師）

研究要旨
【目的】サイバー攻撃を含む多様なハザードに対応するため、病院の機能維持に焦点を当てた「オールハザード型 BCP」の整備が求められている。本研究では、自然災害 BCP との比較を通じて、サイバーインシデント特有の対応視点を抽出し、共通項目とあわせて整理することを目的とした。
【方法】自然災害 BCP 及びサイバーインシデントに関する先行研究をもとに、項目の共通性・特異性を概念的に分類するとともに、システム障害の原因や影響範囲の整理、対応タイムライン、復旧優先度を示す図表を作成する。
【結果】障害の程度を 3 段階（全面停止／一部不具合／端末限定）に分類し、それぞれに応じた初動対応と復旧判断の整理を行った（図 1〜3）。また、復旧優先度一覧により、病院機能の段階的回復に必要なシステムの選別が可能となる構成を提示した。障害の原因や範囲が不明確なサイバーインシデントにおいては、早期の可視化と対応パターンの共有が混乱回避の鍵となる。
【考察】サイバーインシデントでは、従来の自然災害とは異なる障害特性を踏まえた即時判断や代替手段の準備が求められるが、一方で、現状分析や病院行動評価群の活用、脆弱性把握、既存患者対応方針の整理といった視点は災害支援で用いられてきた DMAT 等の知見とも重なる。本研究で示した構成要素は、自然災害・感染症・サイバーインシデントといった異なるハザードに共通する基盤として活用可能であり、実効性あるオールハザード型 BCP の構築に貢献すると考えられる。

≪研究協力者≫
大津赤十字病院　橋本　智広

Ａ．研究目的

近年、地震や風水害といった自然災害に加え、感染症の拡大やサイバー攻撃など、医療機関の機能継続を脅かす多様なハザードが顕在化している。従来の病院向け BCP は主に自然災害への対応を中心に整備されてきたが、これら多様化する脅威に対して個別に BCP を作成・運用することは現実的ではなく、災害種別を問わず病院の機能を維持することに主眼を置いた、いわゆる「オールハザード型 BCP」の必要性が高まっている。

とりわけサイバーインシデントは、施設自体の物理的損傷を伴わない一方で、電子カルテやオーダリング、医療機器の連携等を含む、診療業務に影響を与える情報システムの停止により、診療機能に重大な支障をきたす可能性がある。復旧までの時間や影響範囲が原因によって異なる点も、自然災害とは異なる検

討を要する要素である。

本研究では、オールハザード型 BCP 構築に向け、自然災害BCPの既存知見を活かしつつ、サイバーインシデント発生時における対応項目を整理し、「病院の機能維持」に必要な共通事項と、サイバーインシデント特有の対応事項を明確化することを目的とする。

B．研究方法

本研究では、自然災害を中心とした従来の病院向けBCPに関する先行研究[1)2)]を参照し、BCP に含まれる基本的な構成要素や考え方を把握した上で、比較の視点を設定した。また、サイバーインシデント BCP に関する先行研究[3)]を踏まえ、自然災害との共通点や相違点に着目した分析を行った。

さらに本分担研究では、サイバーインシデント発生時の医療機関における対応を現実的に検討するため、以下の資料・構成を独自に作成した。

- **システム障害の原因と使用不可範囲の整理図**
- **使用不可範囲ごとの対応タイムライン**
- **システム別の復旧優先度案**

なお、BCP 項目の「共通／特有」分類については、本研究では概念的・総論的な視点にとどめ、個別のチェックリストによる具体的整理については、堀内分担研究にて作成した事象別 BCP チェックリストに委ねる。

（倫理面への配慮）

本研究においては特定の個人、実験動物などを対象とした研究は行わないため倫理的問題を生じることは少ないと考えられる。

C．研究結果

1．システム障害の原因と使用不可範囲の整理

サイバーインシデントと一口に言っても、実際のシステム障害の原因は多岐にわたり、たとえばサイバー攻撃（ランサムウェア等）に加え、機械的故障、人的ミス、さらには停電なども要因となり得る。また、原因によって復旧までの時間や予測可能性、障害の範囲（全面停止／一部不具合／端末限定）も異なる。

そこで本研究では、こうした多様な原因と影響の広がりを整理した図を作成し（図 1)、医療者にも視覚的に理解しやすい形で、BCP 検討の“出発点”として活用できる資料とした。

2．使用不可範囲毎の対応タイムラインの作成

BCP において対応方針を決定するには、「どのシステムが、どの程度使えないのか」を迅速に判断し、適切な初動をとる必要がある。しかし、個々のシステムごとに細分化して対応を定めようとすると複雑になりすぎ、現場での活用が困難となる。

そこで本研究では、障害の発生範囲に応じて以下の 3 つのケースに分類し、それぞれのケースにおいて共通的な対応の方向性を整理した（図 2)。

- **ケース 1：全面停止（情報システムが全て使用できない）**
- **ケース 2：一部不具合（情報システムの一部が使用できない）**
- **ケース 3：端末限定（特定の端末に限り使用できない）**

具体的に、ケース１は電子カルテやオーダリング、検査機器の連携等を含む情報システムの全てが停止している状態と定義した。この状態は、明らかに現場担当者が把握できると考える。また、現場担当者だけで判断が難しいケースとして、ケース２およびケース３を

定義する。ケース２は情報システムの一部が停止している状態とし、ケース３は特定端末のみ情報システムの使用が制限されている状態と定義した。情報システム担当者は各現場からの障害発生に関する連絡を受けることが想定される。このとき、迅速な対応を行うには速やかに障害の発生範囲を認識する必要がある。この分類により、現場担当者が障害を認識した際に、共通の“ベクトル”を持って対応できるとともに、情報システム担当者とのコミュニケーションにおける共通の“言語化”も目指した。

３．システム別復旧優先度の整理

診療機能の維持に向けて、システムの復旧を段階的に進めるには「どのシステムから復旧すべきか」の判断が重要となる。先行研究においても、「業務フローを意識して、復旧すべきシステムの優先度（復旧する順序）をあらかじめ設定しておくことが望ましい」とされており[3)]、診療機能の早期回復を目的とした復旧計画が求められている。

また、システムの「診療上の重要度」と「復旧優先度」は必ずしも一致するとは限らない。たとえば、検査機器や放射線装置等の医療機器が医療的に重要であっても、初動では受付・電子カルテ参照・オーダリングといった基本的な診療フローを優先すべき状況もある。特に、新患登録には医事会計システムを用いて登録作業を行うため、新患の診療においては医事会計システムが稼働していなければ電子カルテを用いることはできない。そのため、医事会計システムも優先的に稼働させることも検討されたい。

いずれにしても、復旧の順序は病院の規模や診療体制、導入しているシステム構成などによって異なるため、個別施設においてあらかじめ優先度を検討・定義しておくことが現実的な BCP 運用に資すると考えられる。本研究では、そうした背景を踏まえて、代表的な病院情報システムにおける復旧優先度の目安となる一覧（図 3）を作成した。 これは標準的な構成を想定した叩き台であり、各医療機関が自施設に合わせてカスタマイズする際の参考として位置づける。

なお、今後この内容をより現場実務に沿ったものとするためには、実際の運用を担う情報システム担当者や管理職（例：病院の IT・診療情報管理部門）との検討を通じたブラッシュアップが有効である。

D．考察

本研究では、自然災害とサイバーインシデントという異なるハザードに対する BCP 上の対応項目を比較しつつ、病院機能を維持するために必要な視点の共通性と、サイバーインシデントに特有の対応事項を整理した。以下に、特に重要と考えられる論点を示す。

I. 自然災害との共通点：情報維持と初動体制の重要性

サイバーインシデントにおいても、診療情報の維持と初動対応体制の確保は自然災害と同様に最重要項目である。電子カルテやオーダリングシステムが停止しても、紙カルテの運用や情報のバックアップが準備されていれば、診療の継続は可能である。こうした初動時の対応体制や代替手段の整備は、自然災害における BCP でも基本的な構成要素であり、共通の課題として再確認された。

II. 特有事項：障害の範囲と復旧の見通しに関する不確実性

サイバーインシデントは、外形的な被害が伴わない分、障害の範囲や復旧時間の見通しが立ちにくいという特徴がある。特に、攻撃型のマルウェアによる被害では、機器の物理的

破壊がない一方で、システム全体の停止・検査・復旧作業が長期化する可能性が高い。こうした状況では、“いつ・どこまで復旧できるか”が不明なまま初動対応を迫られるため、BCP 上では複数段階に分けた対応パターンの整理と、医療者が判断しやすい「使用不可範囲による分類」が有効である。

III. 災害特性に応じた項目の選別

サイバーインシデントにおいては、自然災害 BCP に含まれる「避難計画」や「建物の安全確認」等の項目が直接的には必要とならない場面もある。こうした点から、ハザード特性に応じて柔軟に対応項目を取捨選択する視点が求められる。

すべての災害にすべての項目を適用するのではなく、必要なものを重点的に整備することで、BCP の実効性を高めることが期待される。

IV. 病院機能維持に向けた新たな視点：近年の災害対応や支援手法から見えてきた課題

自然災害 BCP の先行研究[1) 2)]においては、病院の被災状況や診療継続の可能性を具体的に判断するプロセスや、支援を受けるための準備、外来・在宅患者への対応方針などが十分に体系化されていなかった。一方、近年の DMAT による病院支援の経験や、その知見を整理した先行研究[4)]による支援手法からは、以下のような病院機能維持に資する具体的視点が改めて重要であることが示唆されている。

① 現状分析と課題整理や病院行動評価群による初動判断の明確化
② EMIS 基本情報の登録による脆弱性把握と外部支援の円滑化
③ ダメージコントロールに向けた具体的な手法の明示
④ 既存外来患者への対応方針の整理

これらの視点は、サイバーインシデントにおいても横断的に有効である。たとえば、現状分析や病院行動評価群の考え方は、情報システムの障害状況を可視化し、初動対応の判断を支援する仕組みとして活用できる。また、ダメージコントロールの考え方は、本研究で提示した「システム別復旧優先度一覧」にも通じており、復旧の段階的判断と診療機能の回復に向けた優先順位付けに資する。

このように、災害種別を問わず適用可能な“共通視点”を BCP に取り入れていくことが、オールハザード型 BCP の実効性を高める上で重要である。

E．結論

本研究では、サイバーインシデントを対象に、医療機関における BCP 対応項目を整理し、自然災害との比較を通じて共通点や特有の課題を明らかにした。その結果、BCP において災害種別を問わず重要とされる共通事項（診療情報の維持、初動体制の確保等）の存在に加え、サイバー特有の障害の不確実性や復旧判断の難しさといった特徴に対応する視点が必要であることが示された。

一方で、自然災害を前提とした従来の BCP では、現場の実態や初動判断に必要な情報整理、障害範囲ごとの対応シナリオ、外来患者対応の計画などが十分に体系化されておらず、これはサイバーインシデントにおいても共通の課題となり得る。こうした視点は、近年の災害対応経験や支援手法の整理から得られた知見であり、今後の BCP 構築において重要な構成要素となる。

本研究で提示した、使用不可範囲による障害分類や、システム別復旧優先度の整理といった考え方は、サイバー対応を契機に、より現実的かつ実務的な BCP 整備に向けた手がかりとなるものである。

今後は、サイバーに限らず、地震・水害・感染症など多様なハザードを念頭に、「病院機能

の維持」という観点を中心に据えた BCP の構築が求められる。その際には、災害種別ごとに個別計画を立てるのではなく、共通基盤となる対応方針を整備した上で、必要に応じて特有事項を上乗せしていく構成が望ましいと考えられる。

≪引用文献≫

1) 厚生労働科学研究費補助金(地域医療基盤開発推進研究事業)「地震、津波、洪水、土砂災害、噴火災害等の各災害に対応したBCP 及び病院避難計画策定に関する研究」(平成 29 年度、研究代表者：本間正人)
2) 厚生労働科学研究費補助金(地域医療基盤開発推進研究事業)「浸水被害も含めた、新たな医療機関の事業継続計画（BCP）策定に資する研究」(令和 4 年度、研究代表者：本間正人)
3) 厚生労働科学研究費補助金「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、研究代表者：鳥飼幸太)
4) 「病院行動評価群 Ver. 4」による病院の被災状況の評価と対応の標準化(阿南英明ら、日本災害医学会雑誌. Vol. 28 No. 3)

Ｆ．健康危険情報

なし

Ｇ．研究発表

1. 論文発表

なし

2. 学会発表

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：なし

2. 実用新案登録 ：なし。

3.その他 ：なし

図 1：システム障害の原因と使用不可範囲

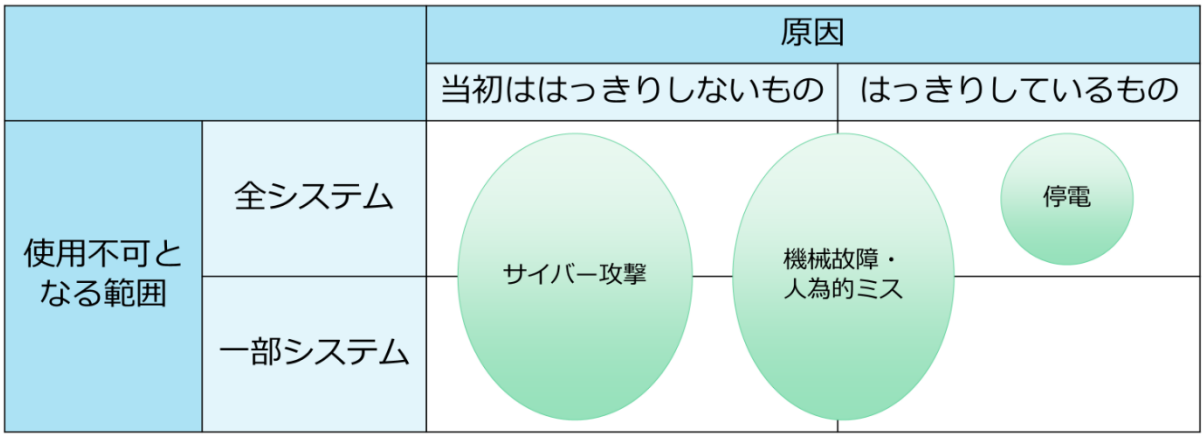
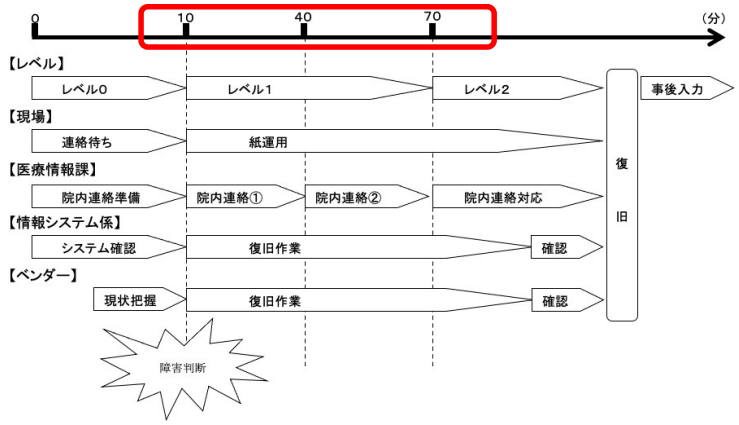


図 2：使用不可範囲毎の対応タイムライン

ケース1：全面停止（情報システムが全て使用できない）

障害判断：10分



ケース2：一部不具合（情報システムの一部が使用できない）

ケース3：端末限定（特定の端末に限り使用できない）

障害判断：30分

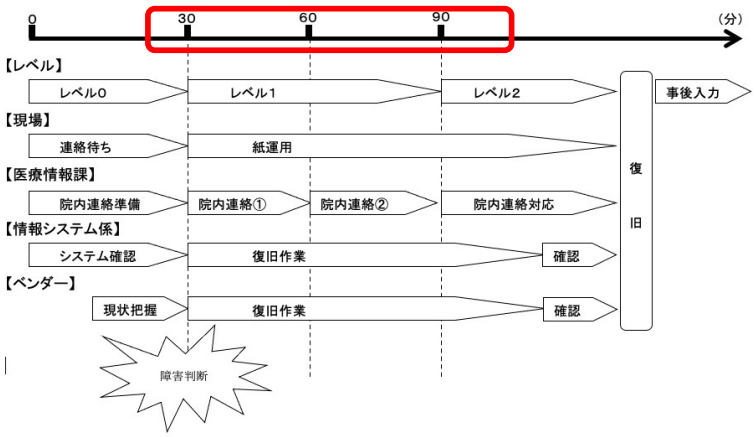


図 3：システム別復旧優先度一覧（一例）

ランク	重要度
SSS	全システムを使用するためのインフラ環境
SS	診療上最低限必要なシステム
S	診療上必要なシステムのうち、重要度が高いもの
A	診療上必要なシステムのうち、重要度が中程度のもの
B	診療上必要なシステムのうち、重要度が低いもの。診療上必要ないが、業務復旧にあたり必要なインフラおよびシステム。
C	診療上影響がないもの

No.	システム名	所轄部署名	重要度	復旧の優先順位
1	エンドポイントセキュリティ	医療情報課	B	10
2	電子カルテシステム	医療情報課	SS	6
3	参照カルテシステム	医療情報課	SS	2
5	地域連携システム	医療情報課	B	10
6	放射線部門システム	医療情報課	A	9
7	麻酔管理システム	医療情報課	S	8
8	重症系管理システム	医療情報課	S	8
9	医事会計システム	医療情報課	SS	5
15	再来受付機	医療情報課	B	10
16	患者呼出表示盤システム	医療情報課	B	10
18	診療支援プラットフォーム(CITA)	医療情報課	S	7