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

IT-BCP手順書作成と地域合同訓練計画に関する研究

研究分担者　楠田 佳緒　京都大学医学部附属病院
研究分担者　油谷 曉　京都大学医学部附属病院
研究分担者　橋本 智広　大津赤十字病院

研究要旨
本研究では、指導的立場のセキュリティ人材（Group A 人材）を有する集中管理機関と、医工系人材を中心とする Group C 人材を有する被指導機関とが共同してサイバー攻撃に対応するための共同 IT-BCP 手順書の確立と、これに基づく合同 IT-BCP 訓練の実効性検証を目的としている。2025 年度は、既存の IT-BCP や国内医療機関におけるサイバー攻撃被害報告書を調査し、被害時に病院がとるべき行動および Group C 人材が単独では対応困難となる項目を抽出した。抽出された項目は「人材（作業）」「物品」「情報」の 3 区分に分類し、集中管理機関への支援要請事項として共同 IT-BCP 手順書のプロトタイプに組み込んだ。併せて、次年度に実施する合同 IT-BCP 訓練に向け、滋賀県内の 2 医療機関との調整を開始し、地域医療連携を活かした訓練実施体制の素案を策定した。本年度の成果により、被指導機関が攻撃を受けた際の対応行動と集中管理機関への支援要請の枠組みが具体化され、次年度の合同訓練による実効性検証に向けた準備が整いつつある。

Ａ．研究目的

本研究では、Group C人材を有する被指導機関がランサムウェア等のサイバー攻撃を受けたことを想定したIT-BCP対応訓練を計画する。本訓練を、被指導機関（Group C病院）と集中管理機関（Group A病院）が共同して実施することで、集中管理機関と被指導機関の役割を明確にした共同IT-BCP手順書を確立するとともに、Group C人材の実践的教育としての合同IT-BCP訓練の実効性について検証する。

2025年度の目的として、共同IT-BCP手順書の作成と、合同訓練の実施計画の策定を行うこととした。

Ｂ．研究方法

B-1　共同IT-BCP手順書の作成

地域の医療機関が協力してIT-BCPを実施するための手順書を作成する。具体的には、医療機関の既存のIT-BCPおよび電子カルテシステム停止時マニュアル、ならびに過去のサイバー攻撃被害報告書を調査する。さらに、調査結果をもとに、集中管理機関（Group A病院）と被指導機関（Group C病院）が共同で運用することを想定した共同IT-BCP手順書のプロトタイプを作成する。

B-2　合同訓練の実施計画

Group C病院がサイバー攻撃を受けたことを想定して、地域の複数の医療機関による合同訓練を計画する。具体的には、合同訓練への協力機関との調整、および合同訓練シナリオ案を検討する。

B-3　倫理的配慮

本研究では、文献調査・資料作成を実施するため、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

C-1　共同IT-BCP手順書の作成

既に公開されている各医療機関および厚生労働省のIT-BCP（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版に基づくBCPひな形等）、ならびに各医療機関で整備されている電子カルテシステム停止時マニュアルを調査した。現在の医療機関では、電子カルテや部門システムに異常が生じた場合、まず「電子カルテシステム停止時マニュアル」の手順が実施される。その後、ネットワーク障害やサイバー攻撃が疑われる事象が確認された場合に「IT-BCP」の手順が実施される運用となっている。本研究では、後者の「IT-BCP」に着目した。

さらに、大阪急性期・総合医療センター等、近年に公表されたサイバー攻撃被害報告書を調査し、サイバー攻撃被災時に病院がとるべき行動を抽出した。次に、これらの行動をとる際にGroup C人材のみでは判断・実施が困難となり混乱が生じうる項目、または、Group A人材へ支援を要請すべき項目を洗い出した。

以上の調査から、Group C人材がGroup A人材へ支援を要請すべき項目について、「人材（作業）」「物品」「情報」の3項目に分類し、それぞれの具

体例を共同IT-BCP手順書のプロトタイプに組み込んだ。「人材（作業）」には、被害調査の技術的支援や、紙運用における人材提供等が含まれ、「物品」には、FAXやクリーンPC等の貸与、「情報」には、フォレンジック調査・初動対応の判断支援等が含まれる。

C-2　合同訓練の実施計画

来年度に実施する合同訓練に向けて、滋賀県内の2医療機関との調整を開始した（担当：橋本、油谷、楠田）。さらに、大津赤十字病院に加え、2医療機関（大津市民病院、琵琶湖中央リハビリテーション病院）に対して、ネットワークに接続されている医療機器を検出するシステムを導入した。本システムの導入により、サイバー攻撃の被災時に攻撃対象となりうるネットワーク医療機器の一覧が作成できた。これにより、地域におけるセキュリティ共通基盤のモデルが構築できた。

また、合同訓練シナリオの作成では、システム停止の通報から始まり、サイバー攻撃の発覚、対応、収束の一連の流れを机上で体験するシナリオ案を作成した。今後、シナリオのブラッシュアップにあたっては、Group C人材が現場で直面する判断項目を含め、集中管理機関からの支援を要請する場面を盛り込むなどして精査する。

D．考察

本年度の調査により、サイバー攻撃被災時に医療機関がとるべき行動の多くが、現場のIT人材だけで完結できない性質であることが明らかとなった。特に、フォレンジック調査の初動判断、代替機器の確保、攻撃手口に関する最新情報の収集といった事項は、平時から関連知識や人的ネットワークを蓄積している集中管理機関の関与なしには適時に実施することが困難であり、被指導機関の現場では混乱が生じやすい領域である。

Group C人材から集中管理機関への支援要請項目を「人材」「物品」「情報」の3区分に整理したことは、被災時に何を、誰に、どのような形で要請すべきかを構造的に示す枠組みを与えるものであり、共同IT-BCP手順書を実用的なもの近づけることができると考えられる。

一方で、共同IT-BCP手順書を実際に運用するためには、平時からの両機関での関係構築、支援要請の経路と判断権限の明確化、ならびに支援提供側である集中管理機関の受け入れ準備の検討が求められる。次年度に予定する合同IT-BCP訓練では、本手順書プロトタイプを訓練シナリオに適用し、Group C人材の判断行動と集中管理機関の応答行動を具体的に観察・評価する予定である。

E．結論

2025年度は、既存のIT-BCPおよびサイバー攻撃被害報告書を調査した。調査結果から、被指導機関(Group C病院)が集中管理機関(Group A病院)に対して支援を要請すべき項目を「人材」「物品」「情報」の3区分で整理し、これらを反映した共同IT-BCP手順書のプロトタイプを作成した。併せて、滋賀県内の2医療機関と合同IT-BCP訓練に向けた調整を開始し、次年度の訓練実施体制の素案を策定した。次年度に実施する合同訓練を通じて、共同IT-BCP手順書の実効性およびGroup C人材に対する実践的教育へと研究を進める。

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