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）
総括研究報告書

# 地域における共通基盤・集中管理体制による サイバーセキュリティの実証のための研究

研究代表者　黒田 知宏　京都大学 医学部附属病院

研究要旨
本研究では、相互チェック・合同 IT-BCP 訓練を通じてセキュリティ向上と人材育成を同時に進める枠組みを作ろうとするものである。初年度は、共通基盤として病院ネットワークに繋がる機器を検出する仕組みの導入と、規範となるチェックリストの策定、及び、相互チェック手順書と IT-BCP 訓練実施体制の策定を実施した。これらの成果により、二年度に具体的なチェック・訓練を実施する基本的な準備が整った。

黒田知宏・京都大学・教授
武田理宏・大阪大学・教授
谷川琢海・北海道科学大学・教授
橋本智広・大津赤十字病院・課長
川眞田実・大阪国際がんセンター・副診療放射線技師長
肥田泰幸・東都大学・講師
鳥飼幸太・群馬大学・准教授
油谷曉・京都大学・講師
楠田佳緒・京都大学・特定講師
芦原貴司・滋賀医科大学・教授
高倉弘喜・国立情報学研究所・教授

## A．研究目的

医療機関を取り巻くセキュリティ人材の不足は深刻化している。少ない人材で喫緊のセキュリティ対策を実施するためには、優秀なセキュリティ人材を集約した指導的な医療機関（集中管理機関）を設置し、関連医療機関のセキュリティ対策の支援を行わせることで、短期的な情報セキュリティ確保を図るとともに、医療と工学技術に伴に明るい臨床工学技士・診療放射線技師を主たる対象としたセキュリティ教育を実施させることで、長期的なセキュリティ人材の養成を図ることが適当である。

本研究では、2023年度厚労科研（201221069A）で示した指導的立場のセキュリティ人材（グループA人材）を有する医療機関（集中管理機関）同士が互いにセキュリティチェックを行う相互チェックの取り組みを通じてセキュリティチェックの手順書と監査項目を策定するとともに、これを複数のグループA人材を有さない医療機関（被指導機関）に適用してその実効性について検証する活動を実施する。この際、セキュリティチェックの効率性と有効性を向上するため、情報資産危険性自動評価技術の共通利用の枠組みを確立する。この枠組みは、集中管理機関が被評価機関の指導を行う際にも活用する。

加えて、グループC人材を有する被指導機関がランサムウェア攻撃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、被指導機関と集中管理機関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、グループ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活動を実施する。

初年度は、相互チェックのための監査項目策定と手順書の策定を行うとともに、IT-BCP訓練の下敷きとなる、参加医療機関の病院ネットワークの状況調査を行った。

## B．研究方法

本研究は、1）集中管理機関同士の相互チェックに必要文書（セキュリティチェック手順書、セキュリティ監査項目一覧）の策定とチェックの実施（相互チェック）、2）集中管理機関と被指導機関との共同 IT-BCP 手順書の策定と IT-BCP 訓練の実施（共同 IT-BCP 訓練）、の二つの研究からなる。

1）相互チェック研究は、（1A）監査項目リストの策定、（1B）相互チェック手順書の策定、（1C）相互チェックの実施、の三つの研究から構成される。本研究では初年度に（1A）を、二年度の前期までに（1B）を実施し、二年度中頃をメドに、グループ A 人材を有する二つの医療機関、京都大学医学部附属病院と、大津赤十字病院の間で、実際に（1C）を実施し、（1A）及

び（1B）研究の成果について、その実用性を評価する。

2）共同 IT-BCP 訓練研究は、(2A) IT-BCP 計画の策定、(2B) 訓練シナリオの策定、(2C) 訓練の実施、の三つの研究から構成される。本研究では、大津赤十字病院を中心に「びわ湖あさがおネット」等の活動を通じて地域全体の行政・医療機関が相互支援体制（医療機関ネットワーク）を有する滋賀県地域、特に、大津市地域において、大津赤十字病院と京都大学医学部附属病院を集中管理機関として実施する。初年度に（2A）を、二年度の前期までに(2B)を実施し、二年度後期に(2C)を実施し、(2A) 及び (2B) 研究の成果について、主にグループ C 人材の実践的教育手法としての実効性の観点から評価する。

C．研究結果

1）相互チェック研究においては、本年はまず(1A)監査項目リストの策定を実施するとともに、(1B)相互チェック手順書の策定準備に着手した。(1A）においては、八つの監査手法と、三つの観点から詳細に検討され、相互チェックのみならず、IT-BCP計画策定に適用出来る構成に纏められた。(1B）においては、先行する医療安全分野の相互チェック手順に関する調査に基づいて、毎年監査する基本項目と、最新の脅威や課題に応じた重点項目を組みあわせることが効果的であること、及び、相互チェック全体を企画・運営する事務局的組織が必要であることを見出した。結果の詳細については、（1A）担当した鳥飼の、（1B）は担当した武田の分担報告書のとおりである。

2）共同IT-BCP訓練研究においては、本年はまず(2A) IT-BCP計画の策定を行うとともに、(2B)訓練シナリオの策定の準備をすすめた。（2A）においては、公開されているIT-BCPや電子カルテシステム停止時マニュアル、及び、サイバー攻撃被害報告書を調査しGroup C人材がGroup A人材へ支援を要請すべき項目等を洗い出して、手順書に纏めた。（2B）においては、訓練対象医療機関を選定し、被災時に掌握が必要な自院のネットワーク医療機器一覧を調査する方法を確立し「共通基盤」のモデルを整えるとともに、訓練シナリオ案の策定を進めた。結果の詳細については、担当した楠田・油谷・橋本の分担報告書のとおりである。

D．考察

本研究の遂行を通して、医療サイバーセキュリティは、高度な技術導入の問題ではなく、極めて泥臭い状況掌握の活動の積み重ねによって実施できるものであることが再確認されたとともに、たとえ「指導的な医療機関」であっても、泥臭く膨大な作業である状況掌握の活動は、必ずしも十分実施できておらず、これを支える「共通基盤」たる技術導入が極めて大きな役割を果たしうることが確認出来た。

E．結論

本研究では、サイバーセキュリティ人材が不足する中で、相互チェック・合同IT-BCP訓練を通じてセキュリティ向上と人材育成を同時に進める枠組みを作ろうとするものである。

本年度の研究では、その前提となる現状を知るための仕組みを「共通基盤」として設定し、その適用を通じて現状を把握するとともに、論理的に求められるチェックリストを作ることを並行して進めた。これらの活動によって、二年度に実施する、相互チェックと合同IT-BCP訓練のシナリオを立てるための準備が整ったと考えられる。

F．健康危険情報

該当無し

G．研究発表

1. 論文発表

該当無し

2. 学会発表

該当無し

3. その他


1) T. Kuroda. Medical Cyber Security of KUHP and Japan. UPM-KU Mini Symposium on Computer-Assisted Systems in Healthcare, Memorial Auditorium of Kyoto University School of Medicine. 2025年6月17日.
2) 黒田. 医療機関が抑えておくべき医療情報セキュリティの基礎. 新社会システム総合研究所 医療･介護戦略特別セミナー. オンライン. 2025年9月19日.
3) 黒田, Greenhalgh. 現場と経営をつなぐサイバーセキュリティ戦略. Claroty Nexus Days. ザ・リッツ・カールトン 京都. 2025年10月10日.
4) 黒田. 医療サイバーセキュリティを地域で支える仕組みを作る試み. 関西健康･医療創生会議シンポジウム. オンライン. 2025年12月15日.
5) T. Kuroda. Medical Cyber Security Strategy of KUHP. Internal Seminar. Helsinki University Hospital. 2026年1月22日.
6) T. Kuroda. Medical Cyber Security Strategy of KUHP. Kyoto-Zurich Joint Symposi

um. University of Zurich. 2026年1月23日.

7) T. Kuroda. Medical Cyber Security Strategy of KUHP. Internal Seminar. University of Oulu. 2026年1月26日.

H．知的財産権の出願・登録状況
（予定を含む。）

該当無し