共同企画 | 2023年11月23日

2023年11月23日(木) 15:00 ~ 16:30 A会場 (KFMホール"イオ")

共同企画2
IT-BCPをどう実現するか（医療情報マネジメント部門連絡会議）

オーガナイザー：鳥飼 幸太（群馬大学医学部附属病院システム統合センター）
座長：鳥飼 幸太（群馬大学医学部附属病院システム統合センター）、平田 哲生（琉球大学病院）

[2-A-6] IT-BCPをどう実現するか

*鳥飼 幸太[1]、田木 真和[1,2]、橋本 智広[1,3] (1. 群馬大学医学部附属病院システム統合センター、2. 徳島大学大学院医歯薬学研究部　医療情報学分野、3. 大津赤十字病院　事務部　医療情報課)

キーワード：IT-BCP、Continuous Diagnostics and Mitigation (CDM)、Asset Management、NIST Cyber Security Framework (CSF)

入院を伴う病院は24時間稼働する組織であり、業務支援を行うITシステムには高い稼働信頼性が求められる。また診療所であっても、昼夜を問わないオンライン診察予約サービスや在宅医療における情報連携にITを利用する場合にも高い稼働信頼性が求められる。稼働信頼性を毀損する要因に対して備え、医療機能を持続させるためにIT-BCP(Business Continuity Plan)が必要である。BCPは「実効性」が必要な計画であり、BCP自体の立案、運営、改訂のサイクルと情報システムのライフサイクルの両方を考慮しつつ運用される。従前、施設ごとの任意準備に委ねられてきた傾向のあるIT-BCPは、稼働信頼性の毀損条件にサイバー攻撃が追加され、更にコロナ後に加速したリモート作業要請が生じたため、全国の医療機関で共通となる対策指針の策定が望まれている。一方、IT-BCP対策実施を可能とする環境としてITインフラ整備が必要との声もあり、病院組織全体として対策を講じていく必要性が強く示唆される。本セッションではサイバー攻撃対応、復旧を実際に遂行されたご経験を大阪急性期・総合医療センター粟倉康之様に、ならびに国立大学病院事務部長会議総務委員会情報セキュリティWG活動の状況について徳島大学病院脇元直彦様より詳説をいただく。今年度厚労省行政推進調査事業として進めている「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」（課題番号23CA2017）の方針ならびに進捗につき中間報告を行う。

IT-BCP をどう実現するか

鳥飼 幸太[*1]、田木 真和[*2]、橋本 智広[*3]
*1 群馬大学医学部附属病院システム統合センター, *2 徳島大学大学院医歯薬学研究部 医療情報学分野,
*3 大津赤十字病院 事務部 医療情報課

How to achieve IT-BCP

Kota Torikai[*1] , Masato Tagi[*2] , Tomohiro Hashimoto[*3]
*1 System Integration Center, Gunma University Hospital, *2 Department of Medical Informatics, Graduate School of Medical, Dental and Pharmaceutical Sciences, The University of Tokushima,
*3Medical Information Section, Administrative Department, Otsu Red Cross Hospital

Hospitals with hospitalization are organizations that operate 24 hours a day and require high operational reliability from IT systems that support their operations. Clinics also require high operational reliability when using IT for day-and-night online consultation reservation services and information linkage for home medical care. An IT-BCP (Business Continuity Plan) is necessary to prepare for factors that may damage operational reliability and to sustain medical functions. The BCP is operated in consideration of both the planning, operation, and revision cycle of the BCP itself and the life cycle of the information system. IT-BCP, which has tended to be left to the voluntary preparation of each facility in the past, is now expected to establish a guideline for measures common to all medical institutions nationwide because cyber attacks have been added to the conditions for damage to operational reliability, and because requests for remote operations have accelerated after the Corona. On the other hand, there are calls for the development of IT infrastructure as an environment that enables the implementation of IT-BCP measures, strongly suggesting the need to take measures for the hospital organization as a whole. In this session, Mr. Yasuyuki Awakura of Osaka Acute & Comprehensive Medical Center will talk about his experience in dealing with and recovering from cyber attacks, and Mr. Naohiko Wakimoto of Tokushima University Hospital will give a detailed account of the activities of the Information Security Working Group of the General Affairs Committee of the Council of Administrative Directors of National University Hospitals. An interim report will be given on the policy and progress of the "Research for Dissemination of Business Continuity Plan (BCP) for Cyber Attack Response in Medical Institutions" (Issue No. 23CA2017), which is being promoted by the Ministry of Health, Labor and Welfare as an administrative promotion research project this fiscal year.

Keywords: IT-BCP, Continuous Diagnostics and Mitigation (CDM), Asset Management, NIST Cyber Security Framework (CSF)

1. IT-BCP シンポジウムの背景

近年の急激な情勢変化や Web 技術の普及を背景とし、医療機関へのサイバー攻撃ならびに被害が顕在化している。日医総研リサーチレポート No.136(1)より、2022 年の医療・福祉分野におけるランサムウェア被害の届出件数は 20 件（警察庁調べ）との報告があり、潜在的にはさらに多くの被害が生じていると考えられる。サイバー攻撃に対する対策を検討するフレームワーク（理論的枠組み）は複数提案されているが、広く知られた方法として①サイバー攻撃の侵攻段階によって対策を分類する方法（NIST Cyber Security Framework (CSF)）、②組織体の資産価値保全の観点から対策を分類する方法(Continuous Diagnostics and Mitigation (CDM))が存在する。サイバー対策の手引きとなる文書やガイドラインはオンラインで情報処理推進機構(IPA)などから入手可能であるが、医療機関における自主的なサイバー対策の質は機関によって差が大きいと考えられる。群馬大学医学部附属病院（以下本院）における医療スタッフからの病院情報システムに関連した要望ヒアリングより背景要因を推測すると、次のような仮説が考えられる。①サイバー攻撃対策は院内の運用全体に影響を与える内容を包含するため、組織的な活動が求められること、②米国の医療機関と異なり、日本の医療機関の殆どは税収を原資とする国民皆保険の診療報酬によって収入の上限が決まっており、事務経費に割り当てられやすい病院情報システムに対する加算等の項目が存在しないこと、③2011 年の東日本大震災ならびに 2020 年の SARS-CoV2 蔓延に対し、医療機関側でデータ保全の必要性ならびに隔離を伴う診療継続環境の必要性が認識され、診療データならびに診療状況情報を自施設以外と送受信する必要性が急速に高まったこと、③医療機関における診療情報の取り扱いは要配慮個人情報に相当し、守秘義務とプライバシー保護の観点から取り扱える役職と権限を限定して運用した経緯があり、④サイバー攻撃の活動が可視化されることが少なく、サイバー攻撃を受けたことがない医療機関では、具体的な被害状況、程度ならびに被害経験から導かれる善後策を正確に掌握することが困難であること、⑤仮に IHE フレームワークで Actor を指定できても、医療機関内における診療ワークフローは必ずしも共通化させる必要性がこれまでなかったため、ワークフローに即して実装・運用するサイバーセキュリティ対策を共通化できないこと、⑤サイバー攻撃対策の実装・運用には、サイバーセキュリティの知識、医療ワークフローの知識ならびに IT システムの知識が求められるが、これらを兼ね備えた人材が慢性的に不足していること。

2. 医療機関共通の IT-BCP 対策の必要性

日本全体の医療機関に対するサイバー攻撃対策向上を考えると、上記①-⑥を考慮しながら、日々高度化するサイバー攻撃に対応するために必要と考えられる活動について以下に検討する。A：サイバー攻撃における分類のうち、特に持続

的標的型攻撃(Advanced Persistent Threat)の被害を受けた医療機関における被害状況や対応に関する詳細な情報共有の機会を設けること、B:医療機関におけるサイバー攻撃対応に関する共通したフォーマットによる現況確認を迅速に行うこと、C:医療機関が個別に担っている医療機能を、サイバーセキュリティ用語における資産管理(Asset Management)の観点から分類し、サイバー攻撃によって人命ならびに患者健康が損なわれるリスクならびに診療機能が損なわれるリスクの観点からの分類（高度急性期/急性期/回復期などの別、病床数の別、2 次医療圏における役割など）に応じ、適切かつ共通実施が可能な IT-BCP 対策について、調査すべき項目の洗い出し、対策項目のチェックリストならびに対策指針について調査・検討し、公共に提案すること。

本シンポジウムでは、活動 A につき、地方独立行政法人大阪府立病院機構大阪急性期・総合医療センター事務局 経営企画マネージャー栗倉康之様より、高度急性期病院における 2022 年度におけるサイバー攻撃対応についてご講演いただく。また活動 B につき、徳島大学病院事務部長 脇元直彦様に、病院長会議総務会との協議内容、情報セキュリティ・IT-BCP 対策の実施状況調査ならびに病院長会議で進行中のサイバーセキュリティ保険等につきご講演いただく。活動 C につき、筆者より今年度厚労省行政推進調査事業として進めている「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」（課題番号 23CA2017）の目的を踏まえた IT-BCP 対策のチェックリストについての検討方針ならびに検討案について講演を行う。

参考文献

1) 坂口一樹、堤 信之、原 祐一 医療機関へのサイバー攻撃の事例研究: 民間病院・診療所の被害事例に学ぶ 日医総研リサーチレポート No.136 (2023)
https://www.jmari.med.or.jp/wp-content/uploads/2023/04/RR136.pdf