2025.04.01

医療福祉RMニュース ＜2025 No.1＞

医療機関におけるサイバーBCP 訓練・演習実施のポイント

【要旨】
- **医療機関におけるサイバーBCP 訓練・演習の必要性は、サイバー攻撃事案の増加や厚生労働省のガイドライン、診療報酬によるインセンティブの付与等によって示されている。**
- **サイバーBCP を踏まえた訓練・演習を企画・実施する際には、自施設の現状や課題等に沿った目的を設定し、それを踏まえた参加者の決定、シナリオ・状況付与の作成等がポイントである。**
- **医療機関においては診療の継続・早期復旧を図り、地域医療等への影響を最小限に抑えるといった本来の目的意識を持って、継続的に訓練・演習に取組むことが求められる。**

１．医療機関におけるサイバーBCP訓練・演習実施の必要性

医療分野におけるサイバー攻撃事案について、警察庁の発表によるとランサムウェアによる被害件数は令和3年度に7件であったものが令和4年度には20件に増加しており、実際に電子カルテ等のデータが暗号化されてしまい、復旧に2か月を要する等して長期間診療継続に影響を及ぼした事例も複数発生している。

また、厚生労働省が策定・公表している「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」（以下「ガイドライン」）では定期的な訓練・演習の実施やその結果をBCPへ反映させる、いわゆるBCM取組みの重要性が示されている。加えて、医療機関の各種取組みへのインセンティブとなる診療報酬では「診療録管理体制加算」が令和6年度の診療報酬改定で見直され、算定の要件に「少なくとも年1回程度定期的に、訓練・演習を実施すること。また、その結果を踏まえ、必要に応じて改善に向けた対応を行っていること」が追加されている。

このことから、サイバーBCPを踏まえた訓練・演習の実施は、すべての医療機関における喫緊の課題であると言える。

本稿では医療機関でサイバーBCP訓練・演習を企画する担当者（以下「企画担当者」）向けに、訓練・演習実施のポイントについて解説する。なお、ここではサイバー攻撃に関する状況付与によって、発生しているインシデントへの対応検討を行うロールプレイ形式での訓練・演習を取り上げる。

２．サイバーBCP訓練・演習を企画・実施する際の手順

一般社団法人日本シーサート協議会が公表している「サイバー攻撃演習訓練実施マニュアル」によると、訓練・演習を企画・実施する際の手順は以下のとおりである。

(1) 訓練・演習目的の明確化

まずは訓練・演習を実施する目的を明確にする。サイバー攻撃を対象とした訓練・演習の目的は主に以下が挙げられる。

表1　サイバー攻撃を対象とした訓練・演習の目的例

■　インシデント対応フローの検証
■　インシデント対応フローの習得
■　サイバー攻撃における、事業継続計画（BCP）の検証
■　CSIRTのインシデント対応能力の向上
■　インシデント対応時の自組織内の情報連携の検証

■　インシデント対応時の組織外情報連携の検証
■　インシデント対応時のリソースの検証
■　インシデント対応時のコミュニケーションツールの検証
■　インシデント対応時のコミュニケーションツールの習得
■　自組織内への啓発活動／意識向上／役割理解促進
■　テクニカルスキルの習得　　等

出典：一般社団法人日本シーサート協議会「サイバー攻撃演習訓練実施マニュアル」

自施設のサイバー攻撃等に対する準備状況やインシデント対応上の課題、過去に実際に発生したインシデント等を踏まえて、表1を参考に目的を決定することが推奨される。

(2) 対象となるシステム及び参加者の決定

次にシナリオ上でインシデントが発生するシステムを決定する。医療機関であれば、診療継続の可否に直結する電子カルテ等の医療情報システムを対象とするのが一般的である。続けて、訓練の参加者を決定する。参加者は訓練・演習の目的や対象となるシステム等を踏まえて決定するが、経営に近い上位の役職者ほど全体的なリスク管理や危機対応が論点となり、一方で、現場に近い職員ほど自身の普段の業務範囲内での技術的な対応が論点となりやすいため、前述した訓練・演習の目的を踏まえて検討することが望まれる。

(3) 訓練・演習手法の決定

(1) (2)で決定した目的等を踏まえ、訓練・演習の具体的な実施方法を決定する。なお、前提として訓練と演習には、それぞれ表２のような目的や実施方法、メリット・デメリットの違いがある。

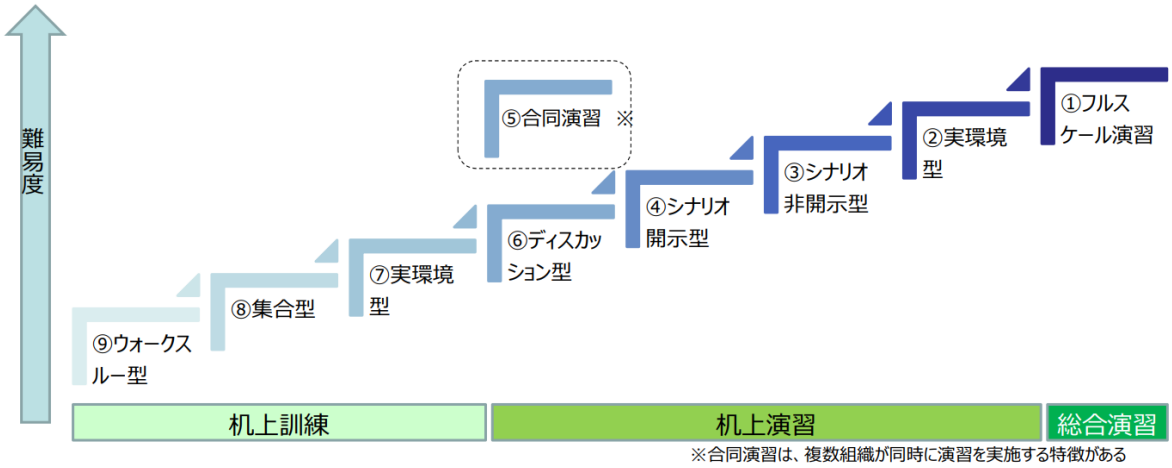
表2　訓練と演習の違い

	目的・実施方法	メリット・デメリット
訓練	・大きな目的は「技能の習得」であり、定められた手順に基づいて迅速・正確に対応ができることを目標とする。 ・ネットワーク切断等の初動対応、証拠保全、ログ抽出、紙カルテ等の紙伝票運用等を実際の手順やシステム・ツールを用いて実行し、ノウハウの習得や課題の抽出を行う。	【メリット】 ・インシデント対応に必要な手順等を習得でき、被害拡大防止等に効果的である 【デメリット】 ・具体的な手順等が決まっていないと実施できない　等
演習	・大きな目的は「検証」であり、困難な状況においても柔軟に判断し、適応する能力（＝レジリエンス）を高めることを目標とする。 ・訓練企画者が作成したシナリオや状況付与に基づいて、訓練参加者はその状況に応じた対応方針等を検討することで、BCPの妥当性確認や組織間の連携及びコミュニケーションの改善等を図る。	【メリット】 ・「訓練」では難しいインシデントへの中長期的な対応を検討できる（システム停止に伴う診療継続方針や具体的な方法の検証等） ・比較的短時間、かつ、会議形式で実行できるため、経営・幹部層や複数の部門を対象にして実施しやすい 【デメリット】 ・シナリオや状況付与の質によって、検証がうまくいかない可能性がある　等

出典：一般社団法人日本シーサート協議会「サイバー攻撃演習訓練実施マニュアル」を基に
ＭＳ＆ＡＤインターリスク総研にて作成

また、ロールプレイ形式の訓練・演習では主に図1のような訓練・演習方法が存在する。

図1　ロールプレイ型の訓練・演習方法（例）



出典：一般社団法人日本シーサート協議会「サイバー攻撃演習訓練実施マニュアル」

企画担当者は、自施設のBCP策定状況や役職員のサイバーインシデントに対する知識や対応の習熟度等も考慮しながら適した訓練・演習方法を選択する必要がある。

(4) シナリオ、状況付与の検討

ここまでに決定した目的等に合わせて、自施設のシステム構成を考慮しつつ、サイバー攻撃を受けた際に実際に発生し得る影響等を可能な限り現実的に想定し、シナリオを作成する。シナリオ作成では攻撃者側の視点に立ち、自施設をどのように攻撃するかを考え、被害を受けるシステムや情報等を想定する。一から検討することが難しい場合は、過去に発生した医療機関へのサイバー攻撃事例について、詳細な報告書等が公表されているものを参考に、自施設で同じ事象が起こることを想定するのも一案である。なお、シナリオ検討では「DDoS攻撃等の攻撃の沈静化を待つしかないシナリオ」や「システム停止等の事象だけで原因が最後まで判明しないシナリオ」は対応が手詰まりになり、検討がうまく行かない可能性が高いためお勧めしない。

シナリオが決定したら、それを踏まえた状況付与を検討する。状況付与では作成したシナリオを防御側からの視点で捉え、自施設のインシデント対応フローに当てはめながら現場で発生する事象を整理し、状況付与の場面等を設定する。設定した状況付与は表3のように訓練・演習内での付与順やシナリオ上での発生日時、付与先（対象となる参加者）等と併せて一覧化する。なお、あらかじめ企画担当者側で参加者に期待するアクション等を洗い出しておき、訓練の目的や参加者のレベルに応じて、状況付与を行う際に同時にヒントを示すなどの工夫も効果的である。

表3に状況付与の例を示した。この例では過去に発生した医療機関へのサイバー攻撃事例を踏まえ、電子カルテ使用不可の報告からマルウェアへの感染が発覚したシナリオとし、インシデント対応フローのうち、異常検知（報告の受付）から診療部門等による応急対応までを状況付与の対象としている。

このように自施設の現状や課題に沿ったシナリオ及び状況付与を設定することで、(1)で設定した訓練・演習目的の達成を目指す。

表3　状況付与の例

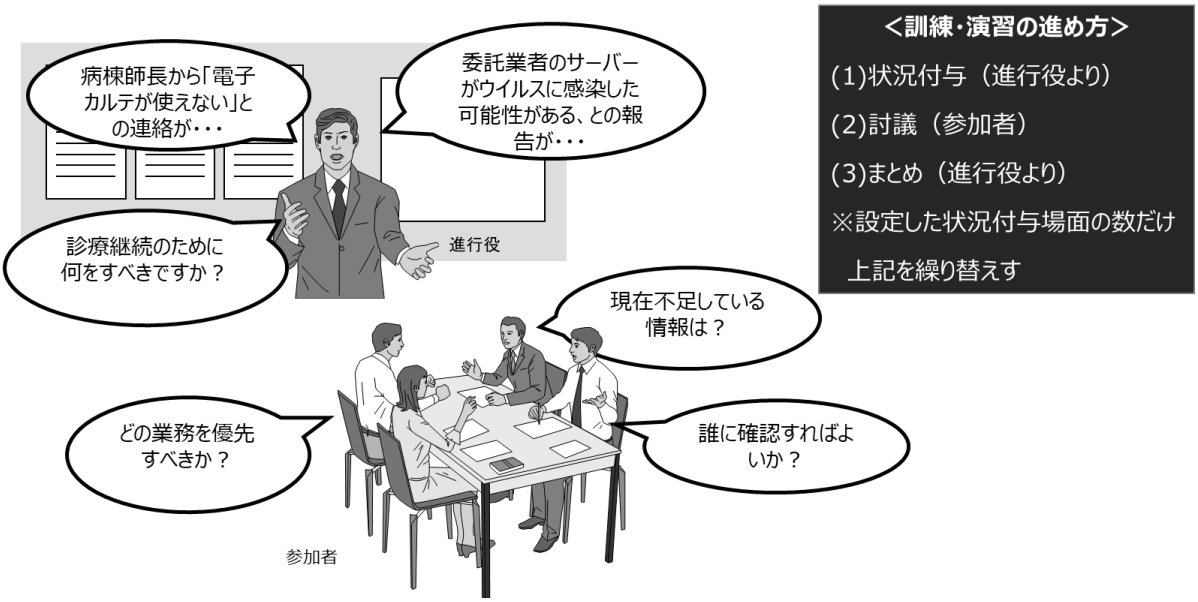
付与順	状況付与			付与先	期待するアクション等
	シナリオ上の日時	概要	内容		
1	○月○日 xx:xx	報告の受付	病棟師長から「電子カルテが使えない」との連絡があった	システム担当部門（者）・CSIRT	・事実確認、情報収集の実施 ・院内への情報共有　　等
2	○月○日 yy:yy	初動対応 原因調査	・システム担当者が電子カルテサーバーを確認したところ、ランサムノート（身代金要求文書）を発見 ・複数の職員から他端末も利用できないとの報告あり	システム担当部門（者）・CSIRT	・ネットワークからの切り離し等の被害拡大防止措置 ・責任者等へのエスカレーション ⇒緊急の幹部会議開催等の検討へ ・連絡体制図に基づくシステムベンダや厚労省窓口等への連絡　等
3	○月○日 zz:zz	応急対応	病院長等の幹部職員が参集し、緊急の会議を開催。外来診療、予定手術等の停止が指示された	・診療・看護部門 ・総務・医事部門	・患者、患者家族等への説明 ・入院患者への診療等の継続 ⇒電子カルテが使用できない場合の継続方法の検討へ　等

ＭＳ＆ＡＤインターリスク総研にて作成

(5) 訓練・演習当日の運営

訓練・演習の当日は企画担当者等が進行役となり、実施する目的や訓練・演習方法を説明した上で、(4)で作成したシナリオや状況付与を参加者へ提示する。参加者は目的や訓練・演習方法に沿って与えられたシナリオ等を踏まえながら、自施設における状況付与ごとに対応方針や具体的な手順、各部門への指示内容等を検討する。具体的な訓練・演習当日の実施イメージは、図２のとおり。

図2　訓練・演習当日の実施イメージ



(6) レビュー

企画担当者は実施した訓練・演習について、参加者へアンケートを実施する等して、「目的の達成度」「訓練・演習への満足度」「訓練・演習を通じて得た気づき（サイバーインシデント対応におけ

る課題等）」「訓練・演習自体の改善点」等についての評価を受け、BCPや訓練・演習の内容に関する課題を洗い出す。洗い出された課題を整理し、それを踏まえたBCPの見直しを検討したり、次回の訓練・演習の企画に活かしたりすることで、BCPの実効性向上やより効果の高い訓練・演習の実施に繋げる。

参加者へ実施するアンケート項目の例は表４のとおり。

表4　参加者へのアンケート項目例

■　演習・訓練自体の満足度
■　演習・訓練を通じて得た気づき
■　BCPの改善や実効性の向上に役に立ったか
■　積極的に参加できたか
■　演習・訓練自体の改善点　　等

出典：一般社団法人日本シーサート協議会「サイバー攻撃演習訓練実施マニュアル」を基に
ＭＳ＆ＡＤインターリスク総研にて作成

３．医療機関におけるサイバーBCPに今後求められること

医療機関におけるサイバーBCPの現状として、令和5年度から実施されている医療法に基づく立入検査でのチェック等により、多くの医療機関で策定フェーズは終了し、今後は研修等による関係者への周知や訓練・演習の実施による検証・見直し等に取組まれていくことと思われる。

訓練・演習等は繰り返し実施することによってマンネリ化してしまう傾向があるが、その多くは「ガイドライン等で義務づけられているから」「加算を取得する要件になっているから」といった外部からの要請を満たすことのみを目的としてしまうことに要因があると思料する。そのような要請を満たすことも重要ではあるが、前述した目的の例で示したように訓練・演習等を通じてBCPの実効性を向上させることで、診療の継続・早期復旧を図り、地域医療や自施設・法人の経営等への影響を最小限に抑えることを本来の目的とすべきである。また、サイバー攻撃にはトレンドが存在し、毎年同じ内容のシナリオや状況付与ではそれに対応できないため、企画担当者は平時から情報収集を行い、その時期のトレンドに合った訓練・演習を企画することが求められる。

各医療機関におかれては、このような目的意識を持って、自施設の現状や課題等に沿った訓練・演習を企画し、継続的に実施いただきたい。

なお、ＭＳ＆ＡＤインターリスク総研では、医療機関におけるサイバーBCPを対象とした訓練・演習の企画や実施の支援が可能なため、気軽に問い合わせ頂きたい。

ＭＳ＆ＡＤインターリスク総研株式会社 リスクコンサルティング本部
リスクマネジメント第四部 社会保障・医療福祉グループ
上席コンサルタント　岡田　拓巳

【参考資料】

1) 警察庁サイバー警察局「サイバー事案の被害の潜在化防止に向けた検討会報告書」令和 5 年 3 月
2) 厚生労働省「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
3) 一般社団法人日本シーサート協議会「サイバー攻撃演習訓練実施マニュアル」令和 5 年 3 月
https://www.nca.gr.jp/activity/pub_doc/drill_manual.html

コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問合せ先、またはあいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
ＭＳ＆ＡＤインターリスク総研株式会社　**https://rm-navi.com/**
リスクマネジメント第四部　社会保障・医療福祉グループ
千代田区神田淡路町2-105 TEL:03-5296-8976／FAX:03-5296-8941