別添２

サイバー攻撃を想定した事業継続計画（BCP）策定の確認表のための手引き

○ 本手引きは、「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表」について、サイバー攻撃を想定した BCP 作成の一助となるよう、解説を加えたものです。貴組織において BCP を作成する際の参考として活用してください。

※ サイバー攻撃を想定した BCP 策定時の留意点

・ 本手引き及び確認表は最低限必要な事項を記したものです。医療機関の特性に応じて、自機関が主体となり必要な事項を整理し定めてください。

・BCP 策定には先だってリスク分析が重要となります。リスク分析は全過程において自機関だけでなく、事業者、その他の関係者の間で、情報および意見を相互に交換（リスクコミュニケーション）することが必要です。

・ BCP は定期的に見直し、必要な項目を更新してください。

・ 医療情報システムとは、医療に関する患者情報（個人識別情報）を含む情報を取り扱うシステムを指します。例えば、医療機関等のレセプト作成用コンピュータ（レセコン）、電子カルテ、オーダリングシステム等の医療事務や診療を支援するシステムだけでなく、何らかの形で患者の情報を保有するコンピュータ、遠隔で患者の情報を閲覧・取得するコンピュータや携帯端末等も、範ちゅうとして想定されます。また、患者情報の通信が行われる院内・院外ネットワークも含みます。

・ 医療機関の規模により作成する BCP の内容も異なると想定されるため、関係団体等により示されている BCP の手引きについても適宜参照して作成してください。

・本手引きの各項目の解説の下部には、それぞれの項目に紐づく「医療情報システムの安全管理に関するガイドライン」関連文書の該当箇所を括弧内に示しております。

【１．平時（平時において、非常時に備え、サイバーセキュリティの体制整備を行う。）】

1-1）情報機器等の把握と適切な管理、全体構成図の作成

必要に応じて医療情報システム事業者等の協力を得ながら、自医療機関が保有する情報機器等の全体を網羅する医療情報システムに関する構成図（外部接続点を含むネットワーク構成図等）を作成する。

サーバ、端末 PC、ネットワーク機器を把握できているか。

院内のサーバおよび端末 PC の OS、IP アドレス、使用用途、脆弱性対応状況、ウイルス対策ソフトの稼働状況等の一覧を整備しておく。なお、各 PC にログオンする際に管理者権限でログオンする PC が分かるようにしておく。また、院内設置のすべての VPN 装置、ファイアウォール、ルータ-等の所在と、IP アドレス、使用用途等を明記した一覧を作成する。

（企画管理編：9.1、システム運用編：8.4）

ネットワーク構成図・システム構成図が整備できているか。

HIS 系、インターネット系等の院内 LAN、外部接続点（ファイアフォール、VPN、地域連携、オンライン資格確認等）のネットワーク構成が判別できるように IP アドレスおよびルーティングがわかる構成図を整備しておく。

（企画管理編：4.4、システム運用編：2、Q&A：概 Q- 6 ）

システム停止が事業継続に与える影響を把握できているか。

各システムが利用できなくなると、どの業務が継続できなくなるか（検査部門システムの場合、検査の受付と検査結果の電子カルテ送信ができなくなる等）といった被害を想定し、代替運用の手順を作成しておく。また、代替運用サーバ、参照サーバ、バックアップデータの保持といった非常時対策状況を確認しておく。

（経営管理編：3.4、企画管理編:11）

サーバ、端末 PC、ネットワーク機器の脆弱性への対応ができているか。

サーバ、端末 PC、ネットワーク機器について、医療機関が管理する機器と、事業者が管理する機器を明確化し、脆弱性情報の収集、脆弱性対応プログラムの適用基準等を定めておく。

（経営管理編：3.4.2、企画管理編：12）

1-2) 非常時に備えたサイバーセキュリティ体制の整備とリスク検知のための情報収集

インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図が整備できているか。

非常時の役割や手順を定め、医療機関の内部や外部関係機関との緊急連絡先や情報伝達ルートを整備し関係者へ周知しておく。契約書やサービス・レベル合意書(SLA）により、非常時の責任分界点や役割分担について事業者等との明示的な合意内容を確認しておく。

（経営管理編：3.4.3、企画管理編：2.1、12.3、Q&A：企 Q-16）

リスク検知のための情報収集体制が整備できているか。

自医療機関に重要な脆弱性情報が事業者から報告されるスキーム（保守契約等）を確立しておく。ファイアウォール、VPN 等外部接続点のアクセスログを定期的に確認する体制を整備しておく。

（企画管理編：12.2、システム運用編：8.2、17）

教育訓練が実施できているか。

策定した BCP が迅速かつ適切に利用できるように、教育訓練を定期的に実施する。システムが利用できなくなることを想定して、障害時マニュアルや伝票運用マニュアルを準備しておく。教育訓練の結果、必要に応じて改善計画を作成する。

（企画管理編：11.⑥）

バックアップの実施と復旧手順が確認できているか。

オフラインバックアップ等サイバー攻撃を想定したデータとシステムのバックアップの実施と復旧手順の確認をしておく。また、復旧手順においては、業務フローを意識して復旧するシステムの優先度（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。

（経営管理編：3.4.1、企画管理編：11.2、システム運用編：11）

【２．検知（医療情報システム等の障害が見受けられる場合は、早期に医療情報システム部門へ報告し、異常内容の事実確認を行う。）】

2-1）システム異常の報告先の把握

異常時の連絡体制図が全職員に把握されているか。また、連絡先等を速やかに取得できるか。

相談窓口の一本化や体系化を組織内で行う。連絡先を院内に掲示したり、情報セキュリティマニュアルなどのわかりやすい箇所に明示する。

（経営管理編：3.4.2）

2-２）システム異常の検知

院内で発生した異常が院内職員によって覚知できるか。

発生部署、発生個所、発生日時、連絡者、異常の状態について、口頭、報告様式等を用いて正確に伝達する。

（経営管理編：3.4.3）

2-３）CSIRT/経営者によるシステム異常の覚知

院内職員から発出されたサイバー被害情報が組織を通じて速やかに CSIRT（対応者）ならびに意思決定者まで到達するか。

連絡経路を組織化し、院内のどの部署から生じたシステム障害であっても、CSIRT と経営者に必ず伝達されるように担当者を整備する。また、組織変更に応じて適宜最新化し、連絡経路が機能することを担保する。

※CSIRT（Computer Security Incident Response Team）：

コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をする。

【３．初動対応（迅速に初動対応を進めて、サイバー攻撃による被害拡大の防止や診療への影響を最小限にする。）】

3-1）原因調査（必要に応じて事業者に依頼）

原因調査のため、「ネットワーク機器やケーブル等の調査」、「電源系統、ブレーカー、ハードウェア、ソフトウェア等の調査」等が実施できるか。また、必要に応じて事業者に依頼できる体制になっているか。

障害の原因としてサイバー攻撃の兆候があるか、医療情報システムのメンテナンス等の問題か、医療情報システム自体の問題か、LAN 設備やケーブルの問題か、設備の電源系統の問題か等調査を実施する。また、情報漏えいの有無を調査する。必要に応じて医療情報システム・サービス事業者等に協力を依頼できる体制にする。

3-2）事業者等への連絡と作業履歴の確認

事業者等への連絡と作業履歴の確認ができるか。

障害の前日等に医療情報システムのメンテナンスやデータ移行等の作業の有無を確認し、該当する場合は、当該作業が障害の原因であるかを確認する。

3-3）被害拡大防止

被害拡大防止に向けた対応ができるか。

3-1 による原因調査の結果、サイバー攻撃の兆候がある場合は、ネットワークの遮断により通信を遮断し感染拡大を防止する。その他、バックドアの無効化、無効にされたセキュリティ機能の復帰、攻撃された脆弱性への対応等の被害拡大防止措置を行う。必要に応じて医療情報システム・サービス事業者等に協力を依頼できる体制を整えておく。

（企画管理編：3.1.5、システム運用編：18.1）

3-4）経営層への報告、経営層による確認と指示、組織内周知

経営層がサイバー攻撃兆候等を認める際の組織内報告を受け、医療情報システム使用中止等の指示を判断できるか。

サイバー攻撃の兆候等がある場合は、経営層に報告し、対象となる医療情報システム等の使用の中止を指示する。経営層は、対応チーム設置、及び対象となる医療情報システム等の使用中止に伴う業務運用（診療体制等）方針について検討し、必要に応じて組織内に周知し、対応を求める。（サイバー攻撃の影響・被害状況・影響範囲等を踏まえて、情報公開の必要性について検討する。）経営層は診療を継続する観点で「医療施設の災害対応のための事業継続計画」も参考にしながら医療機関全体の事業継続計画を策定する。対象となる医療情報システム等の異常・障害時の、診療体制、及び医療情報システム等を代替した業務運用方法（紙カルテ運用、参照系環境構築等）に関する対処についても定めておく。

例）◯紙カルテ運用

・紙伝票の最新化と帳票準備

・運用フローの作成と共有

○ 参照系環境構築

・サーバおよび端末 PC の構築

・プリンタ、印刷用紙、トナー準備

（経営管理編：3.4、企画管理編：11）

3-5）被害状況等調査（フォレンジック調査＊＋証拠保全）と被害状況等の報告

被害状況等調査（フォレンジック調査＋証拠保全）と経営層への被害状況等の報告ができるか。

アクセスログの分析や情報の改ざんや暗号化の有無等からサイバー攻撃の範囲、個人情報漏洩の有無等について調査し、経営層へ報告する。必要に応じて、事業者へ協力を依頼して調査を進める。自機関で証拠保全が可能か検討し、困難な場合は事業者等へ依頼する。経営層へ被害状況等を適時報告する。あらかじめ初動対応の流れについて事業者等と事前に確認しておくこと。

＊フォレンジック調査：

サイバー攻撃で消去・改竄されたデータや攻撃活動のログを取得し、攻撃対象、方法、被害範囲などを解明する調査のこと

（企画管理編：11）

3-6) 組織対応方針確認と外部関係機関への報告等の対応

組織対応方針を確認できるか。

被害状況（診療継続への影響や個人情報漏洩への有無等）に基づいた経営層による対応方針を確認し、対応する。また、被害状況について所管省庁への報告、法的措置、機密情報漏洩等の対応を確認して報告する。

（経営管理編：3.4.3）

【４．復旧処理（復旧計画に基づいて、医療情報システムの事業者及びサービス事業者等と協力して復旧を行う。証拠保存の観点からバックアップデータ等を取得する。）】

4-1）経営層からの復旧指示の確認と実施

復旧指示の確認と実施ができるか。

復旧計画、復旧時間、費用等を踏まえて、経営層は復旧計画を指示し、情報システム担当者等は復旧計画の実施を行う。特に、ワークフローを意識してあらかじめ設定した医療情報システムの「復旧優先度」を基に復旧を行う。復旧優先度は、診療継続を意識して定める「重要度」と異なる場合がある。（Q&A：企 Q-42）

4-2) 医療情報システム等の事業者等へ復旧対応依頼

（医療情報システム等の）電子カルテシステム等の事業者等への対応依頼ができるか。

自機関で復旧が困難な場合、事業者等へ復旧作業を依頼する。

例）・情報システム担当者と事業者間で、バックアップ復元手順や対応者を、平時に定めておく。

・復旧に時間を要する場合、代替として、紙カルテ運用、参照系環境構築を検討する。

（企画管理編：11）

４-3) 再設定や再インストール、バックアップデータ復旧等

再設定や再インストール、バックアップデータの復旧等ができるか。

端末 PC/サーバ復旧手順について、情報システム担当者、事業者等と連携して事前に定め、それに基づき、再設定や再インストール、バックアップからデータ復旧等を実施する。

復旧の際、既知の脆弱性、漏洩した可能性のあるパスワード等に注意する。

（[特集] 医療機関等におけるサイバーセキュリティ:3.3 必要最小限の対策：バックアップ（システム・データ））

４-4) 復旧結果の確認

復旧結果の確認ができるか。

復旧処理について、医療情報システム等が正常に稼働することを確認する。

作業者は手順の進捗状況に合わせて経営層に報告を行い、経営層は組織方針に合わせて運用を変更する。

【5.事後対応（復旧結果の報告を受け、再発防止に向けた検討と再発防止策の周知と実施を進める。）】

5-1) 復旧結果と情報漏えい事実の有無の報告

復旧結果と情報漏えい事実の有無、可能性について、院内での報告を行う方法、報告先、内容を、企画管理者、システム担当者がそれぞれの分担責任として把握しているか。

下記を、経営層に報告する（組織内への周知も行う。）。

・異常の内容、原因、被害状況、復旧工数及び費用等について

・復旧結果について

・情報漏えいの有無、範囲について

5-2）再発防止策の検討・策定

再発防止策の検討および策定を進める体制、能力があるか。管理者、システム担当者がそれぞれの分担責任として把握しているか。

経営層や対策チームを交え、再発防止策の検討・策定を行う。

（経営管理編：1.2.2、3.4.3、企画管理編：2.1.3、3.1.5）

5-3）再発防止策の周知

再発防止策の周知を院内に周知する方法と体制が整備されているか。

確定した再発防止策を、関係者等に周知する。

5-4) 再発防止策の実施

再発防止策の実施が行えるか。

定期的なチェック箇所を割り出し、日々の保守業務へのチェック箇所、実施内容、実施者の落とし込みを行う。

5-5) 事業者等への再発防止策の指示

事業者に対して再発防止策を具体的に提案し、実施可能かつ有効な方法を策定する能力があるか。

策定した再発防止策を事業者へ周知し業務への反映を指示する。指示した再発防止策が実施できているか定期的に確認する。

（企画管理編：2.1.3）

5-6) 外部関係機関への報告と情報公開の検討

情報公開の内容検討を行う体制、連絡先、内容を文書として準備し、必要時に速やかに利用できるか。経営者と担当者により外部関係機関への報告が行えるか。

経営層と担当者が情報公開の内容検討を行う体制、連絡先、内容を文書として準備し、必要時に速やかに利用できる体制を備えておく。関係省庁等外部関係機関への報告とサイバー攻撃の影響・被害状況・影響範囲等を踏まえて、情報公開の必要性および内容について検討し、経営層の意思決定として策定する。

（経営管理編：1.2.2）