事　務　連　絡
令和６年６月６日

各（都道府県／保健所設置市／特別区）　医務主管部局　御中

厚生労働省医政局
特定医薬品開発支援・医療情報担当参事官室

「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

日頃から厚生労働行政に対して御協力を賜り、厚く御礼申し上げます。

「「医療機関におけるサイバーセキュリティ対策チェックリスト」及び「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」について」（令和６年５月 13 日付け医政参発 0513 第６号、厚生労働省医政局特定医薬品開発支援・医療情報担当参事官通知）において、サイバー攻撃を想定した事業継続計画（BCP）については、「今後 BCP 策定に関する手引きを作成し、別途お示しする予定です。」とお示ししたところです。

今般、別添１のとおり、「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表」（以下「確認表」という。）を作成するとともに、別添２のとおり、確認表を分かりやすく解説した「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」、及び別添３のとおり、医療情報システム部門等における事業継続計画（BCP）のひな形を作成しました。

貴職におかれては、本通知について、御了知の上、関係団体、関係機関等に周知徹底を図るとともに、その実施に遺漏なきよう御配慮願います。

なお、本内容については、下記の厚生労働省 HP に公表していることを申し添えます。

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

別添１

サイバー攻撃を想定した
事業継続計画（BCP）策定の確認表

令和６年６月

厚生労働省

サイバー攻撃を想定した事業継続計画（BCP）の作成について

厚生労働省では、令和５年度から、医療法に基づく医療機関に対する立入検査の項目に、サイバーセキュリティ対策を位置付けました。立入検査の際に確認する項目は、「医療情報システムの安全管理に関するガイドライン」から優先的に取り組むべき項目について、「医療機関におけるサイバーセキュリティ対策チェックリスト」（以下「チェックリスト」という。）によりお示ししてきたところです。

昨今の巧妙化したサイバー攻撃の現状において、セキュリティ対策を講じることでリスクを低減させることはもちろん重要ですが、リスクを完全に排除することはできません。

例えば、過去には、

・インシデント発生時の初動対応について十分に協議されておらず、証拠保全が不十分となり、被害範囲の特定ができなかった、
・インシデント発生時に、ネットワーク機器が院内のどこに配置されているかわからず、原因究明に時間を要した、
・ランサムウェアによる攻撃の際に、バックアップが適切に確保できておらず、復旧が難航した、

といった事例が実際に発生しており、このようなケースでは、診療継続を含めた医療機関の機能に重大な影響が生じます。

サイバー攻撃を「どのように防ぐか」だけでなく「発生時にどのように対応するか」という意識で、非常時に診療への影響を最低限に抑えるための対応を、あらかじめ「サイバー攻撃を想定した事業継続計画（BCP）」（以下「BCP」という。）として策定しておくことで、適切な復旧対応等を行うことが可能となります。

こうしたことから、チェックリストの項目としても、医療機関に対してBCPの策定を求めており、今般、BCPの策定に際して参考としていただけるよう、「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表」（以下「確認表」という。）を作成しました。医療機関の特性に応じて必要とされるBCPは様々ですが、今般作成した確認表等や関係団体より発出されている資料等を参考に、貴施設においてもサイバー攻撃を想定したBCPの策定をお願いします。

サイバー攻撃を想定した事業継続計画（BCP）策定の確認表

※医療機関がBCPを策定する際、最低限必要な事項を網羅しているか、確認のために使用するものです

※BCP策定や見直しの際にご活用ください

項番	大項目	確認項目	確認欄
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	サーバ、端末PC、ネットワーク機器を把握できているか。	
		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。	
		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。	
		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。	
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。	
		リスク検知のための情報収集体制が整備できているか。	
		教育訓練が実施できているか。	
		バックアップの実施と復旧手順が確認できているか。	
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。	
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。	
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。	
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。	
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。	
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。	
3-4	経営層への報告、経営層による確認と指示、組織内周知と対応	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。	
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。	
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。また、外部関係機関への報告ができるか。	

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。	
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事業者等への対応依頼ができるか。	
4-3	再設定や再インストール、バックアップデータの復旧等	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。	
4-4	復旧結果の確認	復旧結果の確認ができるか。	
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。	
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。	
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。	
5-4	再発防止策の実施	再発防止策の実施が行えるか。	
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。	
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。	

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）

別添３

医療情報システム部門
事業継続計画（BCP）

〇〇年〇〇月〇〇日　初版

〇〇病院

〇〇部門

目次

第 1 章 総則

1.1　策定目的

本事業継続計画（以下、本 BCP という）は、○○病院（以下、当院という）においてサイバーインシデント発生時における組織的対応の基本方針及び職員の取るべき行動の基本原則を示すことによって、医療安全、情報保全を担保しつつサイバー攻撃に対応するセキュリティ体制の構築、ならびに早期復旧までを視野に入れた活動の実現により、国民に信頼される医療機関として社会福祉に貢献することを目的とする。

1.2　基本方針

当院は、個人情報の保護と医療サービスの継続性を確保するために、以下の方針に基づき、サイバーセキュリティ対策の水準を高めていく。

I.　安全かつ持続的な医療サービス提供を実現する
II.　サイバーセキュリティに対する脅威からの被害から事業を保護する
III.　リスクマネジメントの対象としてサイバーセキュリティを確保する
IV.　平時、非常時を通じて事業継続に関する説明責任を果たす
V.　被害後、医療安全を担保しつつ、迅速かつ合理的な医療業務復旧を行う

1.3　対象範囲

1.3.1 対象とする医療情報システム

対象とする医療情報システムは以下の通り。

I.　電子カルテシステム
II.　医事会計システム（レセプト）
III.　医用画像システム
IV.　各種部門システム（検査、処方など）
V.　オーダリングシステム
VI.　○○○○

1.3.2 想定する事象

本 BCP で想定される事象において、診療業務に影響するものを以下に挙げる。なお、自然災害、大規模停電等による電源喪失などの計画は別に定めるものとする。

I. 診療情報・参照情報・指示情報の確認・参照不能
II. 診療情報・参照情報・指示情報の入力不能
III. スタッフ間の連絡不能
IV. 情報機器・医療機器の操作不能・誤動作
V. ○○○○○○

また、これらの被害を引き起こすサイバー攻撃の例として以下が挙げられる。

I. 不正アクセス等
II. 標的型メール攻撃
III. マルウェア感染（ランサムウェアを含む）
IV. 分散型サービス妨害（DDoS 攻撃）
V. ○○○○○○
VI. 上記の予兆と思われる現象

1.4 文書の管理および周知

本 BCP は○○部門にて、現状を適切に反映した原本および関連資料の整備ならびに管理を行い、経営層の承認を受けた上で、当院の全職員に開示周知する。

第２章 体制整備

2.1　情報機器等の把握と適切な管理

平時において、非常時に備えたサイバーセキュリティの体制整備を以下のとおり行う。

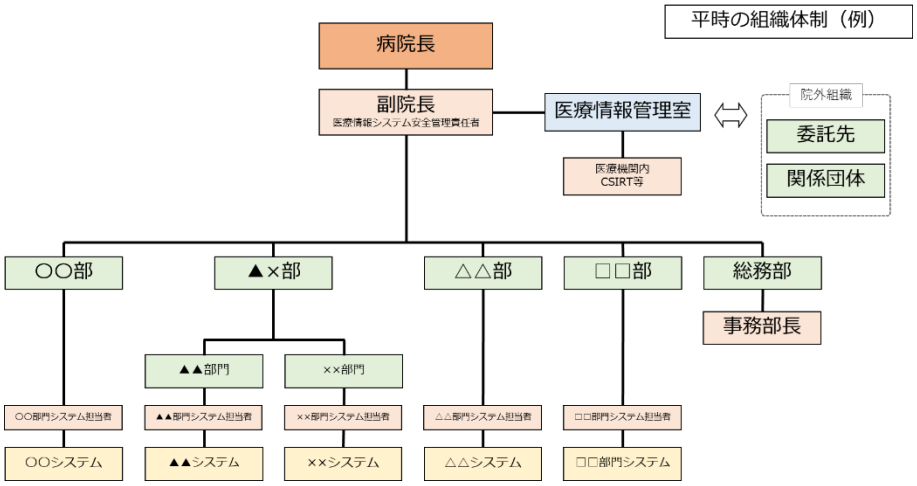
2.1.1 医療情報システム安全管理責任者

○○を、医療情報システム安全管理責任者として定める。△△（理事長、病院長）を当院におけるサイバーセキュリティに関する最高責任者とする。

（医療機関の規模・組織等によっては上記が兼務することも想定される。）

2.1.2 組織体制図

診療継続及び医療情報システムの復旧を目的としたサイバーセキュリティの組織体制を以下のとおり定める。担当部署、担当者、役割についても示す。



図◯：平時の組織体制図（例）

表◯：担当者の役割（例）

役割	担当部署・担当者	役割の概要
医療情報システム最高責任者	病院長	診療継続及び医療情報システムの復旧の計画策定を統括し、最終的な責任を負う。
医療情報システム安全管理責任者	○○	医療情報システム復旧の計画策定に関する各種検討作業を行う。
病院事務部	○○	診療継続の計画策定に関する各種検討作業を行う。
診療部門システム担当者	○○課	各診療部門システムの運用継続計画策定に関する各種検討作業を行う。
委託先	○○社	医療情報システムの運用保守及び緊急時の状況に関する情報提供・対策調整

2.1.3 情報機器台帳

医療情報システム安全管理責任者は、情報機器の現況を反映した管理台帳を以下（または別紙資料）のとおり整備する。併せて、定期的に棚卸しを行い、機器の所在と稼働状況の確認を行う。

表◯：情報機器台帳（例）

管理番号	メーカー	OS	ソフトウェア	ソフトウェアバージョン	IPアドレス	コンピュータ名	設置場所	利用者	登録日	状態	説明
001	A社	Win11	○○電子カルテ	2.0	192.168.○.○	Room1のPC１	Room1	a医師（○○科）	2020/12/1	稼働	
002	A社	Win11	○○電子カルテ	1.2	192.168.○.○	Room1のPC2	Room1	b医師（○○科）	2020/12/1	停止	メンテナンス
003	A社	Win8	○○電子カルテ	2.0	192.168.○.○	Room2のPC１	Room2	c医師（△△科）	2014/10/1	稼働	
004	B社	Win11	○○管理システム	5.0.1	192.168.○.○	Room3のPC１	Room3	a医師（○○科）、b医師（○○科）、c医師（△△科）	2021/8/1	稼働	

（出典：医療機関におけるサイバーセキュリティ対策チェックリストマニュアル ～医療機関・事業者向け～ ）

2.1.4 ネットワーク・システム構成図

医療情報システム安全管理責任者は、医療機関等で導入している医療情報システムの全体構成図（ネットワーク図、システム構成図等）を整備する（ネットワークの全体像が分かりやすいものを作成）。併せて、構成、接続等に変更が生じた場合には構成図の更新を行い、常に最新の状態を保つ。

2.1.5 リスク評価・代替運用

各システムが利用できなくなった場合、その業務内容の代替手段を以下のとおり定める。また、代替運用方法については別途、システム停止時の代替運用マニュアル等にて定める。

表◯：業務内容に対する代替手段（例）

業務内容	システム	代替手段
診療録等	電子カルテシステム	紙運用
処方・検査	オーダリングシステム	紙運用（カーボンコピー）
放射線画像診断	PACS	撮影機器ワークステーションにて画像閲覧
会計	医事会計システム	未収扱いを検討
○○○○○○	○○○○○○	○○○○○○

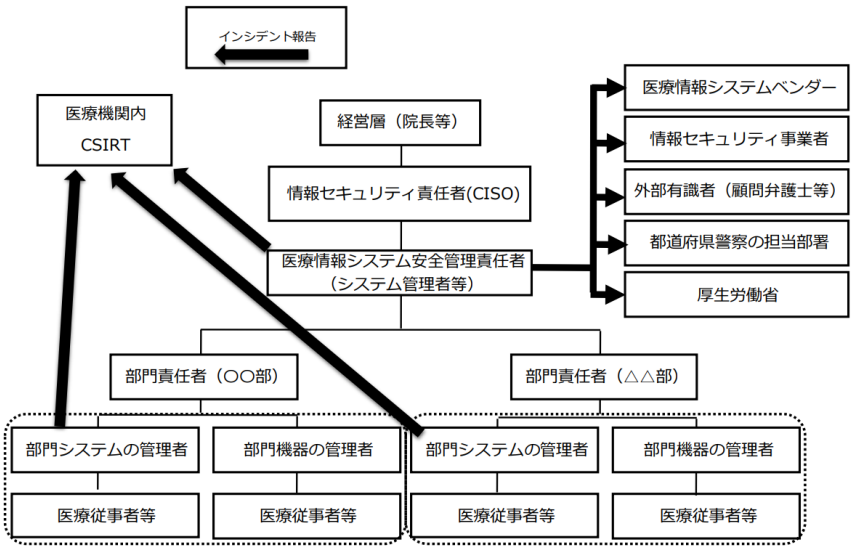
2.1.6 脆弱性に関する対策

医療情報システム安全管理責任者は、契約等で定められた責任分界をもとにサーバ、端末 PC、ネットワーク機器について脆弱性情報の収集を行う。脆弱性が発見された機器について、脆弱性対応プログラムの適応を行う。万が一、適応できない場合の代替手段（隔離運用、隔壁の追加、監視の強化、機器入れ替え等）について事業者等と合意した上で取り決め、実施する。

2.2　非常時に備えたサイバーセキュリティ体制

2.2.1 連絡体制図

診療継続及び医療情報システムの復旧に資するアクションを迅速に行う目的で、サイバーセキュリティの連絡体制（連絡先、担当、メールアドレス、電話番号、連絡目的等）及び外部関係機関の連絡先を以下のとおり定める。



（出典：医療機関におけるサイバーセキュリティ対策チェックリストマニュアル ～医療機関・事業者向け～）

図〇：連絡体制図（例）

表〇：外部関係機関の連絡先一覧（例）

外部関係機関	連絡先
厚生労働省医政局特定医薬品開発支援・ 医療情報担当参事官室	03-6812-7837 igishitsu@mhlw.go.jp
〇〇（都道府県警察の担当部署）	××-××××-××××
〇〇	××-××××-××××
〇〇	××-××××-××××

2.2.2 情報収集体制

当院における各システムの脆弱性情報について事業者等から情報提供を定期的に受け取ることができる体制を以下のとおり構築する。

表◯：事業者等の連絡先（例）

システム	担当	連絡先
電子カルテ	◯◯社	××-××××-×××× ◯◯@◯◯
保守委託先	◯◯社	××-××××-×××× ◯◯@◯◯
放射線撮影機器	◯◯社	××-××××-×××× ◯◯@◯◯
検査機器	◯◯社	××-××××-×××× ◯◯@◯◯
◯◯	◯◯社	××-××××-×××× ◯◯@◯◯

2.2.3 教育体制

本 BCP が迅速かつ適切に利用できるよう、年◯回以上の教育、訓練を実施する。情報セキュリティ責任者（CISO）、医療情報システム安全管理責任者は年間の教育計画に沿った訓練が適切に実施されるように監督する。訓練結果により、事前対策やサイバーインシデント発生時の対応計画等に解決すべき課題が発生した場合、課題の解決もしくは改善に向けた計画の立案をする。

2.2.4 バックアップ体制

サイバーインシデント発生時に備えた、データとシステムのバックアップの頻度、作成方法及び復旧方法について以下のとおり定める。

表◯：バックアップの作成と復旧方法（例）

システム	頻度	作成方法	復旧方法
電子カルテ	1 日	バックアップサーバにデータベースのバックアップを作成する	データベースを再構築した後に、バックアップサーバのデータを復元する
	7 日	磁気テープ・光学メディア・外付け HDD 等にデータベースとシステムファイルのバックアップを作成する	システムの OS を再構築した後に、磁気テープのシステムファイルとデータベースのデータを復元する
◯◯	◯◯	◯◯	◯◯
◯◯	◯◯	◯◯	◯◯

第３章 サイバーインシデント発生時の対応

3.1　異常発見時の連絡先

異常発見時の連絡経路は 2.2.1 の表◯に示す通りとする。あわせて、各担当部門の連絡先は以下のとおり示す。なお、部門システムの管理者は連絡先が全職員に把握されるように明示して、常に最新版で管理し連絡経路が機能することを担保する。

表◯：部門連絡先一覧（例）

部署名	担当者	連絡先
○○部門	○○	××-××××-××××
システム管理室	○○	××-××××-××××
医療情報システム安全管理責任者	○○	××-××××-××××

システム	事業者	担当者	連絡先
電子カルテシステム	○○	○○	××-××××-××××
○○○システム	○○	○○	××-××××-××××
○○○システム	○○	○○	××-××××-××××
○○○システム	○○	○○	××-××××-××××

3.2　システム異常の検知と経営層への情報伝達

システム異常を検知した場合、あらかじめ定めた項目（発生場所、発生箇所、発生日時、連絡者、異常の内容・範囲）について担当部門に報告できるように周知する。なお、口頭による連絡後、「報告様式」を用いて記録を残す。また、院内職員から発出された異常において、医療情報システム安全管理責任者によりサイバー攻撃の可能性が思慮された場合、2.2.1 で作成した連絡体制図を基に、速やかに経営層ならびに関係各所・外部関係機関に共有され、意思決定できるように努める。

3.3　初動対応

サイバーインシデント発生後は、以下のとおり対応する

3.3.1 原因調査

医療情報システム安全管理責任者はサイバーインシデントの原因や被害範囲の特定のために、医療情報システム・サービス事業者へ以下の調査依頼を指示または実施する。

I.　ネットワーク機器やケーブル等の調査
II.　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
III.　情報漏えいの有無に関する調査
IV.　メンテナンスやデータ移行等の作業に関する調査
V.　○○○○○○

3.3.2 被害拡大防止

被害拡大防止のための対応を行う。まずは、バックアップに通ずるネットワークの遮断を行う。次に、外部の通信経路を遮断する。その上で、被害箇所から攻撃範囲および侵入経路の推定を行った上で、セグメンテーション境界において、通信を遮断して感染拡大防止を図る。

3.3.3 経営層への報告

医療情報システム安全管理責任者はサイバーインシデントについて経営層に対して、現在の被害状況を報告するとともにインシデント対応方法と患者安全を担保する運用方針案を提案する。この内容を踏まえて、経営層はシステム停止に伴う診療継続方針（診療体制の確保等）を検討し意思決定する。決定した内容は、速やかに 2.2.1 の連絡体制図で定める組織内ならびに外部関係機関へ周知を行う。

3.4　診療継続

サイバーインシデント対応と診療継続について報告を受けた経営層は以下のとおり対応する。

3.4.1 医療情報システムの縮退運転判断

経営層は医療情報システム安全管理責任者からの提案を受け、医療情報システム等の縮退運転または運転中止を判断する。また、インシデント対応中の診療継続においては、紙カルテの運用等、自然災害時を想定した事業継続計画（もしくはシステムダウン時マニュアル等）に則り運用する。

3.4.2 被害状況等調査（フォレンジック調査＋証拠保全）

医療情報システム安全管理責任者は、証拠保全の作業と診療継続に関する作業を調整しながら両立させる。具体的には、アクセスログの分析や情報の改ざん、暗号化の有無等からサイバー攻撃の範囲、個人情報漏えいの有無等の調査について医療安全を担保しつつ行う。必要に応じて医療情報システム・サービス事業者等へ協力依頼して調査を進める。なお、調査状況は随時経営層に報告する。

3.4.3 組織対応方針の確認と外部関係機関への報告

医療情報システム安全管理責任者の被害状況および調査結果に基づき、経営層は復旧対応方針（復旧に向けた対応、広報への対応）を決定し、その対応を関係者に指示する。また、2.2.1 で定める外部関係機関へ報告を行う。外部関係機関へは被害拡大防止等の観点からできる限り早く連絡する。

3.5 復旧処理

復旧計画に基づいて、以下のとおり対応する。医療情報システム安全管理責任者は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。

3.5.1 復旧指示と復旧作業

医療情報システム安全管理責任者は、経営層からの復旧指示を起点とする復旧対応方針に基づき、システムの復旧作業(システムの再設定、再インストール、バックアップデータからの復元等)並びに検証作業を行う。必要に応じ医療情報システム・サービス事業者に対応を依頼する。あわせて、システム停止中に生じたアナログ情報についてシステムに反映させる選択肢を提示する。経営層は、アナログ情報の反映時期ならびに程度を医療安全の観点を踏まえて意思決定する。

3.5.2 結果の確認

医療情報システム安全管理責任者は、復旧作業により復旧したシステムが安全な状態で正常に稼働したことを確認する。正常に稼働することが確認できた時点で、経営層に報告する。経営層は診療状況を総合的に勘案し、緊急時運用から通常運用への復旧を宣言する。

第 4 章 事後対応

4.1　報告

復旧後、復旧結果と情報漏えい事実の有無等について、経営層及び組織内に報告する。不足していたと考えられる事前対策、連絡先ならびに連絡内容について振り返りを行う。

4.2　再発防止

4.2.1 再発防止策検討・策定

4.1 の後、サイバー攻撃により発生した被害を抑止する手段について検討を行い、実施可能な選択肢を整備し、経営層に提案する。経営層は長期的視点と事業継続性の両立について検討し、安全性を維持するため再発防止策の選択を決定する。経営層は決定した再発防止策について、連絡経路を用いて全職員に周知する。

4.2.2 事業者への指示

経営層によって決定された再発防止策は、医療情報システム安全管理責任者等により、事業者が有するサービスや機器に対して対策を講じる必要があるかどうかを調査し、再発防止策の効果が出るよう対策実施を事業者へ打診する。事業者は、対策実施の時期や方法について、医療機関側と誠実に議論し、計画を立てて実施する。

4.3　情報公開

経営層は、類似のサイバー攻撃による被害拡大に対する警鐘を鳴らす目的、また当院を受診する患者への診療に関連する注意を喚起する目的で、速やかに情報公開を行う。情報公開内容は、知覚日時、現象、被害範囲、想定される攻撃経路、1 次対応、患者対応、復旧状況、事後対策などを含める。報告については、サイバー被害が発生した可能性が高い段階から迅速に行い、情報の更新を含めて複数回行う中で情報の確度を高めていく。