参考資料３-５

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。

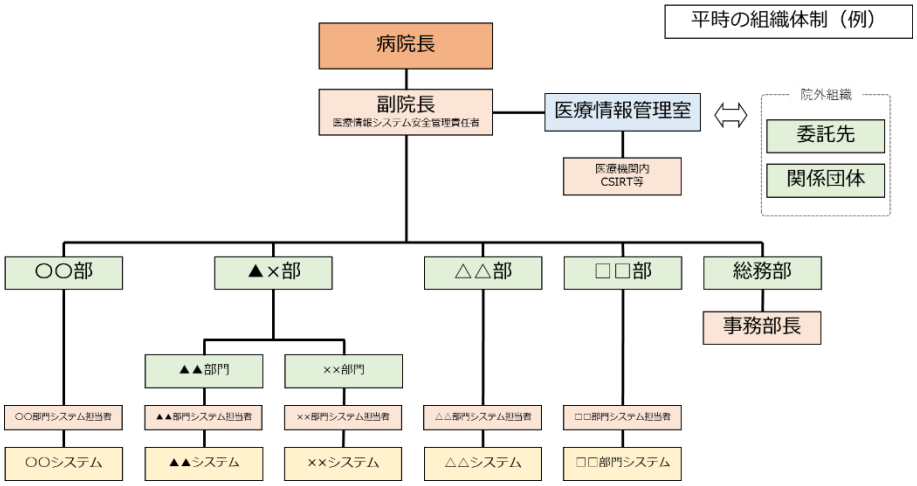
2.1.1 医療情報システム安全管理責任者

○○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
○○○○○○	○○○○○○	○○○○○○

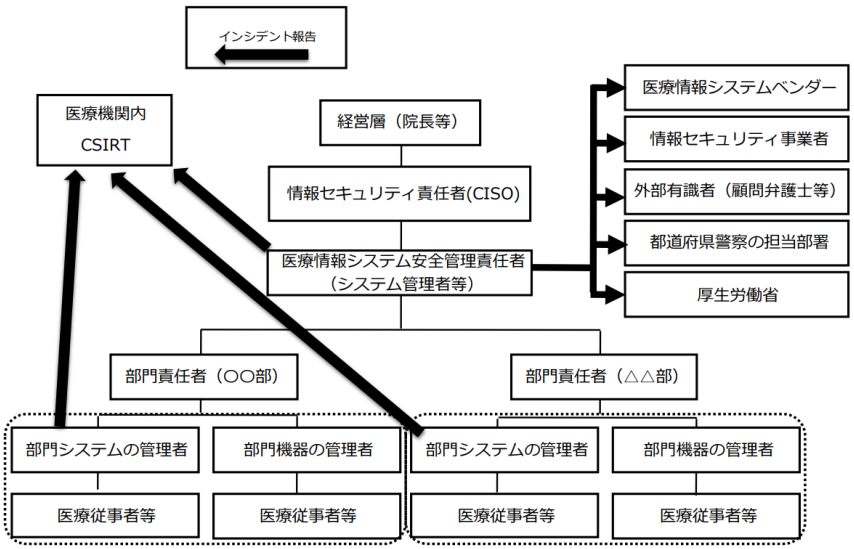
2.1.6 脆弱性に関する対策

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。