事業者名および個人名は不記載としています

国立大学法人東北大学

東北大学病院

ＩＴに関わる
防災・業務継続計画

（略称：病院ＩＴ－ＢＣＰ）

第１版

２０２５年５月

東北大学病院

～ 目　次 ～

制定・改訂履歴			
改訂番号	改訂日	改訂箇所	改訂理由
第１版	2025 年　4 月 24 日	全　体	制　定

作成者：ＢＣＰ委員会、ＢＣＰ事務局

■ 病院ＩＴ－ＢＣＰの審議プロセス

（重要事項）

２０２５年

１月２１日　　メディカルＩＴセンター（ＭＩＴＣ）内にて承認

３月１２日　　ＢＣＰ委員会承認

４月１６日　　運営会議にて第１版 承認

４月２４日　　運営評議会にて第１版 承認

５月　１日　　施行（第１版）

（経常的な事項）

原則、月１回ＭＩＴＣ内にてリスク洗い出しと改善策を審議し、ＢＣＰ事務局およびＢＣＰ委員会と連携しながら改訂作業を行う。

承認責任者：病院長　張替　秀郎

1　総則

1.1　基本方針

本書は国立大学法人東北大学病院（以下、「当院」という）において、当院の防災・業務継続計画（以下、病院ＢＣＰ）の一部として、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。

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。当院の「ＩＴに関わる防災・業務継続計画」（以下「病院ＩＴ－ＢＣＰ」という）を策定する。

【基本方針】

1. **安全かつ持続的な医療サービス提供を実現する**
2. **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**
3. **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**
4. **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**
5. **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**

（参考）

業務継続計画（BCP：Business Continuity Plan）とは：

大地震等の自然災害、感染症のまん延、テロ等の事件、大事故、サプライチェーン（供給網）の途絶、ランサムウェア被害、大規模なシステム障害の発生、突発的な経営環境の変化など不測の事態が発生しても、重要な事業を中断させない、または中断しても可能な限り短い期間で復旧させるための方針、体制、手順等を示した計画のこと。

当院においては、病院ＢＣＰが防災・業務継続計画の中核をなしているが、ＩＴ－ＢＣＰ（本書）はそのサイバーセキュリティに対する対応に特化したものである。

サイバーセキュリティとは：

病院情報システムが機能し、患者情報、医薬品・物流・検査などすべての業務に関する医療情報の安全性が確保されている状態と、その方策のこと。

2　計画・文書体系

2.1　計画・文書の位置づけ

病院ＩＴ－ＢＣＰは、病院ＢＣＰの一部として当院がサイバーセキュリティ上の重大な被害を受けて、その対応を緊急に実施しなければならない場合を想定して策定されたものである。

なお、病院ＩＴ－ＢＣＰは、サイバー犯罪への対応や被害を受けた時また大規模なシステム障害が発生した時の当院の災害対策内規、災害対策マニュアル、災害対策本部マニュアル、消防計画、安全衛生管理指針とも整合させたものとしている。なお自然災害発生時と対応が同様とされるものは、本書では記載せずに、病院ＢＣＰを参照することとする。

2.2　適用の範囲

病院ＩＴ－ＢＣＰは、当院の全職員、施設に適用する。
業務委託先の企業との連携については、協定締結・契約・委託業務内容を含めて検討する。

2.3　文書管理と開示範囲

(1). 病院ＩＴ－ＢＣＰは、ＢＣＰ委員会およびＢＣＰ事務局（病院施設企画課）が文書管理を行い、常に最新版が使用される状態を維持する。（病院ＢＣＰ　P107「６　病院ＢＣＰの維持・改善（業務継続マネジメント（ＢＣＭ)」参照）
(2). 病院ＩＴ－ＢＣＰは、当院の全構成員に開示し、周知する。ただし、個人情報の保護、戦略的対応の秘匿等の観点から、全構成員への開示が適当でない部分は、必要な構成員の範囲での開示とする。
(3). 当院の社会的責任として、必要に応じて病院ＩＴ－ＢＣＰの概要を公開する。
(4). 病院ＩＴ－ＢＣＰは、本部事務機構をはじめ、関係する大学内の他事業場に必要に応じて開示することがある。
(5). 行政機関等からの求めに応じて、病院ＩＴ－ＢＣＰの必要な部分について開示することができるものとする。病院ＩＴ－ＢＣＰの策定・修正の承認は、運営評議会で行い、病院長が承認責任者となる。

3　想定する危機事象

3.1　想定する危機事象

本病院ＩＴ－ＢＣＰは､主に､ランサムウェア被害や大規模なシステム障害が発生した状況を想定する。

対象とする医療情報システムは以下の通り。

(1). 電子カルテシステム
(2). 医事会計システム（レセプト）
(3). 医用画像システム
(4). 各種部門システム（検査、処方など）
(5). オーダリングシステム
(6). 研究や事業等で病院が用意するデータベースシステム類

また、本ＩＴ－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(病院ＢＣＰ)

(1). 診療情報・参照情報・指示情報・会計情報の確認・参照不能
(2). 診療情報・参照情報・指示情報・会計情報の入出力不能
(3). スタッフ間の連絡不能
(4). 情報機器・医療機器の操作不能・誤動作
(5). 個人情報の漏洩

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。

(1). 外部・内部からの不正アクセス等
(2). 標的型メール攻撃
(3). ウィルス感染
(4). マルウェア感染（ランサムウェアを含む）
(5). 分散型サービス妨害（ＤＤｏＳ攻撃）
(6). 上記の予兆と思われる現象

4　危機事象発生時の対応体制

4.1　当院災害対策本部（東北大学病院支部）

・　当院が設置する災害対策本部は、東北大学全体としては「東北大学病院支部」と位置づけされる。

4.1.1　災害対策本部の設置基準

(1)　災害発生時には、病院長が災害対策本部の設置を判断する。平日病院長不在時は、病院長代行（4.1.4 「災害対策本部長が不在等の場合の代行順位」参照）が判断する。
夜間休日などで病院長不在の場合は、メディカルＩＴセンター長が判断し、暫定災害対策本部を設置する。
（病院ＢＣＰ　4.1.1.2「災害対策本部の設置手順」フロー図（図１）参照）

(2)　本部事務機構に東北大学災害対策本部（以下「大学対策本部」という。）が設置され、当院に対して東北大学病院支部の設置の指示があった場合には、その指示に従い、災害対策本部を設置する（病院ＢＣＰ　4.1.2「災害対策本部(東北大学病院支部)組織図」（図３）参照)、病院長が必要と判断した場合（「災害対策マニュアル」参照)。

4.1.1.1　　自動設置基準

以下の場合には、病院長判断を待たずに本部構成員は災害対策本部を設置する。

＜自動設置基準＞

①　ランサムウェア被害が発生し、診療支援システムの全部または一部が動作を停止した場合（レベル４）
②　ランサムウェア被害が予兆される動作・現象が発見されたとき(レベル４)
③　予期せぬ大規模システム障害が発生し、３時間経過しても復旧のめどが立たない場合（レベル３）

（注）ランサムウェア被害とは：
ランサムウェアとは「ransom（身代金)」と「software（ソフトウェア)」からなる造語。感染させた端末やサーバ内のデータを暗号化などによって、利用できない状態にした上で、そのデータを利用できる状態に戻すことと引き換えに身代金（金銭）を要求するマルウェアのこと。情報流出の可能性もある。※https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/ransomware_threat.html

4.1.1.2　　災害対策本部の設置手順

災害対策本部の設置手順は、以下のフロー図（図 1）ならびに災害対策マニュアルに従う。

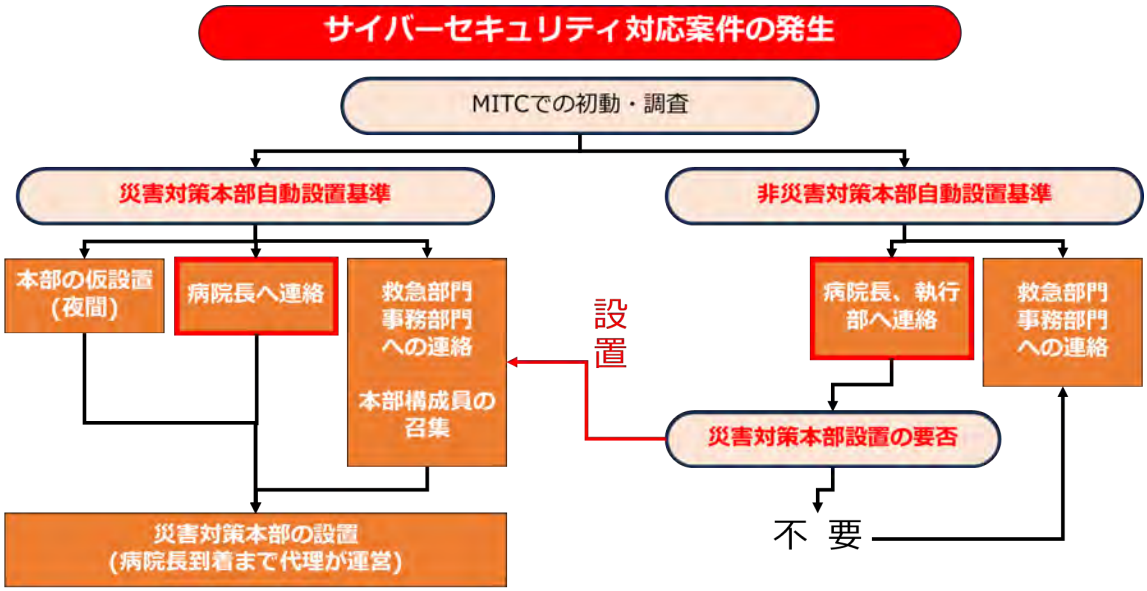

図 1　災害対策本部設置フロー図

・災害対策本部の設置後、災害対策本部長は下図（図２）に基づいて災害レベルを決定し、レベル３以上を含めて必要な場合はＢＣＰを発動するとともに、当院内の被災状況を遅滞なく大学対策本部に報告する。

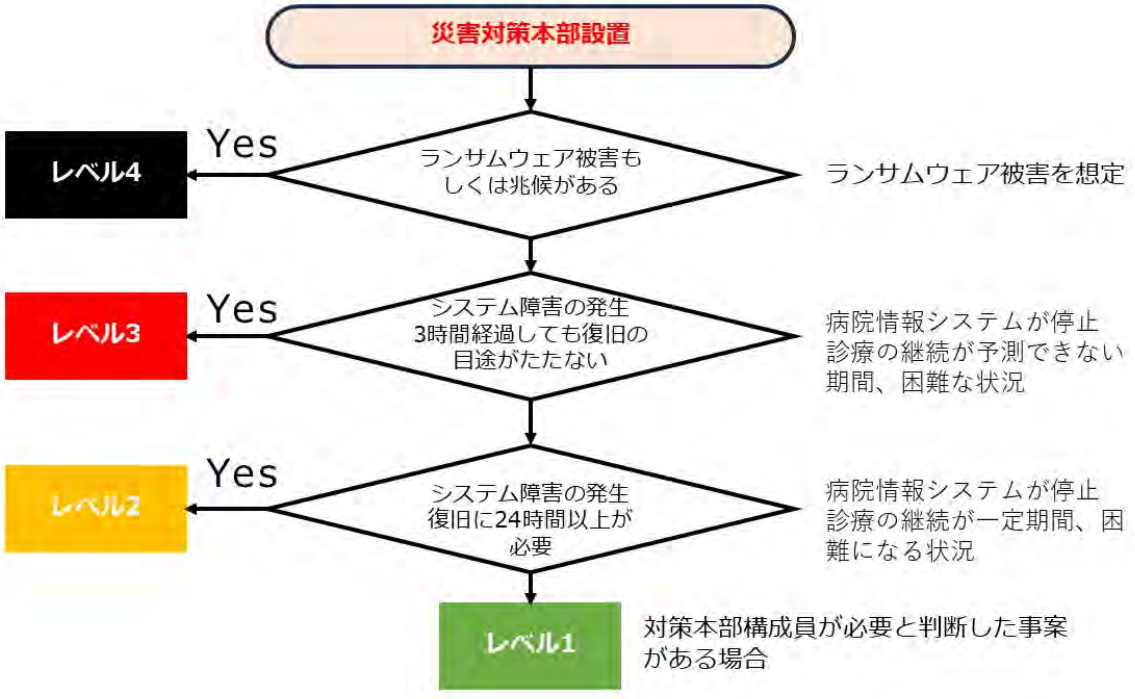

図 2　レベル判断フロー

4.1.2　災害対策本部（東北大学病院支部）組織図

当院の災害対策本部（東北大学病院支部）の組織体制は以下のとおりとする。なお組織図は自然災害と同様として、最新のものは病院ＢＣＰを参照するものとする。

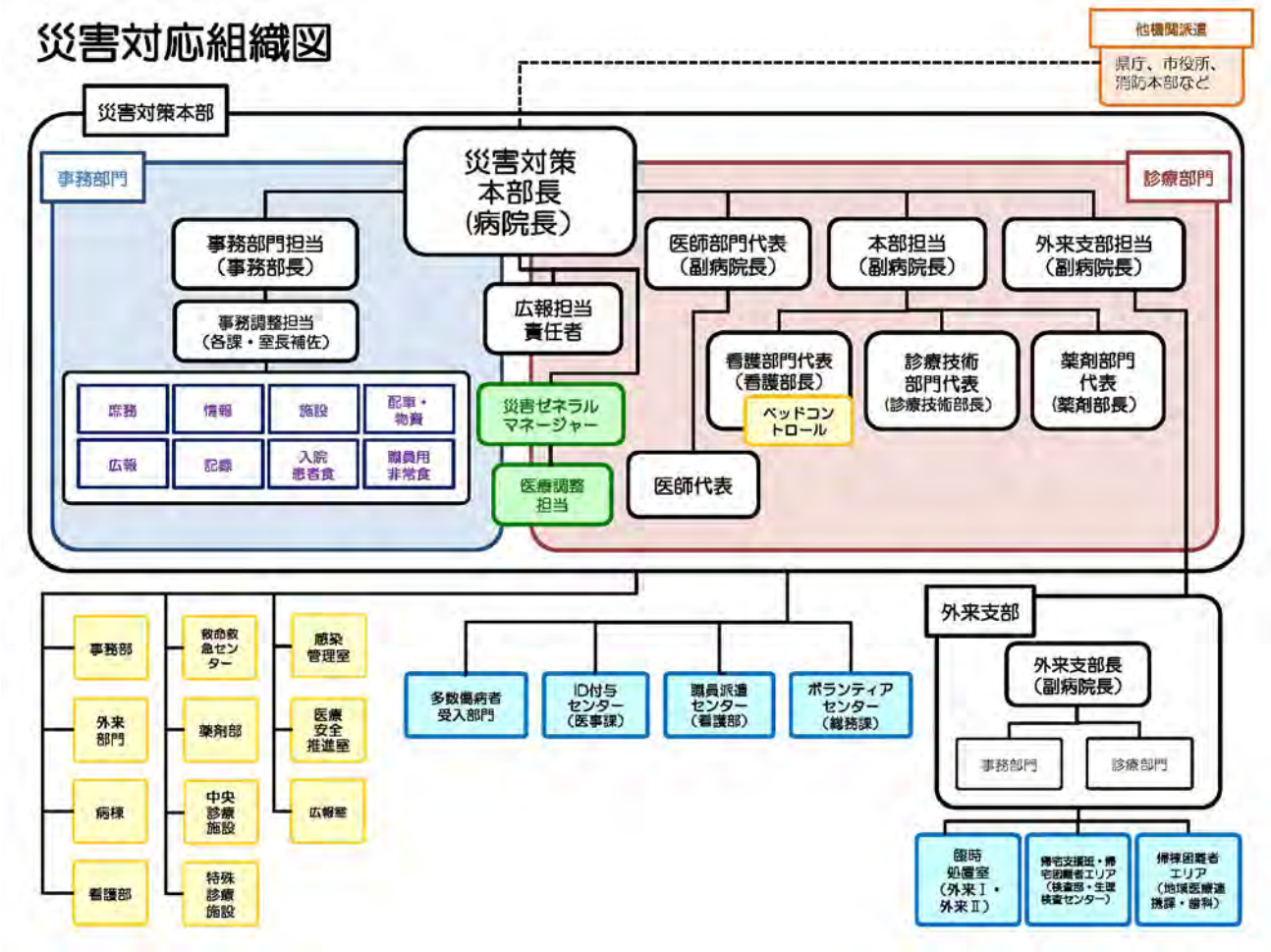

図３　災害対応組織図　「災害対策マニュアル」抜粋

なお、災害対応組織と連携するため、メディカルＩＴセンターは対策本部にリエゾンを派遣し対応する。また必要に応じてメディカル IT センター部長は対策本部にて状況説明を行う。

4.1.3　災害対策本部構成員と役割

表 4−1　本部構成員（「災害対策マニュアル」抜粋）

本　部　構　成　員

No	構成員		平日時間内に発災した場合		時間外に発災した場合	責任者	役割
			平日時間内	不在時			
1	災害対策本部長		病院長	各副病院長	①本部長代行救命センター診療責任医師 ②①から指名された者		本部の統括および指揮、構成員の任命、病院方針の決定、政府機関との調整等。
2	副本部長	本部担当	各副病院長				診療部門統括、病床管理統括、搬入患者割振りの指揮。
3		外来支部担当					外来部門の状況把握・本部内への共有、外来支部への情報提供・指示・調整、外来部門の復旧対応
4		外来支部長					外来部門の対応決定・指揮、外来新設部門設置の指示、帰宅希望者の帰宅誘導
5		医師部門代表					医師の統括、災害関連の情報収集・対応検討
6		広報担当責任者	災害対策本部長が指名した者（平日、時間外ともに） ※マスコミ対応、情報発信等に関する高度な専門性と経験を持っていること。				大学本部との連絡調整、マスコミ対応、報道、広報内容・手段の検討および指示、院内周知に係る統括
7		事務部門担当	事務部長	総務課長（不在時はその他の課長・室長）	①平日時間内と同じ ②本部事務部門担当者		本部事務調整担当の任命・統括、事務業務方針決定・統括、外部機関との調整、情報収集。
8	災害ゼネラルマネージャー		災害対応マネジメントセンター部門（災害対応調整部門・災害コーディネート部門）長		災害対策本部長が指名した者		本部内の事務・診療部門間の調整、医療調整担当統括、災害医療対応の監修。
9	医師代表		救命センター部長	救命センター副部長	①平日時間内と同じ ②①から指名された者		医師部門代表補佐、災害関連の情報収集、高度救命救急センター統括、被害状況確認。
			災害対策本部長が必要に応じ指名する内科医師、外科医師				医師部門代表補佐、医師の勤務調整、災害関連の情報収集。
10	薬剤部門代表		薬剤部長	薬剤部長が指名した副薬剤部長	①平日時間内と同じ ②①から指名された者		薬剤部統括・勤務調整、医薬品の在庫状況と流通の確認。
11	看護部門代表		看護部長	看護部長が指名した副看護部長	夜勤師長		看護部統括・職員の勤務調整、院内の空床確保。
12	診療技術部門代表		診療技術部長	診療技術部長が指名した部門長	①平日時間内と同じ ②①から指名された者		診療技術部統括・職員の勤務調整、各種装置の稼働状況確認、入院患者食の状況把握。
13	事務調整担当		事務部門担当副本部長が指名する 各課・室長または補佐、2名以上		①平日時間内と同じ ②本部事務部門担当者		事務部門担当の補佐、本部内外の事務職員の調整、定例会議事録の校閲、本部内外の情報整理。
14	庶務担当		事務調整担当が指名する　※原則総務課 事務職員、6名以上			総務係長	全館放送、定例会議の議事録作成、本部内諸業務（伝令・電話対応・クロノロ等）、各担当補助。
15	情報担当		事務調整担当が指名する　※原則医療情報室 事務職員、4名以上			運用管理係長	本部内の情報整理、被災地の情報収集、グループウエアによる情報配信。
16	施設担当		事務調整担当が指名する　※原則施設企画室 事務職員、2名以上			設備係長	院内インフラ情報の整理、各施設管理業者との連絡調整。
17	配車・物資担当	配車担当	事務調整担当が指名する　※原則経理課 事務職員、2名以上			契約第一係長	災害対応用車両・公用車の配車調整、道路・ガソリンスタンドの情報確認。
18		物資担当	事務調整担当が指名する　※原則経理課、施設企画室 事務職員、2名以上			契約第二係長	DMATおよび原子力災害医療派遣チーム出動に必要な資機材準備・搬出作業および作業人員確保。
19	広報担当		事務調整担当が指名する　※原則総務課または広報室 総務係広報担当者、広報室員１名以上			広報室副室長	副本部長（広報担当責任者）の補助、報道発表に係る準備・調整、SNS等による情報発信、報道機関からの問合せへの対応。
20	記録担当		事務調整担当が指名する　※原則広報室 広報室員１名以上			広報室副室長	本部内外の写真・映像撮影、副本部長（広報担当）の補助。
21	医療調整担当		災害対策本部長が指名する災害対策委員、DMAT隊員、3名以上			災害対策委員長	EMIS等を使用した情報収集・共有、他機関の派遣チームとの調整、他病院との搬送に関する調整。
22	食糧担当	入院患者食担当	栄養管理室長	栄養管理室長が指名した職員	①平日時間内と同じ ②①から指名された者	栄養管理室長	入院患者食提供業務統括、調理施設被害状況の把握、支援物資（入院患者用）受入の対応
23		職員用非常食担当	施設企画室長	施設企画室長が指名した職員	①平日時間内と同じ ②①から指名された者	施設企画室長	職員用非常食提供の準備、支援物資（職員用・外来患者用）受入の対応
24	災害対策本部長秘書		総合地域医療教育支援部秘書	事務職員	①平日時間内と同じ ②①から指名された者	総合地域医療教育支援部長	本部長の事務業務補佐（電話応対、物品調達、クロノロ、伝令等）

※災害対策本部に招集される構成員、その人数および役割は、災害対策本部長が災害の種類や規模等に応じて調整するため、本表の限りではない。

なお、上記の本部構成員は自然災害対応と同様であり、「災害対策マニュアル」に記載している。最新は災害対策マニュアルとする。また組織にはメディカルＩＴセンター長もしくは指名するものが加わり、対応状況を共有する。

4.1.4　本部構成員の招集基準及び方法

表 4−2　レベル別の召集方法

災害レベル	招集される 災害対策本部構成員	招集方法	
		(大規模な)システム障害の発生	ランサムウェア被害の発生
レベル４ ランサムウェア被害の発生	災害対策本部構成員 一覧全員	①　知りえた時、自主登院 ②　本部構成員ＭＬにて招集 ③　本部構成員専用問い合せ窓口を設置、本部構成員が問い合わせる	
レベル３ システムダウンを伴う被害の発生(３時間以内の復旧判断が困難)	災害対策本部構成員 一覧全員	①　知りえた時、自主登院 ②　本部構成員ＭＬにて招集 ③　本部構成員専用問い合せ窓口を設置、本部構成員が問い合わせる	
レベル２ システムダウンを伴わない被害の発生	災害対策本部構成員一覧より災害対策本部長が必要と認めたもの		該当本部構成員個人に通知
レベル１ IT インシデント(ウィルス感染等)の発生	災害対策本部構成員一覧より災害対策本部長が必要と認めたもの		該当本部構成員個人に通知

4.1.5　災害対策本部設置場所

【災害対策本部設置場所】
　東病棟 4 階；第 5 会議室

【代替場所】
　第 5 会議室がなんらかの事情により使用できない場合は、以下の順に代替となる災害対策本部を設置する。代替本部として使用できるよう、必要な資機材、電源、通信設備の設置を行う。

　①医学部 3 号館 7 階：共用会議室
　②仮管理棟 4 階：第 1 会議室

(大学病院配置図)

4.1.6　災害対策本部の活動

災害対策本部はシステムの被害、復旧計画に基づいて意思決定ならびに関連部署への指示を行う。

- ランサムウェア被害発生直後、本部は迅速に病院内の被害状況を把握
- 災害レベルの決定
- 診療の継続とその範囲(外来・入院・救急・新患受付)
- 災害復旧(システム復旧)を指示
- 個人情報流出被害の拡大防止を指示
- メディア対応(被害状況・経緯・個人情報の漏洩・復旧見込み)
- 身代金の対応
- 関係機関への報告(ＣＳＩＲＴ・厚労省・文科省・個人情報保護委員会・警察など)
- 関係医療機関との連携
- 院内関係者の情報統制

5. ランサムウェアもしくは大規模システム障害対応

ＩＴ対応として、以降を加える。なお自然災害対応の場合と異なる場合は、本記載事項が優先される。

5.1　役割

ＩＴ対応として下記のものは復旧作業において次の役割を担う。

表 5−1：担当者の役割

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	ＭＩＴＣ部長	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	事務部長	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	医療情報管理課	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。
主な委託先	＊＊＊＊＊	電子カルテサーバを中心とする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・対策調整を行う。
	＊＊＊＊＊	ネットワークシステムおよび仮想サーバシステムを中心とする病院ネットワークの運用保守及び緊急時の状況に関する情報提供・対策調整を行う。

5.2　対象システム・ベンター

ＩＴ－ＢＣＰとして対象とする主な情報システム・機器として下記を挙げる。

表 5−2　ベンダーならびに情報システム一覧

【ベンダー一覧】

No.	部門システム名	ベンダー名
1	医事会計システム　＊＊＊＊＊	＊＊＊＊＊
2	＊＊＊＊　自動再来受付システム	メーカー名：＊＊＊＊＊ 契約先：＊＊＊＊＊
3	自動現金入金機	＊＊＊＊＊
4	検体検査システム・細菌検査システム	＊＊＊＊＊
5	採血管準備システム	＊＊＊＊＊
6	輸血管理システム　＊＊＊＊＊	＊＊＊＊＊
7	病理・細胞診検査業務緯線システム　＊＊＊＊＊	＊＊＊＊＊
8	栄養給食管理システム　＊＊＊＊＊	＊＊＊＊＊

9	院内物流システム　＊＊＊＊＊	メーカー名：＊＊＊＊＊ 契約先：＊＊＊＊＊
10	薬剤業務支援システム　＊＊＊＊＊	＊＊＊＊＊
11	病棟業務支援システム　＊＊＊＊＊	＊＊＊＊＊
12	麻薬管理システム	＊＊＊＊＊
13	調剤鑑査支援システム	＊＊＊＊＊
14	全自動錠剤散薬分包機	＊＊＊＊＊
15	抗がん剤調製支援システム	＊＊＊＊＊
16	ＤＷＨ	＊＊＊＊＊
17	経営支援システム（財務連携）	＊＊＊＊＊
18	物品一括調達システム	＊＊＊＊＊
19	総合滅菌管理システム	＊＊＊＊＊
20	看護勤務管理システム　＊＊＊＊＊	＊＊＊＊＊
21	ナースコールシステム（ICU/HCU/救命センター）	＊＊＊＊＊
22	ナースコールシステム（一般病棟）	＊＊＊＊＊
23	モバイルカルテ　＊＊＊＊＊	＊＊＊＊＊
24	患者待合案内表示システム	メーカー名：＊＊＊＊＊ 契約先：＊＊＊＊＊
25	統合画像保存・管理システム	＊＊＊＊＊
26	放射線部門業務システム　＊＊＊＊＊	＊＊＊＊＊
27	放射線治療　＊＊＊＊＊	＊＊＊＊＊
28	3D 画像解析システム　＊＊＊＊＊	＊＊＊＊＊
29	3D 画像解析システム　＊＊＊＊＊	＊＊＊＊＊
30	3D 画像解析システム　＊＊＊＊＊	＊＊＊＊＊
31	3D 画像解析システム　＊＊＊＊＊	＊＊＊＊＊
32	放射線画像診断システム	＊＊＊＊＊
33	生理検査システム　＊＊＊＊＊	＊＊＊＊＊
34	内視鏡部門管理システム　＊＊＊＊＊	＊＊＊＊＊
35	手術麻酔管理システム	＊＊＊＊＊
36	手術映像画像統括システム　＊＊＊＊＊	＊＊＊＊＊
37	集中治療支援システム	＊＊＊＊＊
38	化学療法支援システム	＊＊＊＊＊
39	NICU/GCU 部門システム　＊＊＊＊＊	＊＊＊＊＊
40	救命救急システム　＊＊＊＊＊	＊＊＊＊＊
41	周産期カルテシステム	＊＊＊＊＊
42	治験管理システム　＊＊＊＊＊	＊＊＊＊＊
43	眼科専用電子カルテシステム	＊＊＊＊＊
44	統合画像参照システム ＊＊＊＊＊	＊＊＊＊＊
45	地域医療連携システム　＊＊＊＊＊	＊＊＊＊＊
46	地域連携部門システム	＊＊＊＊＊

47	透析部門システム	＊＊＊＊＊
48	リハビリテーション支援システム　＊＊＊＊＊	＊＊＊＊＊
49	てんかんシステム	＊＊＊＊＊
50	歯科カルテシステム　＊＊＊＊＊	＊＊＊＊＊
51	診断書作成支援システム　＊＊＊＊＊	＊＊＊＊＊
52	文書管理システム　＊＊＊＊＊	＊＊＊＊＊
53	自動尿測定システム	＊＊＊＊＊
54	感染管理支援システム	＊＊＊＊＊
55	ＭＥ機器管理システム	＊＊＊＊＊
56	歯科技工システム	＊＊＊＊＊
57	貴金属・人工歯請求	＊＊＊＊＊
58	循環器動画ネットワークシステム	＊＊＊＊＊
59	血液ガス管理支援システム　＊＊＊＊＊	＊＊＊＊＊
60	耳鼻咽喉聴力検査システム	＊＊＊＊＊
61	診療案内表示システム	メーカー名：＊＊＊＊＊ 契約先：＊＊＊＊＊
62	インシデントレポートシステム	＊＊＊＊＊
63	電子カルテシステム(ハード/インフラ)	メーカー名：＊＊＊＊＊ 契約先：＊＊＊＊＊
64	ネットワークシステム・仮想サーバシステム	運用保守及び緊急時の状況に関する情報提供・対策調整
65	材料管理システム	＊＊＊＊＊

情報機器台帳は更新等があることから、ＭＩＴＣが管理する「９次システム端末管理台帳」を参照のこと

5.3　システムの代替え手段

システム停止時においては、下記の代替え手段で対応する。詳細は各部門の対応となるが、原則的には自然災害発生時と同様の対応となる。

表 5−3：業務内容に対する代替手段

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	紙運用。未収扱いを検討
入退院受付	電子カルテシステム	新規入院停止。退院処理は紙運用
救急受付	電子カルテシステム	原則停止。やむを得ない場合に限り紙運用
新規外来	電子カルテシステム 再来受付機	原則停止

5.4　システム関係者での連絡体制

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。

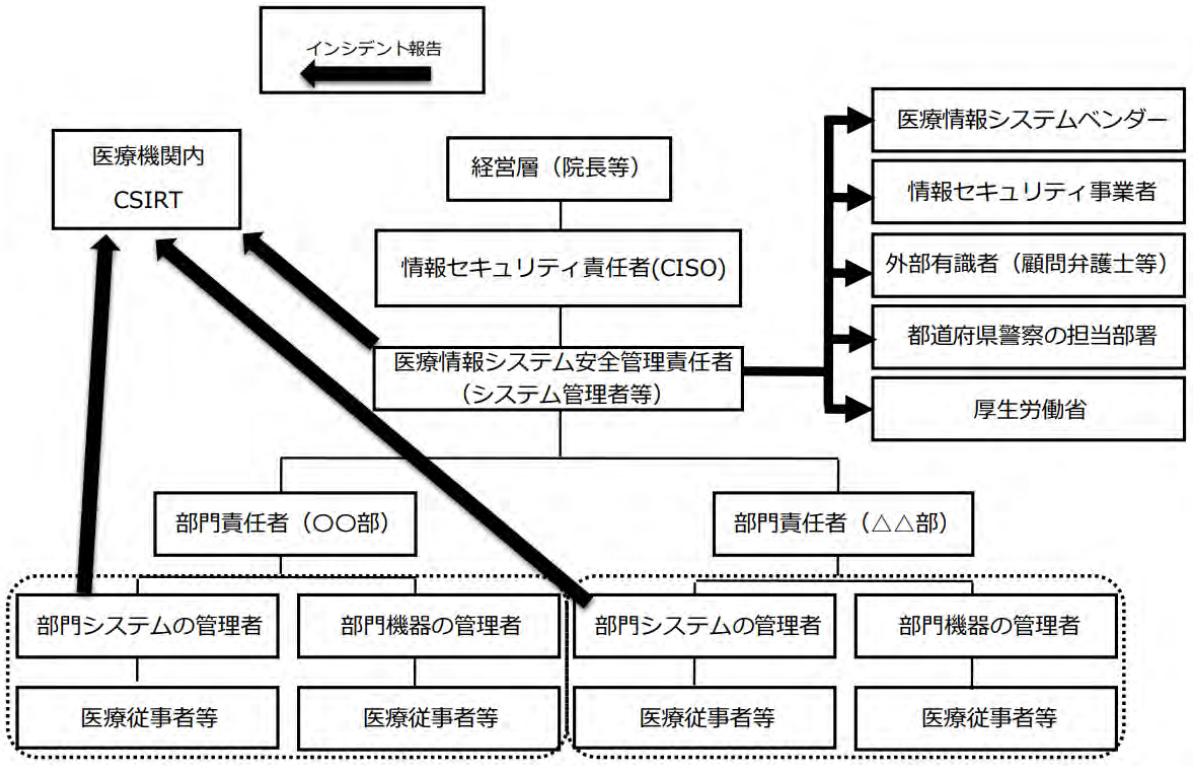

図 5-4：連絡体制図

表：5－4　外部関係機関の連絡先一覧

外部関係機関	連絡先
厚生労働省＊＊＊＊＊ ＊＊＊＊＊	＊＊＊＊＊ ＊＊＊＊＊
文部科学省＊＊＊＊＊ ＊＊＊＊＊	＊＊＊＊＊ ＊＊＊＊＊
宮城県＊＊＊＊＊ ＊＊＊＊＊	＊＊＊＊＊
仙台市　＊＊＊＊＊	病院ＢＣＰを参照
消防(救急関係)	病院ＢＣＰを参照
宮城県医師会	病院ＢＣＰを参照
仙台市医師会	病院ＢＣＰを参照
ＭＭＷＩＮ関係	病院ＢＣＰを参照
個人情報保護委員会	病院ＢＣＰを参照
メディア関係	病院ＢＣＰを参照
弁護士関係	病院ＢＣＰを参照

大学本部	病院ＢＣＰを参照
ＣＳＩＲＴ	＊＊＊＊＊ ＊＊＊＊＊
ＭＭＷＩＮ	ＭＩＴＣ連絡網を参照

5.5　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、平時ならびに被害時に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 5−5：主な事業者等の連絡先

システム	担当	連絡先
電子カルテ	＊＊＊＊＊	＊＊＊＊＊
保守委託先	＊＊＊＊＊ ＊＊＊＊＊	＊＊＊＊＊

上記以外は表 5−2 ベンダー一覧を参照のこと。

5.6　バックアップ体制と復旧

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 5−6：バックアップの作成と復旧方法

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から復元する
	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、磁気テープなどからシステムファイルとデータベースを復元する
ＨＩＳ部門 仮想※1	１日	ＯＳにマウントされた「＊ドライブ（バックアップ管理サーバ）」に業務データのバックアップを取得 「＊ドライブ（バックアップ管理サーバ）」に取得したデータはテープに２次バックアップとして取得	ＯＳにマウントされた「＊ドライブ（バックアップ管理サーバ）」より業務データのバックアップからデータの復元を行う

ＭＩＴＣ部門仮想※2	１日	冗長化された筐体で、仮想マシンが稼働しているストレージ上での日次スナップショットの取得およびもう一方の筐体へのデータコピー	仮想マシンをバックアップされているスナップショットから復旧する。復旧元のデータは仮想マシンが稼働するストレージ上の日次スナップショットまたはもう一方の筐体のスナップショットからデータ復旧する

※1 モバイルソリューション、自科検査、インシデントレポート、リハビリ、物流、文書管理、統合画像、病理、栄養、生理検査、放射線、看護勤務、治験、歯科カルテ、臨床研究

※2 重症・手術、心電図、救急、産科、調剤支援、眼科、医用画像、材料、診断書、ＤＰＣ、ＭＥ機器、ナースコール、血液ガス分析、患者案内

6. 被害対応

6.1 初動

サイバーインシデント発生後は、以下のとおり対応する

6.1.1 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。

① ネットワーク機器やケーブル等の調査
② 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
③ 情報漏えいの有無に関する調査
④ メンテナンスやデータ移行等の作業に関する調査

6.1.2 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。

6.1.3 病院執行部への報告

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病院執行部に対して、現在の被害状況を報告するとともに、状況に応じて災害対策本部立ち上げや、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、病院執行部もしくは対策本部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、速やかに図５．４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。

6.2 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。

6.2.1　医療情報システムのフォールバック(縮退運転)の判断

病院執行部は医療情報システム安全管理責任者からの提案を受け、自動設置基準を満たさない場合は、災害対策本部の立ち上げおよび災害レベルの宣言について判断し、同時に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あるいは診療制限においては、紙カルテの運用等、自然災害時を想定した本体ＢＣＰ（もしくはシステム停止時マニュアル等）に則り運用する。

6.3　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、調査状況は随時災害対策本部および病院執行部に報告する。

6.3.1　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、災害対策本部および病院執行部は復旧対応方針（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、表 5−4 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。

6.4　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。

6.4.1　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、災害対策本部および病院執行部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。システムの復旧程度に応じて、診療制限解除の方針と計画について意思決定し、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。災害対策本部および病院執行部は、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。

6.4.2　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、災害対策本部および病院執行部に報告する。病院執行部は対策本部の判断等を参考にして、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。

7.　事後対応

7.1　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、災害対策本部および病院執行部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。

7.2　再発防止

7.2.1　再発防止策検討・策定

7.1 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、病院執行部および運営会議に提案する。病院執行部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。病院執行部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。

7.2.2　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。

7.2.3 情報公開

病院執行部は、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。

以上

関連資料リスト

1. 東北大学病院災害対策内規
2. 東北大学病院災害対策マニュアル【R4.11】
3. 東北大学病院災害対策本部マニュアル【R4.11】
4. 東北大学病院災害対策マニュアル 外来部門【R4.11】
5. 東北大学病院消防計画
6. 安全衛生管理指針
7. 東北大学病院ＢＣＰ委員会内規

＜編集＞

メディカルＩＴセンター

医療情報管理課

ＢＣＰ委員会

委員長　　副委員長

委員

ＢＣＰ事務局


TUH
東北大学病院