第８節　医療情報システムの安全管理

１．はじめに

近年、医療機関を狙ったランサムウェア（データの暗号化やロックなどを行って使用できない状態にし、それを元に戻すかわりに金銭を要求する悪意のあるウイルス）による被害が病院・診療所を問わず広がっている。また、物理的盗難や不適切な持ち出し、ＵＳＢメモリの紛失、設定ミスによるメール誤送信などの事故も発生している。

高度化・巧妙化するサイバー攻撃によって診療行為の停止を余儀なくされる事態や医療情報の漏洩等が生じれば、患者、地域・社会に大きな損害を与え、医療機関の運営・経営にも多大な影響をもたらす。こうしたことから医療法施行規則に第 14 条第２項「病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティを確保するために必要な措置を講じなければならない」が新設され(2023 年４月１日施行)、2023 年３月 10 日発出の産情発 0310 第２号通知（厚生労働省大臣官房医薬産業振興・医療情報審議官）では下記が示された。

① 「必要な措置」として医療機関は、最新の「医療情報システムの安全管理に関するガイドライン」(以下「安全管理ガイドライン」という）を参照の上、サイバー攻撃に対する対策を含めセキュリティ対策全般について適切な対応を行う。

② 厚労省は、安全管理ガイドラインに記載されている内容のうち、優先的に取り組むべき事項について「チェックリスト」を作成し、各医療機関で確認できる仕組みを講じる。チェックリストは、下記３の⑵**（３頁）**を参照いただきたい。

サイバーセキュリティの確保は「医療情報システム」を導入・運用している医療機関に義務付けられたものであるが、ガイドラインでは「医療情報システム」を「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・取得するようなコンピュータや携帯端末も範疇として想定している。また、患者情報が通信される院内・院外ネットワークも含まれる」としている。インターネットと接続した監視カメラも含まれ、多くの医療機関が該当すると想定される。

本節では、下記２～４で医療情報システムの安全管理の概要をお示しするとともに、医療機関が効率的にサイバーセキュリティに取り組むことができるよう、**５頁**以降に「情報セキュリティ指針の一例」をまとめた。

本節の作成にあたっては「医療 ISAC」の深津博代表理事に監修をいただいた。深津博代表理事には、専門用語の使い方や考え方など、細かな箇所まで確認いただいた。この場をお借りして感謝申し上げる。

医療 ISAC は、医療情報システムの安全管理に関わるセミナー・ワークショップの開催や調査、情報提供、小規模医療機関向けの安価なセキュリティソリューションの提供を行っている。

医療 ISAC の活動については下記を参照いただきたい。

医療 ISAC　https://m-isac.jp/

２．医療情報システムの安全管理に関するガイドライン

⑴　2023 年５月に策定された「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）は下記により、構成されている。

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

①　「経営管理編」（経営層＝「医療情報システム安全管理責任者」向け） ②　「企画管理編」（医療情報システムの安全管理を行うために必要な運用管理の管理責任者＝「（医療情報システム）企画管理者」向け） ③　「システム運用編」（システムの運用担当者向け） ④　「概説編」（安全管理責任者、企画管理者、システム運用担当者） ⑤　「Ｑ＆Ａ」（安全管理責任者、企画管理者、システム運用担当者） ⑥　「用語集」（安全管理責任者、企画管理者、システム運用担当者）

⑵　ガイドラインでは、主に下記の実施を求めている。なお、診療録管理体制加算、データ提出加算、医師事務作業補助体制加算をはじめ、医療情報管理を要する診療報酬においては「医療情報システムの安全管理に関するガイドライン」を遵守することが施設基準に定められているので、留意されたい。

①　組織としての安全管理等に関する基本的な方針や計画の策定 ※　情報セキュリティ方針や事業継続計画（BCP：Business Continuity Plan）の整備 ②　安全管理等に必要な組織・体制の整備 ③　組織における安全管理のルールとなる規程類の整備 ④　上記に基づく運用 ⑤　外部の事業者に業務を委託する場合は、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」、その他の法令等に掲げる基準を満たした医療情報システム・サービス事業者（Ｐマーク（プライバシーマーク）又は ISMS（ISO27001）認証を取得している）を選定し、当該事業者との責任分界、役割分担、協働体制などを明確にし、遵守状況を確認する。

なお、厚生労働省は診療所向けに「小規模医療機関等向けガイダンス」を発表（下記 URL 参照）し、①診療所は、院長（又は事務長）が医療情報システムの安全管理に関する企画管理を行うことでも良い、②組織図を作成する意義は低い、等としているが、「情報セキュリティ方針」の策定やインシデントへの対策と対応などの取り組みは必要である。

https://www.mhlw.go.jp/content/10808000/001102587.pdf

３．立入検査での点検項目と、優先的に取り組むべき厚生労働省チェックリスト

⑴　2023 年６月改定の「医療法第 25 条第１項の規定に基づく立入検査要綱」では、「2-19 サイバーセキュリティの確保」のチェック項目として下記を新たに追加した。

①　必要な措置は「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」参照 ②　ガイドライン第 6.0 版のうち、医療機関において優先的に取り組むべき事項として、「『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』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５年６月９日医政参発 0609 第１号）で示す、「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」に必要な事項が記入されていることを確認する。 チェックリスト　https://www.mhlw.go.jp/content/10808000/001125392.pdf マニュアル　https://www.mhlw.go.jp/content/10808000/001105752.pdf ※チェックリストは⑵を参照いただきたい。 ③　チェックリストにおいて医療機関に求める項目のうち、インシデント発生時の連絡体制図については、連絡体制図の提示を求めることにより、その有無を確認する。体制図に記載する連絡先は、下記が想定される。

ア　外部委託業者
イ　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
TEL:　03-6812-7837　MAIL:　igishitsu@mhlw.go.jp
ウ　個人情報保護委員会（個人情報保護法第 26 条に基づく場合）
https://www.ppc.go.jp/personalinfo/legal/leakAction/
エ　都道府県警のサイバー犯罪窓口
※都道府県警察のサイバー犯罪相談窓口は、下記参照（下記ページで不明な場合は都道府県警のお問合せください）　https://www.npa.go.jp/bureau/cyber/soudan.html
オ　独立行政法人情報処理推進機構（事後報告）
・コンピュータ不正アクセス届出制度
https://www.ipa.go.jp/security/todokede/crack-virus/about.html
・コンピュータウイルス届出制度
https://www.ipa.go.jp/security/todokede/crack-virus/about.html
・ソフトウェア等の脆弱性関連情報に関する届出制度
https://www.ipa.go.jp/security/vuln/report/index.html

⑵　医療機関用の「チェック項目」は下記の通りで、医療法第 25 条第 1 項に基づく立入検査において点検される。事業所確認用チェック項目は 24 頁を参照いただきたい。

【2023 年度中に整備が必要な項目】

１．体制構築
⑴　医療情報システム安全管理責任者を設置している。
２．医療情報システムの管理・運用
≪医療情報システム全般≫
⑴　サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。
⑵　リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。（事業者と契約していない場合は不要）
⑶　事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。（事業者と契約していない場合は不要）
≪サーバ≫
⑷　利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。
⑸　退職者や使用していないアカウント等、不要なアカウントを削除している。
⑹　アクセスログを管理している。
≪ネットワーク機器≫
⑺　セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。
⑻　接続元制限を実施している。
３．インシデント発生に備えた対応
⑴　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）への連絡体制図がある。

【2024 年度中に整備が必要な項目】

２．医療情報システムの管理・運用
≪サーバ≫
⑺　セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。
⑼　バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。
≪端末 PC≫
⑷　利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。
⑸　退職者や使用していないアカウント等、不要なアカウントを削除している。
⑺　セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。
⑼　バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。
３．インシデント発生に備えた対応
⑵　インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。

⑶　サイバー攻撃を想定した事業継続計画（BCP）を策定、又は令和６年度中に策定予定である。

⑶「令和４年度の医療法第 25 条第１項の規定に基づく立入検査の実施について」（通知）では、「個人情報保護法第 26 条第１項及び第２項の規定に基づき、個人情報取扱事業者は、サイバー攻撃その他の要因により、個人データの漏えい等が発生し、個人の権利利益を害する恐れがある場合には個人情報保護委員会への報告及び本人への通知を行うことが義務づけられたことに留意すること」とされている。

４．ガイドラインの遵守等が要件とされている診療報酬

診療報酬の施設基準や算定要件等で「医療情報システムの安全管理に関するガイドライン」の遵守を求めている点数がある。これらの点数を届出・算定している場合は、適時調査や個別指導でも点検が行われる可能性があるので、留意されたい。

⑴　点数又は加算そのものの要件とであるもの
- A207 診療録管理体制加算（許可病床数 400 床以上の病院は、ガイドラインの遵守に加えて、専任の医療情報システム安全管理責任者を配置し、当該責任者は、職員を対象として、少なくとも年１回程度、定期的に必要な情報セキュリティに関する研修を行っている）
- A207-2 医師事務作業補助体制加算
- A245 データ提出加算
- B001・9 外来栄養食事指導料の注４・注６
- B009 診療情報提供料（Ⅰ）の検査・画像情報提供加算
- B009-2 電子的診療情報評価料

⑵　電子的方法により個々の患者の診療情報等を他の医療機関、保険薬局等に提供する場合
- B009 診療情報提供料（Ⅰ）
- C005-2 在宅患者訪問点滴注射管理指導料

⑶　電子カルテなどを含む医療情報システムと共通のネットワーク上の端末においてカンファレンスを実施する場合又は個人情報を画面上で取り扱う場合
- A000 初診料及び A001 再診料の外来感染対策向上加算
- A234-2 感染対策向上加算
- A246 入退院支援加算１
- B004 退院時共同指導料１の注１
- B005 退院時共同指導料２の注１、注３
- B005-10 ハイリスク妊産婦連携指導料２
- B015 精神科退院時共同指導料
- C011 在宅患者緊急時等カンファレンス料
- C013 在宅患者訪問褥瘡管理指導料
- I016 精神科在宅患者支援管理料

⑷　電子的方法によって、個々の患者の診療に関する情報等を送受信する場合
- E 画像診断管理加算
- E 遠隔画像診断
- E 歯科画像診断管理加算

⑸　患者の個人情報を含む医療情報の送受信を行う場合
- A301-3 脳卒中ケアユニット入院医療管理料

⑹　ガイドラインに準拠した体制であることが望ましいとされている施設基準
- 外来データ提出加算、在宅データ提出加算、リハビリテーションデータ提出加算

⑺　電子カルテシステム（オーダリングシステムを含む。）について、「医療情報システムの安全管理に関するガイドライン」等に準拠した体制であり、当該体制について、規程を文書で整備していることが求められる施設基準
- A207-2 医師事務作業補助体制加算

情報セキュリティ指針の一例

【編注】　医療情報の取扱い方法や使用機器は医院ごとに大きく異なるため、例示を参考に各医療機関の実情に応じ、委託先の医療情報システム提供事業者に協力を得て、整備をお願いしたい。

第１条　医療情報システムの安全管理に関する基本的な考え方

高度化・巧妙化するサイバー攻撃によって診療行為の停止を余儀なくされる事態や医療情報の漏洩等が生じれば、患者、地域・社会に大きな損害を与え、医療機関の運営・経営にも多大な影響を及ぼす。

この方針は、当院における医療情報の安全管理の推進を図るため、下記に掲げる事項を遵守し、安全かつ適切に医療情報の管理を行う体制を確立するために必要な事項を定めるものである。

① 医療情報システムの安全管理に関係する法令等を遵守する。

② 医療機関等で業務に従事する職員や関係するシステム関連事業者等に対して、医療情報システムに関係する法令等を遵守させる。

なお、医療機関は委託先の医療情報システム提供事業者がＰマーク（プライバシーマーク）又は ISMS（ISO27001）認証を取得していることを確認する必要がある。また経済産業省は、医療機関等と契約する医療情報システム提供事業者を対象に、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第 1.1 版」を作成しており、事業者に対してはＰマーク又はＩＳＭＳの取得とともにガイドラインに沿った対応の実施を求めている。

第２条　本指針の対象

① 本指針は、当院における医療情報システムの導入、運用、利用、保守及び廃棄に関わるすべての者を対象とする。

② 本指針で対象とする医療情報は、医療に関する患者情報（個人を識別できる情報）を含む情報を言う。

③ 本指針が対象とする医療情報システムは、医療情報を保存するシステムだけではなく、医療情報を扱う情報システム全般をいう。ただし、医療情報を含まない会計・経理システム等（患者への費用請求に関する情報しか取り扱わないものに限る）は、本指針における医療情報システムには含まない。

④ 本指針の対象者及び本院の全ての職員は、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」（下記 URL）を十分理解する。

https://www.mhlw.go.jp/content/001120905.pdf

⑤ 医療 IoT 等、医療機器／医療情報システムのどちらかよく分からない対象には、厚生労働省・医機連による「医療機関における医療機器のサイバーセキュリティ確保のための手順書第２版」に準拠した対応を業者に求める。

第３条　医療情報システムの安全管理体制の構築

【編注】診療所においては、「院長（又は事務長）が医療情報システムの安全管理に関する企画管理を行う」旨の方針でもよい。

⑴　院長など経営層は厚生労働省ガイドライン「経営管理編」を読み、内容を把握する。なお、医療情報安全管理を直接実行するために**「医療情報システム安全管理責任者」を設置（【編注】安全管理責任者の設置は、令和５年度中に実施）**する。

⑵　○○○○を「(医療情報システム) 安全管理責任者」として配置する。

①　「(医療情報システム) 安全管理責任者」は、厚生労働省ガイドライン「企画管理編」を読み、内容を把握する。

②　「(医療情報システム) 安全管理責任者」は、下記の学習の計画立案に責任を負う。

a . 全職員を対象に年２回程度実施が求められている「医療安全管理のための職員研修」の研修項目の一つに「医療情報システムの安全管理の重要性と基本的な取り組み」を含める。

b . 医療情報システムの操作に関わる各部において、新規採用時及び年１回程度、操作のマニュアル及びインシデント対策に関する学習を行う。

【編注】医療安全管理委員会を設置している医療機関（病院・有床診療所は設置が義務付け）は、「(医療情報システム) 安全管理責任者」を医療安全管理委員とすることが望ましい。一般社団法人ソフトウェア協会が厚生労働省委託事業の一環として医療情報セキュリティ研修を実施しているので、これらも参考にする。（下記 URL 参照）

https://mhlw-training.saj.or.jp/info-20230511/

⑶　医療情報システムの実装・運用の実務担当者は、厚生労働省ガイドライン「システム運用」編を読み、内容を把握する。

第４条　セキュリティ対策の構築

【編注】第４条は、業者と相談（又は委託）して実施する。

⑴　医療情報システムおよび IoT 機器（インターネット利用機器）の利用対策

①　ウイルス感染などのインシデントが発生した場合、侵入経路や影響範囲などを特定して速やかに対応ができるよう、医療情報システムに関する全体構成図（ネットワーク構成図／システム構成図）を作成、年１回点検・確認し、最新状態を維持する。

②　インターネット利用機器については、製造販売業者から提供を受けたサイバーセキュリティ情報を基にリスク分析を行い、取り扱いの注意点について周知・徹底する。また、医院としても定期的にサイバーセキュリティ情報をインターネットで把握し、対策を行う。

【編注】例えば月の初日をサイバーセキュリティチェックの日として取り組むことなどが考えられる。

③　医療情報システムや IoT 機器（インターネット利用機器）は、製品出荷後にファームウェア(内蔵ソフトソフト)等に関する脆弱性が発見されることがあることから、

セキュリティ上重要なアップデートを必要なタイミングで適切に実施又はアップデートが困難な場合に代替措置を講じる。アップデートの必要性の発生情報の取得、修正プログラムの入手方法、修正プログラムの適用方法（いつ誰がどのような手段で適用するか？）等について、具体的に検討して、マニュアル等に明記し、それに沿った運用を行う。

④ 使用が終了又は使用を停止したシステムや IoT 機器（インターネット利用機器）はネットワークから遮断する。

⑤ インターネットと院内ネットワークの間に、ファイアウォール（不正アクセスを防ぐソフトや機器）や UTM（複数のセキュリティ機能を集約した製品）を設置設定することが望ましい。

⑥ システムへのアクセス制御として、特定のユーザのみのアクセスを許す場合は接続元の IP をホワイトリスト化し、アクセス制限を実施する。

⑦ ログイン試行回数に制限を設け、設定回数以上に連続して失敗した場合は一定時間アクセスを禁止する等のロックアウト機能を設定することが望ましい。

⑧ 医療従事者のシステムへのログインパスワードは 10 桁以上（13 桁以上が望ましい）とし、定期的な変更は要請しない

⑨ 医療従事者等の利用者の ID/パスワードは利用者毎にユニークなものとし、共通ＩＤやパスワードは設定しない

⑩ 退職者の ID/パスワードは速やかに削除する

⑪ アンチウイルスソフトのアップデートについても、アップデータの入手方法、適用方法（いつ誰がどのような手段で適用するか？）等について、具体的に検討して、マニュアル等に明記し、それに沿った運用を行う。

⑫ 施設毎のポリシーに応じて論理的・物理的に構成分割されたネットワークを整備し、新規システムの追加導入時等に、ポリシーの変更やそれに伴うリスクの評価を行い、必要なセキュリティ対策を実施する。

⑬ VPN（Virtual Private Network＝仮想専用線）を利用する場合は、その VPN がインターネット VPN（SSL-VPN、IP-SEC-VPN)、専用線 VPN（IP-VPN）ないし、広域イーサネットのいずれに該当するかを確認し、それぞれの方式に応じたリスクの評価とセキュリティ対策を実施する。

⑭ アンチウイルスソフトを導入し、定義ファイルを常に最新の状態に保つ。

⑮ 不正アクセス対策として二段階認証等を導入する。

⑯ セキュリティ対策を十分に行うことが難しいウェアラブル端末（手首や腕、頭などに装着するコンピュータデバイス）や在宅設置の IoT 機器（インターネット利用機器）を患者等に貸し出す際は、事前に、情報セキュリティ上のリスクと、患者等が留意すべきことについて患者等へ説明し、同意を得る。また、機器に異常や不都合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供する。

⑰ 「非常時のユーザアカウントや特権アカウントの利用方法や利用できる機能」の管理手順は次の通り。

ア. 正常なユーザ認証が不可能な場合に備えて非常時用のユーザアカウントを用意する。

イ. 非常時用のユーザアカウントは、通常時は使用しないことを周知・徹底する。

ウ.　非常時用のユーザアカウントについて、使った痕跡が残る運用（ブレークグラス）とする。

エ. 非常時用ユーザアカウントを使用した場合、正常復帰後は継続使用ができないように変更する。

⑱　重要なファイルは適宜バックアップ(データをコピーし､別の記録装置に保存する)をとり、不正ソフトウェアの混入による影響が波及しない手段で管理する。

⑲　未知のウイルス等による攻撃等への対策として、ふるまい検知機能等を有する EDR（Endpoint Detection & Response）等の対策を導入することが望ましい。

⑳　自施設の外部攻撃対象領域(EAS：External Attack Surface)の調査把握と、それに基づく脆弱性対策等の対策を実施することが好ましい。(下記の経済産業省のガイダンス参照)

「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織の IT 資産を発見し管理する～」を取りまとめました　(METI/経済産業省)

https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

⑵　2027 年度時点で稼働していることが想定される医療情報システムを、今後、新規導入又は更新する場合は、二要素認証（暗証番号、所有、生体の３要素中、２つで認証する）を採用するシステムの導入、又はこれに相当する対応を行う。

⑶　無線 LAN（Wi-Fi）の利用制限（【編注】⑶は、令和５年度中に整備）

①　業務用無線 LAN（Wi-Fi）について

ア. 適切な利用者以外に業務用無線 LAN を利用されないようにする。

イ. 未登録端末を接続させない仕組みなど不正アクセス対策を実施する。

ウ. 不正な情報取得防止のため、WPA2-AES、WPA2-TKIP 等により通信を暗号化する。

エ. 電波を発する機器（来訪者向け Wi-Fi やゲーム機等）による電波干渉に留意する。

オ. 意図したエリア内に限ってサービスが提供されるようにする。

②　来訪者向け無線 LAN（Wi-Fi）について

ア. 来訪者向け無線 LAN は、業務用無線 LAN と分離し、両者の電波干渉に留意する。

イ. 意図したエリア内に限ってサービスが提供されるようにする。

⑷　医療機関等がネットワークを通じて通信を行う際に、通信の相手先が正当であることを認識するための相互認証を行う。また診療録等のオンライン外部保存を受託する事業者と委託する医療機関等が、互いに通信目的とする正当な相手かどうかを認識するための相互認証機能を設けることが好ましい。

第５条　使用機器一覧表の作成及び適正な廃棄方法の実施

【編注】小規模医療機関等で使用機器が少なく、一覧表の作成がなくても管理が可能であれば一覧表の作成はなくても良い。なお、廃棄の場合は業者に委託するなどし

てデータ消去をしっかりと行う。

⑴　「(医療情報システム) 企画管理者」は、医院で用いる「医療に関する患者情報（個人識別情報）を含む情報」を扱う下記の機器の一覧表を作成する。

① 医院で用いる端末（カードリーダー、タブレット端末、スマートフォン、パソコン、電子カルテ（電子カルテと連動する会計システム等を含む)）、部門システム

② 医院で用いるネットワーク機器（ハブ、Wi-Fi ルータ、VPN ネットワークスイッチ、ファイアウォール機器など）

③ 医院で用いる記録媒体（USB、HDD、SSD、光学ドライブなど）

④ 医院で用いるサーバ（ネットワーク上で他のコンピュータの指示を受け情報処理結果を返す役割を持つコンピュータやソフトウェア、画像や検査結果など患者情報の蓄積が可能な医療機器を含む）

⑤ 監視カメラなど、患者の個人情報を扱う機器でインターネット接続しているもの。

⑵　機器を廃棄する場合は、「データ消去後に HDD/SSD 破砕・廃棄を行う」廃棄業者（株式会社〇〇）に委託し、廃棄し、その旨を記録する。

【編注】外部業者のサーバ等を利用する場合は、外部業者との間でサイバーセキュリティに関する契約（第９条【別紙１】**(12～15 頁参照)**）を行っておく。

（使用機器一覧表の例）

種別	管理番号	メーカー	管理場所	管理責任者	備考
パソコン	PC-001	〇〇	医事課	医事課長	
~~パソコン~~	~~PC-002~~	~~〇〇~~	~~医事課~~	~~医事課長~~	2023/5/8 業者廃棄
パソコン	PC-003	〇〇	医事課	医事課長	
USB	U-001	〇〇	医局	医局長	
USB	U-002	〇〇	医局	医局長	
USB	U-003	〇〇	医局	医局長	
USB	U-004	〇〇	医事課	医事課長	
:	:	:	:	:	

第６条　機器の使用管理簿の作成

【編注】小規模医療機関等で使用機器が少なく、一覧表の作成がなくても管理が可能であれば使用管理簿の作成はなくても良い。

⑴　「(医療情報システム) 企画管理者」は、機器の仕様管理簿を作成する。

⑵　医療情報システムの実装・運用の実務担当者は、使用にあたって、起動時にウイルスチェックを行い、使用後は電源を OFF（常時電源 ON の機器を除く）にした上で所属長に終了の報告を行う。

（管理簿の例）

種別	管理番号	メーカー	管理場所	管理責任者
パソコン	PC-001	〇〇	医事課	医事課長
使用年月日	使用者印	開始時間	終了時間	管理者印

年　月　日		時　　分	時　　分	
年　月　日		時　　分	時　　分	
年　月　日		時　　分	時　　分	

第７条　私物の機器の業務使用の禁止

⑴　USB メモリを含めた職員の私物の機器は、原則として診療に関する業務で使用しない。

⑵　やむを得ず私物の機器を用いざるを得ない場合は、所属長の許可を得、ウイルスチェックを行った上で使用し、使用後はデータ削除を行う。所属長はその旨を記録する。

第８条　医療情報システム関連法令の把握

⑴　医療情報システムの安全管理を推進する前提として、下記の法律について把握する。

①　個人情報の保護に関する法律（平成 15 年法律第 57 号）

【編注】医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンスは、下記 URL 参照

https://www.mhlw.go.jp/content/001120905.pdf

②　e-文書法、厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令（平成 17 年厚生労働省令第 44 号）及び「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」（平成 17 年３月 31 日付け医政発第 0331009 号・薬食発第 0331020 号・保発第 0331005 号厚生労働省医政局 長・医薬食品局長・保険局長連名通知。平成 28 年３月 31 日最終改正）

③　「診療録等の保存を行う場所について」（平成 14 年３月 29 日付け医政発第 0329003 号・保発第 0329001 号厚生労働省医政局長、保険局長連名通知。平成 25 年３月 25 日最終改正）

⑵　診療録の作成にあたっては医師法、各法令が定める内容に沿って作成する。なお、電子署名を施す場合には、電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）第２条に基づく電子署名を行うほか、本ガイドラインに基づき適切な措置を講じる。

【編注】電子署名を施す医療機関でない場合は、なお書き以降は不要。

第９条　機器購入時の留意点及び外部業者との契約について

⑴　医療情報機器の購入にあたっては、脆弱性について確認を行うとともに、購入した後に脆弱性が判明した場合の報告を求める。仮に脆弱性が判明した場合は「セキュリティパッチ」（脆弱性等を修正するプログラム）が適用されるまで使用を中止する。

⑵　外部業者に医療情報システムの管理を委託する場合は、下記が確認できる委託契約書（**【別紙１】（12～15 頁参照）**）を締結する。

①　契約先の事業者内に、医療情報システムの管理責任者がいること。（【編注】①は、令和５年度中に整備）

②　契約先の事業者は、提供するソフトウェア・機器等の脆弱性に関して、医療機関への導入時、以降適時、 求められる安全性に関する状況（初期パスワードの変更、脆弱

性の更新状況）を確認し、医療機関にその結果を報告し、対応すること。

③　ネットワーク機器（VPN（仮想専用線）機器を含むインターネットとの接続を制御するルータ）について

ア. ネットワーク機器にセキュリティパッチ（最新ファームウェア（内蔵ソフト）や更新プログラム）を適用していること。（【編注】アは、令和５年度中に整備）

イ. ネットワーク機器にアクセス制限を実施していること。（【編注】イは、令和５年度中に整備）

④　サーバについて

ア. サーバにセキュリティパッチ（最新ファームウェア（内蔵ソフト）や更新プログラム）を適用していること。（【編注】アは、令和６年度中に整備）

イ. バックグラウンド（見えないところ）で動作している不要なソフトウェア及びサービスを停止している（【編注】イは、令和５年度中に整備）。

ウ. サーバでアクセス記録（アクセスログ）の管理をしている。

⑤　契約先の事業者は、インシデント発生時、事前に明確化している責任分界点に応じて対応できる体制を整えていること。

⑥　契約先の事業者は、バックアップについての保管及び取り扱いについて、当院に取り扱い説明書等の文書として提供していること。

【編注】セッション乗っ取り、IP アドレス詐称等のなりすましを防止するため、原則として医療機関等が経路等を管理する、オープンではないネットワークを利用することも重要であり、これが実施できる場合は方針にも書き込む。

⑶　外部業者に医療情報機器の廃棄を委託する場合は、データ消去後に HDD/SSD 破砕・廃棄を行うことが確認できる委託契約書**（別紙１（12～15 頁参照））**を締結する。

【編注】医療情報の記録が作成される医療機器等を使用する場合は、下記を追加する。

⑷　電子カルテシステム等で PC 等の汎用入力端末により記録が作成される場合

①　診療録等の作成・保存を行う場合は、確定された情報を登録できる仕組みをシステムに備えると。その際、登録する情報に、入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時を含める。

②　「記録の確定」を行うに当たり、内容を十分に確認できるようにする。

③　「記録の確定」は、確定を実施できる権限を持った確定者に実施させる。

④　確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、原状回復のための手順を検討しておく。

⑤　一定時間経過後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確なルールを運用管理方針に定める。

⑥　確定者が何らかの理由で確定操作ができない場合における記録の確定の責任の所在を明確にする。例えば、「（医療情報システム）企画管理者」が記録の確定を実施する等のルールを運用管理方針に定める。

⑦　一旦確定した診療録等を更新する場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合わせることができるようにする。

⑧　同じ診療録等に対して複数回更新が行われた場合でも、更新の順序性が識別できるようにする。
⑨　代行入力が行われた場合には、誰の代行がいつ誰によって行われたかの管理情報を、代行入力の都度記録する。
⑩　代行入力により記録された診療録等は、できるだけ速やかに（原則２４時間以内）確定者による「確定操作（承認）」が行われるようにする。この際、内容の確認を行わずに確定操作を行わない。

⑸　臨床検査システム、医用画像ファイリングシステム等、特定の装置又はシステムにより記録が作成される場合
①　運用管理方針等に当該装置により作成された記録の確定ルールを定義する。その際、当該装置の管理責任者や操作者の氏名等の識別情報（又は装置の識別情報）、信頼できる時刻源を用いた作成日時を記録に含める。
②　確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、原状回復のための手順を検討しておくこと。

【別紙１】外部業者（システムベンダ等）との契約書に盛り込むべき項目（案）

【編注】
契約書策定にあたっては、契約書医療機関及び事業者の責任分界点（どこまでが、どちらの責任であるのか）について、責任の所在を契約書等で明確にする必要がある。
下記に盛り込むべき項目案を示したが、各医療機関が実施する委託内容によって契約書の内容は異なることから、実際には業者や顧問弁護士等と相談し、契約書を締結いただきたい（契約書は適宜見直す）。
また、契約内容をベースに医療機関における取り扱いマニュアルの提供を求める。

１．外部業者（システムベンダ等）の要件

①　医療情報システム提供事業者はＰマーク（プライバシーマーク）又はＩＳＭＳ（ISO27001）認証を取得している。
②　事業者内に、医療情報システムの管理責任者がいる。
③　事業者は、提供するソフトウェア・機器等の脆弱性に関して、医療機関への導入時、以降適時、 求められる安全性に関する状況（初期パスワードの変更、脆弱性の更新状況）を確認し、医療機関にその結果を報告し、対応する。
④　ネットワーク機器（VPN（仮想専用線）機器を含むインターネットとの接続を制御するルータ）にセキュリティパッチ（最新ファームウェア（内蔵ソフト）や更新プログラム）を適用する。（【編注】④は、令和５年度中に整備）
⑤　サーバでアクセス記録（アクセスログ）の管理をする。
⑥　ネットワーク機器にアクセス制限を実施する。
⑦　インシデント発生時、事前に明確化している責任分界点に応じて対応できる体制

を整えている。

⑧ 事業者は、バックアップについての保管及び取り扱いについて、当院に取り扱い説明書等の文書として提供する。

⑨ 「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第 1.1 版」に沿った対応を行う。

２．新規購入時及び管理

① 外部業者は、システムがどのような情報機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかを明らかにし、システムの機能仕様を明確に定義する。

② 外部業者は、情報機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスを規定する。

③ 外部業者は、医療情報システムで利用するシステム、サービス、情報機器等の品質を定期的に管理するための手順を作成し、これに従い必要な措置を講じ、「(医療情報システム) 企画管理者」に報告する。

④ 外部業者は、医療情報システムの目的に応じて速やかに検索表示又は書面に表示できるよう措置を講じる。

３．通常運用時（軽微な障害への対応を含む）の取扱い

⑴ 管理責任

① 医療情報システムの保守作業の方法及び監督に関する事項**（遠隔操作による保守作業実施機器を確認（【編注】下線部は令和５年度中に整備）**し、遠隔操作により保守作業を行う場合は、外部からの不正なアクセスを排除することを求めるか、それが契約できない場合は、実地による保守点検とする）を定める。

② 事業者から、製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう（【編注】②は、令和５年度中に整備）。

③ 医療情報システムの運用管理に関する定期的な点検と改善策の協議を行う。

④ 脆弱性情報は、直ちに医療機関に連絡を行い、パッチなど必要な対応を行う。

⑵ 通常の取扱い

① 医療情報（診療録等を含む）の取扱いについて、トラブル対応も含めて事業者は別途マニュアルを作成する。医療機関はマニュアルに沿って操作を行う。

② 下記の対処方法についてマニュアルに記載する。

ア. 基本的な操作方法

イ. 医療機関がネットワークに接続できない場合の対処

ウ. ネットワークが不通の場合又は著しい遅延が発生している場合の対処

エ. 医療機関が受け取った保存情報を正しく受信できなかった場合の対処

オ. 伝送情報の暗号化に不具合があった場合の対処

カ. 医療機関の認証に不具合があった場合の対処

③ 動作確認等の作業で事業者が個人情報を含むデータを使用するときは、保守終了

後に確実にデータを消去するとともに、その結果を報告する。

④ 診療録等の外部保存を受託する事業者は、受託する事業者の管理者を含め、保存を受託した個人情報にアクセスできない。

⑤ 保守を実施するためにサーバに事業者の作業員（保守要員）がアクセスする際には、保守要員の専用アカウントを使用させ、個人情報へのアクセスの有無並びに個人情報にアクセスした場合の対象個人情報及び作業内容を記録する。これは利用者を模して操作確認を行う際の識別・認証についても同様である。

⑥ リモートメンテナンス（保守）によるシステムの改造・保守作業を行う場合には、当該作業の終了後速やかにアクセスログを報告する。

【編注】保守に関する作業計画書と照合する確認し、確認する。

⑦ リモートメンテナンス（保守）において、やむを得ず事業者がファイルを医療機関等へ送信等を行う場合、送信側で無害化処理が行われていることを確認する。

⑧ 診療録等を保管している設備に障害が発生した場合等で、やむを得ず診療録等にアクセスをする必要がある場合も、医療機関等における診療録等の個人情報と同様の秘密保持を行うと同時に、外部保存を委託した医療機関等に許可を求める。

４．サイバー攻撃への対応の取扱い

⑴ 事故発生時等

① サイバー攻撃（強い疑いを含む）が発生した場合、下記について事業者が別途作成するマニュアルに盛り込む。

ア. 緊急対処方法（LAN ケーブルの遮断など）

イ. 事業者の 24 時間連絡体制（日曜や深夜を含めた緊急連絡）の確保

ウ. 障害が起こった場合に障害部位を切り分ける責任

エ. 医療機関が情報交換を中止する場合の対処

② 事故発生に関する適切な情報提供義務・説明

⑵ 事後の対応

① 医療情報について何らかの不都合な事態が生じた場合、医療機関と事業者は原因追及と再発防止策の実施を優先させる。

② 医療情報について何らかの不都合な事態が生じた場合、事業者は医療機関の求めに応じて必要な分析と情報提供を行い、医療機関の質問に真摯に対応する。

③ 医療機関等が事態発生及び原因と対処法等を外部に説明する必要がある場合、事業者は医療機関の求めに応じて説明を補佐する。

④ 損害に対する費用分担について、事故原因が受託する事業者にある場合は事業者が負う。事故原因が医療機関にある場合は医療機関が負う。事故原因の責任分界が不明内場合等は、協議により決定する。

５．他の医療機関などとの間でのネットワークを通じた患者情報の交換

① 情報処理関連事業者の提供するネットワークを通じて患者情報を交換する場合

ア． 提供元医療機関等と提供先医療機関等は、ネットワーク経路における責任分界

点を定め、不通時や事故発生時の対処を含め、契約等で合意しておく。

イ． 情報処理関連事業者との管理責任の分担について責任分界点を定め、情報処理関連事業者の管理責任の範囲及びサービスに何らかの障害が起こった際の対処主体を明らかにしておく。ただし、通常運用における責任及び事後責任は、委託の場合、原則として提供元医療機関等にあることに留意する。

② 提供元医療機関等と提供先医療機関等が独自に接続する場合及び共同利用により他の医療機関等が収集した医療情報を利用する場合

あらかじめ、責任分界などを規約や契約などで明確にする。

６．その他

その他、医療情報システムの安全管理に関するガイドラインに準じて対応する。

第 10 条 「(医療情報システム) 企画管理者」の業務指針

「(医療情報システム) 企画管理者」は、下記を実施又は委託先事業者によって実施されていることを確認する。

【編注】乗っ取り、IP アドレス詐称等のなりすましを防止するため、原則として医療機関等が経路等を管理する、オープンではないネットワークを利用することも重要であり、これが実施できる場合は方針にも書き込む。

⑴ サーバについて、以下を実施する（【編注】⑴は、令和５年度中に整備）。

① 利用者の職種・担当業務別の情報区分ごとのアクセス利用権限を設定している。

② 退職者や使用していないなど、不要なアカウントを速やかに削除する。

③ アクセス記録（アクセスログ）を管理する。

⑵ ネットワーク機器（VPN（仮想専用線）機器を含むインターネットとの接続を制御するルータ）についてセキュリティパッチ（最新ファームウェア（内蔵ソフト）や更新プログラム）を適用している。（【編注】⑵は、令和５年度中に整備）。

⑶ 端末 PC について、以下を実施する（【編注】⑶は、令和６年度中に整備）。

① 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。

② 退職者や使用していないアカウント等、不要なアカウントを削除している。

③ セキュリティパッチ（最新ファームウェア（内蔵ソフト）や更新プログラム）を適用している。

④ バックグラウンド（見えないところ）で動作している不要なソフトウェア及びサービスを停止している。

⑷ その他、下記を実施する。

① サーバでアクセス記録 (アクセスログ) の管理をしている。アクセスログについて、職員のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるよう記録するとともに、定期的にログを確認する。

② ネットワーク機器にアクセス制限を実施している。アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を実施する。

③ アクセスログの記録に用いる時刻情報は、信頼できるものを利用する。利用する時

刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を保つ。

⑸　職員に下記の取扱いの徹底を周知する。

ア．　マニュアルに沿った機器等の利用を行う。

イ．　USB・光ディスク等の記憶媒体は、ウイルスチェックを行った上で使用する。

ウ．　不審メールの添付ファイルを開封しない。

エ．　万が一、不審メールの添付ファイルを開封してしまった場合は、ただちに LAN ケーブルを外し、「(医療情報システム) 企画管理者」に連絡する。

オ．　なりすましメール対策の国際標準である DMARC(Domain-based Message Authentication, Reporting, and Conformance：RFC7489)の導入を行うことが望ましい

第 11 条　医療情報システムの運用に関する職員業務方針

医療情報システムにアクセスする職員は、職員業務方針（別紙２）を励行する。

【別紙２】医療情報システム職員業務方針

１．医療情報システムへのアクセスについては、職員の識別・認証を行う。

①　職員の識別・認証に、ユーザ ID とパスワードを用いる場合は、それらの情報について職員本人以外は知り得ないようにする（医療情報システムの運用担当者であっても、利用者のパスワードを推定できないようにする)。

ア．　パスワードのメモ書きなどはしない。

イ．　生年月日など類推が可能なパスワードの設定を行わない。

②　利用者の識別・認証に IC カード等のセキュリティ・デバイスを用いる場合、IC カードの破損等を想定し、緊急時の代替手段による一時的なアクセスルールを用意する。

③　医療情報システム内のパスワードファイルは、パスワードを暗号化（不可逆変換による）した状態で管理・運用する。また、識別に IC カード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理方針にて定める。

④　職員の職種・担当業務ごとに、アクセスできる診療録等の範囲（アクセス権限）を定め、アクセス権限に沿ったアクセス管理を行う。

２．データ使用時の取扱い

①　職員が個人情報を含むデータを使用するときは、他の者が画面等を見ることができないようにするなど、漏えい等に留意する。

②　個人情報を入力・参照できる端末から長時間離席する際は、コンピュータ及び端末をログオフ状態にしておくか、職員認証機能で管理されたスクリーン及びキーボードのロック機能によって保護する。

３．ウイルスチェック及びマクロ等の無害化処理を行う。

①　システム起動時、記録媒体の使用時、外部からの情報受領時には、不正なソフト

ウェアが混入していないかウイルスチェックを実施する。
② 常時不正なソフトウェアの混入を防ぐ適切な措置をとる。
③ メールやファイル交換、データ保存にあたっては、下記を実施する。
ア. 実行プログラム（マクロ等含む）が含まれるデータやファイルは送受信を禁止する。やむを得ず使用する場合は、無害化処理等を行う。
イ. 保守等でやむを得ずファイル送付等を行う場合、送信側で無害化処理が行われていることを確認する。
ウ. 不審メールの添付ファイルを開封しないことを徹底するが、不審メールの添付ファイルを開封してしまった場合は、ただちにＬＡＮケーブルを外し、「(医療情報システム）企画管理者」に連絡する。

４．ネットワークを介した通信

① ネットワークを通じた通信は、「(医療情報システム）企画管理者」が許可した相手及び方法でのみ実施する。
② 新規に通信を行う相手については、「(医療情報システム）企画管理者」の許可を受け実施する。
③ データのダウンロードについては、「(医療情報システム）企画管理者」の許可を受けた上で、他の医療情報システムや医療機器と接続がされていないパソコン等を使用して実施し、ダウンロード実施後にウイルスチェックを行う。

第 12 条　サイバー攻撃等を想定した事業継続計画（BCP）の策定

サイバー攻撃を受ける等システムに重大な障害が発生したことを想定した事業継続計画（BCP）を策定している（【編注】BCP の策定は、令和６年度中に整備）。

【別紙３】サイバー攻撃等を想定した事業継続計画（BCP）の一例

１．サイバー攻撃に対する予防の徹底

① 医療情報システム安全管理方針及びネットワーク構成図を作成し、経営層及び医療情報を取り扱う職員にその内容の周知・徹底を図る。
② 重要なファイルは適宜バックアップをとり、不正ソフトウェアの混入による影響が波及しない手段で管理する。

２．サイバー攻撃の疑いを把握した場合

① 発生事象の写真撮影を行う。
② 発生事象の原因が物理的問題（電源やケーブル等）でないことを確認する。
③ 「(医療情報システム）企画管理者」に報告し、不正ソフトウェア混入の兆候（HP の改ざんや患者情報の暗号化、データの紛失・消去等）がある場合は、安全管理責任者の指示により当該端末・機器のネットワーク接続を物理的に遮断する。ただし証拠保全のため、当該端末・機器の電源を停止してはならない（電源を切ると調査に必要なログが消滅することがある)。

④　類似の事象が起こっていないか、確認する。
⑤　医療情報に関する不具合発生報告書を記載の上、「(医療情報システム) 企画管理者」に状況報告を行う。

３．サイバー攻撃があった場合（攻撃を強く疑う場合を含む）

⑴　「(医療情報システム) 企画管理者」は、医療情報に関する業務システムを停止し、院長など経営管理層、「(医療情報システム) 企画管理者」、各部門の長による対策会議を招集し、他の情報機器及び医療への影響の調査等被害の確認を行う。

①　攻撃内容と範囲の特定
ア. 発生日時
イ. 発生場所
ウ. 発生機器が属するネットワーク
エ. 発生事象
オ. 事象発生の原因と考えられる操作等

②　証拠保全の実施
ア. 発生事象の写真撮影（再掲）
イ. ログの取得

③　当該端末・機器のネットワーク接続の物理的遮断

⑵　対策会議は外部委託業者に連絡し、下記の対応を検討する。

①　診療継続の可否（診療継続のための条件整備）
②　データ復旧の可否
③　情報漏洩の可能性の有無
④　被害拡大防止策（今後の被害拡大の可能性の把握も）
ア. ネットワークの遮断の確認
イ. バックアップデータの確認（オフラインによる）
ウ. ネットワークや電子カルテの利用停止の判断

外部委託業者	電子カルテ	TEL:　〇〇-〇〇〇〇-〇〇〇〇 MAIL:　〇〇〇〇@〇〇〇〇.〇〇.〇〇
	サーバ	TEL:　〇〇-〇〇〇〇-〇〇〇〇 MAIL:　〇〇〇〇@〇〇〇〇.〇〇.〇〇
	〇〇	TEL:　〇〇-〇〇〇〇-〇〇〇〇 MAIL:　〇〇〇〇@〇〇〇〇.〇〇.〇〇

⑶　対策会議は、被害内容を検討した上で必要に応じて下記に連絡・相談する。

厚生労働省	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 TEL:　03-6812-7837 MAIL:　igishitsu@mhlw.go.jp
個人情報保護委員会	個人情報保護委員会（個人情報保護法第 26 条に基づく場合） https://www.ppc.go.jp/personalinfo/legal/leakAction/
警察	都道府県警のサイバー犯罪窓口

		TEL：　〇〇-〇〇〇〇-〇〇〇〇 MAIL：　〇〇〇〇@〇〇〇〇.go.jp ※都道府県警察のサイバー犯罪相談窓口は、下記参照（下記ページで不明な場合は都道府県警のお問合せください） https://www.npa.go.jp/bureau/cyber/soudan.html
	事後報告	独立行政法人情報処理推進機構 ①　コンピュータ不正アクセス届出制度 https://www.ipa.go.jp/security/todokede/crack-virus/about.html ②　コンピュータウイルス届出制度 https://www.ipa.go.jp/security/todokede/crack-virus/about.html ③　ソフトウェア等の脆弱性関連情報に関する届出制度 https://www.ipa.go.jp/security/vuln/report/index.html

⑷　対策会議は、被害拡大防止のための措置を講じるとともに、下記の内容について職員への周知と患者への広報を行う。

①　攻撃内容と範囲

②　外部業者、厚労省、警察と連絡をしながら対処を行っていること

③　診療継続の可否（診療制限を含む）

４．サイバー攻撃からの復旧

⑴　対策会議は、外部業者の協力を得ながら復旧体制と、対策優先度の整理を行う。例えば、サイバー攻撃を受けた医療機器等と論理的・物理的に接続されていない機器、又は、攻撃を受けた医療機器等以外の機器が影響を受けていないことを確認した上で、バックアップからの重要なファイルの復元を試みることなど

⑵　対策会議は再発防止対策（体制の脆弱性と運用手順、セキュリティ対策の見直し、教育・訓練）の取り組みを検討・実行する。

※　BCP には災害（地震、水害、落雷、火災等並びにそれに伴う停電等）への対応についても記載するが、その際「医療情報及び医療情報システムの保管場所は、災害による障害に対策を講じた場所に設置する」ことなどを記載しておく。

第 13 条　情報管理（管理・持ち出し・破棄等）

⑴　医療情報及び情報機器の持出しは、保守業務を行う事業者を含めて原則禁止とする。

①　やむを得ず持ち出しを行う場合は、持ち出す情報及び機器について持ち出し日時・返却日時を含め、「（医療情報システム）企画管理者」による許可を得る。

②　「（医療情報システム）企画管理者」は、医療情報が格納された可搬媒体及び情報機器**（サーバ、端末 PC、ネットワーク機器）の所在を台帳等により管理（【編注】下線部は令和５年度中に整備）の所在を第５条「使用機器一覧表の作成及び適正な廃棄方法の実施」に掲げる一覧表を作成して管理・**定期的に棚卸を行う。

③　やむを得ず医療情報及び情報機器等を持ち出さざるを得なかった場合における盗難、

置き忘れ等に対応する措置として、医療情報や情報機器等に対する暗号化やアクセスパスワードの設定等、容易に内容を読み取られないようにする。

④ やむを得ず持ち出した情報機器等について公衆無線ＬＡＮは利用しない。

⑤ やむを得ず持ち出した医療情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールするとともに、原則として情報機器に対する変更権限がない設定を行う。業務に使用しないアプリケーションや機能については削除又は停止するか、業務に対して影響がないことを確認する。

⑵ 外部のネットワークや他の外部媒体に接続する場合は、不正ソフトウェア対策ソフトやパーソナルファイアウォール（不正アクセスを防ぐソフトや機器）の導入等により、情報端末が情報漏洩、改ざん等の対象にならないような対策を実施する。

⑶ 医療情報・医療情報処理機器の廃棄

① 医療情報の破棄については、当該情報を有する部門の長、「（医療情報システム）企画管理者」及び経営責任者の合議で行うこととし、その内容（廃棄内容、日時、廃棄方法等）を記録・保管する。

② 情報処理機器自体を破棄する場合は、外部業者に委託する。委託にあたっては、契約書を締結し、契約に基づいて廃棄されたことを証憑または事業者説明により確認する。

第 14 条　患者等への医療情報の閲覧

患者等に医療情報を閲覧させる場合、医療情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、例えば、システムやアプリケーションを切り分け、ファイアウォール（不正アクセスを防ぐソフトや機器）、アクセス監視、通信の TLS 暗号化、PKI（Public Key Infrastructure：公開鍵暗号基盤認証）等の対策を実施する。

第 15 条　インシデント発生時の対応

⑴ インシデント発生時は、「【参考６】インシデント（非常時）対応マニュアル」に沿って対応する。

⑵ インシデント発生時には、下記の連絡を行う（【編注】⑵は、令和５年度中に整備）。

① 直ちに「（医療情報システム）企画管理者」及び院長に報告する。

② 「（医療情報システム）企画管理者」又は院長は、直ちに外部委託業者に連絡を行い相談する。

外部委託業者　TEL:○○-○○○○-○○○○　MAIL:○○○○@○○○○.○○.○○

③ 必要に応じて、下記へ連絡を行い、相談する。

ア.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

TEL:　03-6812-7837

MAIL:　igishitsu@mhlw.go.jp

イ.都道府県警のサイバー犯罪窓口

⑶ インシデント発生時には、診療継続のために必要な情報を検討する。また、データや

システムのバックアップの実施と復旧手順を確認している。（【編注】⑶は、令和６年度中に整備）。

⑷ 非常時用ユーザアカウントを使用した場合、正常復帰後は継続使用ができないように変更する。

第 16 条　システム設計・運用に必要な方針類と文書体系

「(医療情報システム）企画管理者」は各種方針等を作成し、必要に応じて見直す。

① 外部業者（システムベンダ等）との間で責任分解を明確化（どこまでが、どちらの責任であるのか）した契約書等

【編注】「【別紙１】外部業者との契約書に盛り込むべき項目案」**(12～15 頁)** 参照

② サイバー攻撃を受けた場合の**院内の連絡体制、連絡・相談する外部業者や厚生労働省、警察などの連絡先を定め（【編注】下線部は令和５年度中に整備）、サイバー攻撃を想定した事業継続計画（BCP）を策定（【編注】BCP の策定は、令和６年度中に整備）**している。

【編注】「【別紙３】サイバー攻撃を想定した事業継続計画（BCP）の一例」**(17～19 頁)** 参照

③ 医療情報システムにおいて採用するシステム、サービス、情報機器等の機能仕様や利用方法に関する資料

【編注】取扱い説明書などを一括して保管しておく。

④ 医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図等)、及びシステム責任者・関係者一覧（設置事業者、保守事業者等含む）

【編注】小規模な医療機関では不要（作成が安全管理に有効かどうかで判断）

⑤ 医療情報システムの維持及び運用に必要な手順

【編注】この安全管理方針及び、外部業者によるマニュアルなど

⑥ 医療情報システムの利用者が適切に医療情報システムの利用ができることを目的とした方針

【編注】「【別紙２】医療情報システム職員業務方針」**(16～17 頁)** 参照

⑦ 非常時や情報セキュリティインシデントが生じた場合の手順等

【編注】「【別紙３】サイバー攻撃を想定した事業継続計画（BCP）の一例」**(17～19 頁)** 参照

【参考１】サイバーセキュリティチェックリスト（厚労省）

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

医療機関確認用

	チェック項目	確認結果（日付）	備考
医療情報システムの有無	医療情報システムを導入、運用している。 （「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ （　/　）	

○令和５年度中

※以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
※２（２）及び２（３）については、事業者と契約していない場合には、記入不要です。
※1 回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付）			備考
		1回目	目標日	2回目	
1 体制構築	⑴　医療情報システム安全管理責任者を設置している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**				
	⑴　サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	⑵　リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	⑶　事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	サーバについて、以下を実施している。				
	⑷　利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	⑸　退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	⑹　アクセスログを管理している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	ネットワーク機器について、以下を実施している。				
	⑺　セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	⑻　接続元制限を実施している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
3 インシデント発生に備えた対応	⑴　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）への連絡体制図がある。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	

- 各項目の考え方や確認方法等については、「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～」をご覧ください。
  https://www.mhlw.go.jp/content/10808000/001105752.pdf
- 立入検査の際は、チェックリストに必要な事項が記入されているかを確認します。

○令和６年度中

※以下項目について、令和６年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

	チェック項目	確認結果（日付）			備考
		1回目	目標日	2回目	
2 医療情報システムの管理・運用	**サーバについて、以下を実施している。**				
	⑺　セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	⑼　バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	端末 PC について、以下を実施している。				
	⑷　利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	⑸　退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	⑺　セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	⑼　バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
3 インシデント発生に備えた対応	⑵　インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	⑶　サイバー攻撃を想定した事業継続計画（BCP）を策定、又は令和６年度中に策定予定である。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	

● 各項目の考え方や確認方法等については、「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～」をご覧ください。

https://www.mhlw.go.jp/content/10808000/001105752.pdf

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

事業者確認用

○令和５年度中

※以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください 。
※1 回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付）			備考
		1回目	目標日	2回目	
1 体制構築	⑴ 事業者内に、医療情報システム等の提供に係る管理責任者を設置している。	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**				
	⑵ リモートメンテナンス（保守）している機器の有無を確認した。	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	
	⑶ 医療機関に製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出した。	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	
	サーバについて、以下を実施している。				
	⑷ 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	
	⑸ 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	
	⑹ アクセスログを管理している。	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	
	ネットワーク機器について、以下を実施している。				
	⑺ セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	
	⑻ 接続元制限を実施している。	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	

○令和６年度中

※以下項目について、令和６年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

	チェック項目	確認結果（日付）			備考
		1回目	目標日	2回目	
2 医療情報システムの管理・運用	**サーバについて、以下を実施している。**				
	⑺ セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	
	⑼ バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	
	端末 PC について、以下を実施している。				
	⑷ 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	
	⑸ 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	
	⑺ セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	
	⑼ バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ （ / ）	（ / ）	はい・いいえ （ / ）	

● 各項目の考え方や確認方法等については、「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～」をご覧ください。
https://www.mhlw.go.jp/content/10808000/001105752.pdf

事業者名：

【参考２】「（医療情報システム）企画管理者」用サイバーセキュリティチェックリスト
（徳島県作成:レイアウトは保団連で整理）

※下記について現場で定期的にチェックを行う。Lv. １（最低限の対策)、Lv. ２（基本的な対策)、Lv. ３（対策ができている）であり、全ての項目でLv. ２（＝ゴチック表記）以上を目標に整備する。

https://anshin.pref.tokushima.jp/med/experts/docs/2023022200010/

	チェック項目	Lv	対策
1	○サイバーセキュリティにかかる最新動向の収集（インシデント情報やセキュリティ専門知識を持つ者等からの情報発信等）を実施していますか。 ○医療情報システムベンダ及びサービス事業者から技術的対策や医療情報システムのアップデート等の情報を収集していますか。	1	サイバーセキュリティにかかる情報を収集している。
		2	**収集した情報を基にサイバーセキュリティ対策の実施について、医療情報システムベンダ等に相談し、対応している。**
		3	医療情報システムベンダ等とサイバーセキュリティ対策に関する契約を締結している。
2	医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図等） ※最新の状態を維持し、新設したインターネット回線やVPN（仮想専用線）機器等は記載している。	1	ネットワーク・システムの構成の概要がわかる。
		2	**ネットワーク・システムの詳細な構成図が作成されている。**
		3	新規導入した回線や医療機器等も構成図に反映され、現状を把握できている。または、把握できるように部門間でも連携がとれている。
3	医療情報システムに関するシステム責任者一覧（設置事業者等含む）は、最新の状態を維持していますか。	1	医療情報システムに関する責任者が決まっている。
		2	**医療情報システムに関する責任者（医療情報システムベンダ及びサービス事業者等含む）の一覧表等が作成され、文書化されている。**
		3	医療情報システムに関する責任者が定期的に見直され、一覧表等が最新の状態になっている。
4	バックアップは、正常に取得できていますか。バックアップの一部は、オフラインバックになっていますか。	1	院内ネットワーク上にバックアップを取得しているが、オフライン保管はしていない。
		2	**重要なシステムのバックアップを取得し、オフライン保管している。**
		3	定期的にバックアップ状況を管理している。
5	医療情報システムへのアクセスにおける利用者は、契約終了等に合わせて、アクセス権限を無効化していますか。	1	医療情報システムのアカウントは、利用者の担当業務に合わせてアカウントを付与している。
		2	**契約終了等に合わせてアカウントの無効化を実施している。**
		3	定期的にアカウントの棚卸を行い、不要なアカウントが無い事を確認している。
6	医療情報システムへのアクセスにおける利用者は、人事異動等による利用者の担当業務の変更等に合わせて、アクセス権限の変更を行っていますか。	1	医療情報システムのアカウントは、利用者の担当業務に合わせてアカウントを付与している。
		2	**担当業務の変更等に合わせて、アクセス権限の変更を行っている。**
		3	定期的にアクセス権限の棚卸を行い、不要なアクセス権を付与していない事を確認している。
7	アクセスログは取得できていますか。大量のログイン失敗の形跡等の	1	医療情報システムのアクセスログを取得し、大量のログイン失敗の形跡等の不審なログがないかチェックし

	不審なログはありませんか。		ている。
		2	**VPN 機器等のアクセスログを取得できるように保守事業者等に依頼している。**
		3	各種アクセスログを統合管理するシステムを導入している。アクセスログを分析し、不審なアクセスがある場合は、調査を実施している。
8	医療情報システムの時刻は合っていますか。	1	―
		2	**医療情報システムの時刻が合っている／合わせている。**
		3	時刻が自動で合うようにシステムを構成している。
9	ウイルス対策ソフトのパターンファイルは更新されていますか。	1	ウイルス対策ソフトを導入しているが、パターンファイルの更新状況は管理していない。
		2	**ウイルス対策ソフトのパターンファイル更新を定期的に確認している。**
		3	ウイルス対策ソフトの管理システム等により、パターンファイルの更新状況を一元管理している。
１０	OS のセキュリティ・パッチを適用していますか。	1	OS のセキュリティ・パッチ適用について、医療情報システムベンダー等に確認している。
		2	**OS のセキュリティパッチを定期的に適用している。**
		3	WSUS サーバ等により、OS のセキュリティパッチの更新を一元管理している。
１１	脆弱性が検出されたネットワーク機器（VPN（仮想専用線）機器等）は、ファームウェア（内蔵ソフト）を更新していますか。	1	ネットワーク機器を把握している。
		2	**必要に応じてファームウェアを更新するように依頼している。**
		3	必要に応じてファームウェアの更新するように保守業者と契約を締結している。
１２	システム構築時、適切に管理されていない記録媒体の使用時、外部からの情報受領時には、不正ソフトウェアが混入していないか確認していますか。	1	持込み機器は、ウイルスチェックを実施して持込むよう依頼している。
		2	**最新の状態に更新したウイルス対策ソフトでウイルスチェックしている。**
		3	医療情報システムの利用端末やネットワークに接続する記録媒体、機器等を技術的に制御している。
１３	保守作業等の医療情報システムに直接アクセスする作業の際には、作業者、作業内容及び作業結果を確認していますか。リモートから保守作業を行われた場合も同様に確認できていますか。	1	保守作業の作業日時、作業者、作業内容、作業結果等を確認している。
		2	**保守作業のリモートアクセスは、あらかじめ申請を求めている。（緊急時は事後報告をする）**
		3	保守作業のリモートアクセスは許可なくできない仕組みとしている。
１４	外部に持ち出す情報機器（ノートパソコン、スマートフォン等）や記録媒体（USB メモリ等）の管理を実施していますか。	1	外部に情報機器等を持ち出す場合は許可をしている。
		2	**外部に情報機器等を持ち出す場合は、持出の記録を作成している。**
		3	持出しには、暗号化機能を有効にした情報機器や記録媒体を使用させている。
１５	職員が個人の USB メモリ等の許可していない外部媒体を使用していませんか。	1	医療情報システムを利用する端末には、許可していない外部媒体を接続しないように周知している。
		2	**外部媒体を接続する場合は申請が必要になる。**
		3	接続できる外部媒体を資産管理ソフト等により制限している。
１６	職員が業務に関係がないウェブサイトを閲覧していませんか。	1	業務に関係のないウェブサイトを閲覧しないように周知している。
		2	**医療情報システムの利用端末からはウェブサイトを閲**

			覧できない／閲覧できるウェブサイトを制限している。
		3	インターネットへの接続を監視するシステムを導入している。
１７	職員は、見知らぬ相手先等からの添付ファイル付きの電子メールやリンク先のクリックは注意していますか。（受信メールの信頼性を確認する、添付ファイルを開かない、安易にクリックしない等）	1	電子メールの添付ファイル・リンクのクリックに注意する等、不審なメールの取扱いについて周知している。
		2	**医療情報システムの利用端末からは電子メールを利用できない。**
		3	標的型メール訓練等による対応訓練を行っている。
１８	重要情報は電子メール本文に書くのではなく、添付ファイルに書いてパスワードなどで保護していますか。なおパスワードは別手段で知らせる、あるいは事前に取り決めておく等の手法とセットで行うこと。	1	宛先を注意し誤送信しないよう周知している。
		2	**電子メールで重要情報を送る場合は添付ファイルにパスワードを設定し、別手段でパスワードを連絡している。**
		3	メールの誤送信を防止するシステムを導入している。
１９	職員は、身に覚えのないメールや添付ファイルを開いてしまった場合は、すぐにシステム管理者へ連絡していますか。	1	不審なメールを開いた場合の連絡先を周知している。
		2	**不審なメールを開いた場合の対応手順を現場に配布している。**
		3	標的型メール訓練等による対応訓練を行っている。
２０	職員は、システムの異常があった場合、院内のどこに連絡し、相談すればいいのか知っていますか。	1	システム異常が発生した場合の連絡先を周知している。
		2	**システムの異常が発生した場合の対応手順を現場に配布している。**
		3	職員に対して、定期的にサイバーセキュリティ対策の教育を実施している。

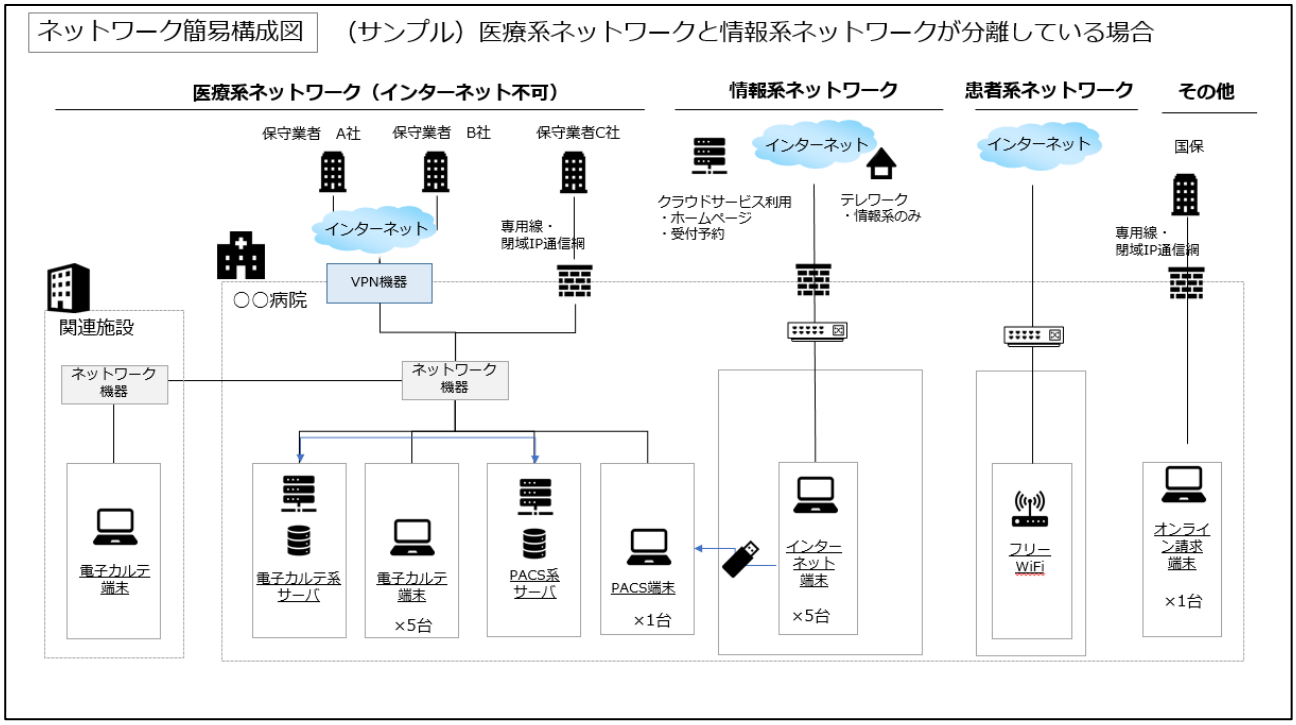
【参考３】医療情報に関する不具合発生報告書（一例）
（徳島県作成「インシデントチェックリスト」を、保団連で一部改変）

徳島県ホームページ https://anshin.pref.tokushima.jp/med/experts/docs/2023022200010/

事象発生確認年月日	年　月　日		
事象発生場所	場所（　　）　機器名称（　　） ※機器管理番号（　　） ※発生ネットワーク（　　）		
報告者	課　氏名		
発生事例パターン	1	脅迫文が表示された。	□
	2	ファイルが暗号化されて開けない。	□
	3	アカウントがロックされてパソコンにログインできない。	□
	4	医療情報システムにアクセスができない。	□
	5	普段見慣れないファイルがある。	□
	6	院内から不審なサイト等への通信を確認した。	□
	7	不審なメールや SMS 等で、クラウドサービスにログインを要求されてログイン情報を入力した。	□
	8	インターネット VPN（仮想専用線）装置に、不審なログインログがある。	□
	9	パソコン（Windows）のログインに、不審なログインログがある。	□
	10	医療情報システムのログインに、不審なログインログがある。	□
	11	医療情報システムのログインに、不審なログインログがある。	□
	12	HP の改ざんを確認した。	□
	13	不審なメールに添付されたファイルやリンク先のクリックを行った。	□
	14	メールに添付されたファイル(Excel、Word)を開いたが違和感がある。	□
	15	その他（下記に記載）	□
発生事象の詳細	（下記に記載）		
緊急措置	対象 PC の LAN ケーブル切離、無線 LAN 接続を OFF		□
	「(医療情報システム）企画管理者」へ連絡		□
	証拠保全 対象 PC や機器の電源を停止しないよう張り紙 発生事象の写真撮影、ログの取得		□
	類似事象確認		□

【参考４】ネットワーク構成図（一例）　（徳島県作成）

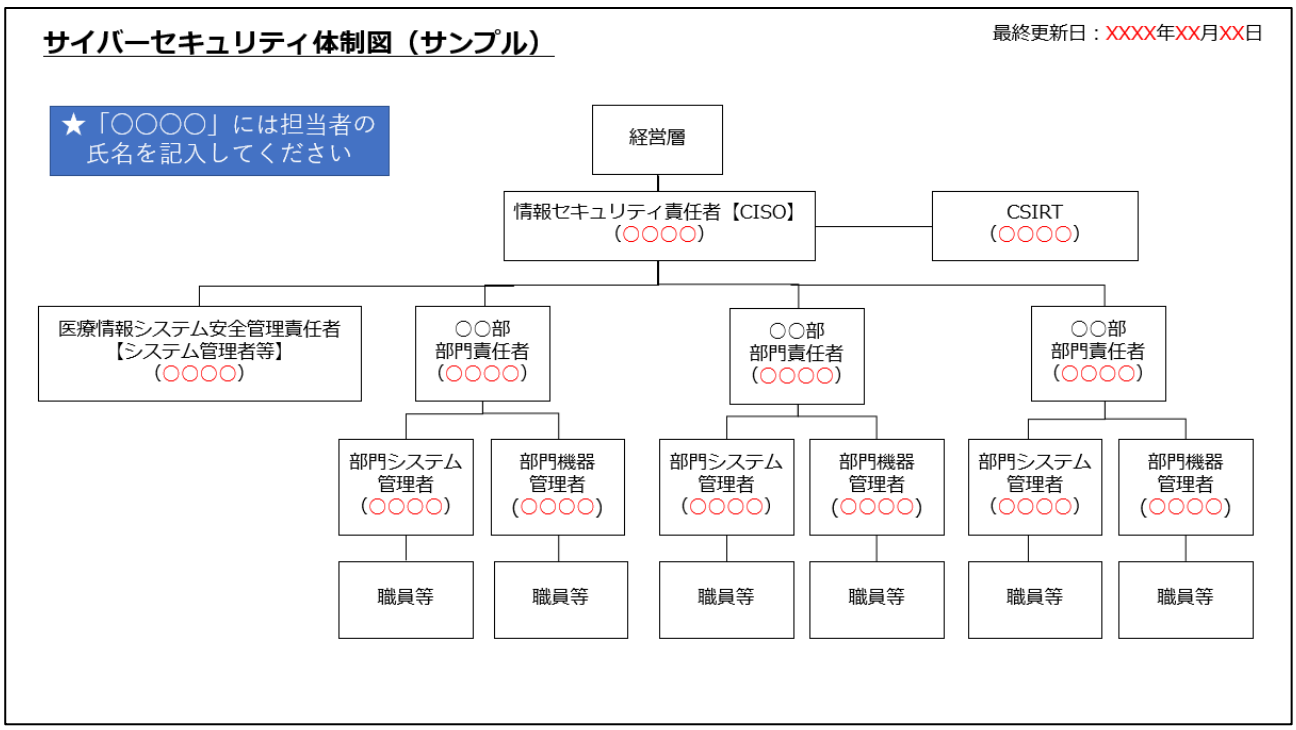
徳島県ホームページ　https://anshin.pref.tokushima.jp/med/experts/docs/2023022200010/



※ネットワーク構成図は、ネットワーク構築業者に作成を依頼してください。

【参考５】サイバーセキュリティ体制図（一例）　（徳島県作成）

徳島県ホームページ　https://anshin.pref.tokushima.jp/med/experts/docs/2023022200010/



【参考６】　職能別インシデント（非常時）対応マニュアル

Ⅰ　経営層のインシデント（非常時）対応マニュアル

１．非常時に備えたサイバーセキュリティ体制の整備

①　非常時における役割や手順を、定める（本マニュアル）。

②　委託業者の緊急連絡先や情報伝達のルート、所管官庁等の連絡先を整備する。なお、「(医療情報システム) 企画管理者」を本医院の担当窓口とする。

外部委託業者	電子カルテ	TEL:　〇〇-〇〇〇〇-〇〇〇〇 MAIL:　〇〇〇〇@〇〇〇〇.〇〇.〇〇
	サーバ	TEL:　〇〇-〇〇〇〇-〇〇〇〇 MAIL:　〇〇〇〇@〇〇〇〇.〇〇.〇〇
	〇〇	TEL:　〇〇-〇〇〇〇-〇〇〇〇 MAIL:　〇〇〇〇@〇〇〇〇.〇〇.〇〇
厚生労働省	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 TEL:　03-6812-7837　　MAIL:　igishitsu@mhlw.go.jp	
個人情報保護委員会	個人情報保護委員会（個人情報保護法第 26 条に基づく場合） https://www.ppc.go.jp/personalinfo/legal/leakAction/	
警察	都道府県警のサイバー犯罪窓口 TEL:　〇〇-〇〇〇〇-〇〇〇〇 MAIL:　〇〇〇〇@〇〇〇〇.go.jp ※都道府県警察のサイバー犯罪相談窓口（下記ページで不明な場合は都道府県警のお問合せください） https://www.npa.go.jp/bureau/cyber/soudan.html	
事後報告	独立行政法人情報処理推進機構 ①コンピュータ不正アクセス届出制度 https://www.ipa.go.jp/security/todokede/crack-virus/about.html ②コンピュータウイルス届出制度 https://www.ipa.go.jp/security/todokede/crack-virus/about.html ③ソフトウェア等の脆弱性関連情報に関する届出制度 https://www.ipa.go.jp/security/vuln/report/index.html	

③　本マニュアルを元に非常時を想定した訓練等を実施し、決めた役割や手順通りに動けるかどうか定期的に確認する。

④　他の医療機関等でサイバー攻撃等の事象を発見した場合は、サイバー攻撃の原因や対応方法等に関する情報収集を行い、対策が必要な事項を院内で共有する。

⑤　一定規模（400 床）以上の病院や、地域で重要な機能を果たしている医療機関等においては、情報セキュリティ責任者（CISO）等の設置や、初動対応体制（CSIRT 等）を整備する。

２．異常発生時の指示（対策会議の発足、被害状況の調査等）

① 「(医療情報システム) 安全管理者」からサイバー攻撃を兆候について報告を受けた後、対策会議発足の必要性を検討する。

② 被害状況の調査（対策会議を発足させる場合は、その旨も）等について「(医療情報システム) 安全管理者」へ指示をする。

３．被害発生確認後の関係省庁への報告、法的措置などの検討

① 「(医療情報システム) 安全管理者」から被害状況の報告（診療継続への影響や個人情報や機密情報等の漏えい・減失・棄損の有無等）を受け、下記の対応方針について指示を行う。(対策会議発足の場合は対策会議で検討・指示)

ア. 厚生労働省医政局への報告

イ. 所轄の地方公共団体や個人情報保護委員会への報告

ウ. 法的措置や証拠保全等

② 必要に応じて顧問弁護士やベンダ・委託事業者等へ相談する。法的措置の検討に時間を要する場合は、証拠保全や復旧対応を同時に進める。

※ 医療情報システムがサイバー攻撃(サイバー攻撃の可能性を含む) を受けた場合や、サイバー攻撃により障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案であると判断される場合は、厚生労働省医政局研究開発振興課医療情報技術推進室（下記 URL）へ連絡する。

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

４．被害からの復旧、関係省庁等への報告

⑴ 復旧計画の確認

○ 「(医療情報システム) 安全管理者」から証拠保全の結果や復旧に向けた計画、必要工数や費用等について確認する。

⑵ 被害状況等の関係省庁等への報告、法律専門家（弁護士）へ相談

① 被害状況について警察へ届出をする。

② 個人情報の漏えい、滅失又は毀損等のおそれがある場合は個人情報保護委員会や厚生労働省、所轄警察、所轄の地方公共団体等へ速やかに報告を実施する。

③ 法的措置について弁護士等の法律専門家に相談する。証拠保全の結果も踏まえて検討を進める。検討に時間がかかる場合は、再発防止の取組を先に進める。

⑶ 復旧指示

○ 復旧に向けた計画、工数、費用等を踏まえて、復旧指示を実施する。必要に応じて予算の手当を実施する。

⑷ 再発防止策

○ 「(医療情報システム) 安全管理者」からの報告を受け再発防止策の検討を指示する。

⑸ 情報公開の検討

○ サイバー攻撃の影響や被害状況・範囲等を踏まえ、情報公開の必要性を検討する。

Ⅱ.「(医療情報システム) 企画管理者」のインシデント（非常時）対応マニュアル

１．体制整備

⑴　非常時に備えたサイバーセキュリティ体制の整備

①　非常時における役割や手順を、定める（本マニュアル)。

②　委託事業者の緊急連絡先や情報伝達のルート、所管官庁等の連絡先を整備する。なお、「(医療情報システム) 安全管理者」を本施設の担当窓口とする。

③　本マニュアルを元に非常時を想定した訓練等を定期的に実施し、決めた役割や手順通りに動けるかどうか定期的に確認する。

④　他の医療機関等でサイバー攻撃等の事象を発見した場合は、サイバー攻撃の原因や対応方法等に関する情報収集を行い、対策が必要な事項を院内で共有する。

⑤　一定規模以上の病院や、地域で重要な機能を果たしている医療機関等においては、情報セキュリティ責任者（CISO)等の設置や、初動対応体制（CSIRT 等）を整備する。

⑵　全体構成図の作成

①　医院におけるシステム及びネットワークの状況を調査し、全体構成図（ネットワーク構成図・システム構成図等）及びシステム責任者一覧（設置事業者等含む）を作成し、ネットワーク構成の変更がある都度、ネットワーク構成図の更新を実施する。

②　全体構成図は、必要に応じてベンダ等の委託事業者の協力を得ながら作成する。

③　全体構成図を活用し、早期の異常を検知できるように、日常から医療情報システムの稼働状況や負荷状況、ネットワークの状況を監視・把握するとともに、侵入検知等の装置や体制を構築する。

⑶　バックアップの実施及び日常的な異常検知

①　医療情報システムおよびデータのバックアップが適切に実施されているか、定期的に確認する。

②　データバックアップについては、ランサムウェア対応になっているかどうか確認を行い、適切な世代管理（最低３世代以上）を行う。

③　医療情報システムや機器等の障害を監視し、異常等の検知を行う

２．異常事象発生時の事象確認と原因調査

⑴　医療従事者・利用者、外部業者などからの連絡に基づく異常事象の確認

○　「(医療情報システム) 企画管理者」は、医療従事者・利用者や外部業者等からの連絡に基づき、異常の事象について確認する。

⑵　原因調査

①　重大な障害がある場合、その原因がどこにあるのか調査を行う。

ア. サイバー攻撃の兆候（ＨＰの改ざんや患者情報の暗号化、データの紛失・消去・窃取、外部へまたは外部からの通信量の増加、不正ソフトウェア対策ソフト等による検知等)

イ. ベンダ等委託事業者によるメンテナンス等に起因する問題

ウ.　医療情報システム自体に起因する問題
エ.　ネットワーク機器・設備やケーブルの問題
オ.　設備の電源系統の問題
② 情報漏えい・減失・棄損や、情報持ち出しの有無についてもあわせて調査する。
③ 必要に応じてベンダ等委託事業者に協力依頼をして調査を進める。

３．原因の究明と当面の対策

⑴ ベンダ及び委託事業者等へ確認

① 障害の前日等に、医療情報システムや医療機器等のメンテナンスの実施やデータ移行等の作業実施の有無を確認する。
② メンテナンスやデータ移行等の作業実施の場合は、ベンダ等委託事業者に、前日の作業が障害の原因となっていないかどうか確認する。

⑵ ネットワーク機器やケーブル等の調査

○ 医療機関内の他のサーバ等へのアクセスが可能かどうか調査し、ネットワーク機器やケーブル等の問題がどうか調査を実施し、対象の機器やケーブルの絞り込みをする。

⑶ 電源系統、ブレーカ、ハードウェア等の調査

① 医療情報システムや機器等の起動ができるかどうか確認する。
② 起動ができない場合は電源やブレーカ等の電源系統の確認や機器自体の故障、ハードウェア自体の故障の有無やアプリケーションの状況の調査等を実施する。

⑷ サイバー攻撃の兆候がある場合

○ サイバー攻撃の可能性について、不正ソフトウェアや不正アクセスに関する技術的な相談として、情報処理推進機構（IPA)情報セキュリティ安心相談窓口（03-5978-7509）等に相談する。

４．異常事象の内容別対処方法

⑴ 不正メールの受信

① 類似メールの受信状況と反応した医療従事者等を把握する。
② 不正メールの送信元ドメインからの新たなメールの受信停止設定を行う。

⑵ 不正メールに対応し、ＩＤやパスワード等を入力してしまった場合

① 入力したＩＤやパスワードを変更する。
② 類似メールの受信状況や反応した医療従事者等を把握する。
③ 不正メールの送信元ドメインからの新たなメールの受信停止設定を行う。

⑶ 不正ソフトウェアをダウンロードした場合

① 端末のネットワークを切断する。
② ネットワーク上の接続機器のチェックを実施する。
③ 類似メールの受信状況や反応した医療従事者等を把握する。
④ 不正メールの送信元ドメインからの新たなメールの受信停止設定を行う。

⑷　端末が停止した場合、又は動作が遅い等の動作不良の状態の場合

①　ネットワークやサーバの負荷状況を確認する。

②　必要に応じてベンダ等委託事業者に協力依頼をする。

⑸　端末のデータアクセスが不良

①　端末、ネットワーク、サーバの負荷状況を確認する。

ア. 機器の電源ランプの稼働時の点滅の確認

イ. 通信量のチェック

ウ. ping による接続確認

エ. HDD ケーブルの不安定やネットワークループの発生の有無の確認

②　必要に応じてベンダ等委託事業者に協力依頼をする。

５．サイバー攻撃の可能性がある場合

⑴　経営層への報告と対策会議の発足の検討

①　サイバー攻撃の兆候がある場合は、経営層へ報告する。

②　感染の疑いがある医療情報システムや機器等の使用の中止を指示する

③　必要に応じて対策会議を発足させる。

⑵　被害状況の調査等

①　下記について調査を行う。

ア. 医療情報システムへのアクセスログの分析を行い、情報の改ざん・窃取・暗号化の有無等からサイバー攻撃（不正ソフトウェア混入等）の範囲、個人情報の漏洩・減失・棄損の有無等について調査する。

イ. 必要に応じてベンダ等委託事業者へ協力依頼して調査を進める。

②　経営層へ被害状況の調査結果について報告する。

ア. 異常発見日時

イ. 異常が発生箇所や診療への影響

ウ. 今後の被害拡大の可能性

エ. 攻撃元や攻撃手法（判明する場合）

オ. 被害発生の要因

カ. 講じうる対応策　等

６．証拠保全の実施

⑴　証拠保全

①　異常事象が発生した機器の電源を切断したり、再起動したりしない。

②　異常事象について、写真に撮る。

③　自機関及び委託業者で証拠保全が実施可能か検討し、困難な場合はベンダ等委託事業者に依頼する。（日常から複数の医療情報システムのベンダ等の委託事業者と危機対応についてコミュニケーションを取っておく。）

⑵　経営層への報告

○　経営層へ証拠保全の結果や復旧に向けた計画や工数、費用等について報告を実施す

る。

７．診療継続の判断と対応

⑴　診療継続の判断
①　診療継続の判断を行う。
②　診療継続にあたって紙カルテでの運用など、条件を検討する。
⑵　診療継続の要件の周知
○　通常の診療と異なる対応をする必要がある場合は、職員及び患者に周知する。

８．個人情報保護法対応

被害当事者となり得る患者等に、個別に通知を行う。
被害当事者の人数が多く個別通知が困難な場合は、記者会見等も考慮する。
個人情報保護法に則り、個人情報保護委員会に報告を行う。

９　復旧処理

⑴　ベンダ及び委託事業者等へ依頼
①　自機関及び委託業者で証拠保全が実施可能か検討し、困難な場合はベンダ及び委託事業者等へ依頼する。
②　証拠保存の観点からログデータのバックアップを取得する。
⑵　再設定や再インストール、バックアップデータのリストア等
①　（ベンダ等の委託事業者に）状況を確認し、バックアップを実施する。
②　不正ソフトウェア混入等の場合は、（ベンダ等の委託事業者の協力を得て、）可能であればクリーンインストールを実施する。
③　ソフトウェアに問題が生じている場合は、設定変更や再インストールで解決するかどうか（ベンダ及び委託事業者等へ）確認する。
④　再インストール後に、ソフトウェアのアップデートやバックアップデータのリストアが必要な場合は実施する。
⑶　復旧結果の確認
①　復旧処理を行った医療情報システムや機器等が正常に稼働するか否かを確認する。
②　正常に稼働することが確認できたら、医療従事者や利用者へ連絡する。

１０.事後対応

⑴　経営層への報告
○　下記について経営層へ報告する。 ア.復旧結果 イ.異常の内容、原因、被害状況、復旧にかかった工数や費用等 ウ.情報漏えいの事実の有無や範囲
⑵　再発防止策の検討・実施

① 対策会議で再発防止策を検討、実施する。 ② 再発防止策について、医療従事者・利用者へ周知する。
⑶ ベンダ及び委託事業者等の委託業者への再発防止策の指示
① 検討した再発防止策について、ベンダ等の委託事業者へその内容を周知し、委託業務への反映を指示する。 ② 定期的に委託業者の業務をチェックし、指示した再発防止策が実施できているかどうか確認する。

Ⅲ．医療従事者・利用者等のインシデント（非常時）対応マニュアル

１．体制整備

⑴　**非常時に備えたサイバーセキュリティ体制の整備**
①　非常時における役割や手順を、定める（本マニュアル）。
②　委託業者の緊急連絡先や情報伝達のルート、所管官庁等の連絡先を整備する。なお、「(医療情報システム）企画管理者」を本医院の担当窓口とする。
③　本マニュアルを元に非常時を想定した訓練等を実施し、決めた役割や手順通りに動けるかどうか定期的に確認する。
④　他の医療機関等でサイバー攻撃等の事象を発見した場合は、サイバー攻撃の原因や対応方法等に関する情報収集を行い、対策が必要な事項を院内で共有する。
⑤　一定規模以上の病院や、地域で重要な機能を果たしている医療機関等においては、情報セキュリティ責任者（CISO)等の設置や、初動対応体制（CSIRT 等）を整備する。

２．異常発生時の対応

⑴　異常事象の確認
①　医療情報システムや機器等に障害等の異常を感じた場合、サイバー攻撃の兆候（HP の改ざんや患者情報の暗号化、データの紛失・消去・窃取等）があるかどうか確認する。
②　異常事象の記録・撮影を行う。
⑵　ケーブル等の切離（電源は停止しない）
①　サイバー攻撃の兆候（HP の改ざんや患者情報の暗号化、データの紛失・消去等）がある場合は、ケーブル等の切断を実施する。
②　現場で判断が難しい場合は、不用意に電源停止や端末再起動等はしない。
⑶　「(医療情報システム）企画管理者」への連絡
○　「(医療情報システム）企画管理者」へ異常の内容、発生日等について報告を実施する。
⑷　「(医療情報システム）企画管理者」の指示に基づく、機器の使用停止
①　「(医療情報システム）企画管理者」の指示に従い、該当する医療情報システムや機器等の使用を停止する。
②　必要に応じて、目視での保険証などの確認、紙カルテによる運用等を行う。

３．再発防止

再発防止策の実施
○　「(医療情報システム）企画管理者」から周知された再発防止策について、日常の業務への落とし込みを実施するともに、定期的にチェックをする。

Ⅳ．ベンダ及び委託業者等のインシデント（非常時）対応マニュアル

１．体制整備

全体構成図の作成
○　システム・ネットワーク構成図の作成に対する協力を依頼する。

※　システムのセキュリティ管理責任者を確認する

２．異常発生時の対応

⑴　異常の原因、影響調査
○　医療情報システムや機器等に障害等の異常が発生した場合は、異常内容、影響範囲、講じうる対応策等につき調査・提案を依頼する。
⑵　連絡
①　ベンダ等の委託事業者は、医療情報システムや機器等に障害等の異常を発見した場合は、「(医療情報システム）管理者」へ異常内容、影響範囲、講じうる対応策等を報告するように求める。 ②　サイバー攻撃による被害状況の調査の支援を依頼する。 ③　障害の原因調査の支援を依頼する。

３．再発防止

⑴　再発防止策の相談
○　再発防止策の検討にあたり、相談・技術的支援を依頼する。
⑵　再発防止策の指示
①　再発防止策について、ベンダ等の委託事業者へその内容を周知し、指示する。 ②　ベンダ等の委託事業者に対し、再発防止策を委託業務に反映するように依頼する。定期的に委託業者の業務をチェックし、指示した再発防止策が実施できているかどうか確認する。
⑶　再発防止策の実施の点検
○　定期的に委託業者の業務をチェックし、指示した再発防止策が実施できているかどうか確認する。