サイバーセキュリティ対策

（担当者向け）

令和7年２月
長崎県福祉保健部医療政策課

1－1　サイバー攻撃とは

コンピュータシステムやネットワークに悪意をもった攻撃者が不正に侵入し、データの窃取・破壊や不正プログラムの実行等を行うこと。

サイバー攻撃の例

・マルウェア
・分散型サービス拒否（DDoS）攻撃
・フィッシング、SQL インジェクション攻撃
・クロスサイト スクリプティング（XSS）
・ボットネット
・ランサムウェア

1－2 過去の事例

2022年10月31日　大阪府　大阪急性期・総合医療センター

電子カルテシステムに障害が発生し、緊急以外の手術や外来診療の一時停止など**通常診療が出来ない状況**となった。

2024年5月19日　岡山県精神医療センター

電子カルテを含む総合情報システムに障害が発生。保存されていたデータのうち**最大約4万人分の患者情報等が流失**した。

甚大な被害

サイバー攻撃に対する適切な対策
サイバーセキュリティ対策

2－1 根拠法令等（医療法）

医療法第17条

第6条の10から第6条の12まで及び第13条から前条までに定めるもののほか、病院、診療所又は助産所の管理者が、その構造設備、医薬品その他の物品の管理並びに患者、妊婦、産婦及びじよく婦の入院又は入所について、遵守すべき事項については、厚生労働省令で定める。

医療法施行規則第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（サイバーセキュリティ基本法第二条に規定するサイバーセキュリティをいう。）を確保するために必要な措置を講じなければならない。

2－2 根拠法令等（通知・ガイドライン）

（1）R5.3.10付産情発0310第2号　厚生労働大臣官房等通知
「医療法施行規則の一部を改正する省令について」

（2）R5.5.31付産情発0531第1号　厚生労働大臣官房等通知
「医療システムの安全管理に関するガイドライン第 6.0 版」の策定について

（3）R6.5.13付医政参発第6号　厚生労働省医政局参事官等通知
「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（令和6年版）」
「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

（4）R6.6.6付厚生労働省医政局参事官事務連絡
「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

（5）R6.8.1付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等事務連絡
「医療機関等におけるサイバーセキュリティ対策の取組みについて（周知依頼）」

参考【厚生労働省等ホームページから入手可能な資料等】

■医療機関に対するサイバーセキュリティ対策リーフレット（令和5年10月）

URL→HTTPS://WWW.MHLW.GO.JP/CONTENT/10808000/001180153.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（令和6年5月）

URL→HTTPS://WWW.MHLW.GO.JP/CONTENT/10808000/001253950.PDF

■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（令和5年5月）

URL→HTTPS://WWW.MHLW.GO.JP/STF/SHINGI/0000516275_00006.HTML

■医療機関におけるサイバーセキュリティー対策チェックリストの実践ガイド

（公益社団法人日本医師会・会員向け冊子/2024年9月発行）

3　医療情報システムの安全管理の目的

サイバー攻撃等の情報セキュリティインシデントによる医療情報流出や不正利用を防ぐ。

→ サイバー攻撃からの医療情報システムを保護する対策
→ セキュリティインシデント発生時の速やかな対応による被害拡大の防止等

・取り扱う医療情報
病歴等の機微性の高い情報を含む個人情報

・有用性
複数の部門で同時に情報を確認できる

安全管理の必要性
一般の情報管理よりも高い水準で行われることが求められる

情報システムの3要素

- 機密性　情報資産に対し、許可された者のみがアクセスできる
- 完全性　情報資産が正確かつ完全な形で使用できる
- 可用性　情報資産に対し、許可された者が必要な時にアクセスできる

4 施設管理者の責務

（1） サイバーセキュリティ対策チェックリストの実施

令和6年度版チェックリストによる遵守項目の確認。（ｽﾗｲﾄﾞ2-2（3））

（2） 医療情報システム安全管理責任者の設置

情報ｾｷｭﾘﾃｨ方針の整備、情報ｾｷｭﾘﾃｨ対策の整備、職員研修、ｾｷｭﾘﾃｨﾘｽｸや自組織の対策の現状についての経営層への報告（ｽﾗｲﾄﾞ2-2（2））

（3） 医療情報システムの管理・運用

医療情報システムの台帳を整備し、機器の情報管理、脆弱性の改善、利用者のID・パスワード管理を行う。（ｽﾗｲﾄﾞ2−2（2）、（3））

（4） 業務継続計画（BCP）の策定等

インシデント発生時の医療情報システム復旧手順、関係機関への報告・連絡先、職員への教育・訓練等。（ｽﾗｲﾄﾞ2-2（4））

▶管理者に求められる上記内部統制等はチェックリストで確認できます。

5-1 サイバーセキュリティ対策チェックリスト

✔ 医療機関情報システム導入の有無を把握する。

👉 医療情報システムがある場合はチェックリストで確認ください。

医療機関情報システムとは・・
医療情報＊を取り扱うシステムのこと。保存システムに限らず、閲覧・取得する端末やそれらを繋ぐネットワーク機器等も含みます。
＊医療に関する患者情報（個人識別情報）を含む情報

例えば
レセコン、電子カルテ、オーダリングシステム、院内・外ネットワークシステム等

対象と考えられないもの
医療情報を含まない会計・経理システム
医療情報を含まない設備維持のためのコンピュータ等

5-2 サイバーセキュリティ対策チェックリスト

✔ 医療情報システム安全管理者を設置する。

👉 次の役割が求められています。

・リスク評価及びリスク管理方針を踏まえた情報セキュリティ方針の整備

・適切な情報セキュリティ対策の整備
（チェックリスト記載のセキュリティ対策等）

・職員等に対する定期的な情報セキュリティ研修の実施

・上記を推進していくために、経営層に対してセキュリティリスクや自組織の対策の現状について報告すること。

誰が・・
ガイドラインでは経営層が望ましいとされていますが、企画管理者（システムの企画や管理に担当する者）の兼務も可能とされています。

5-3 サイバーセキュリティ対策チェックリスト

✔ 医療情報システムについて、サーバー、端末PC、ネットワーク機器の台帳管理を行っている

👉 台帳への記載内容には次の内容が考えられます。(後頁例掲載)

- 機器の名称(モデル・製造番号など)
- 製造業者名
- ソフトウェア(バージョン含む)
- IPアドレス
- コンピュータ名
- 設置場所
- 利用者
- 登録日(購入日)など

参考 【ネットワーク機器台帳】

使用機器の一覧

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	

「令和6年度版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「マニュアル」抜粋

5-4 サイバーセキュリティ対策チェックリスト

✔ 医療情報システムについて、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に確認する。

👉 リモートメンテナンスは便利ですが、外部から侵入されるリスクも高くなります。予め、施設でリスクを把握しておきます。

✔ 医療情報システムについて、事業者から医療情報セキュリティー開示書（MDS/SDS）を提出してもらう。

👉 MDSは製造業者の、SDSはサービス業者が作成する当該医療機関におけるセキュリティー対策の状況が記載された文書です。医療情報システム事業者は、医療機関から提出を依頼された際は応じるよう、厚労省から要請を受けています。

参考 【セキュリティ開示書】

製造業者による医療情報セキュリティ開示書チェックリスト（医療情報システムの安全管理に関するガイドライン第5版対応）		回答欄	
作成日			
製造業者			
製品名称			
バージョン			
※本開示書の適合性をJIRA/JAHISが証明するものではありません。		プルダウン選択（はい/いいえ/対象外）	備考番号の入力(数字)（なし="-"）
医療機関における情報セキュリティマネジメントシステムの実践（6.2）			
1 扱う情報のリストを提示してあるか？（6.2.C1）	はい いいえ 対象外 備考 -		-
物理的安全対策（6.4）			
2 覗き見防止の機能があるか？（6.4.C5）	はい いいえ 対象外 備考 -		-
技術的安全対策（6.5）			
3 離席時の不正入力防止の機能があるか？（6.5.C4）	はい いいえ 対象外 備考 -		-
4 アクセス管理の機能があるか？（6.5.C1）	はい いいえ 対象外 備考 -		-
4．1 アクセス管理の認証方式は？（6.5.C1）			
・記憶(ID・パスワード等)	はい いいえ 対象外 備考 -		-
・生体認証(指紋等)	はい いいえ 対象外 備考 -		-
・物理媒体（ICカード等）	はい いいえ 対象外 備考 -		-
・その他（具体的な方法を備考に記入してください）	はい いいえ 対象外 備考 -		-
・上記のうちの二要素を組み合わせた認証	はい いいえ 対象外 備考 -		-
4．1．1 パスワードを利用者認識手段として利用している場合、パスワード管理は可能か？（6.5.C11(1)～6.5.C11(3)）			
	はい いいえ 対象外 備考 -		-
4．1．2 セキュリティ・デバイスを用いる場合に破損等で本人の識別情報が利用できない際の代替機能があるか？（6.5.C3）			
	はい いいえ 対象外 備考 -		-
4．2 利用者別、職種別の情報区分ごとのアクセス管理機能があるか？(6.5.C6)	はい いいえ 対象外 備考 -		-
4．3 アクセス記録(アクセスログ)機能があるか？（6.5.C7）	はい いいえ 対象外 備考 -		-

「令和6年度版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「マニュアル」等抜粋

5-5 サイバーセキュリティ対策チェックリスト

✔ 利用者の職種、担当業務別の情報区分毎のアクセス権限を設定する。

👉 どの職員が何にアクセスできるか整理し、個別にアカウントを発行。
誰が、どの情報に、アクセスできるかを決定します。

例えば・・・
電子カルテの病名入力はシステム管理者や医師のみ、
その他職種は閲覧のみとする等

👉 PWを用いた認証には、今後、多要素認証の導入・切り替えが求められています（ガイドライン：令和9年度稼働見込みのシステムから）

参考【利用者IDの一覧】

No.	所属部署	性	名	電話番号	ユーザID	説明	権限	状態
001	システム管理	abc	def	****	abc@def	安全管理責任者	Admin	使用可
002	A科	efg	hij	****	efg@hij	使用者	User	使用可
003	A科	klm	nop	****	klm@nop	使用者/退職予定	User	使用可（23年３月まで）
004	B科	qrs	tuv	****	qrs@tuv	使用者	User	使用可

誰が、どの情報に、どんなことができるかを決めて整理

使用のないｱｶｳﾝﾄは、無効化又は削除して台帳を整理する

「令和6年度版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「マニュアル」抜粋

5-6 サイバーセキュリティ対策チェックリスト

✔ 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（又は無効化）している。

👉 人事異動や退職の都度、確認し、台帳管理を行います。
アカウントの削除と無効化では意味が異なるので注意が必要。

✔ サーバーのアクセスログを管理している。

👉 アクセスログ（通信記録）を取得し、不正な利用がないことを確認します。アクセスログ機能の有無はサービス事業者に確認することで把握できます。ガイドラインでは、アクセスログの保管は1年程度が望ましいとされています。

参考【アクセスログの記録】

ユーザーID	氏名	時刻	カテゴリ	操作情報
abc@def	abcdef	2023/5/16　8:30:00	管理メニュー	ログイン
abc@def	abcdef	2023/5/16　8:30:20	管理メニュー	起動
abc@def	abcdef	2023/5/16　8:31:00	入力メニュー	起動
abc@def	abcdef	2023/5/16　8:32:00	入力メニュー	カルテ入力

1年程度保持することが
望ましい

5-7 サイバーセキュリティ対策チェックリスト

✔ セキュリティーパッチ（最新ファームウェアや更新プログラム）を適用している。

- OSやアプリケーションソフトの脆弱性が解消された最新の修正プログラム（セキュリティーパッチ）を適用し、サイバー攻撃からのリスクを低減します。

- ネットワーク機器等が最新プログラムに対応できていない、又は動作確認が取れていない場合もあるため、適用時にはサービス事業者に予め確認ください。

5-8 サイバーセキュリティ対策チェックリスト

✔ ネットワーク機器について、接続元制限を実施している。

- 外部からの不正な接続を防ぐため、ネットワーク機器の管理事業者等に接続元制限を依頼します。

  具体的には・・・

  IPアドレス・プロトコル・ポート番号の制限を行い、接続先と接続元を限定する。許可リスト方式（事前に登録した機器のみが通信できる方式）で設定・管理を行う。

- 接続元の制限が難しい場合には、多要素認証や端末認証を導入する等、高度な認証方法を利用してください。

5-9 サイバーセキュリティ対策チェックリスト

✔ 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。

- サーバ及び端末PCにおいて、必要のないソフトウェアやサービス等が動作していないか確認を行い、不要なものがある場合はソフトウェアやサービス等をシステムから削除又は停止します。

- 担当者では判断困難と考えるため、各機器やソフウェアの製造者やシステム構築事業者等に必要な設定等を相談ください。
また、インターネット上から不用意にダウンロード／インストールするのは控えてください。

5-10 サイバーセキュリティ対策チェックリスト

✔ インシデント発生時における組織内と外部関係機関への連絡体制図がある。

👉 有事に連絡や報告が必要な連絡先を連絡体制図に記載します。

主な外部関係機関・・・

- 医療情報システム事業者（レセコン・電子カルテ事業者等）
- 情報セキュリティ事業者
- 外部有識者（顧問弁護士等）
- 都道府県警察の担当部署
- 厚生労働省
- 各都道府県衛生主管部（局）
- 保険会社（サイバーリスク保険に加入している場合）
- 日本医師会サイバーセキュリティ対応相談窓口

サイバー攻撃を受けた場合、まずは下記へ連絡

1　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

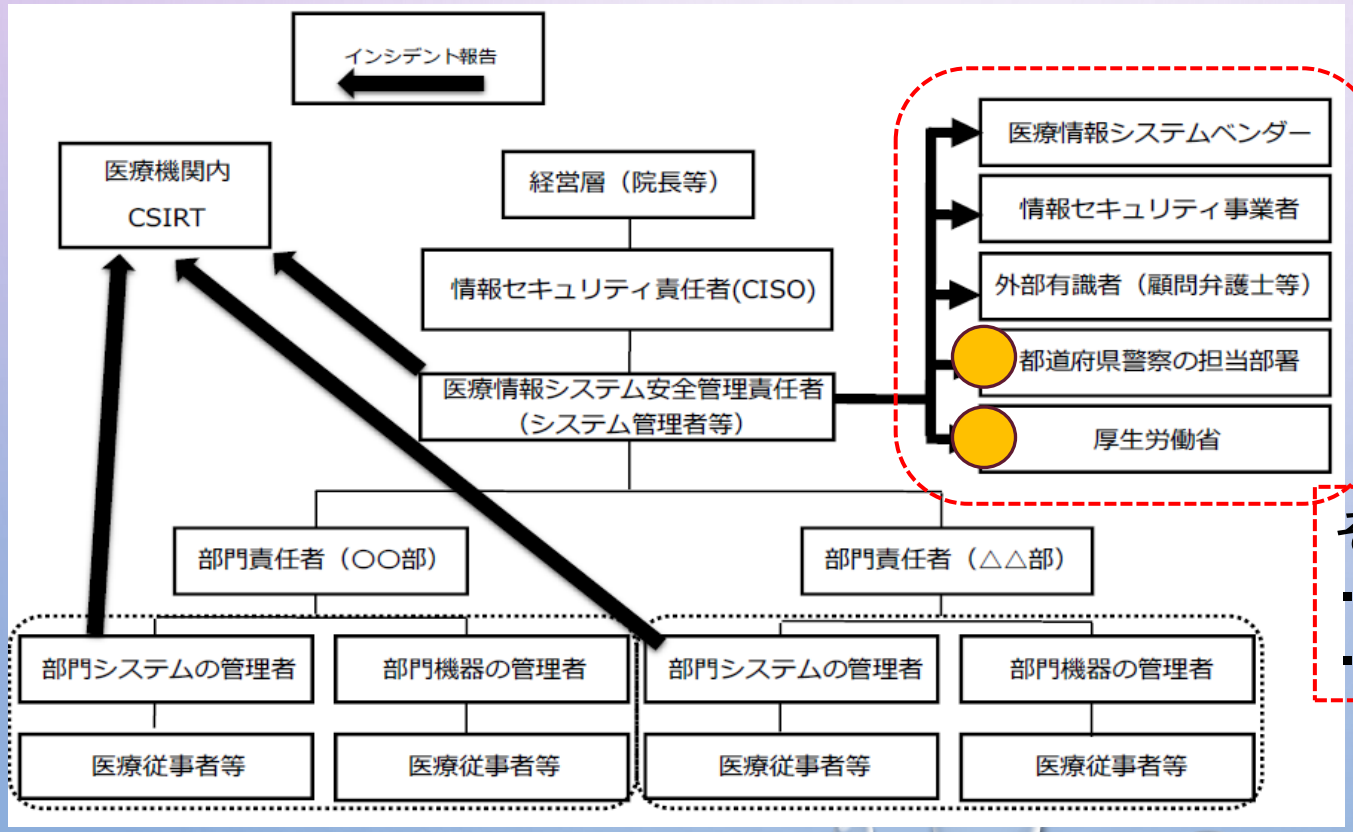
2　長崎県警察本部サイバー犯罪対策課
TEL 095-820-0110

3　管轄保健所等	連絡先
長崎県福祉保健部医療政策課	095-895-2464
長崎市保健所地域保健課	095-829-1153
佐世保市保健所保健福祉政策課医事・薬事係	0956-24-1111（代表）
西彼保健所企画調整課	095-856-0691
県央保健所企画調整課	0957-26-3304
県南保健所企画調整課	0957-62-3287
県北保健所企画調整課	0950-57-3933
五島保健所企画保健課	0959-72-3125
上五島保健所企画保健課	0959-42-1121
壱岐保健所企画保健課	0920-47-0260
対馬保健所企画保健課	0920-52-0166

参考 【連絡体制図】

厚生労働省連絡先
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

長崎県警察本部サイバー犯罪対策課
TEL 095-820-0110



その他
・長崎県医療政策課
・管轄保健所など

「令和6年度版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「マニュアル」抜粋

5-11① サイバーセキュリティ対策チェックリスト

✔ 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。

👉 医療情報システムが停止した際に、診療を継続するために必要なデータ・情報を洗い出します。

👉 バックアップは複数世代（3世代以上が推奨）取得してください。

例えば・・・日次バックアップの3世代とは「3日前時点のデータ」、「2日前時点のデータ」、「前日時点のデータ」の3つを指します。

👉 バックアップは、ネットワークから切り離した環境で異なるメディアでの保管が推奨されます。

5-11② サイバーセキュリティ対策チェックリスト

✔ 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。

👉 誰が、何を、どのようにデータ復旧を行うか整理し、復旧手順書等を作成ください。

👉 復旧時には、システム構築事業者等の支援を受け、下記対策を講じる必要があります。

- ▸攻撃時に無効にされたセキュリティ機能を復旧する。
- ▸脆弱性を特定し、是正措置を行う。
- ▸不正に作成されたり、盗まれたID・PW等は使わない等

5-12 サイバーセキュリティ対策チェックリスト

✔ サイバー攻撃を想定した事業継続計画（BCP）を策定している。

👉 自然災害時のBCPと整合性を取りながら、サイバー攻撃特有の事象を想定した対応方針や手順を文章化します。

👉 非常時の体制面
非常時の定義、役割、責任、意思決定者、報告フロー等

👉 具体的な対応
▸発生事案への対応
被害範囲の把握、証拠の保全、原因調査、NWの遮断、代替手段、監督官庁等への連絡、広報対応、法令対応等
▸業務の復旧
システム・データの復旧、バックアップ取得対応等
（参照・スライド5-11，12）

参考 事業継続計画（BCP）の策定

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３

医療情報システム部門
事業継続計画（BCP）

○○年○○月○○日　初版
○○病院
○○部門

策定したBCPの内容は後頁の確認表を用いて確認を行います。

参考
【BCP策定の確認表】

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

▶ｽﾗｲﾄﾞ2-2（4）

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。	

参考【医療情報システムに対する医療機関等の責任】

医療機関等の責任	通常時の責任	管理方法・体制等に関する説明責任
		管理及び監査を実施する責任
		定期的に見直し、必要な改善を行う責任
	非常時の責任	情報セキュリティインシデントの原因・影響等に関する説明責任
		再発防止策等の善後策を講じる責任
第三者への業務委託時の責任		適切な事業者を選定する責任 受託事業者の過失等に対する管理責任
第三者への医療情報提供時の責任		個人情報等を遵守し第三者へ医療情報を安全に提供する責任 ＊書面等により医療機関等と第三者それぞれが負う責任の範囲を明確化する

表:「医療情報システムガイドライン6.0版 経営管理編」要約

６ まとめ

医療情報システムは、利便性が高い一方で、患者さんの病歴など重要な個人情報を取り扱っています。

そのため、適切な運用・管理が行われなければ、サイバー攻撃を受けた場合、医療機能が停止するだけでなく情報漏洩等により大きな損害を招くことになります。

対策に近道はなく、医療情報システムに関する正しい情報を取得し、適切に運用・管理することが大切です。