【導入研修】
立入検査の対応に向けた
医療機関におけるサイバーセキュリティ対策研修

令和５年度医療情報セキュリティ研修 及びサイバーセキュリティインシデント発生時初動対応支援・調査等事業

（受託事業者：一般社団法人ソフトウェア協会）

本研修の流れ

長丁場になりますので、途中に休憩をはさみます。

- 第１部
  - チェックリスト導入の背景
  - チェックリストの概要
  - 令和６年度対象項目の紹介と対応に向けて
    - 2 医療情報システムの管理・運用
      - （9） 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
      - （2）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。
      - （3）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。
  - チェックリスト（組織面）
    - 1．体制構築
      - （1）医療情報システム安全管理責任者を設置している。
    - 3 インシデント発生に備えた対応
      - （1）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）の連絡体制図がある。
- 第２部
  - チェックリスト対応（技術面）
    - 2．医療情報システムの管理・運用
      - （1）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。
      - （2）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した。
      - （3）事業者から製造業者/サービス事業者によるセキュリティ開示書（MDS/SDS）を提出してもらう。
      - （4）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。
      - （5）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。
      - （6）アクセスログを管理している。
      - （7）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。
      - （8）接続元制限を実施している。
  - おわりに

*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をここでは「チェックリスト」と略します。

本研修の流れ

長丁場になりますので、途中に休憩をはさみます。

- **第１部**
  - **チェックリスト導入の背景**
  - **チェックリストの概要**
  - **令和６年度対象項目の紹介と対応に向けて**
    - **２ 医療情報システムの管理・運用**
      - **（９） 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**
      - **（２）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。**
      - **（３）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。**
  - **チェックリスト（組織面）**
    - **１．体制構築**
      - **（１）医療情報システム安全管理責任者を設置している。**
    - **３ インシデント発生に備えた対応**
      - **（１）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）の連絡体制図がある。**
- 第２部
  - チェックリスト対応（技術面）
    - ２．医療情報システムの管理・運用
      - （１）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。
      - （２）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した。
      - （３）事業者から製造業者/サービス事業者によるセキュリティ開示書（MDS/SDS）を提出してもらう。
      - （４）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。
      - （５）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。
      - （６）アクセスログを管理している。
      - （７）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。
      - （８）接続元制限を実施している。
  - おわりに

*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をここでは「チェックリスト」と略します。

はじめに

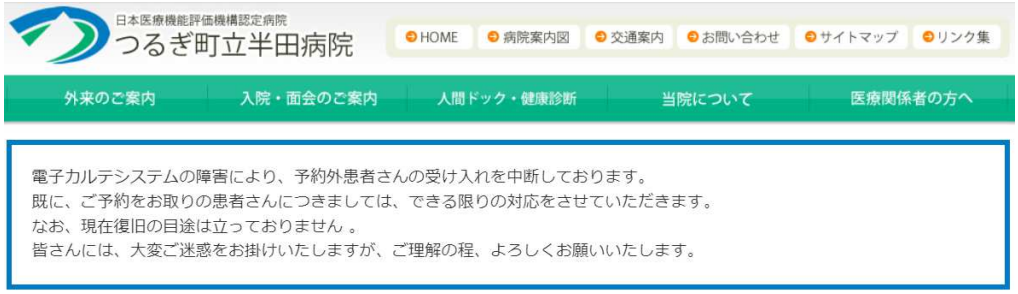
はじめに
「継続発生している医療機関でのインシデント」

- 2022年10月31日
  大阪府立病院機構
  大阪急性期・総合医療センター

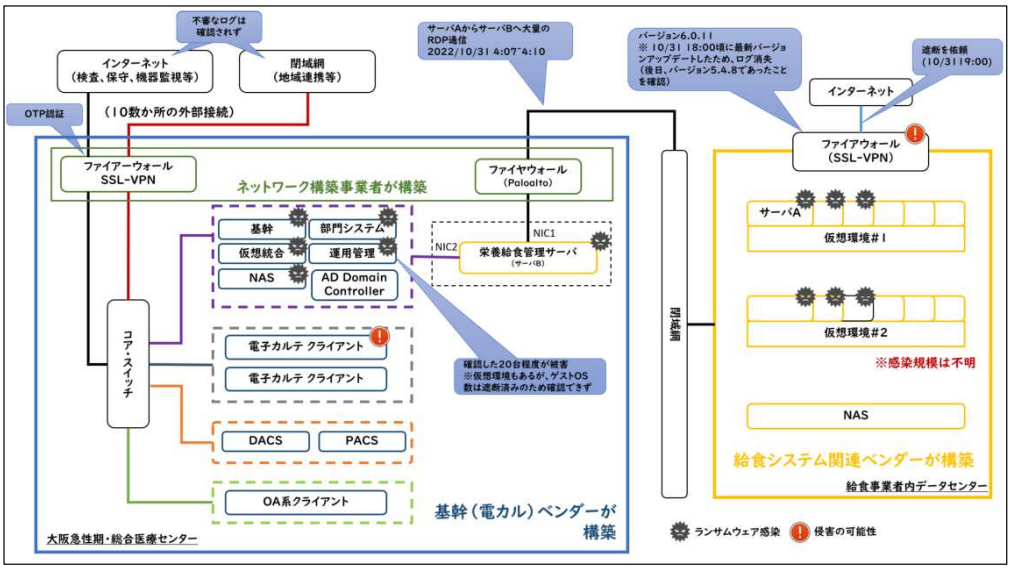
https://www.gh.opho.jp/

- 2021年10月31日
  つるぎ町立半田病院

https://www.handa-hospital.jp/



はじめに
「大阪急性期・総合医療センターのインシデント」



情報セキュリティインシデント調査委員会報告書について | 地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター (opho.jp)

はじめに

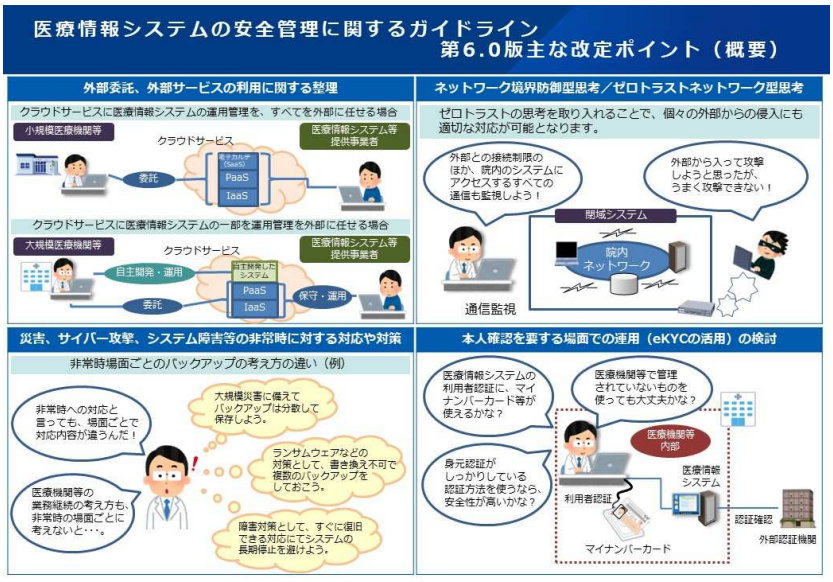
「医療機関で発生しているインシデントを受けて」

- セキュリティ教育支援ポータルサイト Medical Information Security Training（MIST）
  - 継続的なセキュリティ教育の実施
  - インシデントの通報と対応支援

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

はじめに

「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」（以下、ガイドライン）



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

はじめに

「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ついて」

- 医療機関等におけるサイバーセキュリティ対策については、ガイドラインを参照の上、適切な対応を行うこととしているところ、このうちまずは医療機関が**優先的に取り組むべき事項**をチェックリストにまとめました。また、医療機関におけるチェックリストを用いた確認の実効性を高めるために、チェックリストマニュアルを作成しました。 医療機関及び医療情報システム・サービス事業者は、本マニュアルを参照しつつチェックリストを活用して、サイバーセキュリティ対策を行ってください。

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

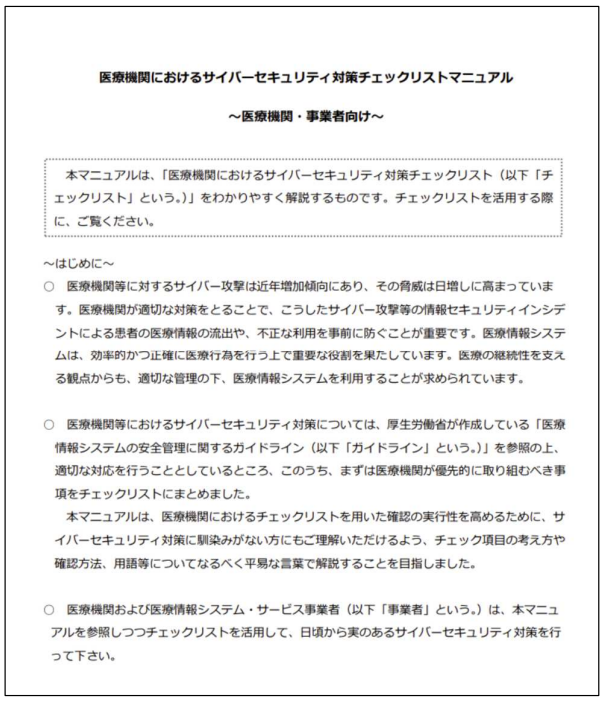
*以下項目は令和5年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*2（2）及び2（3）については、事業者と契約していない場合には、記入不要です。
*1回目の確認で「いいえ」の場合、令和5年度中の対応目標日を記入してください。

	チェック項目	確認結果 (日付) 1回目	目標日	2回目	備考
1 体制構築	（1） 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。**				
	（1） 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（　/　）	
	（2） 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（　/　）	
	（3） 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。				
	（4） 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（　/　）	
	（5） 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（　/　）	
	（6） 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。				
	（7） セキュリティパッチ（最新ファームウエ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（　/　）	
	（8） 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	（1） 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（　/　）	

はじめに

「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」

- チェックリストに対応するためのマニュアルが用意されていますので、併せてご確認ください。



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～

本マニュアルは、「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（以下「チェックリスト」という。）」をわかりやすく解説するものです。チェックリストを活用する際に、ご覧ください。

～はじめに～

○ 医療機関等に対するサイバー攻撃は近年増加傾向にあり、その脅威は日増しに高まっています。医療機関が適切な対策をとることで、こうした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患者の医療情報の流出や、不正な利用を事前に防ぐことが重要です。医療情報システムは、効率的かつ正確に医療行為を行う上で重要な役割を果たしています。医療の継続性を支える観点からも、適切な管理の下、医療情報システムを利用することが求められています。

○ 医療機関等におけるサイバーセキュリティ対策については、厚生労働省が作成している「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「ガイドライン」という。）」を参照の上、適切な対応を行うこととしているところ、このうち、まずは医療機関が優先的に取り組むべき事項をチェックリストにまとめました。

本マニュアルは、医療機関におけるチェックリストを用いた確認の実行性を高めるために、サイバーセキュリティ対策に馴染みがない方にもご理解いただけるよう、チェック項目の考え方や確認方法、用語等についてなるべく平易な言葉で解説することを目指しました。

○ 医療機関および医療情報システム・サービス事業者（以下「事業者」という。）は、本マニュアルを参照しつつチェックリストを活用して、日頃から実のあるサイバーセキュリティ対策を行って下さい。

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

はじめに
「チェックリストの準備対応について」

用意
- 医療機関は「医療機関確認用」を、事業者には「事業者確認用」を利用する。
- システムを提供している事業者ごとに確認する。なお、事業者と契約がない場合は事業者確認用を用いた確認は不要。

記入
- 「はい」または「いいえ」に〇をつけて確認した日を記入する。なお、確認しきれなかった場合は「いいえ」を記入し、対応日を記入する。（※注）

確認
- 医療機関向け、事業者向けの全てのリストを確認記入内容に相違が無いか関係者で確認を行う。
- 記入内容に相違が無いか関係者で確認を行う。

送付
- 事前送付など、保健所の指示に従い対応してください。

※注：今年度の立入検査では「参考項目」については確認対象外ですが、Ｒ６年度中には参考項目を含め、全ての項目で「はい」に○がつくように取り組んでください。

はじめに
「チェックリストの使い方」

各項目の対応状況を担当部門や事業者に確認する。

保健所の検査前に確認を行い、「はい・いいえ」を選択

確認した日を記入し、「いいえ」の場合は、目標日を記載する。

全ての項目を「はい」にするよう努める

目標日の後、2回目のチェックを各自実施する。はい・いいえを確認し、チェック日を記入する。

〇 **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 1回目 (日付)	確認結果 目標日	確認結果 2回目	備考
1 体制構築	（1） 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。**				
	（1） 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 (/)	
	（2） 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 (/)	
	（3） 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。				
	（4） 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 (/)	*注
	（5） 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 (/)	*注
	（6） 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。				
	（7） 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 (/)	*注
	（8） 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	（1） 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 (/)	

***注：一部参考項目**

はじめに
「令和6年度対応を意識した対応の準備」

- 令和5年度に含まれていない項目
  - 2 医療情報システムの管理・運用
    - （9） 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
    - （2）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。
    - （3）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。

２． 医療情報システムの管理・運用
（９） 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。
＜実施背景＞

購入した端末PCでは、業務と関係ないソフトウェアが入っていたり、動作したりしている場合があり、中にはコンピュータウイルスに関連する動作の場合もあります。

例：業務端末でのゲームアプリなど

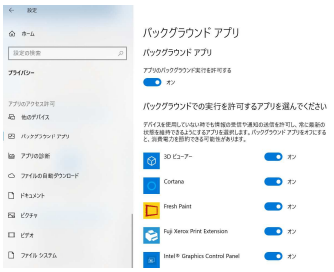
２．医療情報システムの管理・運用

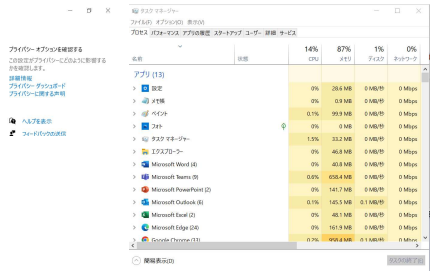
（９） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。

＜実施方法＞

Windowsの設定やタスクマネージャーなどから不要なソフトウェアが動いていないか確認し、不要なソフトウェアがあった場合は停止しましょう。

特に大規模な医療機関であれば、アプリ制御等を行い、情報部門で管理をしている場合があります。





参考：不要なアプリやプロセス

- どれが不要かは、環境にも依存するためにここでは言及することができません。
- 消去する内容によっては、コンピュータが動作しなくなる可能性があるため、インターネット等で検索を行いながら自身の環境を確認したり、販売店やシステムインテグレーター、メーカーなどに確認したりして対応を行いましょう。

3 インシデント発生に備えた対応

（２）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。

＜実施背景＞

サーバ・端末 約2300台のうち 約1300台が感染 （疑い含む） → 感染したサーバ・端末のうち詳細な調査を行う機器を選定し保全 → クリーンインストールにより再構築 （サーバ・全端末） → 部門システムや医療機器との連携接続設定 → バックアップデータをリストア → システム復旧

No	項目	概要	対応期間	稼働時期	主な診療再開状況（予定）
1	関連サーバや端末の保全	詳細調査を実施するために、また法執行機関の証拠としての保存や利用を踏まえ、感染した環境のデータを保護	11月1日～11月9日	-	・紙カルテ対応に切り替え ・DACS※の情報をもとに患者対応 ・11/4～予定手術再開
2	電子カルテ参照環境の構築	電子カルテシステムのバックアップが確認できたため、個別に電子カルテを参照できる環境を構築	11月1日～11月9日	11月10日	・患者対応を拡充 ・11/10～救急診療再開
3	電子カルテシステムの再構築	基幹システム（電子カルテ、オーダリング、医事会計）の再構築を行い、通常どおり電子カルテの参照や記事入力、オーダーができる環境を構築	11月7日～12月11日	12月中旬	・電子カルテ運用の順次再開 ・12月中旬に初診、新入院の受け入れを拡大
4	部門システムの再構築	各部門システムの再構築は、サーバ再セットアップのうえ、基幹システムとの接続やテスト等を実施し、システム全体の運用を再開できる環境を構築	11月下旬～1月上旬	順次稼働 *1月には全面復旧予定	・重要な部門システム（調剤、検査、画像、給食など）から順次連携接続を再開し診療機能を回復 ・1月に通常診療を完全復旧

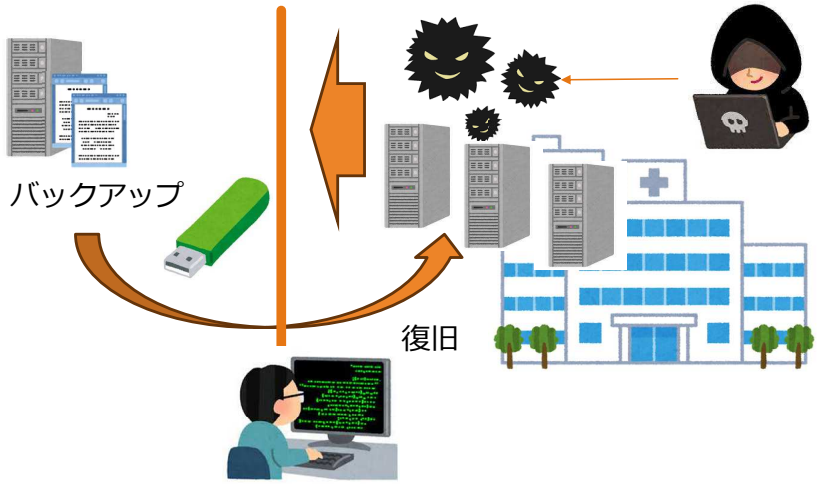
※DACS：診療記録文書統合管理システム（Document Archiving and Communication System）
作成媒体を問わず電子カルテを含めた全ての診療記録文書を統合的に管理し、文書を時系列に文書種ごとに閲覧する事が可能となるシステム

https://www.gh.opho.jp/important/785.html

3 インシデント発生に備えた対応

（２）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。

＜実施方法＞



- オンラインバックアップではサイバー攻撃によって被害が及ぶ可能性があるため、オフライン等のバックアップを検討し、実施する。
- 重要な情報はUSBなどの別の媒体に格納したり、イミュータブルバックアップなどの変更ができないバックアップを検討、実施する。
- たとえ、ランサムウェアに感染してもシステムが早期に復旧できるよう復旧手順を確認。
  - 事業者に対応方法を確認する。
  - 復旧の優先順位付けを行う。
  - 復旧手順の文書化。
- システムやデータのバックアップとしてクラウドを活用する。（なお、接続方法やタイミングには注意が必要）

3 インシデント発生に備えた対応

（3）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。

＜実施背景＞

項目	つるぎ町立半田病院 （半田病院）	大阪急性期・総合医療センター （大阪急性期C）
報告書	コンピュータウイルス感染事案有識者会議調査報告書 https://www.handa-hospital.jp/topics/2022/0616/index.html	情報セキュリティインシデント調査委員会報告書 https://www.gh.opho.jp/important/785.html
インシデント発生 （復旧までの期間）	21年10月31日～1月3日	22年10月31日～1月10日
バックアップ	オンライン	オンライン・オフライン
事業継続計画	あり	あり
演習	あり	あり

3 インシデント発生に備えた対応

（3）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。

＜実施方法＞

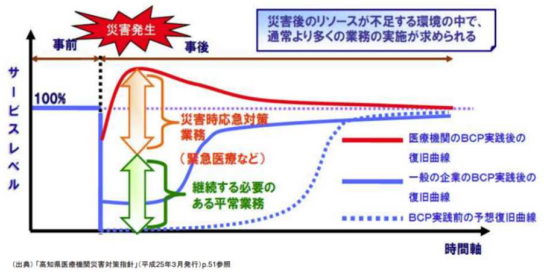
- 事業継続計画（Business Continuity Planning）とは？
  - 大規模災害等の発生時にも医療を継続的に提供できるようにするための計画です。
    2つのランサムウェア事案の学びから、BCPにサイバー攻撃を鑑みる必要があります。

作成方法については、厚生労働省が手引きを公開しています。

医療施設の災害対応のための事業継続計画（BCP）

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/kenkou/kekkaku-kansenshou/infulenza/kenkyu_00001.html

医療機関に期待されるレベルのBCP



（出典）「高知県医療機関災害対策指針」(平成25年3月発行) p.51参照

１．体制構築
（１）医療情報システム安全管理責任者を設置している。

１．体制構築
（１）医療情報システム安全管理責任者を設置している。

＜実施背景＞

医療行為は機器やシステムなしでは提供が難しい現実

システムの安全性確保のための継続的な活動

インシデント発生時の対応の中心

医療情報とは？

- 医療に関する患者情報（個人識別情報）を含む情報。

医療情報システムとは？

- 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（サーバ、端末PC（≒エンドポイント,医療機器）、ネットワーク機器）を対象。

（参考）医療情報システムとは？

- 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**を想定する。
- これには、医療情報システム・サービス事業者（※）により提供されるシステムだけでなく、医療機関等において**自ら開発・構築されたシステム**が含まれる。
- なお、**医療情報を含まない患者への費用請求に関する情報しか取り扱わない会計・経理システム等**は**医療情報システムには含まない**。

（※）医療情報システムの製造、開発、販売及び保守を行う事業者や、医療情報システムを活用したサービスの提供、保守等を行う事業者など、医療機関等が医療情報システムを利用・管理する上で関係する事業者全般を想定。

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 概説編 [Overview]
https://www.mhlw.go.jp/content/10808000/001102570.pdf

１．体制構築
（１）医療情報システム安全管理責任者を設置している。
＜実施概要・ケーススタディ＞

項目	内容
どのような人が適任か？	例えば、非常時に電子カルテシステムの停止や、ネットワークの遮断要否を判断できるような経営層が適任です。
責任者がシステムに関する知識を持っていない場合は？	前提知識を有する担当者等に上記のような対応が行える権限を委譲するか、セキュリティ研修を活用してスキルアップを図りましょう。
どのように決めたらよいですか？	経営会議や幹部会等で議論し、経営者の承認を経て、決定しましょう。
いつまでに設置したらよいですか？	早急に検討し、今年度中に決定しましょう。
外部の事業者を責任者にしても良いですか？	医療行為やシステムを理解し、病院経営を判断できるような外部事業者であれば適任ですが、相当する人物は稀だと思われます。

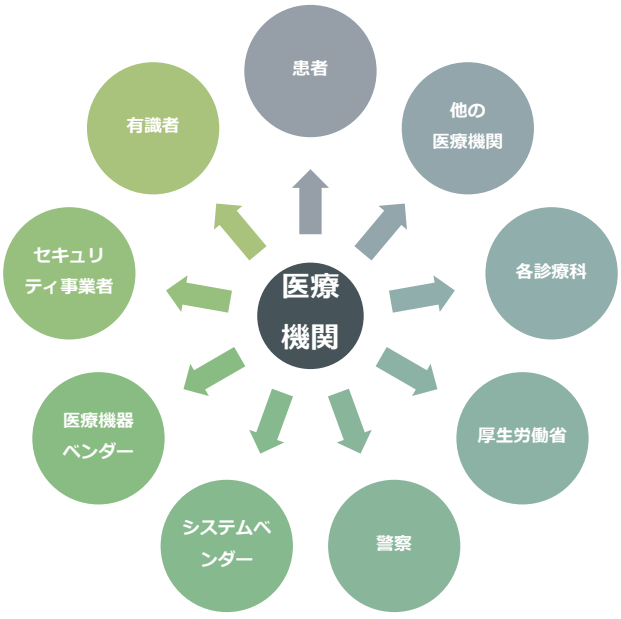
3 インシデント発生に備えた対応

（１）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）の連絡体制図がある。

3 インシデント発生に備えた対応

（１）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）の連絡体制図がある。

＜実施背景＞



インシデントが発生すると、連絡・連携するところがたくさん…

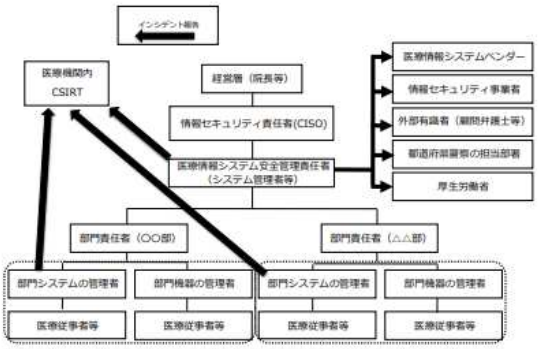
3 インシデント発生に備えた対応

（１）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）の連絡体制図がある。

＜実施方法＞

インシデントが発生すると、相当数の組織や人との連携が必要です。事前にどこに連絡をしたらいいのか連絡体制図（組織内外含む）を作っておきましょう。なお、体制図をきれいに作るよりも誰に連絡するのかを明確にして、連絡リストや院内の連絡網をきちんと整備しておきましょう。

●連絡体制図の例



*Computer Security Incident Response Team

【外部連絡リスト】

No	カテゴリ	組織名	担当者名	電話番号
1	公的機関	＊＊警察		
2		厚生労働省		
3	事業者	A社		
4		B社		
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

3 インシデント発生に備えた対応

（１）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）の連絡体制図がある。

＜参考＞

【連絡方法】

A.厚生労働省への連絡

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

B.「インシデントかも」からご連絡

（https://mhlw-training.saj.or.jp/）

ご連絡頂ければ、現場対応の支援が可能です。連絡体制に組み込んでおきましょう。

第1部 終了

本研修の流れ

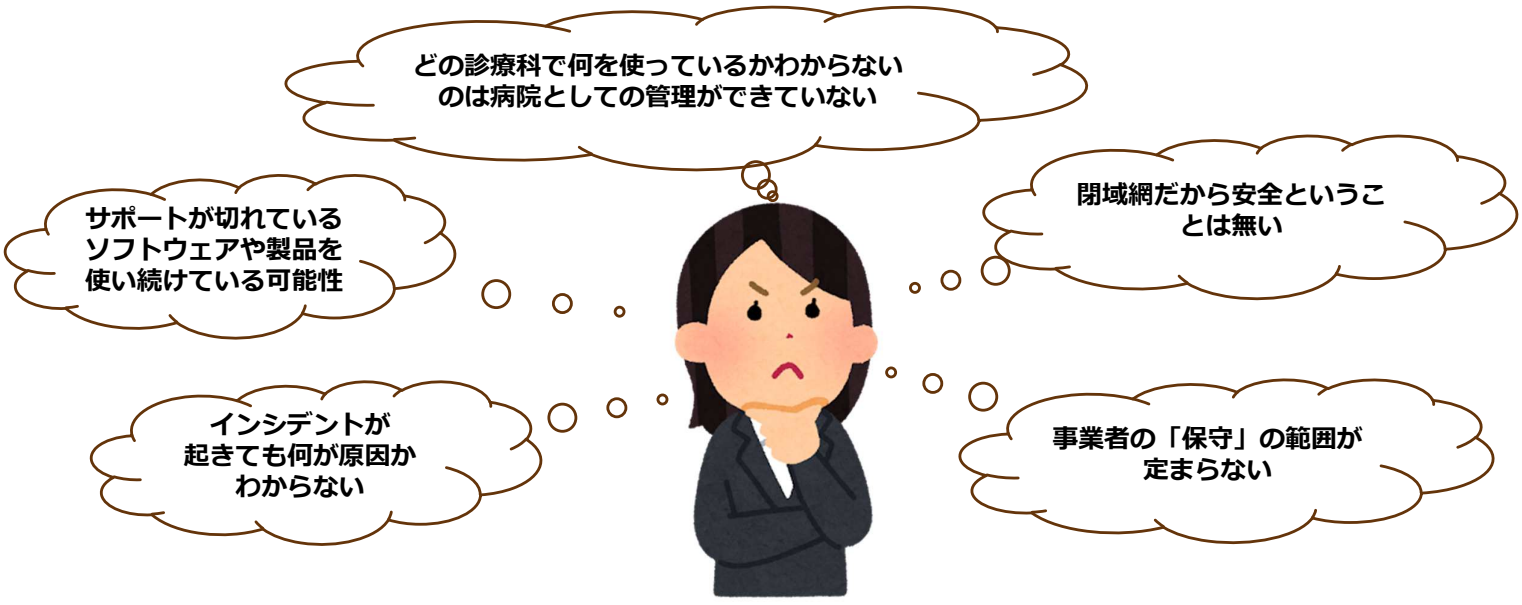
- 第１部
  - チェックリスト導入の背景
  - チェックリストの概要
  - 令和６年度対象項目の紹介と対応に向けて
    - 2 医療情報システムの管理・運用
      - （9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。
    - 3 インシデント発生に備えた対応
      - （2）インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。
      - （3）サイバー攻撃を想定した事業継続計画（BCP）を策定、又は令和６年度中に策定予定である。
  - チェックリスト（組織面）
    - 1．体制構築
      - （1）医療情報システム安全管理責任者を設置している。
    - 3 インシデント発生に備えた対応
      - （1）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）の連絡体制図がある。

- **第２部**
  - **チェックリスト対応（技術面）**
    - **2．医療情報システムの管理・運用**
      - **（1）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。**
      - **（2）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した。**
      - **（3）事業者から製造業者/サービス事業者によるセキュリティ開示書（MDS/SDS）を提出してもらう。**
      - **（4）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。**
      - **（5）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。**
      - **（6）アクセスログを管理している。**
      - **（7）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。**
      - **（8）接続元制限を実施している。**
  - **おわりに**

*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をここでは「チェックリスト」と略します。

２．医療情報システムの管理・運用
（１）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。

２．医療情報システムの管理・運用
（１）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。
＜実施背景＞



２．医療情報システムの管理・運用
（１）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。
＜実施方法＞

医療情報システムで用いる情報機器等について機器台帳を作成して管理する

- 医療情報システムで用いる情報機器とは？
  - 院内にある情報システムや機器の全て。主に電子カルテシステムに関係するサーバやPC／外部接続を行うためルータなどのネットワーク機器／医事会計システムのサーバや端末など
- 機器台帳にはどのような情報が必要なのか？
  - 機器メーカー、OS、使用しているソフトウェア（バージョン）、IPアドレス、コンピュータ名、設置場所、利用者など。
  - 利用しているクラウドサービスがある場合はその情報も書きましょう。

経営層は定期的に管理状況に関する報告を受け、管理実態や責任の所在が明確になるよう、監督・管理する

- 各医療機関における、経営会議、幹部会議、医療安全管理委員会等の経営者が集まる会議体の議題に加え、システムの稼働状況や対応状況などを確認、報告、共有を行う。

２．医療情報システムの管理・運用
（１）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。
＜ケーススタディ①＞

一部のシステムで実施できている場合は？

- 「はい」は、医療情報システムの範囲において、機器台帳が網羅的に作られている状態を示します。そのため、一部のみの対応の場合は「いいえ」を選択し、対応するため期日を記載しましょう。

ソフトウェアのバージョン情報など詳細がわからない場合は？

- 基本的には上記と同様です。ソフトウェアも含み、機器の管理を行っていく必要があります。そのため、「いいえ」を選択し、対応するための期日を記載しましょう。対応は上記同様に早期対応に向けた取り組みをお願いします。（例：OS ,Office ,Adobeなど）

全ての端末や機器の台帳は、どの範囲なのか？

- 医療情報システムの対象の端末や機器の全てです。特に優先的に対応すべき対象は、ネットワーク接続を行っているシステムや機器です。

２．医療情報システムの管理・運用
（１）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。
＜ケーススタディ②＞

事務系のシステムなどは対象範囲ですか？

- **今回のチェックリストの範囲はあくまでも医療情報システムです。なお、医療情報システム以外のシステムについては今回のチェック対象外ですが、ITガバナンス確立の観点から適切に管理・運用することが望ましいです。**

令和５年度中の対応は難しいのですが？

- **こちらは参考（一部参考）項目になっていないため、今年度中の対応をお願いします。**

定期的に経営者が管理対応を行っていることを証明するには？

- **対象の会議の議事録や機器台帳に確認したことがわかるように証跡を残しましょう。**

２．医療情報システムの管理・運用
（２）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した。

２．医療情報システムの管理・運用
（２）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した。

<実施背景>

リモートメンテナンスとは？

- 機器やシステムの保守や運用を行うにあたって、遠隔で医療情報システムに接続し、作業を行う仕組み全般のことです。

２．医療情報システムの管理・運用
（２）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した。

<実施方法>

項目	内容
何を確認するの？	２（１）の機器管理において確認した、ネットワーク機器（ルーターやセキュリティ機器等）の接続ポイント（インターネット接続、閉域網での接続等）を用いて、事業者が外部から保守しているかどうかを確認しましょう。
閉域網やインターネット環境など、外部との接続が確認できた場合は？	リモートメンテナンスがどのように行われているか確認しましょう。リモートメンテナンスしている端末は安全であるか（最新のパッチが適用され、サポート内のソフトウェアを使用し、マルウェア等の脅威検出が無いか等）、接続してくる端末を制限しているか（送信元IPアドレス制限）などを確認しましょう。
いつまでに確認したらよいですか？	早急に確認しましょう。
確認したらどうしたらよいですか？	２（１）の台帳にリモートメンテナンスの有無を明確にし、文書化しましょう。

2．医療情報システムの管理・運用
（2）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した。

<ケーススタディ>

一部のシステムで実施できている場合は？

- 「はい」は、医療情報システムの範囲において、網羅的に確認ができた状態を示します。そのため、一部のみの対応の場合は「いいえ」を選択し、対応するため期日を記載しましょう。なお、医療情報システム以外のシステムについては今回のチェック対象外ですが、ITガバナンス確立の観点から状況の把握を行い適切に管理・運用することが望ましいです。

リモートメンテンナンスの有無は確認したが、接続してくる環境が安全かわからない？

- まずはリモートメンテナンスの状況把握が最優先です。まずは、有無が確認でき文書化していれば「はい」として問題ありません。しかし、外部事業者を経由したインシデントが発生しており、安全確認は早急に行い、医療機関としての把握に努めましょう。

証跡は必要か？

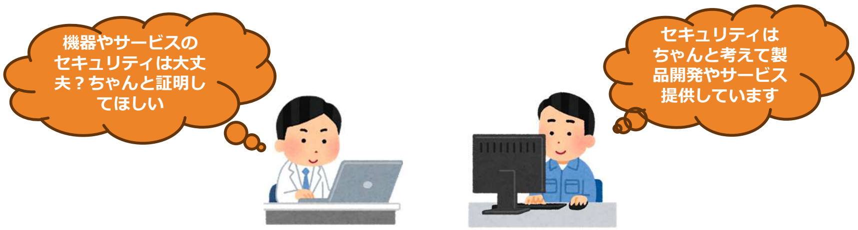
- 対象の会議の議事録や機器台帳等に確認したことがわかるように記入し、事業者からの証跡もできる限り提出をしてもらいましょう。（例：所定の申請書や接続端末のパッチ適用や検索結果画面のスクリーンショットなど）

2．医療情報システムの管理・運用
（3）事業者から製造業者/サービス事業者によるセキュリティ開示書（MDS/SDS）を提出してもらう。

2．医療情報システムの管理･運用
（3）事業者から製造業者/サービス事業者によるセキュリティ開示書（MDS/SDS）を提出してもらう。
<実施背景>

MDS/SDSとは

- 製造業者による医療情報セキュリティ開示書（Manufacturer Disclosure Statement for medical information security, MDS）、サービス事業者による医療情報セキュリティ開示書（Service provider Disclosure Statement for medical information security, SDS）を意味し、各製造業者/サービス事業者の医療情報システムのセキュリティ機能に関する標準的な記載方法を業界団体（JAHIS/JIRA）が定めたものです。



製造やサービス提供している事業者が、適切にセキュリティを実装できているか、ガイドラインに沿ったものになっているのかをまとめた文書です。
医療機関はリスクアセスメントやレビューを行いやすくすります。

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5.1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JAHIS/JIRA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　個人情報が入力・参照できる端末の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（具体的な組み合わせを備考に記入してください）	はい　いいえ　対象外	備考	-		-
4．1．1　パスワードを利用者認証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.C13(1)～(5))	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　利用者の職種・担当業務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	-		-
4．3．1　アクセスログを利用者が確認する機能があるか？(6.5.C7)	はい　いいえ　対象外	備考	-		-
4．3．2　アクセスログへのアクセス制限機能があるか？(6.5.C8)	はい　いいえ　対象外	備考	-		-
5　時刻情報の正確性を担保する機能があるか？(6.5.C9)	はい　いいえ　対象外	備考	-		-
6　不正ソフトウェア対策を行っているか？(6.5.C10)	はい　いいえ　対象外	備考	-		-
7　無線LANを利用する場合のセキュリティ対策機能はあるか？(6.5.C14)	はい　いいえ　対象外	備考	-		-
情報及び情報機器の持ち出しについて(6.9)					
8　ソフトウェアのインストールを制限する機能があるか？(6.9.C9)	はい　いいえ　対象外	備考	-		-

JAHIS**「製造業者による医療情報セキュリティ開示書」**
https://www.jahis.jp/standard/detail/id=565

2．医療情報システムの管理･運用
（3）事業者から製造業者/サービス事業者によるセキュリティ開示書（MDS/SDS）を提出してもらう。
<実施方法>

- **医療情報システムについてセキュリティが適切に実装されているか、MDSやSDSの提出を求めましょう。**

２．医療情報システムの管理・運用
（３）事業者から製造業者/サービス事業者によるセキュリティ開示書（MDS/SDS）を提出してもらう。

<ケーススタディ>

全てのMDS/SDSは入手できていないのですが？

- **「はい」は、全てのMDS/SDSが提出されている状態を示します。そのため、「いいえ」を選択し、提出を求めていきましょう。**

提出はされているのですが、適切に記入されていない気がするのですが？

- **なぜ記入が行えていないのか事業者に確認しましょう。特に空欄の場合はその理由を確認しましょう。なお、医療機関での対応が難しい場合は、対象の事業者に限らず提供事業者側の団体などにも相談や共有をしましょう。**

事業者に求めても提出してくれないのですが？

- **継続的に提出を求めていきましょう。それでも提出されない場合は、提供事業者の団体などにも問い合わせをしてみましょう。**

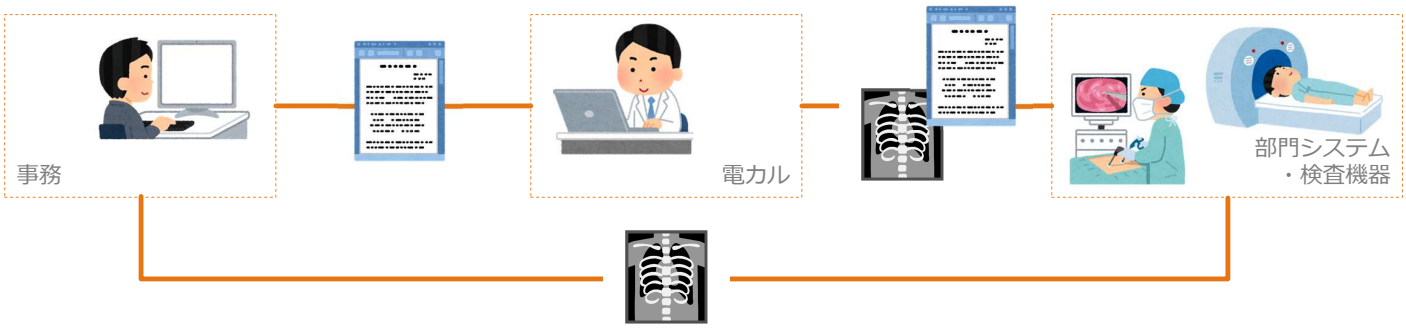
２．医療情報システムの管理・運用
（４）利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。

2．医療情報システムの管理・運用

（4）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。

<実施背景>

誰でも医療情報や病院情報にアクセスできる環境だったら？



システム利用で大切なことは、アクセス制御や権限管理、
きちんとアクセス時に認証・認可する仕組みがあるか否か。

2．医療情報システムの管理・運用

（4）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。

<実施方法>

誰が、どの部署が、情報にアクセスする権限があるのかを確認、設定、規程化する

- **例示：安全管理責任者、管理者、一般使用者、参照者など**

利用者台帳などを作成し、管理をする

- **例示**
  - **Active Directoryなどの組織のシステム管理者が使用者を管理するためのシステムや技術を用いて設定する。**
  - **資産管理ツールなどを用いて管理を行う。**
  - **マニュアルにある最低限の台帳を作る。**

※令和5年度は端末PC（エンドポイント）は参考項目です。

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
・	・	・	・	・	・	・	・	・

２．医療情報システムの管理・運用

（４）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。

<ケーススタディ>

システム上、管理者や使用者を分けているが規程がない

- 規程が無い場合、適切に運用できているか判断基準がない状況です。そのため、誰にどのような権限を付与するのか。誰ならどの情報にアクセスすることができるのか。まずは簡易的でもいいので、規程を作成しましょう。そのため、「いいえ」を選択し、対応する期日を記載しましょう。

規程や設定はできているが、定期的な確認や棚卸、経営者への報告が行えていない

- 定期的にアクセス状況や棚卸を行うようにしましょう。最初に導入したまま見直しや対応が行えていない場合は「いいえ」を選択し、現状確認から経営者への報告・承認までを期限を決めて実施しましょう。

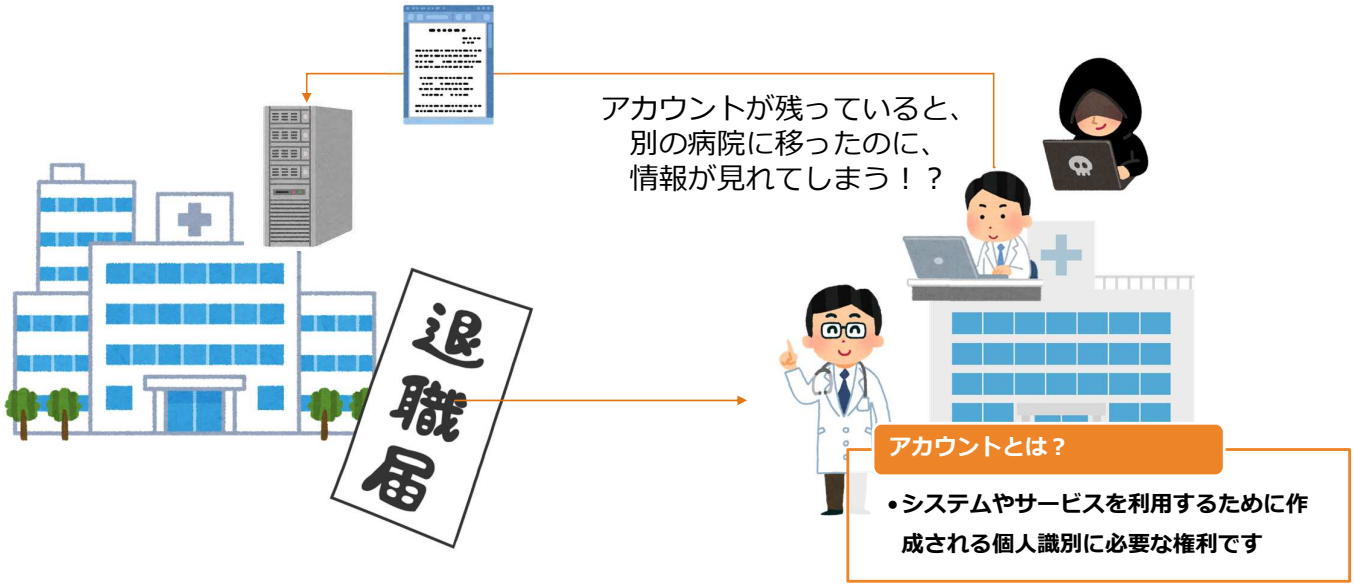
事業者に委託しているため、管理状況がわかりません

- 契約形態にもよりますが、基本的には医療機関が医療情報システムを使用していることに変わりはありません。自院の状況を事業者に確認し、対応状況を把握し、規程の作成やセキュリティ設定の強化などに努めましょう。

２．医療情報システムの管理・運用

（５）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。

2．医療情報システムの管理・運用
（5）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。
<実施背景>



2．医療情報システムの管理・運用
（5）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。
<実施方法>

- ２（４）の情報を参考にし、使用していないアカウントと不要なアカウントを削除しましょう。

アカウント	種類	概要
中/大規模組織	管理者	パソコンやシステムを管理する権限者（Administrator）
	標準ユーザー	パソコンやシステムに影響しない範囲での変更や利用を行える利用者
小規模組織/個人	Microsoftアカウント	インターネット接続を行ってサービスを利用する利用者
	ローカルアカウント	パソコン上でアカウントを作成し、サービスを利用する利用者

※令和5年度は端末PC（エンドポイント）は参考項目です。
つまり、特にサーバ側のアカウントやエンドポイントでも管理者として運用されていないか確認しましょう。

２．医療情報システムの管理・運用
（５）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。
＜ケーススタディ＞

削除はできていないが、無効化はしているが？

- 無効化できていれば、「はい」を選択いただいて、問題ございません。

以前対応したが、最近は確認できていないのですが？

- 退職者などの組織に関係のないアカウントを残しておくことは健全ではありません。「いいえ」を選択し、定期的な確認及び体制確立に向けた対応を行いましょう。

退職者ではあるが、患者や業者の連絡や引継ぎの関係上、残しているが？

- 退職者のアカウントを残しておくことは組織としてはあまり健全ではありません。早期にアカウントを削除するための対応を行いましょう。

２．医療情報システムの管理・運用
（６）アクセスログを管理している。

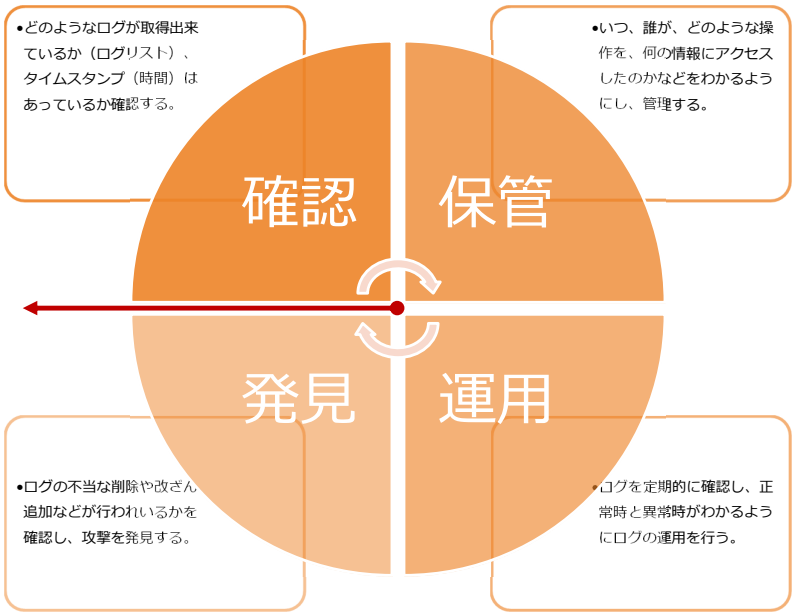
2．医療情報システムの管理・運用
（6）アクセスログを管理している。
<実施背景>

アクセスログとは？

- PCやサーバまたはアプリケーションやデータへの接続履歴のことをいう。Windowsのイベントログや端末の操作ログ、Active DirectoryサーバやWebサーバへの接続履歴なども含められる。

誰が何をしていたのか、どこを出入りしたのかなどを把握できないと、
通常利用なのか、攻撃者による侵入なのか判断できません。

2．医療情報システムの管理・運用
（6）アクセスログを管理している。
<実施方法>



定例会などで定期的に検出状況を確認し、アクセスログの「管理」をしましょう。

各機器でどのようなログがとれるか確認
「ログリスト」
↓
定常的に取得できるログによる報告
（例：FW、AD、資産管理ツールなど）

●アクセスログの例

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
abc@def	abcdef	2023/5/17 12:30:00	管理メニュー	ログオフ
ghi@jkl	ghijkl	2023/5/17 8:40:00	管理メニュー	ログイン
ghi@jkl	ghijkl	2023/5/17 8:40:30	管理メニュー	起動
ghi@jkl	ghijkl	2023/5/17 8:45:00	管理メニュー	ログオフ
・	・	・	・	・

2．医療情報システムの管理・運用
（6）アクセスログを管理している。
＜ケーススタディ＞

アクセスログと言っても様々あるが、どのレベルで管理できていれば良いのか？

- 医療情報システムに不正なアクセスや操作が無いかログを確認し、追跡できる状況であれば、「はい」を選択して問題ありません。しかし、ログリストなどを作成し、どのようなログが取れているのかを整理し、組織としての管理体制の確立を目指しましょう。またログの保存期間についてはできる限り長く残すことを推奨します。

ログは取れているはずだが、見たことがない？

- アクセスログを管理できている状況とは言えません。適切な運用が行われているか事業者とも協議しながら確認し、何のログが取得できているのか、どのような運用状況なのかなど確認し、ログの管理体制を確立しましょう。

全てのシステムでは実施てきていない？

- 医療機関としてログが管理できる状態（＝サイバー攻撃の予兆や発生を検知できる状況）とは言えないため、その状態を目指し対応を行いましょう。

アクセスログはベンダーに依頼しないと解析できない？

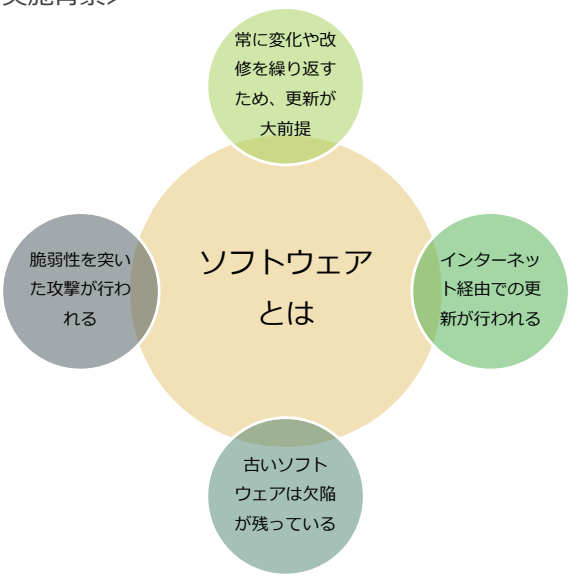
- どのような契約になっているのか、ログを入手することができないのか改めて確認しましょう。万が一、ログをベンダーから取得し管理することができない場合は、どのようなログを取得し、インシデント発生時にどのような対応を行うのか。インシデントの予兆はどのように伝えてくれるのか。ログ対応に生じる費用はいくらなのかなど、事前に確認しておきましょう。

2．医療情報システムの管理・運用
（7） 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。

2．医療情報システムの管理・運用

（７） 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。

＜実施背景＞



＜閉域網神話が招いている現実＞

・ソフトウェアの更新が行われていない。

・セキュリティ対策ソフトのルールや定義ファイルが更新されていない。

・侵入されてしまったら攻撃が拡大しやすい。

2．医療情報システムの管理・運用

（７） 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。

＜実施方法＞

台帳を用いて、全ての端末やシステム、機器等のソフトウェアおよびそのバージョン情報などを確認する。

サポート切れのソフトウェアを使用していないか、事業者に確認をする。

できる限り、最新のソフトウェア更新する。サポート内ソフトウェアであることは必須。

規程を確認し、規程通りの運用が行えているか。行えていない場合は、規程を作成または項目を追加しましょう。

※令和5年度は端末PC（エンドポイント）は参考項目です。
今年度は特にネットワーク機器やサーバの構成情報を確認しましょう。

２．医療情報システムの管理・運用
（７） 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。
<ケーススタディ>

一部のシステムで実施できている場合は？

- **「はい」は、医療情報システムの範囲において、網羅的に確認ができた状態を示します。そのため、一部のみの対応の場合は「いいえ」を選択し、対応するため期日を記載しましょう。なお、医療情報システム以外のシステムについては今回のチェック対象外ですが、ITガバナンス確立の観点から状況の把握を行い適切に管理・運用することが望ましいです。**

セキュリティパッチが適用できないといわれたら？

- **なぜ適用できないかを確認し、台帳や議事録等に理由や受容しているリスクを把握しましょう。また、契約面での課題も考えられるので、現状の運用・保守契約がどのようになっているのか確認し、運用・保守の理解を事業者と共通認識を持つようにしましょう。なお、厚生労働省からの通達やガイドラインの通り、ソフトウェア更新を行うよう促していますので、ガイドラインへの順守を含め事業者に対応を求めていきましょう。**

どれくらいの頻度で更新を行っていたら適切なのか？

- **可能な限り、常に最新のものへの更新が必要です。参考として、主たる定義ファイルの更新はセキュリティメーカーは１日１回程度公開され、またパッチ対応はPCI DSS*を例とする1か月以内の適用とされています。**

*PCI DSSとは、クレジットカードのシステムを安全に運用するためのガイドラインです。

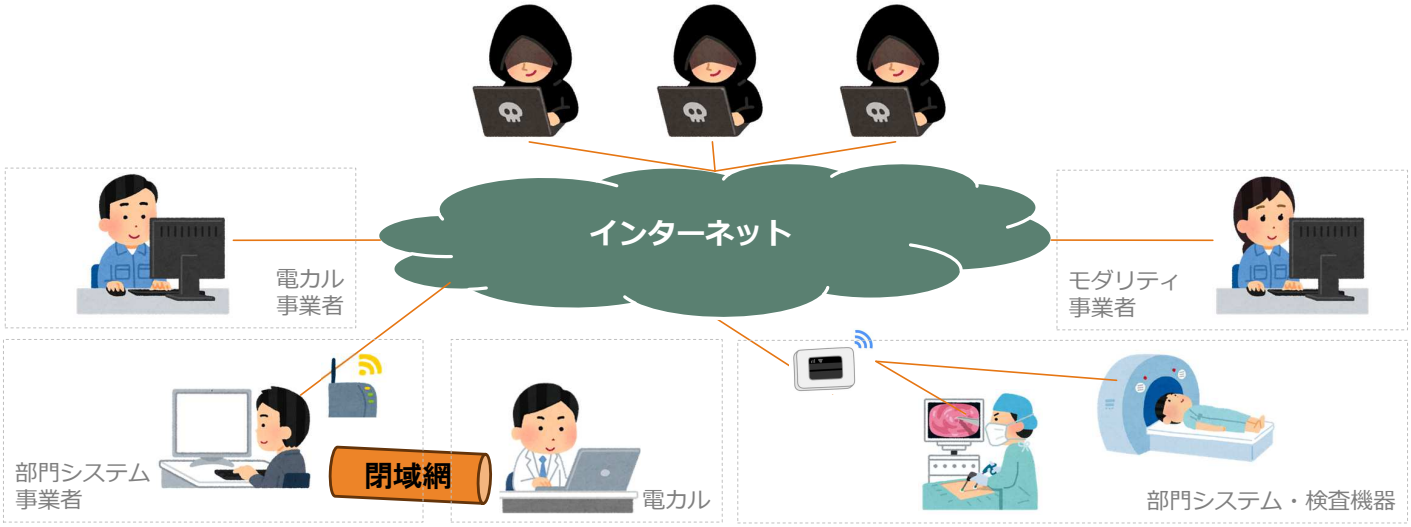
２．医療情報システムの管理・運用
（８）接続元制限を実施している。

2．医療情報システムの管理・運用

（８）接続元制限を実施している。

＜実施背景＞

誰でもアクセスできる状況だと、攻撃者もアクセスできてしまう…



2．医療情報システムの管理・運用

（８）接続元制限を実施している。

＜実施方法＞

ファイアウォールなどを用いて、接続できるIPアドレスを限定する。
（送信元アドレス制限）

特定の地域（国内）のアドレスからしかアクセスできないようにする。
（ジオブロック（地域制限））

無線LANのセキュリティ対策を行う。
（MACアドレス認証,IEEE802.1x認証など）

2．医療情報システムの管理・運用
（8）接続元制限を実施している。
<ケーススタディ>

一部のシステムで実施できている場合は？

- 「はい」は、医療情報システムの範囲において、網羅的に確認ができた状態を示します。そのため、一部のみの対応の場合は「いいえ」を選択し、対応するため期日を記載しましょう。なお、医療情報システム以外のシステムについては今回のチェック対象外ですが、ITガバナンス確立の観点から状況の把握を行い適切に管理・運用することが望ましいです。

制限を行うのにさらに費用が必要と言われた？

- 運用・保守上の設定変更の範囲内と考えられるため、事業者と話をしましょう。

事業者から制限されると困るといわれた？

- なぜ困るのか確認した上で、病院としての方針を定め、伝えましょう。外部接続を許すことはそれだけリスクや管理が複雑化することになることを理解した上で対応しましょう。

おわりに

医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）（令和４年11月10日）

医療機関のサイバーセキュリティ対策について、自治体を通じて医療機関等へ注意喚起しております。

１．サプライチェーンリスク全体の確認

２．リスク低減のための措置

３．インシデントの早期検知

４．インシデント発生時の適切な対処・回復

５．金銭の支払いに対する対応

６．ランサムウェア特設ページ

https://www.mhlw.go.jp/content/10808000/001079508.pdf

医療機関向けサイバーセキュリティ対策研修等について

- 2023年９月の立入検査対策用のセキュリティ研修を皮切りに、経営者、システム・セキュリティ管理者、初学者等を対象にした研修。
- 加えて、導入研修では大阪急性期Cのインシデントに関する事例勉強会を実施。
- 経営者やシステム・セキュリティ管理者向けには、大阪急性期Cの現地視察会を実施。
- e-learningによる継続的な教育、アーカイブ配信等による振り返り等が可能。

研修種別	受講対象	実施方法	研修概要
導入研修（9月研修開始）	医療機関等の従事者	オンライン	立入検査の項目に含まれたサイバーセキュリティの対応・対策に向けた医療機関におけるサイバーセキュリティチェックリストに基づいた研修
			2023年3月末に公開された大阪府立病院機構　大阪急性期・総合医療センターの「情報セキュリティインシデント調査委員会報告書」をベースにインシデントの内容、発生原因、対策、BCPの見直し等について学習
初学者等向け研修（10月研修開始）	サイバーセキュリティの基礎知識を習得したい方	オンライン	サイバーセキュリティインシデントが身近であることを認識頂くとともに、システムや端末を使うにあたって、自分たちで今すぐできる備えなどについて学習
		ワークショップ	「今、実施しているセキュリティの工夫」「セキュリティの悩み」等をテーマにグループ単位で議論し情報共有を行う
経営者向け研修（10月研修開始）	医療機関等の経営に携わる方	オンライン	つるぎ町立半田病院、大阪府立病院機構　大阪急性期・総合医療センター等のインシデント事例、経営者として必要なサイバーセキュリティの意識と知識について学習
		ワークショップ	「自組織の経営とセキュリティの考え方」「セキュリティでできていること、できていないこと」等をテーマにグループ単位で議論し情報共有を行う
		現地視察	大阪府立病院機構　大阪急性期・総合医療センターの視察およびインシデントの概要、ITガバナンスの重要性について学習
システム・セキュリティ管理者向け研修（10月研修開始）	医療機関等のシステム・セキュリティ管理する方	オンライン	現在あるIT資産を活用したセキュリティ対策について学習Active Directory（AD）入門、認証・認可や特権管理の重要性などについて学習
		演習	インシデントレスポンス対応、マルウェアの感染体験やログ調査などの演習
		現地視察	大阪府立病院機構　大阪急性期・総合医療センターの視察およびインシデントの概要、インシデント対応の勘所について学習
e-learning	医療機関等の従事者	WEB	情報セキュリティの基礎、サイバー攻撃手法、インシデントレスポンス等の基本コンテンツ他、各研修の動画をアーカイブとして配信

※研修内容等については、変更される場合がございます。詳細は本事業のポータルサイト（MIST）をご確認ください。
※アーカイブ形式の実施を一部予定しております。

最後に

クラウド環境を利用している場合は？

- クラウド環境利用にあたっても「使用許諾」などの契約が存在します。ログ管理やインシデント発生時の対応など、使用許諾の確認とサービス事業者にチェックリストに基づく確認を行いましょう。

サプライチェーンの情報資産も対応しないといけないの？

- 現時点では医療機関のシステムが対象です。しかしながら、サプライチェーン経由での攻撃も発生しているため、取引のある事業者がどのようなセキュリティ対応を行っているのかは定期的に確認するようにしましょう。

現状のセキュリティ対策が行き届いていない？

- これまでの「閉域網だから大丈夫」という考え方を見直し、セキュリティの強化に努めましょう。

ありがとうございます