令和6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　（一般社団法人ソフトウェア協会）

【立入検査研修】 準備コース

BC Signpost株式会社
松山 征嗣

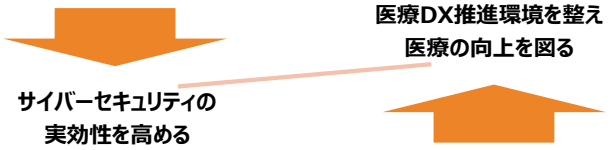
立入検査研修
目次

準備コース

- チェックリスト概要
- チェックリストのマニュアルについて
- チェックリストの進め方
- 「医療情報システムの有無」について
- 用語解説

「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、「医療情報システムの安全管理に関するガイドライン」を参照の上、適切な対応を行う必要があります。
- このうち医療機関が**優先的に取り組むべき事項**をチェックリストとしてまとめられています。
- このチェックリストによってサイバー攻撃を回避できると約束されるものではありません。
- 令和５年度より、本チェックリストが医療法第25条第１項に基づく立入検査においてサイバーセキュリティ確保のために必要な取組を行っているかの確認に使用されています。



医療情報システムの安全管理に関するガイドライン
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
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マニュアル」

- 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が作成、公開されています。
  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。

- 令和６年度版でチェックリストおよびマニュアルが更新されていますので見落としが無いようご注意ください。

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

チェックリストの準備対応、進め方

用意

- 医療機関は「医療機関確認用」を使用してください。事業者には「事業者確認用」への記入を求め、回収してください。
- 「事業者確認用」については、事業者との契約がない場合は不要です。

記入

- 「はい」または「いいえ」に〇をつけて確認した日を記入してください。
- 確認しきれなかった場合は「いいえ」とした上で、対策に係る令和６年度中の目標日を記入してください。
- チェック項目の対象となるものが無いことが明らかな場合は、「いいえ」とした上で、備考に対象外と明記してください。

確認

- 回収した事業者向けの全てのリストを確認し、記入内容に相違が無いか確認してください。
- 医療機関確認用における回答は各項目それぞれについて施設全体を総合してください。

提出

- 提出方法は所管保健所の指示に従い対応してください。

チェックリストの掲載先

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

シートの用意

医療機関は「医療機関確認用」を、事業者には「事業者確認用」を使用してください。
それぞれPDF版とExcel版が公開されていますので、使用、管理しやすい方をお使いください。

システムを提供している事業者ごとに確認、協力を求めてください

「事業者確認用」については、事業者との契約がない場合は不要です。

事業者の皆様は医療機関からの協力要請に対してご協力をお願いします

Excelシートの場合は施設、事業者毎にファイルを作成してください。
PDFの場合は施設、事業者毎に印刷し、記入してください。

シートの記入

少なくとも年1回はチェックリストを用いた点検を行なってください。

「はい・いいえ」を選択し、確認日を記入してください。

「いいえ」の場合は、チェック項目内容を満たす「目標日」を記入してください。

全ての項目を「はい」にするよう努めましょう

※令和５年度から確認されている項目

各項目の対応状況を担当部門に確認し、総合して評価してください。

多数の事業者からシステム提供を受けている場合は、医療機関として全体を総合して評価してください。

目標日の後、2回目のチェックを各自実施してください。

はい・いいえを確認し、チェック日を記入してください。

確認

証跡は必要か？

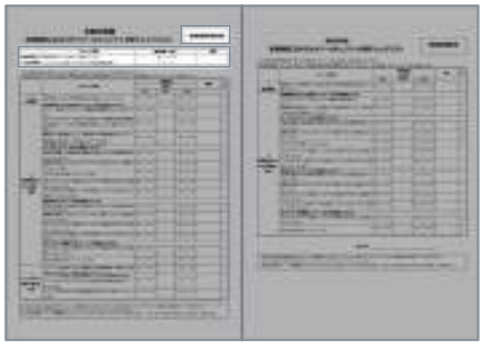
- 回答の根拠となる文書やデータを求められれば提示できるように準備しておきましょう。

一部のシステムで実施できていない場合は？

- 「はい」は、医療情報システムの範囲(後述)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。
- 備考欄には「いいえ」となっている理由について記載してください。

事業者から提出されてこない場合は？

- 回答が得られない理由をメールや文書などで求めてください。



医療情報システムの有無

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。

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）、ネットワーク機器等を含む。

システムの例

- レセコン
- 電子カルテ
- オーダリングシステム

マニュアルにも例示

- 調剤システム、臨床検査システム等、各種部門システム
- PDI作成装置、インポート装置
- 各種撮影装置、検査装置（※）
- レポートシステム、遠隔画像診断システム

医療情報が発生するもの
医療情報を参照するもの

- オンライン資格確認端末
- 医事会計システム
- 予約システム
- 受付機・精算機
- 受付案内表示システム

患者の個人情報、
患者個人識別情報に紐づくもの

- これらシステムを構成する機器およびそこで動作するソフトウェアは全て安全管理の対象です
- インターネットへの接続の有無は関係ありません
- 製品化されたシステムではなく、内製したシステムや、汎用のソフトウェアなどを使用して医療情報を扱う業務を行っている場合も対象となります
  - PC
  - サーバ
  - ストレージ
  - テープ装置、外部ディスク装置
  - タブレット、携帯端末
  - モニター
  - ネットワーク機器（ファイアウォール、スイッチ、ルータ、VPNルータ　等）

※薬機法上の「管理医療機器」であっても、サーバや他の端末等と連携して動作する情報システムの側面を持つものは対象として考える必要があります

用語解説

1. 体制構築

■ 医療情報システム安全管理責任者

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

＜医療情報システム安全管理責任者の役割＞

- 教育・訓練を含む情報セキュリティ対策の推進
- 情報セキュリティ方針の策定

- 経営層の就任が望ましい
- 企画管理者（システム部門長等）による兼務の場合、経営層によるバックアップ、裁量が与えられているか

2. 医療情報システムの管理・運用

■ サーバ　端末PC　ネットワーク機器

WindowsやLinux（リナックス）、MacOSといったOS（基本ソフト）で稼働

端末PC

ノートパソコン

- 職員の手元で使用されるパソコン

デスクトップパソコン

ミニPC

・デスクトップパソコンとしての利用
・案内表示用モニタの表示用等に利用される場合もある

サーバ

タワー型サーバ

ラックマウント型サーバ

例）NEC社サーバ製品

- ファイルサーバなどネットワーク経由で共用するものを稼働させる

各社専用のファームウェア（OS,基本ソフト）で稼働

ネットワーク機器

例）Fortinet社ルーター製品

例）Yamaha社ルーター製品

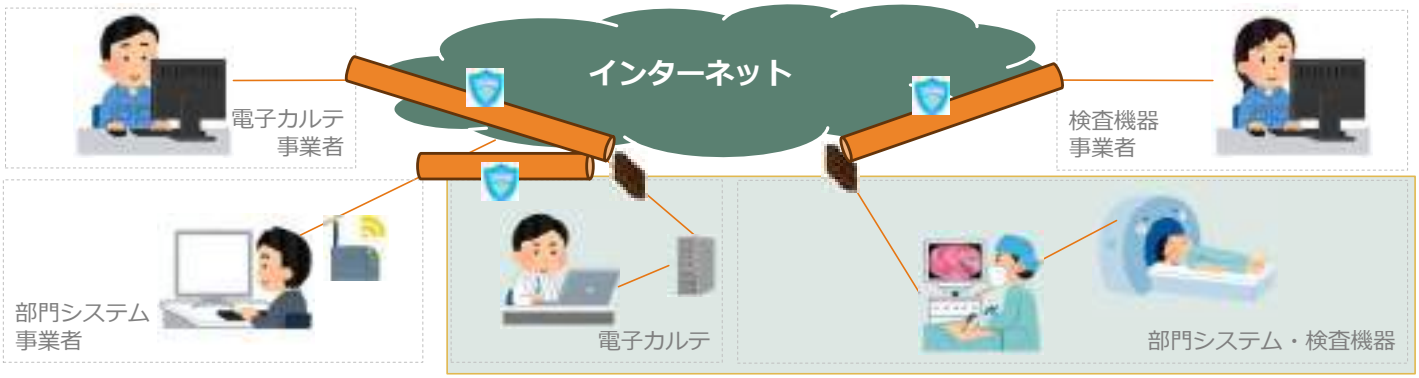
例）Cisco社ネットワークスイッチ製品

2. 医療情報システムの管理・運用

■ リモートメンテナンス（保守）

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。
- 専用線相当の回線サービスや、IPSec-VPNやSSL-VPNなどインターネット間を暗号通信で繋ぐVPN接続などさまざまな接続形態があり機密性を確保した通信手段により実施されるものですが、構成や運用に不備があるとセキュリティホールになる可能性があります。
- 近年では、LTEや5GなどのSIMを装着したモバイルルーターが設置されている場合があります。その場合、有線での導入と異なりインターネット回線は引き込み工事がないため気が付きにくくなりますので一層の注意が必要となります。



特定の人だけが通れる裏口を作るイメージです

2. 医療情報システムの管理・運用

■ 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）

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、医療情報システムの安全管理に関する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なります。

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=1119

2. 医療情報システムの管理・運用

■ アカウント

システムにおいて、ユーザー管理は構成ごとに異なることが多くなります。それぞれのアカウント情報の趣旨とあわせて、混同しないよう整理、管理する必要があります。

サーバのアプリケーション機能を利用する際の「アカウント」
→電子カルテ　メールサーバ　ECサイト　ネットバンク　など

サーバ/アプリケーション　アカウント登録状況

ID名	役割	アカウント種別	使用者
systemadmin	システム管理者	管理者	IT管理部門メンバー
d0200123	医師	医師	XX先生
n0220246	看護師	看護師	YYさん

PCへログインする「アカウント」
→ ユーザーID　利用者ID

端末PC/OS　アカウント

ID名	役割	Windows アカウント種別	使用者
Administrator	システム管理者	管理者	IT管理部門メンバー
user	一般利用者	標準ユーザー	一般職員

サーバ/OS　アカウント登録状況

ID名	役割	Windows アカウント種別	使用者
Administrator	システム管理者	管理者	IT管理部門メンバー
user	一般利用者	標準ユーザー	一般職員

サーバのOS機能を利用する際の「アカウント」
→　実際は端末PCからネットワーク越しに使用することが大半なので
サーバ自体に個別の利用者IDは登録されていないことが多い
ファイル共有サーバ　プリントサーバ　など

2. 医療情報システムの管理・運用

■ アクセス利用権限

誰が、どの情報に、どんなことができるかを決めるルール

目的

誰がどの情報を操作したか、責任の所在を明確にする（真正性）

重要な情報に、関係のない人がアクセスしてしまうのを防ぐ（機密性）

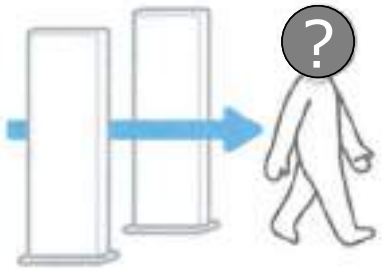
不正な操作を防ぎ、システムやデータの安全性を確保する（完全性）

電子カルテをイメージした例	記事入力	病名	検査結果	処方オーダ
 システム管理者	○ 入力可能	○ 入力可能	△ 閲覧のみ	○ 入力可能
 医師	○ 入力可能	○ 入力可能	△ 閲覧のみ	○ 入力可能
 看護師	○ 入力可能	△ 閲覧のみ	△ 閲覧のみ	△ 閲覧のみ
 医事事務員	○ 入力可能	△ 閲覧のみ	△ 閲覧のみ	× 閲覧不可

2. 医療情報システムの管理・運用

■ 退職者、使用していないアカウント、不要なアカウント

退職された方がそのままIDを保持していたら？



放置	• 入館ゲートを通過 • 不正侵入を誘発
削除	• 入館ゲートでブロック • 過去の記録との名寄せ確認ができない
無効化	•入館ゲートでブロック •過去の記録との名寄せ確認が可能になる •個人情報の保有期限に考慮が必要となる場合も

2. 医療情報システムの管理・運用

■ アクセスログ

業務システムでは処理が正しく行われていたことの裏付け、記録を「ログ」と呼びます。
アクセスログは、対象の「サーバ」または、機能である「アプリケーション」によって記録されることで
何かあったときにそこで起きた事象を確認する証拠となります。

When いつ	日時	Where どこで	発生箇所	Who 誰が	利用者ID	What 何を	対象データ	How どのように	アクション	Result 結果	OK / NG	Why なぜ	理由

入館の記録は何のため？

セキュリティ確保	責任の所在の明確化	利用状況の把握
•不審者の侵入を防ぐ •来訪者の安全を守る	•事故発生時、誰がいつ出入りしていたか明確にする	•混雑状況を把握し、利用便性を向上させる

●アクセスログの例

ユーザーID	氏名	時間	カテゴリ	操作情報
abc@def	abcdef	2023/5/16 6:30:09	管理メニュー	ログイン
abc@def	abcdef	2023/5/16 6:30:28	管理メニュー	起動
abc@def	abcdef	2023/5/16 6:31:08	入力メニュー	起動
abc@def	abcdef	2023/5/16 6:32:08	入力メニュー	カンテ入力
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 6:40:08	管理メニュー	ログイン
ghi@jkl	ghijkl	2023/5/17 6:40:38	管理メニュー	起動
ghi@jkl	ghijkl	2023/5/17 6:45:08	管理メニュー	ログオフ

2. 医療情報システムの管理・運用

ソフトウェア　脆弱性

脆弱性とは・・・？

- ソフトウェアで発覚したバグ、不具合
- 設計時点では想定されなかった箇所や、想定を超えるの方法によって問題となるもの

2. 医療情報システムの管理・運用

セキュリティパッチ　ファームウェア　更新プログラム

総務省　国民のためのサイバーセキュリティサイトより
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/end_user/general/03

パッチ セキュリティパッチ	• パッチとはソフトウェアの不具合を修正するための更新プログラムを指します • セキュリティ上の問題を修正するものをセキュリティパッチよ呼びます
ファームウェア	• ネットワーク機器など組み込み型の装置、アプライアンスと呼ばれる機器のOS、ソフトウェアをイメージすることが多いです
更新プログラム	• バージョンアップなども含め、更新、アップデート用のプログラムなど広い解釈があります

2. 医療情報システムの管理・運用

バックグラウンド

優先度の高い処理（プロセス、ジョブ）
画面上のアプリなど

フォアグラウンド

バックグラウンド

ウイルス対策などの保護機能

見えないところで動いているプロセス、ジョブ

使用されないプロセス、ジョブが蓄積しているとシステム全体の動作に影響することがあるため、無駄なものは停止する、立ち上げない

2. 医療情報システムの管理・運用

不要なソフトウェア及びサービス

業務上必要なもの

ウイルス対策などの保護機能

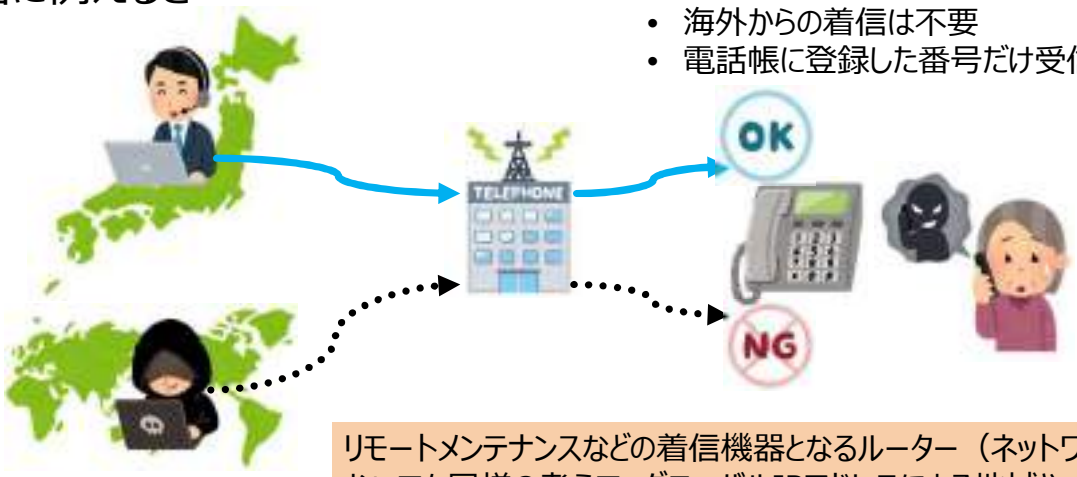
業務上不要なもの

- 組織として確認していない、認めていないアプリはインストールすべきではない
- 不必要なアプリ、サービスが起動されていることによってシステムのパフォーマンスを浪費することになる
- セキュリティ上の問題があった場合に無駄な対応労力を要することになる

2. 医療情報システムの管理・運用

■ 接続元制限

電話に例えると・・・



- 海外からの着信は不要
- 電話帳に登録した番号だけ受信

リモートメンテナンスなどの着信機器となるルーター（ネットワーク機器）においても同様の考えで、グローバルIPアドレスによる地域や、番号を制限する方法があります。

3.インシデント発生に備えた対応

■ インシデント

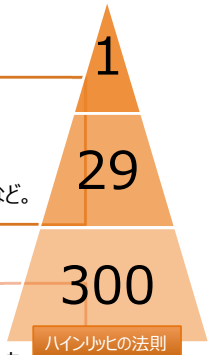
医療の場合

アクシデント

- 実際に**患者に被害**が及んだ医療事故
- 誤った薬剤を投与して**患者の容体が悪化**した場合など。

インシデント

- 患者に実害が発生しなかったが、ミスやエラーが発生した事象。
- 誤った薬剤を投与しようとしたが、投与前に気づいて修正した場合など。
- いわゆる「**ヒヤリハット**」。



サイバーセキュリティの場合

アクシデント

- アクシデントという表現はあまり使われない。

インシデント

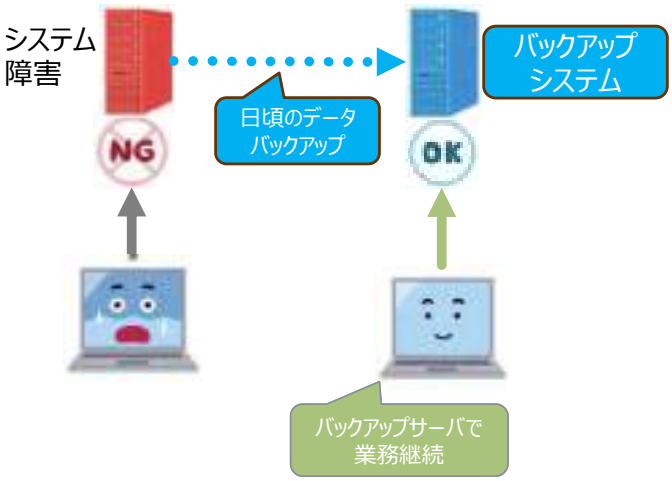
- 情報セキュリティ上の脅威となる事象。
- サイバーセキュリティインシデントは、企業や組織の情報資産が管理者の意図しない状態に置かれることを意味する。
- **マルウェア感染**、**不正アクセス**、**情報漏洩**など。

3.インシデント発生に備えた対応

■ バックアップ

バックアップの主な目的、理由

システム業務を「継続」するための方策

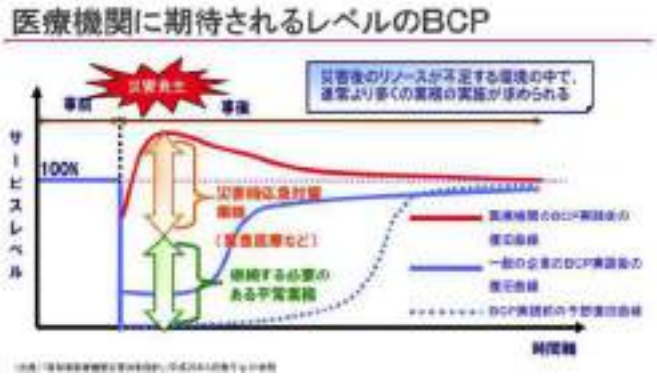


システム障害から「復元」するための方策

3.インシデント発生に備えた対応

■ 事業継続計画（BCP）

- 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。



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

- 災害拠点病院用のBCP策定について
  - 病院BCPを策定するための手引き
  - 病院BCP：（災害拠点病院用）改訂第２版
- 災害拠点病院以外の医療機関のBCP策定について
  - 医療機関（災害拠点病院以外）における災害対応のためのBCP作成の手引き
  - 医療機関（災害拠点病院以外）における災害対応のためのBCP作成指針
  - 災害拠点病院以外の医療機関におけるBCPチェックリスト

サイバー攻撃等によるシステム障害は、災害時における医療機関の復旧曲線とは異なり、一般企業の復旧曲線と同様となりますので
災害による事業継続計画とは別に、サイバー攻撃を想定した事業継続計画の策定が必要となっています。

参考情報

医療機器におけるサイバーセキュリティについて（厚生労働省 医薬局）

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000179749_00009.html

「医療情報システムの安全管理に関するガイドライン」だけでなく、医療機器に関するセキュリティの管理についても手引書等が発出されていますのでご参考ください

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）（令和６年８月１日）

https://www.mhlw.go.jp/content/10808000/001283914.pdf

サイバー攻撃リスク低減のための最低限の措置

- パスワードを強固なものに変更し、使い回しをしない
- IoT 機器を含む情報資産の通信制御を確認する
- ネットワーク機器の脆弱性に、ファームウェア等の更新を迅速に適用する

詳細は別添文書をご確認ください

立入検査研修
準備コース　終了

別途、医療機関向け前編、後編、
または、保健所向けについても
お申し込みの上、ご受講ください

ありがとうございました。