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】 医療機関向けコース　前編

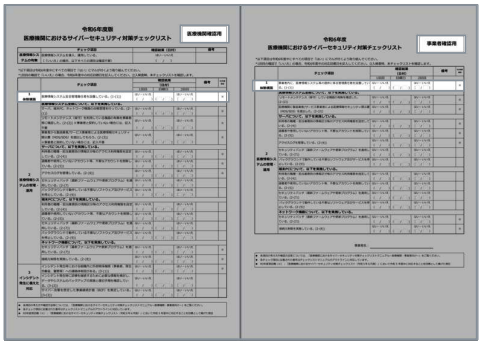
BC Signpost株式会社
松山 征嗣

立入検査研修
目次

医療機関向け　前編

主に組織、システム全体的なもの

- １．体制構築
- ３．インシデント発生に備えた対応
- ２．医療情報システムの管理・運用
  – 全般



1．体制構築

1．体制構築

医療情報システム安全管理責任者を設置している。(1-(1))

<実施方法>

医療情報システム安全管理責任者の役割が明確化され、組織内で周知されている必要があります。

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、
  経営層による後ろ盾、支援があるか、
  役割を遂行するための裁量が与えられているか

1．体制構築

医療情報システム安全管理責任者を設置している。(1-(1))

<ケーススタディ>

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役職者、経営層の方が適任です
- 組織内管理規程等の文書にてその役割の定義、組織図等で従事する方の氏名がわかるようにしておきましょう

責任者がシステムに関する知識を持っていない場合は？

以下、いずれかの対応が必要です。

- 責任者自身がセキュリティ研修等を活用して知識、判断力を向上させる
- 前提知識を有する職員を任命し、権限を委譲する
- 前提知識を有する職員や外部専門家を補佐として公式に配置し、責任者が判断の責任を負う

外部の事業者を責任者にしても良いですか？

●外部の事業者に組織としての責任を移転することはできません

●診療報酬、診療録管理体制加算の施設基準では『専任』の医療情報システム安全管理責任者を配置することとしているため、責任者は常勤の職員であることが望ましいと考えられます

- 専従：勤務時間のすべてをその業務に従事すること *
- 専任：主業務として業務時間の5割以上をその業務に充てること *
- 専ら：専従と専任の中間。業務時間の概ね8割程度の業務を行なっている *

＊割合については施設要件の解釈を参考としています。
新規開業医のための保険診療の要点（総論） ／ 東京都医師会
https://www.tokyo.med.or.jp/doctor/practicing_docs/general/03

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

1．体制構築

医療情報システム安全管理責任者を設置している。(1-(1))

<事業者における医療情報システム安全管理責任者>

顧客・施設に対しての責任者

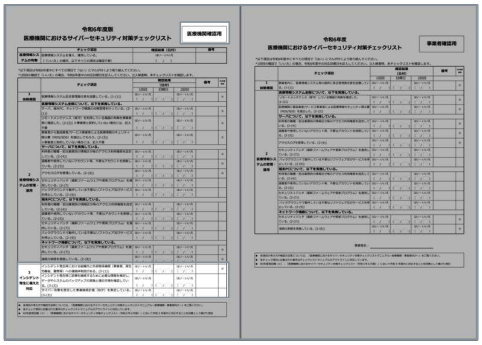
- 製品または顧客を担当する事業部門長や、導入システムのプロジェクトマネージャー等
- 導入後、保守フェーズ終了まで含めて対応できる体制

＋

提供製品・サービス単位（全社）

- PSIRTのように、横断的に製品・サービスを管理する組織の設置が望まれる
  - インシデント発生時の情報集約、ハンドリング
  - 共通的に構成されるソフトウェアやハードウェアなどの脆弱性評価やリスクアセスメント
  - 他の顧客、提供先へのリスク管理情報展開

PSIRT（Product Security Incident Response Team）：
組織が提供する製品の脆弱性に起因するリスクに対応するための組織内機能です。自社製品の脆弱性への対応、製品のセキュリティ品質管理・向上を目的としており、国内の製品開発者においても徐々に設置が進んでいます。
https://www.jpcert.or.jp/research/psirtSF.html



3．インシデント発生に備えた対応

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-(1))

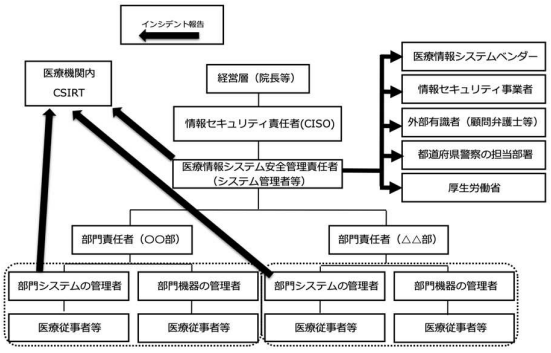
3．インシデント発生に備えた対応

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-(1))

<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		都道府県		
4		＃＃保健所		
5	事業者	A社		
5		B社		
6	近隣施設	X総合病院		
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

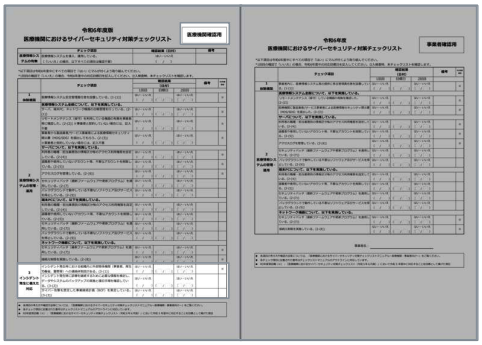
3．インシデント発生に備えた対応

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-(1))

＜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/）
本事業の実施期間内はこちらへご連絡頂ければ現場対応の支援を含めた相談が可能です。
連絡体制に組み込んでおきましょう。



3．インシデント発生に備えた対応

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-(2))

【令和６年度より通常確認へ移行】

3．インシデント発生に備えた対応

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-(2))

＜実施方法＞

サイバー攻撃によって被害が及ぶ可能性の低い、離れた場所へのバックアップ

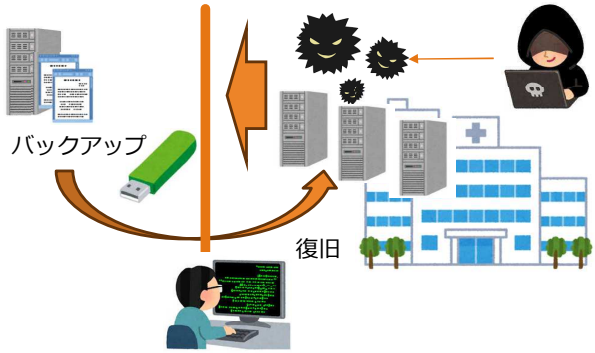
- オフライン環境
- オフサイト環境
- クラウド環境（接続方法やタイミングには注意が必要）

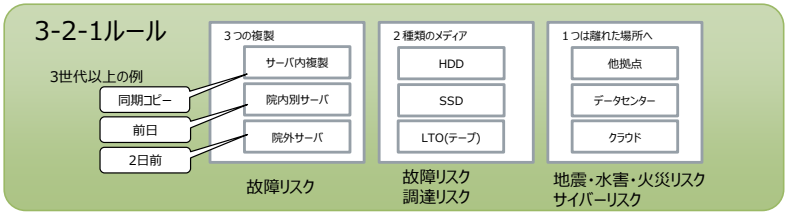
書き換えが困難な媒体へのバックアップ

- イミュータブルストレージ（Write Once Read Many）
- テープや一時接続のUSBストレージなどの外部媒体

システムを早期復旧するための復旧手順の確認、訓練

- 復旧の優先順位付けを行う
- 事業者に対応方法を確認する
- 復旧手順の文書化（有事の際に確認できる管理方法）

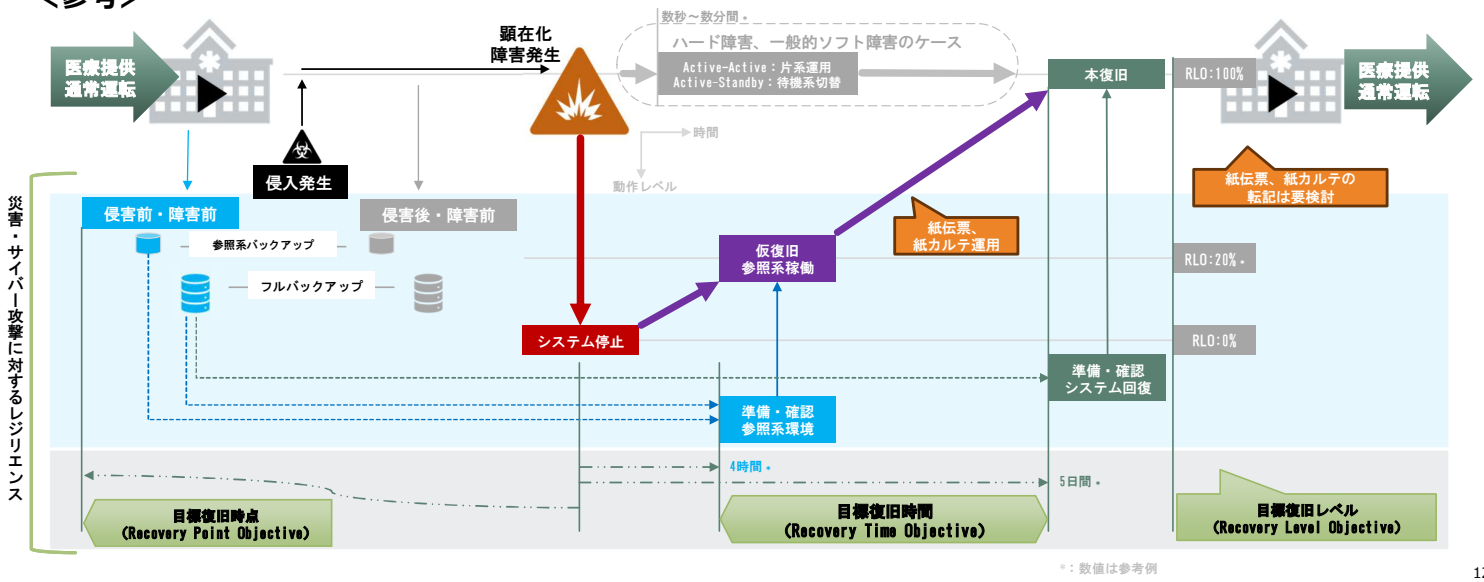




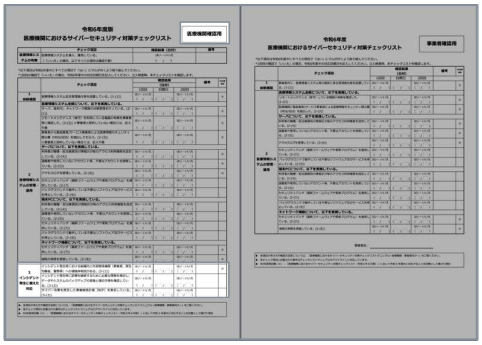
3．インシデント発生に備えた対応

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-(2))

＜参考＞



＊：数値は参考例



3．インシデント発生に備えた対応

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。(3-(3))

【令和６年度より通常確認へ移行】

3. インシデント発生に備えた対応

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。(3-(3))

＜実施方法＞

意思決定プロセス、緊急時の体制や手順を整備しましょう

- 非常事態の認定
  （サイバー攻撃事態の想定）
- 業務継続の可否判断
- 非常時における業務手順
- 初動対応組織と、
  インシデント対応手順

- 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。
  - サイバー攻撃による被災を含めたBCPについて作成または見直す必要があります。
- 参考情報として、厚生労働省がサイバー攻撃を想定した事業継続計画（BCP）策定の確認表等を公開しています。

サイバー攻撃を想定した事業継続計画（BCP）策定の確認表等
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

- 【医療機関用】サイバー攻撃を想定したBCP策定の確認表のための手引き（令和６年６月）
- 【医療機関用】サイバー攻撃を想定したBCP策定の確認表（PDF）（令和６年６月）
- 【医療機関用】サイバー攻撃を想定したBCP策定の確認表（Excel）（令和６年６月）

- 【薬局用】サイバー攻撃を想定したBCP策定の確認表のための手引き（令和６年６月）
- 【薬局用】サイバー攻撃を想定したBCP策定の確認表（Excel）（令和６年６月）

- 医療情報システム部門等におけるBCPのひな形（PDF）（令和６年６月）
- 医療情報システム部門等におけるBCPのひな形（Word）（令和６年６月）

3. インシデント発生に備えた対応

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。(3-(3))

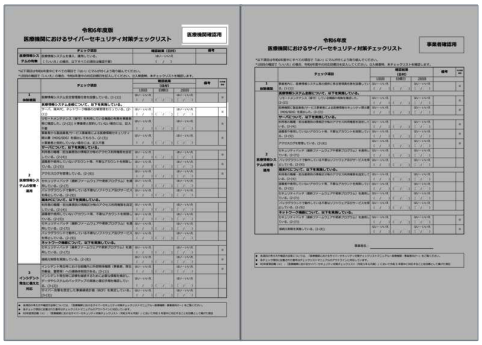
＜参考＞

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（平常時において、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発覚られる場合は、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。	
4	復旧処理（復旧計画に基づいて、医療情報システムの事業者及びサービス事業者等と協力して復旧を行う。証拠保存の観点からバックアップデータ等を取得する。）		
4-1	経営層からの復旧指示の確認と実施	復旧指示の確認と実施ができるか。	
4-2	医療情報システム等の事業者等へ復旧対応依頼	医療情報システム等の事業者等への対応依頼ができるか。	
4-3	再設定や再インストール、バックアップデータの復旧等	再設定や再インストール、バックアップデータの復旧等ができるか。	
4-4	復旧結果の確認	復旧結果の確認ができるか。	
5	事後対応（復旧結果の報告を受け、再発防止に向けた検討と再発防止策の周知と実施を進める。）		
5-1	復旧結果と情報漏えい事実の有無の報告	復旧結果と情報漏えい事実の有無、可能性について、院内での報告を行う方法、報告先、内容を、企画管理者、システム担当者がそれぞれの分担責任として把握しているか。	
5-2	再発防止策の検討・策定	再発防止策の検討および策定を進める体制、能力があるか。管理者、システム担当者がそれぞれの分担責任として把握しているか。	
5-3	再発防止策の周知	再発防止策の周知を院内に周知する方法と体制が整備されているか。	
5-4	再発防止策の実施	再発防止策の実施が行えるか。	
5-5	事業者等への再発防止策の指示	事業者に対して再発防止策を具体的に提案し、実施可能かつ有効な方法を策定する能力があるか。	
5-6	外部関係機関への報告と情報公開の検討	情報公開の内容検討を行う体制、連絡先、内容を文書として準備し、必要時に速やかに利用できるか。 経営者と担当者により外部関係機関への報告が行えるか。	

サイバー攻撃を想定した事業継続計画（BCP）策定の確認表等
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html



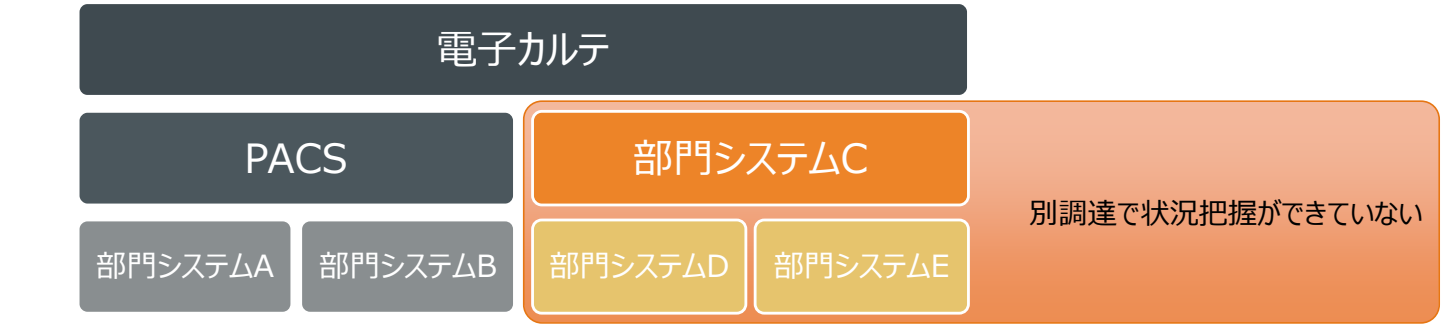
2． 医療情報システムの管理・運用

サーバ、端末PC、ネットワーク機器の台帳管理を行っている。(2-(1))

2． 医療情報システムの管理・運用

サーバ、端末PC、ネットワーク機器の台帳管理を行っている。(2-(1))

＜実施背景＞



- 閉域網だから安全ということは無い
- サポートが切れているソフトウェアや製品を使い続けている可能性
- インシデントが起きても何が原因かわからない
- 事業者の「保守」の範囲が定まらない

2． 医療情報システムの管理・運用

サーバ、端末PC、ネットワーク機器の台帳管理を行っている。(2-(1))

管理対象の確認

準備コースより再掲

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

2． 医療情報システムの管理・運用

サーバ、端末PC、ネットワーク機器の台帳管理を行っている。(2-(1))

<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、更新しましょう

機器台帳にはどのような情報が必要なのか？

- 院内ネットワークに繋がる情報機器、繋がらないものでも情報のやり取りが発生するような機器は管理、監督が必要です。
- 医療情報に直接触れることがないとしても、リモート保守関連のネットワーク機器については特に注意を払う必要があります。
- クラウドサービスの利用がある場合はその情報も管理が必要です。
- 台帳ではそれら機器の所在や利用者、ソフトウェアやサービスのバージョンなどが明確になるようにしてください。

■ 機器台帳の例

最終更新日： 2024年7月1日
最終更新者： 鈴木一郎

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	

■ クラウドサービスの場合の例

- サービス提供事業者
- サービス名称／用途
- ドメイン／アドレス
- 利用場所／アクセス経路
- 利用者／グループ
- 利用者認証方法
- 利用開始日
- 利用状況

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・管理しましょう

執行部が参加する会議体
- 経営会議
- 幹部会議
- 医療安全管理委員会

- **システムの稼働状況や対応状況など、確認・報告・共有**
- **議事録等の記録**

2． 医療情報システムの管理・運用

サーバ、端末PC、ネットワーク機器の台帳管理を行っている。(2-(1))

<ケーススタディ>

事務系のシステムなどは対象範囲ですか？

- 患者関連情報を扱う医療事務等であれば対象範囲と見なしますが、職員の給与や勤怠、財務など組織内事務は対象外です。

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？

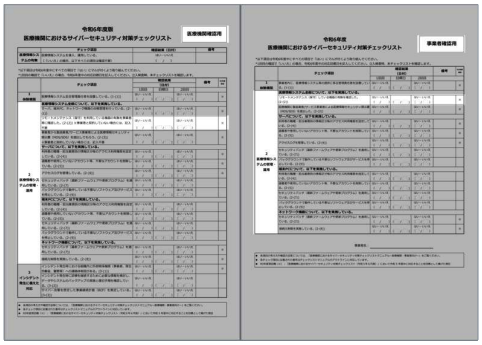
- ソフトウェアも含み、機器の管理を行っていく必要があります。そのため、「いいえ」を選択し、対応するための期日を記載しましょう。
- 早期対応に向けた取り組みをお願いします。（例：OS ,Office ,Adobeなど）

セキュリティに関する設定や対策を記載する必要はありますか？

- セキュリティ対策の有無や種類、バージョンなども可能であれば記載しておくとより良いです
- 利用者の認証方法、認証サーバ情報なども整理しておくとより良いです

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
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-(2))

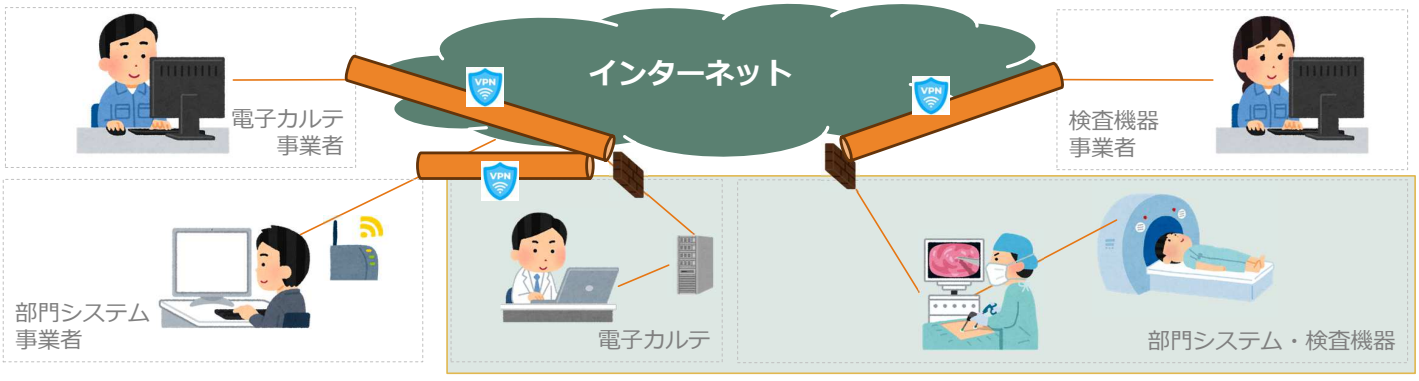
準備コースより再掲

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）を利用している機器の有無を事業者に確認した。(2-(2))

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

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-(2))

<実施方法>

外部からアクセスして行われる業務はありますか？　アクセス出来る仕組みがありますか？

- 2 -(1) 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）について、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。
- 端末やサーバが、２系統のネットワークに接続されることで、ネットワーク機器が医療システムのネットワークに直接接続されないケースも見受けられます。そのような構成も管理対象として適切な管理が必要となります

外部から接続可能な構成である場合、目的及び接続方法について確認しましょう

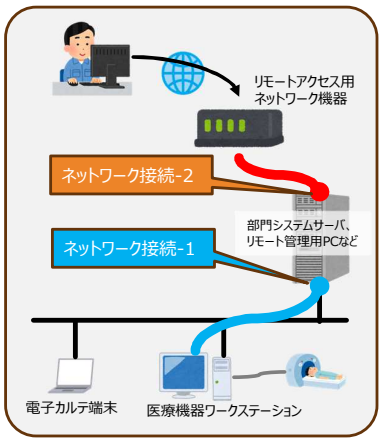
- リモートメンテナンスは誰が、どこから、どのようにして行われているか確認しましょう。
  - –接続してくる端末の制限（接続元IPアドレス制限など）
  - –アクセスするユーザーIDの付与先（個人毎か共用か）
  - –認証方法（不正ログインを防ぐための認証手順、認証強度）
  - –リモートメンテナンスしている端末の安全状態（最新のパッチ適用／サポート内ソフトウェアの使用／マルウェア等の脅威検出が無いか等）
  - –リモートメンテナンスを実施するタイミング、連絡の有無

確認ができていない場合は、早急に確認しましょう。
サイバー攻撃リスクに施設規模や地域は関係ありません。
安全のために重要な事とご認識ください。

台帳への記入と、定期的に運用状況の確認をしましょう

- 2-(1)の機器管理台帳にてリモートメンテナンスの有無を明確にし、利用状況が適切であるかを定期的に確認しましょう。
- 立入検査で確認を求められた場合に、説明できる状態にしましょう。

２系統のネットワーク接続、
「２枚挿し」による見落としに注意



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）を利用している機器の有無を事業者に確認した。(2-(2))

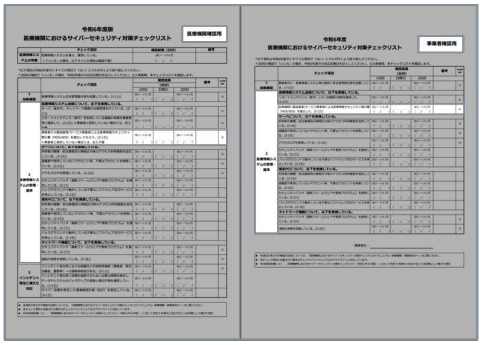
<ケーススタディ>

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？

- 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

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-(3))

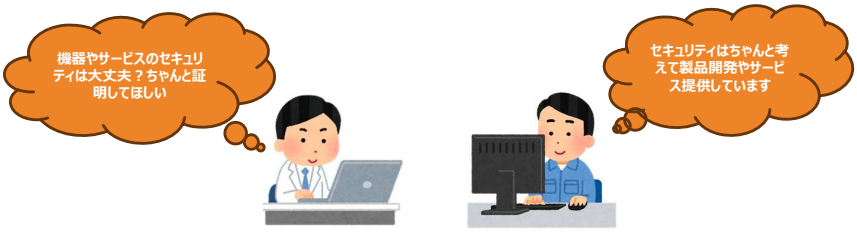
準備コースより再掲

2．医療情報システムの管理・運用

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-(3))

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。


サービス事業者による医療情報セキュリティ開示書（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版対応）

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

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-(3))

＜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の提出を求めるところです。取りまとめている業界団体*から、医療情報システムの安全管理に関するガイドライン６．０版に対応した**最新版**が**2024年9月12日に公表**されています。
- 最新版での提供が間に合わない場合は、旧5.2版ベースのものでも構わないので提出を求めましょう。
- なお、最新版の場合も含め、サイバーリスクへの想定、対応などに関して不足する情報については別途情報の開示を求め、管理情報に加えて行くようにしましょう。

サービス事業者による医療情報セキュリティ開示書（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版対応）			回答欄	
作成日				
サービス事業者				
サービス名称				
バージョン				
※本書式を作成したJAHIS/JIRAは、製品設計・設置・保守等の認証・試験・検査等は行っていません。また、特定の医療機関等における特定の目的・ニーズを満たすこと、あるいは個々の製品またはサービスの性能を保証するものではありません。この書式への記入内容は、記入した製造業者/サービス事業者が全責任を負います。			プルダウン選択（はい/いいえ/対象外/該当/非該当）	備考番号の入力（数字）（なし="-"）
診療録及び診療諸記録等の医療情報の取扱いを受託する際の基準				
1　診療録及び診療諸記録等の外部保存を受託するか？	該当 非該当	備考		
1．1　保存場所が「病院、診療所、医療法人等が適切に管理する場所」の場合、安全管理ガイドラインで示された選定基準と情報の取扱い要件を満たすか？	はい いいえ 対象外	備考		
1．2　保存場所が「医療機関等が外部の事業者との契約に基づいて確保した安全な場所」の場合、安全管理ガイドラインで示された選定基準と情報の取扱い要件を満たすか？	はい いいえ 対象外	備考		
医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践				
2　扱う情報のリストを医療機関等に提示できるか？	はい いいえ 対象外	備考		
組織的安全管理対策（体制、運用管理規程）				
3　医療情報システムを運用する際に、医療情報システムの企画管理者を設置しているか？	はい いいえ 対象外	備考		
4　医療情報システムを運用する際に、技術担当者を指定しているか？	はい いいえ 対象外	備考		
5　個人情報が参照可能な場所に対しては、入退管理のルールを定めているか？	はい いいえ 対象外	備考		
6　情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成しているか？	はい いいえ 対象外	備考		
7　医療機関等との契約に安全管理に関する条項を含めているか？	はい いいえ 対象外	備考		
8　個人情報を含む医療情報システムの業務を外部委託する場合、委託元である医療機関等との契約に再委託先を含めた安全管理に関する条項を含めているか？	はい いいえ 対象外	備考		
9　運用管理規程等において組織的安全管理対策に関する事項等を定めているか？	はい いいえ 対象外	備考		
物理的安全対策				
１０　個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠しているか？	はい いいえ 対象外	備考		
１１　個人情報を入力・参照できる端末が設置されている区画は、許可されたもの以外立ち入ることができないように対策されているか？	はい いいえ 対象外	備考		
１２　個人情報が保存されている機器が設置されている区画への入退管理を実施しているか？	はい いいえ 対象外	備考		
１２．１　入退出の事実を記録しているか？	はい いいえ 対象外	備考		
１２．２　入退者の記録を定期的にチェックし、妥当性を確認しているか？	はい いいえ 対象外	備考		
１３　個人情報が保存されている機器等の重要な機器に盗難防止策を講じているか？	はい いいえ 対象外	備考		
１４　個人情報が入力・参照できる端末に覗き見防止の機能があるか？	はい いいえ 対象外	備考		
１５　サービス事業者の管理端末に覗き見防止対策が取られているか？	はい いいえ 対象外	備考		
技術的安全対策				
１６　離席時に権限を持たない者による不正入力を防止する対策が行われているか？	はい いいえ 対象外	備考		
１７　アクセス管理の機能があるか？	はい いいえ 対象外	備考		
１７．１　利用者の認証方式は？				
・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		
・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		
・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		
１７．１．１　パスワードを利用者認証手段として利用しているか？	はい いいえ 対象外	備考		
１７．１．１．１　他の手段と併用した際のパスワードの運用方法を運用管理規程に定めているか？	はい いいえ 対象外	備考		
１７．１．１．２　本人確認の実施の際、本人確認方法を台帳に記載しているか？	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=1119

＊ 一般社団法人保健医療福祉情報システム工業会（JAHIS）医療システム部会セキュリティ委員会
一般社団法人日本画像医療システム工業会（JIRA）医用画像システム部会セキュリティ委員会

2．医療情報システムの管理・運用

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-(3))

＜ケーススタディ＞

提出はされているのものの、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業界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、提供事業者の業界団体などにも問い合わせをしてみましょう。

立入検査研修
医療機関向け前編終了

別途、医療機関向け後編についても
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。