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

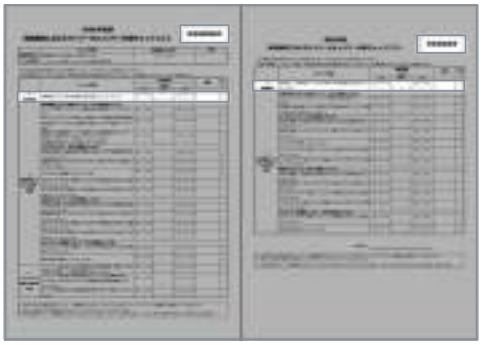
BC Signpost株式会社
松山 征嗣

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

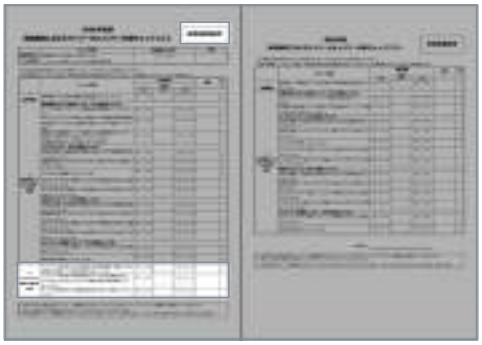
- 製品または顧客を担当する事業部門長や、導入システムのプロジェクトマネージャー等
- 導入後、保守フェーズ終了まで含めて対応できる体制

＋

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		
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

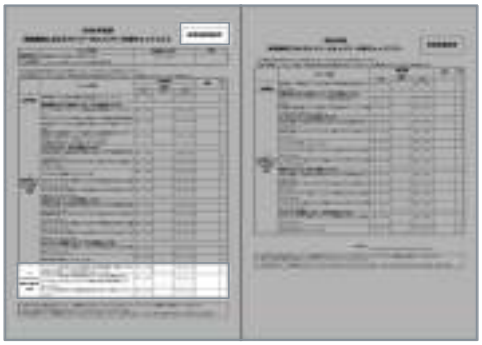
3．インシデント発生に備えた対応

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

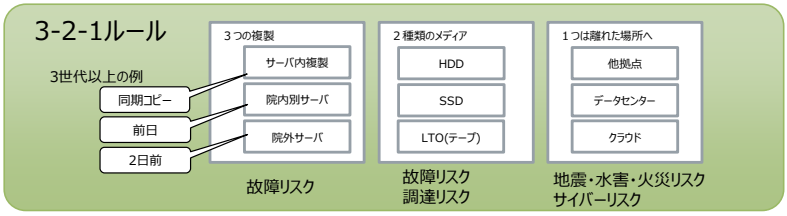
- オフライン環境
- オフサイト環境
- クラウド環境（接続方法やタイミングには注意が必要）

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

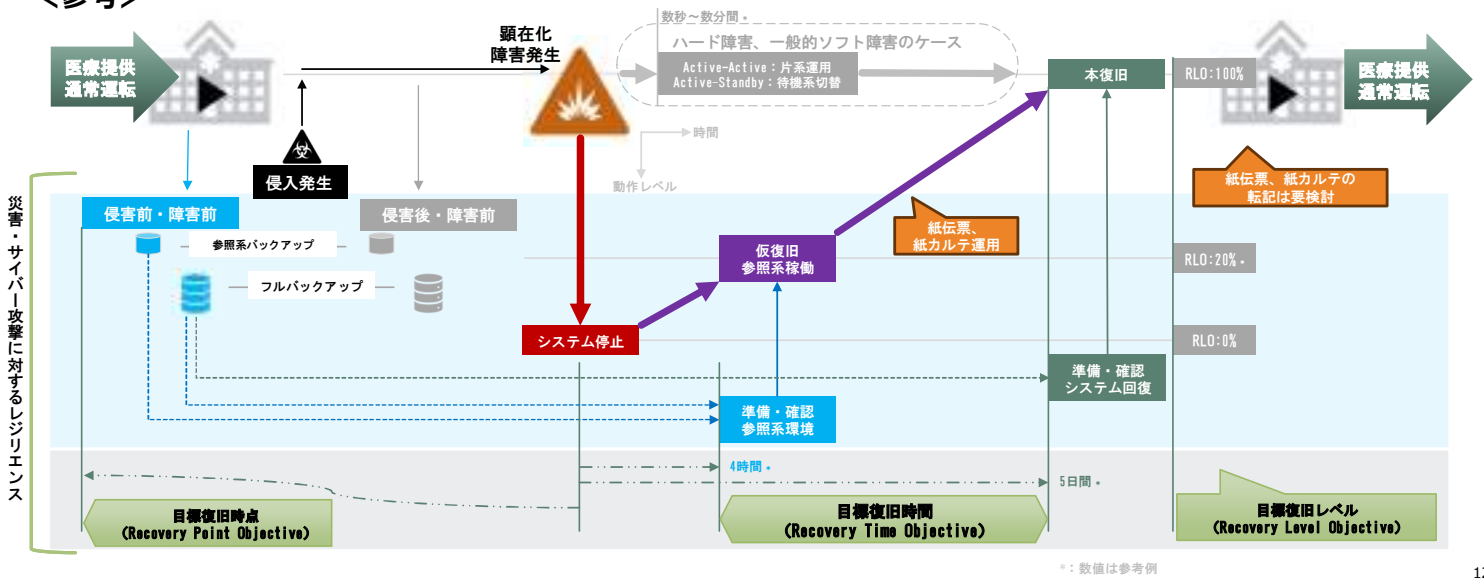
- 復旧の優先順位付けを行う
- 事業者に対応方法を確認する
- 復旧手順の文書化（有事の際に確認できる管理方法）



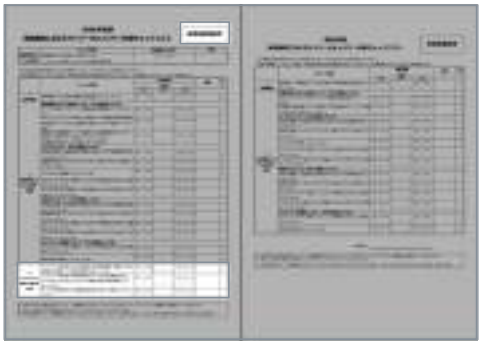
3．インシデント発生に備えた対応

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

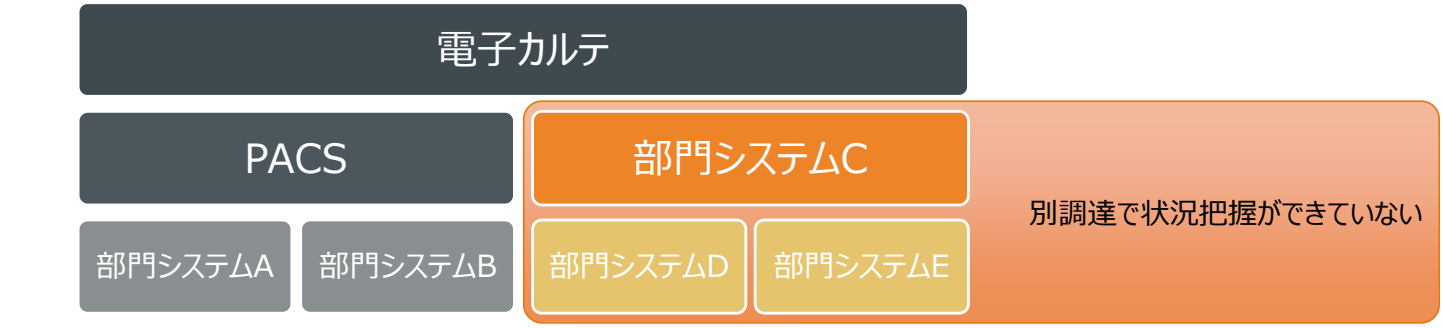
２． 医療情報システムの管理・運用

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

■ 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))

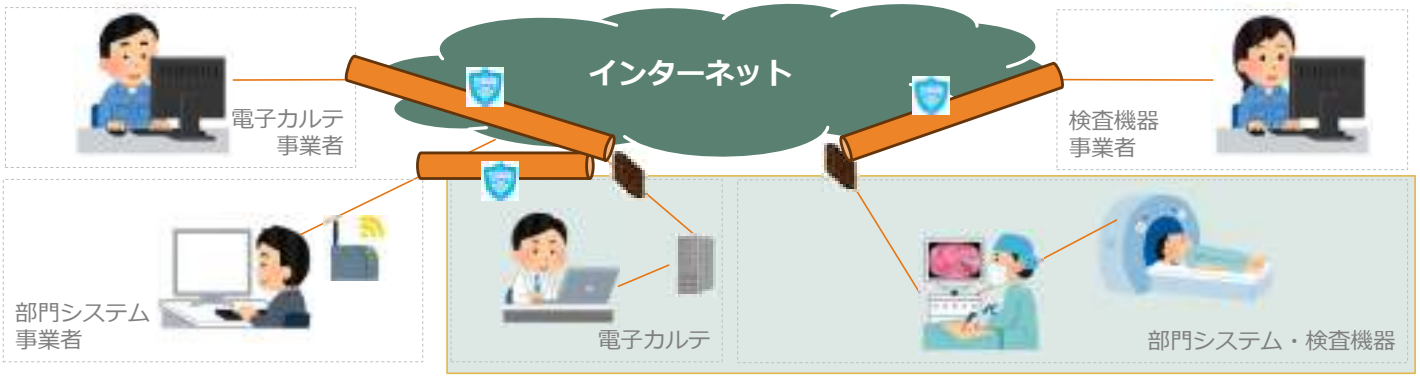
準備コースより再掲

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

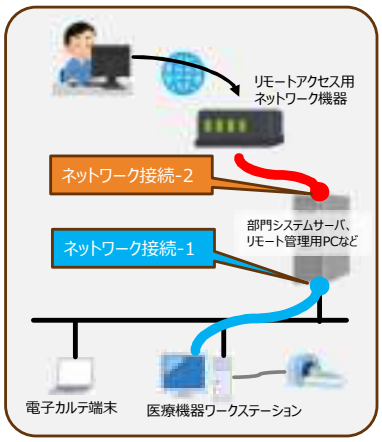
- リモートメンテナンスは誰が、どこから、どのようにして行われているか確認しましょう。
  - –接続してくる端末の制限（接続元IPアドレス制限など）
  - –アクセスするユーザーIDの付与先（個人毎か共用か）
  - –認証方法（不正ログインを防ぐための認証手順、認証強度）
  - –リモートメンテナンスしている端末の安全状態（最新のパッチ適用／サポート内ソフトウェアの使用／マルウェア等の脅威検出が無いか等）
  - –リモートメンテナンスを実施するタイミング、連絡の有無

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))

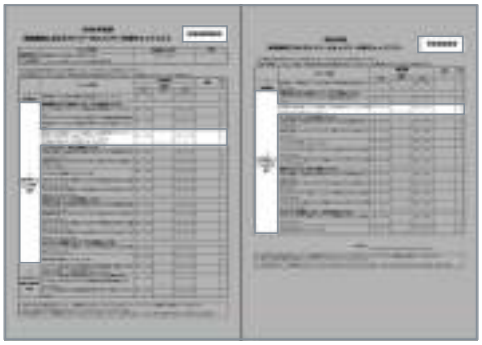
<ケーススタディ>

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。

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。

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。