厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

令和６年度全国薬務関係主管課長会議　説明資料

医政局

特定医薬品開発支援・医療情報担当参事官室

Ministry of Health, Labour and Welfare of Japan

令和５年６月２日 医療ＤＸ推進本部決定

医療DXの推進に関する工程表（概要）

基本的な考え方

○　医療DXに関する施策の業務を担う主体を定め、その施策を推進することにより、①国民のさらなる健康増進、②切れ目なく質の高い医療等の効率的な提供、③医療機関等の業務効率化、④システム人材等の有効活用、⑤医療情報の二次利用の環境整備の5点の実現を目指していく

○　サイバーセキュリティを確保しつつ、医療DXを実現し、保健・医療・介護の情報を有効に活用していくことにより、より良質な医療やケアを受けることを可能にし、国民一人一人が安心して、健康で豊かな生活を送れるようになる

マイナンバーカードの健康保険証の一体化の加速等

○　2024年秋に健康保険証を廃止する

○　2023年度中に生活保護（医療扶助）でのオンライン資格確認の導入

全国医療情報プラットフォームの構築

○　オンライン資格確認等システムを拡充し、全国医療情報プラットフォームを構築

○　2024年度中の電子処方箋の普及に努めるとともに、電子カルテ情報共有サービス（仮称）を構築し、共有する情報を拡大

○　併せて、介護保険、予防接種、母子保健、公費負担医療や地方単独の医療費助成などに係るマイナンバーカードを利用した情報連携を実現するとともに、次の感染症危機にも対応

○　2024年度中に、自治体の実施事業に係る手続きの際に必要な診断書等について、電子による提出を実現

○　民間PHR事業者団体やアカデミアと連携したライフログデータの標準化や流通基盤の構築等を通じ、ユースケースの創出支援

○　全国医療情報プラットフォームにおいて共有される医療情報の二次利用について、そのデータ提供の方針、信頼性確保のあり方、連結の方法、審査の体制、法制上あり得る課題等の論点について整理し検討するため、2023年度中に検討体制を構築

電子カルテ情報の標準化等

○　2023年度に透析情報及びアレルギーの原因となる物質のコード情報について、2024年度に蘇生処置等の関連情報や歯科・看護等の領域における関連情報について、共有を目指し標準規格化。2024年度中に、特に救急時に有用な情報等の拡充を進めるとともに、救急時に医療機関において患者の必要な医療情報が速やかに閲覧できる仕組みを整備。薬局との情報共有のため、必要な標準規格への対応等を検討

○　標準型電子カルテについて、2023年度に必要な要件定義等に関する調査研究を行い、2024年度中に開発に着手。電子カルテ未導入の医療機関を含め、電子カルテ情報の共有のために必要な支援策の検討

○　遅くとも2030年には、概ねすべての医療機関において、必要な患者の医療情報を共有するための電子カルテの導入を目指す

診療報酬改定DX

○　2024年度に医療機関等の各システム間の共通言語となるマスタ及びそれを活用した電子点数表を改善・提供して共通コストを削減。2026年度に共通算定モジュールを本格的に提供。共通算定モジュール等を実装した標準型レセコンや標準型電子カルテの提供により、医療機関等のシステムを抜本的に改革し、医療機関等の間接コストを極小化

○　診療報酬改定の施行時期の後ろ倒しに関して、実施年度及び施行時期について、中央社会保険医療協議会の議論を踏まえて検討

医療DXの実施主体

○　社会保険診療報酬支払基金を、審査支払機能に加え、医療DXに関するシステムの開発・運用主体の母体とし、抜本的に改組

○　具体的な組織のあり方、人員体制、受益者負担の観点を踏まえた公的支援を含む運用資金のあり方等について速やかに検討し、必要な措置を講ずる

医療DXに関する主な見直し内容（検討中）について

第６回「医療DX令和ビジョン2030」
厚生労働省推進チーム
（令和７年１月22日）資料１

１．電子カルテ情報共有サービス関係

※地域医療介護総合確保法、感染症法等

①電子カルテ情報共有サービスを法律に位置づけ
- 医療機関等から支払基金への電子カルテ情報（３文書６情報）の提供を可能とする
- 支払基金における電子カルテ情報の目的外利用の禁止
- 運用費用の負担者・負担方法

②次の感染症危機に備えた対応
- 医療機関の負担軽減のため、感染症の発生届について、電子カルテ情報共有サービスを経由しての提出を可能とする
- 感染症対策上必要な時、厚労大臣が支払基金に対して、電子カルテ情報の提供指示を可能とする

２．PMH （自治体と医療機関・薬局をつなぐ情報連携基盤）関係

※PMH：Public Medical Hub

※公費負担医療制度各法、支払基金法、健康増進法等

①マイナ保険証１枚で医療費助成を受けられる仕組みの整備（公費負担医療・地方単独医療費助成のオンライン資格確認の制度化）

②自治体検診情報の医療機関等への電子的共有を可能とする

３．医療情報の二次利用関係

※地域医療介護総合確保法、がん登録推進法、児童福祉法、難病法、感染症法、健康増進法、次世代医療基盤法等

①厚生労働大臣が保有する医療・介護の公的DBについて、現行の匿名化情報の利用・提供に加え、仮名化情報の利用・提供を可能とする

②電子カルテ情報DB（仮称）・自治体検診DB（仮称）を新たに設置し、匿名・仮名化した情報の利用・第三者提供を可能とする

③　①・②の仮名化した情報について、相互に連結解析を可能とする。また、次世代医療基盤法に基づく仮名加工医療情報との連結解析を可能とする

４．支払基金の抜本改組関係

※支払基金法等

①厚生労働大臣が「医療DX総合確保方針（仮称）」を策定し、支払基金が「医療DX中期計画（仮称）」を策定する

②支払基金を医療DXの実施主体とする観点から、法人の名称、目的、業務規定等を見直す

③一元的で柔軟かつ迅速な意思決定体制とするため、現行の理事会体制の見直し、国や地方関係者の参画、医療DXの専門家の参画

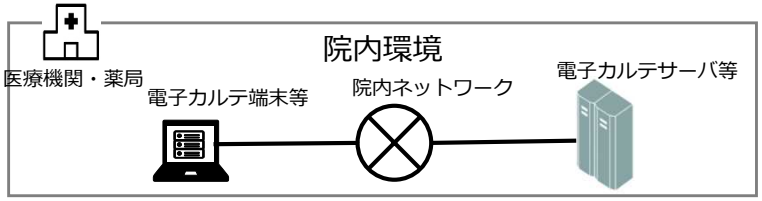
病院の情報システムに関する現状・課題、目指すべき姿

第６回「医療DX令和ビジョン2030」
厚生労働省推進チーム
（令和７年１月22日）資料３

現状・課題

- **少子高齢化の進展等により、医療費増加と担い手不足が課題となる中で、より質が高く効率的な医療提供体制を構築していく必要がある。そのためには、医療DXを進め、医療情報の共有と利活用を推進することが必要。一方、コロナ禍以降、病院経営は厳しい状況にあり、特に昨今、病院の情報システム（電子カルテ、レセコン、部門システム等）関連経費が増加し、病院経営を圧迫している。**
- **これまで、病院では主にオンプレ型システムを採用。インフラ（サーバー等）やデータベース、アプリケーションを病院ごとに独自にカスタマイズした上に、大規模なシステム更改が必要になるため、昨今の物価・人件費上昇の中でシステム関連費用の高騰につながっている。**
  ※病院・ベンダーにおけるシステム人材確保も困難になってきている。
- **また、電子処方箋等の医療DXの各取組を進めていく上でも、オンプレ型では、医療機関毎にシステム改修が発生するとともに、生成AI等の最新技術やサービスを活用する上でも、オンプレ型では一定の制約がある。**
- **さらに、オンプレ型システムでは、院内のサーバーのセキュリティ対応や多数の部門システムの外部接続点の確認等に関する病院側負担が大きく、セキュリティ面の脆弱性が解消できていない。**

【オンプレ型システムのイメージ】



システム構成

インフラ（サーバ等）、ミドルウェア（データベース等）、アプリケーションを病院ごとに構築

目指す姿

- **情報セキュリティ対策を向上させながら、病院の情報システム費用の低減・上昇抑制を図り、経営資源を医療提供に振り向けられる体制を整備する。**
- **情報通信技術の進歩を踏まえ、将来的に、各病院が生成AI等の最新技術やサービスを活用しやすくすることで、医療従事者の負担を軽減しながら、より安全で質の高い医療を実現できるようにする。**

第６回「医療DX令和ビジョン2030」
厚生労働省推進チーム
（令和７年１月22日）資料３

病院の情報システムの刷新に関する方針

①現在のオンプレ型のシステムを刷新し、電子カルテ/レセコン/部門システムを一体的に、モダン技術を活用したクラウド型システムに移行する。
目標：2030年までのできる限り早い時期に、希望する病院が導入できる環境を整備
※具体的には、複数病院で共同利用する方式や、クラウドのメリットを活かすためのマネージドサービスの活用を図る。また、医療従事者の負担軽減やより安全で質の高い医療につなげるべく、最新技術やサービスを活用しやすくするためのAPIの組み込み等を行う。
※画像等の一部の部門システム等で病院の判断でオンプレ型が残存する場合でも、標準化やセキュリティ対策の強化を図る。

②国がシステムの標準仕様を示し、その標準仕様に準拠した病院の情報システムを民間事業者が開発し、小規模病院やグループ病院等から段階的な普及を図る。この標準仕様を2025年度を目途に作成する。
※現在、小規模医療機関を中心に、共同利用型のクラウド型電子カルテが普及し始めているため、こうした製品の活用も図る。

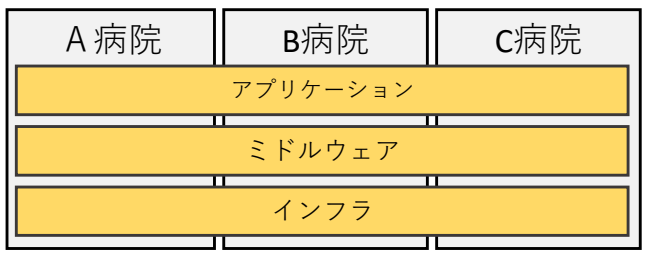
③標準仕様に準拠した病院の情報システムは、インフラからアプリケーションまでを共同利用することとし、医療機関ごとに生じていた個別のカスタマイズを極力抑制する。これらにより、病院情報システム費用の低減・上昇抑制や、病院ごとに生じていたシステム対応負荷の軽減を図る。
※複数病院で共同利用する際に、サイバー攻撃やシステム障害等による全面障害となる事態も想定し、システムの標準仕様を検討する。

④標準仕様に準拠したシステムへの円滑な移行のため、データ引継ぎの互換性の確保等を図る。
また、医療DXサービス（電子カルテ情報共有サービス等）とのクラウド間連携を進める。

⑤上記と並行して、医薬品・検査等の標準コード・マスタ、並びにこれらの維持管理体制の整備を進めるとともに、現場における標準コード・マスタの利用の徹底を図る。

アプリまでをクラウド化し複数病院で利用

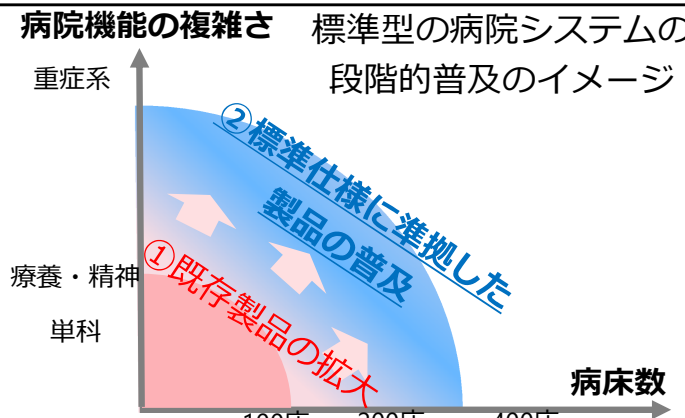
インフラ～アプリケーションをクラウド化し複数病院（マルチテナント）で共同利用。



【標準仕様に盛り込む主な要素例】

- 電子カルテ、レセコン、部門システムについて、マネージドサービス等のモダン技術の活用
- 医薬品、検査、処置等に関する標準マスターの組み込み
- 標準交換規約（API仕様を含む）を用いたデータ連携機能の組み込み
- データ引き継ぎの互換性を確保等

標準型の病院システムの段階的普及のイメージ



医療機関・薬局のサイバーセキュリティについて

医療法施行規則の改正（2023/4/1施行）

第十四条　病院又は診療所の管理者はその病院又は診療所に存する医薬品、再生医療等製品及び用具につき医薬品医療機器等法の規定に違反しないよう必要な注意をしなければならない。

第十四条　病院又は診療所の管理者はその病院又は診療所に存する医薬品、医療機器及び再生医療等製品につき医薬品医療機器等法の規定に違反しないよう必要な注意をしなければならない。

2　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、**サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）の確保のために必要な措置を講じ**なければならない。

薬機法施行規則の改正（2023/4/1施行）

（薬局の管理者の業務及び遵守事項）
第十一条（略）
2　法第八条第三項の薬局の管理者が遵守すべき事項は、次のとおりとする。
一　保健衛生上支障を生ずるおそれがないように、その薬局に勤務する薬剤師その他の従業者を監督し、その他その薬局の業務につき、必要な注意をすること。
二　（略）

（薬局の管理者の業務及び遵守事項）
第十一条（略）
2　法第八条第三項の薬局の管理者が遵守すべき事項は、次のとおりとする。
一　保健衛生上支障を生ずるおそれがないように、その薬局に勤務する薬剤師その他の従業者を監督し、その薬局の構造設備及び医薬品その他の物品を管理し、その薬局の業務に係る**サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）の確保のために必要な措置を講じ**、その他その薬局の業務につき、必要な注意をすること。
二　（略）

令和6年度版 医療機関等におけるサイバーセキュリティ対策チェックリスト

- 厚生労働省においては、令和５年４月から、医療法に基づく医療機関に対する立入検査に、サイバーセキュリティ対策の項目を位置付けている。（薬局については、同様に、薬機法施行規則を改正して対応）
- 立入検査の際に確認する項目については、医療情報システムの安全管理に関するガイドラインから特に取り組むべき重要な項目を抽出し、「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」により示している。
- 令和５年度においては、チェックリストの一部項目について、令和６年度に確認するものを参考項目として位置づけていたが、令和６年度において、すべての項目を確認することとした。
- 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「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～」（令和６年５月13日付け医政参発0513・第6号医政局特定医薬品開発支援・医療情報担当参事官通知）を発出した。薬局に対しても、同様に、薬局版のチェックリストを発出している（医政参発0513第８号・医薬総発0513第１号）。
- 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

医療機関等用

○ 令和５年度中


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

医療機関等用

○ 参考項目（令和６年度中）

令和５年度版


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

医療機関等用

令和６年度版

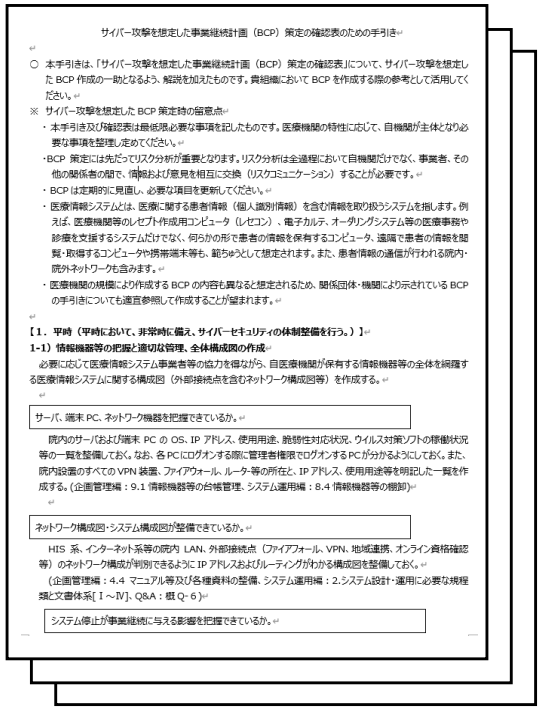
サイバー攻撃を想定した事業継続計画（BCP）のための確認表等

サイバー攻撃を想定した事業継続計画（BCP）策定のための確認表、確認表の解説を加えた「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」及び「サイバー攻撃を想定したBCPのひな形」を作成。

サイバー攻撃を想定したBCP策定のための確認表

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。	

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


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

○ 本手引きは、「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、サイバー攻撃を想定した BCP 作成の一助となるよう、解説を加えたものです。貴組織において BCP を作成する際の参考として活用してください。

※ サイバー攻撃を想定した BCP 策定時の留意点

・本手引き及び確認表は最低限必要な事項を記したものです。医療機関の特性に応じて、自機関が主体となり必要な事項を整理し定めてください。

・BCP 策定には先だってリスク分析が重要となります。リスク分析は全過程において自機関だけでなく、事業者、その他の関係者の間で、情報および意見を相互に交換（リスクコミュニケーション）することが必要です。

・BCP は定期的に見直し、必要な項目を更新してください。

・医療情報システムとは、医療に関する患者情報（個人識別情報）を含む情報を取り扱うシステムを指します。例えば、医療機関等のレセプト作成用コンピュータ（レセコン）、電子カルテ、オーダリングシステム等の医療事務や診療を支援するシステムだけでなく、何らかの形で患者の情報を保有するコンピュータ、遠隔で患者の情報を閲覧・取得するコンピュータや携帯端末等も、範ちゅうとして想定されます。また、患者情報の通信が行われる院内・院外ネットワークも含みます。

・医療機関の規模により作成する BCP の内容も異なると想定されるため、関係団体・機関により示されている BCP の手引きについても適宜参照して作成することが望ましいです。

【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

必要に応じて医療情報システム事業者等の協力を得ながら、自医療機関が保有する情報機器等の全体を網羅する医療情報システムに関する構成図（外部接続点を含むネットワーク構成図等）を作成する。

サーバ、端末 PC、ネットワーク機器を把握できているか。

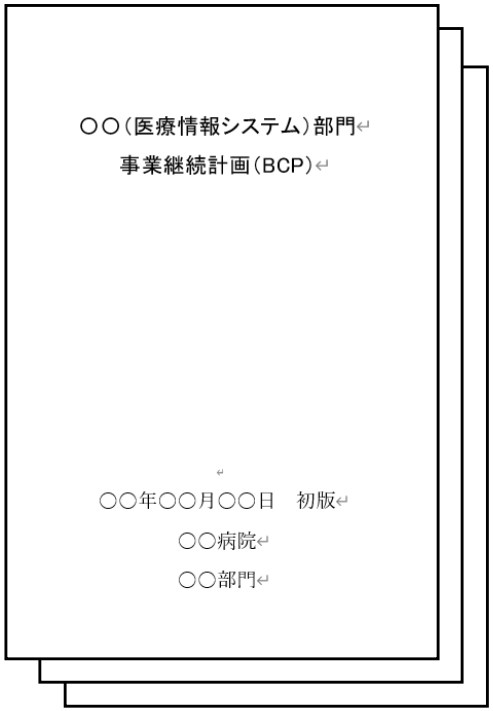
院内のサーバおよび端末 PC の OS、IP アドレス、使用用途、脆弱性対応状況、ウイルス対策ソフトの稼働状況等の一覧を整備しておく。なお、各 PC にログオンする際に管理者権限でログオンする PC が分かるようにしておく。また、院内設置のすべての VPN 装置、ファイアウォール、ルーター等の所在と、IP アドレス、使用用途等を明記した一覧を作成する。（企画管理編：9.1 情報機器等の台帳管理、システム運用編：8.4 情報機器等の棚卸）

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。

HIS 系、インターネット系等の院内 LAN、外部接続点（ファイアフォール、VPN、地域連携、オンライン資格確認等）のネットワーク構成が判別できるように IP アドレスおよびルーティングがわかる構成図を整備しておく。（企画管理編：4.4 マニュアル等及び各種資料の整備、システム運用編：2.システム設計・運用に必要な規程類と文書体系[Ⅰ～Ⅳ]、Q&A：概 Q-6）

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。

サイバー攻撃を想定した
BCPのひな形



2024/6/6　HP公表
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

令和６年度厚生労働省におけるセキュリティ研修の強化と提供について
支援ポータルサイトのご案内

医療機関向け

セキュリティ教育支援ポータルサイト
Medical Information Security Training (MIST)

厚生労働省
厚生労働省委託事業

事業について | 研修内容 | コンテンツ集 | コラム | 講師・技術者リスト | 関連リンク | お問い合わせ | インシデントかも？

研修内容

立入検査研修 | 経営者向け | システム・セキュリティ管理者向け | 初学者等向け研修 | 講師育成研修 | E-learning

2024年10月11日より一部の研修コース名を変更いたしました。変更内容については、こちらをご確認ください。

令和６年９月より開始

ポータルサイトURL：https://mhlw-training.saj.or.jp/

研修種別	コース名	受講対象	実施方法	研修概要
立入検査研修	準備コース	医療機関等保健所関係者	オンライン	医療法に基づく立入検査において、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対策チェックリスト」に基づいた研修 令和6年度に追加された項目等について重点的に解説
	医療機関向けコース	医療機関等保健所関係者		
	保健所向けコース	保健所関係者		
経営者向け研修	ITガバナンスコース	医療機関等の経営に携わる方	オンライン	令和5年度に実施した研修を基にガバナンスの基礎やIT-BCPの基本的な考えや対応方法等について学習
	経営者視点コース			経営者としてサイバーセキュリティを考える重要性を「経営指標」「経営資源の最適配置」など俯瞰した内容でサイバーセキュリティを学習
	IT-BCPコース			過去のインシデント事例を基にIT-BCPの実装、災害BCPの違いなど、ランサムウェア事案を踏まえて学習
システム・セキュリティ管理者向け研修	復習コース ・Windowsセキュリティ編 ・Networkセキュリティ編	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	Windows標準機能を用いた、セキュリティ対策やネットワークセキュリティについて学習
	新規Aコース ・インシデント対応　平時編			インシデント対応「平時」および「初動・封じ込め」について学習
	新規Bコース ・インシデント対応 初動・封じ込め編			
	連携Aコース*	医療機関等のシステム・セキュリティ管理する方 *連携コースは、A・B・Cの3コースで構成していますが、それぞれのコースを単体でご受講可能です。	ワークショップ	RFPおよびネットワーク構成図作成に必要な前提スキルとなる、ネットワークの基礎、セキュリティの基礎について学習
	連携Bコース*			ネットワーク更改に向けて、RFP(提案依頼書)、RFI(情報提供依頼書)に必要な要素について学習
	連携Bコース*		机上演習	インシデントハンドリングに使用できるネットワーク構成図の作成・管理について学習
初学者等向け研修	Aコース ・セキュリティの重要性	医療機関等の中で、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	一般的なサイバー攻撃の概要および家庭でも役立つ対策について学習
	Bコース ・リスクの理解と対策			医療機関で発生したインシデント事例を中心に、脅威と対策について学習
講師育成研修		自院でIT-BCPの策定等に携わる方	対面	IT-BCPの必要性を正しく認識し、自院でIT-BCPの策定や訓練を実施できるようになるための、座学やワークショップを提供