資料３－３

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

厚生労働省におけるサイバーセキュリティに関する取り組み

Ministry of Health, Labour and Welfare of Japan

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BCP策定のための確認表等 作成の経緯

○　サイバー攻撃が増加する近年の状況を踏まえ、「医療情報システムの安全管理ガイドライン」においては、医療サービスを提供し続けるための事業継続計画（BCP）として、医療機関がサイバー攻撃を非常時と判断するための基準、手順、判断者及び復旧への手順をあらかじめ定めておくことと明記されている。

○　また、医療機関への立入検査の際に利用される「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」においても「サイバー攻撃を想定したBCP」を令和６年度中に策定することとしており、サイバー攻撃によるシステム障害発生時に備えたBCP作成を医療機関に求めている。

○　さらに、2024年度診療報酬改定において、「非常時を想定した医療情報システムの利用が困難な場合の対応や復旧にいたるまでの対応についてBCPを策定すること」が診療録管理体制加算の要件となっている。

○　しかしながら、令和６年に厚生労働省が実施した「病院における医療情報システムのサイバーセキュリティ対策に係る調査（調査機関：令和６年２月１日～３月８日）」においては、サイバー攻撃によるシステム障害発生時に備えてBCPを策定している医療機関は27%にとどまり、その策定状況は十分ではない事が明らかになった（調査対象医療機関数8171、有効回答数5353施設）。（参考：令和５年調査時23%）

○　そのため、サイバー攻撃を想定した医療機関における策定の一助となるよう、BCP策定のための確認表等を厚生労働科学特別研究事業において作成した（令和６年６月６日付け事務連絡「「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」）。

令和５年度厚生労働科学特別研究事業「医療機関におけるサイバー攻撃対応のための事業継続計画（BCP）の普及に向けた研究」

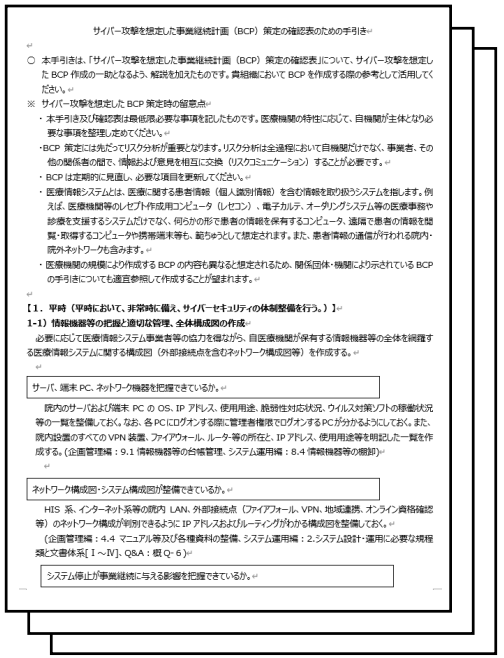
サイバー攻撃を想定した事業継続計画（BCP）のための確認表等

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。

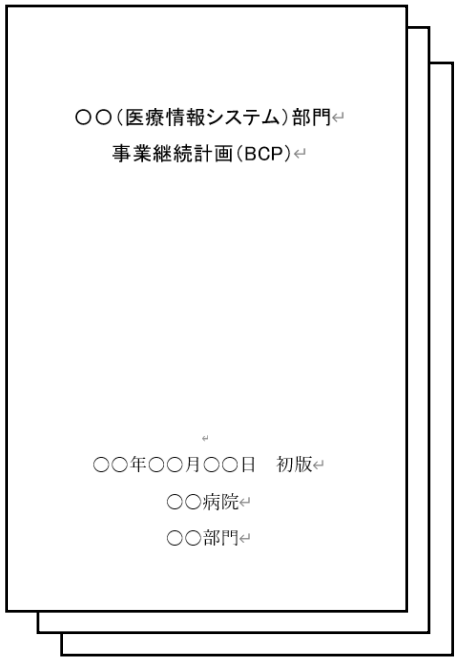
院内のサーバおよび端末 PC の OS、IP アドレス、使用用途、脆弱性対応状況、ウイルス対策ソフトの稼働状況等の一覧を整備しておく。なお、各 PC にログオンする際に管理者権限でログオンする PC が分かるようにしておく。また、院内設置のすべての VPN 装置、ファイアウォール、ルータ等の所在と、IP アドレス、使用用途等を明記した一覧を作成する。（企画管理編：9.1 情報機器等の台帳管理、システム運用編：8.4 情報機器等の棚卸）

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（ファイアウォール、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

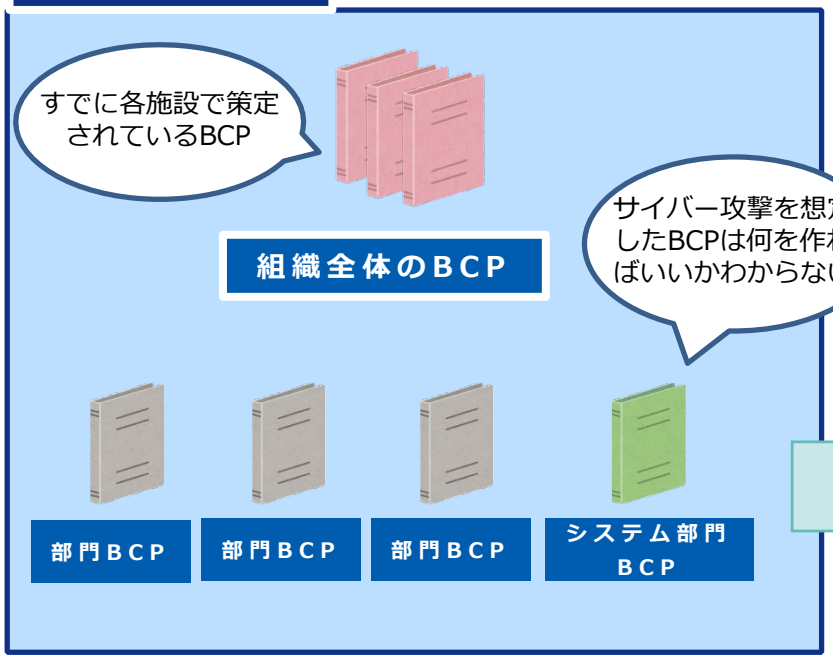

○○（医療情報システム）部門
事業継続計画（BCP）

○○年○○月○○日　初版
○○病院
○○部門

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

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

イメージ



事業継続のための方針・基準に関する記載の例

- サイバー攻撃を受けた際に医療機関等が医療サービス提供を継続する方法の記載
- 段階毎に医療情報システムをどのように利用・切り替え・縮退するかの記載 など

医療情報システム部門の継続・復旧手順に関する記載の例

- 医療情報システムや医療機器等の障害が見受けられる場合に、早期に医療情報システム安全管理責任者へ報告し、異常内容の事実確認を行う記載
- 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記載
- 医療情報システムのベンダ及びサービス事業者等と協力して短時間で復旧を行う記載 など

医療情報システム部門のBCP

組織全体のBCP

サイバー攻撃を想定した事業持続計画（BCP）策定の確認表を参考にする範囲
※ 医療情報システム部門のない医療機関についても、適宜参考として作成。

参考：2024年度診療報酬改定

【診療録管理体制加算1】（新設）140点

・非常時を想定した**医療情報システムの利用が困難な場合の対応や復旧にいたるまでの対応について業務継続計画（BCP）を策定**し、少なくとも年1回程度、定期的に訓練・演習を実施すること。また、その結果を踏まえ、必要に応じて改善に向けた対応を行っていること。

「医療情報システムの契約における当事者間の役割分担等に関する確認表」

○　近年の医療機関における情報セキュリティインシデント発生時の課題として、医療情報システムに関する契約の際に、医療機関と医療情報システム・サービス事業者との役割分担等が適切に協議されていなかったことが挙げられる。

○　契約上役割分担等が曖昧な点について、可能な限り、事前に双方の役割分担等について取り決め、有事の際に即座に対応できるよう、契約の段階で合意形成文書（契約書やサービス・レベル合意書（SLA）等）に落とし込むことが重要である。役割分担等を事前に取り決め、医療情報システム全体を漏れなく俯瞰的にとらえることは、情報セキュリティインシデントの予防にもつながるものと考えられる。

○　こうしたことから、医療情報システムの契約において、医療機関と事業者が役割分担等を協議する上で必要な項目について、具体化を図ることを目的として、総務省・経済産業省・厚生労働省において「医療情報システムの契約のあり方等に関する有識者委員会」を開催し、確認表として取りまとめた。

医療情報システムの契約における当事者間の役割分担等に関する確認表

Part１　主に医療機関が実施する項目

（契約を締結する上で医療機関が主体となって、必要に応じてシステム関連業者の協力を得ながら実施することが望ましい項目の例）

＊が付けられている用語については、別添の「用語の解説」を適宜参照すること。

項番	項目	内容	初回確認（　/　）	完了日（日付）	備考欄
A	事業者選定・事業者管理				
1	事業者からの開示資料の確認	事業者から開示を受けたサービス仕様適合開示書[*1]等（MDS/SDS[*2]、MDS2[*3]等）を確認しているか。	はい・いいえ	（　/　）	
2	事業者管理	①事業者との契約・協働体制を把握・管理できているか。	はい・いいえ	（　/　）	
		②医療情報を第三者提供する場合の管理体制が整備されているか。	はい・いいえ	（　/　）	
B	医療機関の内部体制				
1	「医療情報システムの安全管理に関するガイドラ	「医療情報システムの安全管理に関するガイドライン」を確認した	はい・いいえ	（　/　）	

医療情報システムの契約における当事者間の役割分担等に関する確認表

Part２　医療機関と事業者が共同で実施する項目

（技術的な対策等医療機関だけでは実施することが困難な事項で、役割分担等を明確にしておくことが望ましい項目の例）

＊が付けられている用語については、別添の「用語の解説」を適宜参照すること。

項番	項目	内容	初回確認（　/　）	完了日（日付）	備考欄
A	共通				
1	「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」の確認	事業者は「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」を確認する。	はい・いいえ	（　/　）	
2	複数事業者間の役割分担	医療機関が複数事業者と契約する場合における、事業者間の役割分担及び抜け漏れがないことを確認する。	はい・いいえ	（　/　）	

2024/６/３　HP公表

https://www.meti.go.jp/shingikai/mono_info_service/medical_information_system/index.html

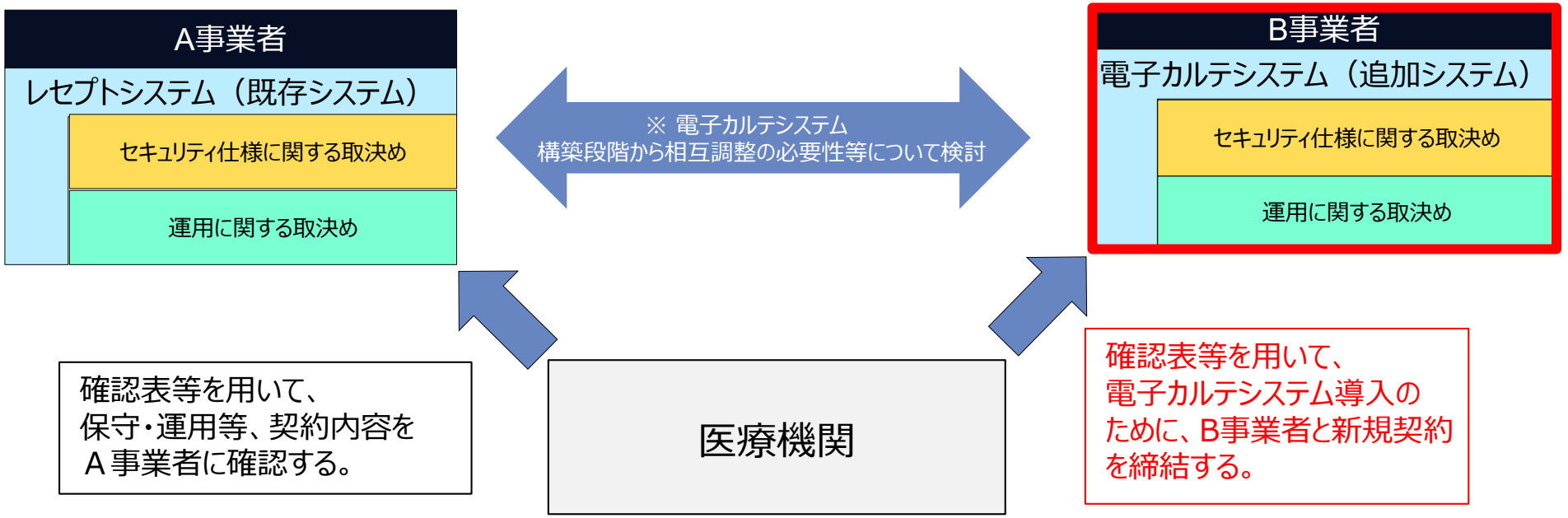
「医療情報システムの契約における当事者間の役割分担等に関する確認表」の利用イメージ

具体的には、以下の例のように、新規契約等で機器の導入が医療機関において発生した場合に、新規で契約を行う事業者や既存で契約を行っている事業者と医療機関の間で役割分担の抜けがないように、確認表を用いて保守・運用等の契約内容について相互に調整等を行い取り決める。

（例）既にレセプトシステム（A事業者）を導入しており、新たに電子カルテシステムを導入するためにB事業者と契約を締結する場合

- 医療機関は、確認表等を用いて、保守・運用等、既存の契約内容をＡ事業者に確認する。
- 加えて、電子カルテシステムの導入に際して、確認表等を用いて、B事業者との契約内容を確認する。

※ 事業者間の役割及び抜け漏れがないように、電子カルテシステム構築段階から事業者間で相互調整等を行う。
B事業者は、医療機関との新規契約の中で、A事業者との相互調整の必要性等について検討を行う。
A事業者は、医療機関との既存契約の中で、B事業者との相互調整の必要性等について検討を行う。



推進枠

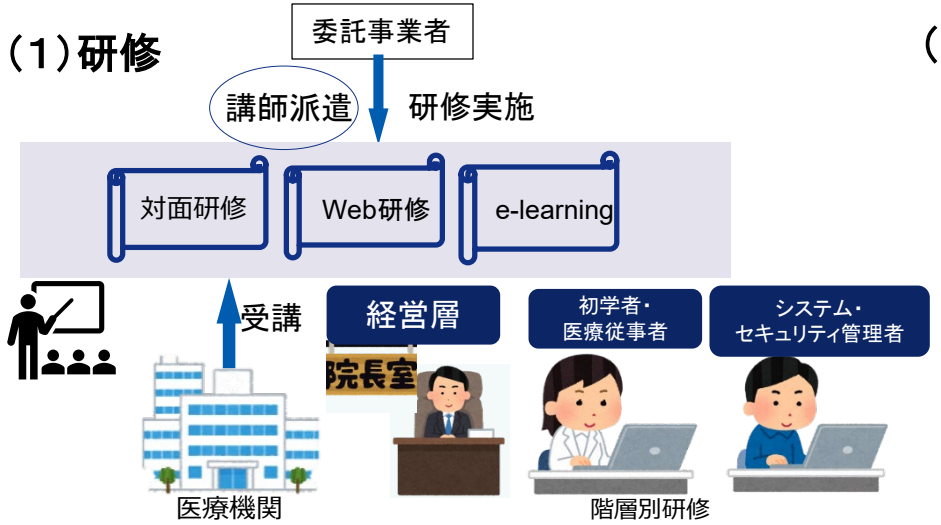
医療分野におけるサイバーセキュリティ対策調査事業

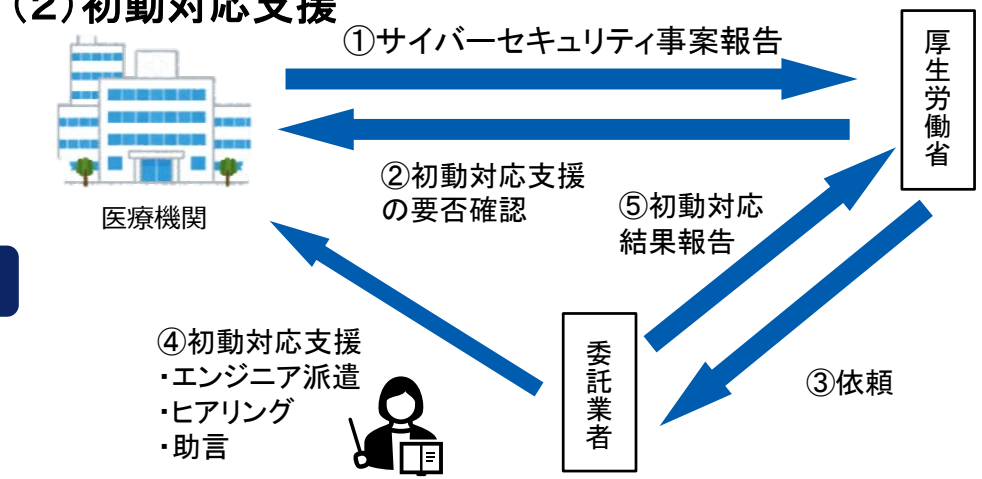
令和６年度概算要求額　1.0億円（1.0億円）　※（）内は前年度当初予算額

1　事業の目的

○医療機関のセキュリティ対策は、「医療情報システムの安全管理に関するガイドライン」に基づき、各医療機関が自主的に取組を進めてきているところである。昨今のサイバー攻撃の増加やサイバー攻撃により長期に診療が停止する事案が発生したことから実施した緊急的な病院への調査では、自主的な取組だけでは不十分と考えられる結果であった。
○医療機関の医療情報システムがランサムウェアに感染すると、保有するデータ等が暗号化され、電子カルテシステム等が利用できなくなることにより、診療を長時間休止せざるを得なくなることから、医療機関におけるサイバーセキュリティ対策の充実は喫緊の課題となっている。
○医療機関のサイバーセキュリティ対策の徹底を図るべく、医療従事者や経営層等へのセキュリティ対策研修の実施、及び医療機関においてサイバーセキュリティインシデントが発生した際の初動対応支援を実施することを目的とする。

2　事業の概要・スキーム





※事業の拡充としては、サイバーセキュリティインシデントに備え、BCPに沿った訓練等の研修の実施とサイバー攻撃の被害が増加している事を踏まえた、初動対応支援可能な医療機関数の増加である。

3　実施主体等

委託先：委託事業（民間事業者）

4　事業実績

◆ 研修受講者数：約9000人（約3500人）
※　令和５年度実績
括弧は令和４年度

◆ 初動対応支援数：２件
※令和５年度実績
（令和４年度から開始）

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

令和６年９月より開始

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

▼研修種別と内容

種別	内容　※
経営者向け研修	セキュリティの重要性理解を求め、経営者に気づきを与える研修。今年度は以下の3コースを提供予定。 ・IT ガバナンスコース 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」「組織の制度との連動性」など俯瞰した内容で学習 ・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	技術の深掘りを図る一方で、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する研修。ワークショップ、実機演習など対面型の研修も実施。 今年度は以下の3コースを提供予定。 ・復習コース 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。 ・新規コース SecBok(※1)より「OS の基礎」「IT・セキュリティ基礎」「セキュリティマネジメント」の指標を用いた内容を学習 ・連携コース 国立研究開発法人情報通信研究機構（NICT）のサイバーセキュリティネクサス（CYNEX）を利用し、インシデント対応体験やログ解析などの調査方法をワークショップや演習を通じて学習
初学者等向け研修	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、日常でも役立ち、自分たちで今すぐできる備え等ついて学習する研修。今年度は情報処理推進機構が公開している「情報セキュリティ10大脅威2024」などを参考に2コース提供予定。
立入検査コース	医療法に基づく立入検査において、「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。昨年度参考項目だった「サイバー攻撃を想定した事業継続計画（ BCP ）の策定方法等」についても解説予定。
講師育成コース	自医療機関で IT-BCP を策定し、それを用いた訓練を実施、ファシリテートできる人材を育成する研修
e-learning	過去の各研修の動画をアーカイブとして配信