資料７－３

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組

厚生労働省医政局医療情報担当参事官室

Ministry of Health, Labour and Welfare of Japan

令和7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おり、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「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」等により示している。（薬局については、同様に、薬機法施行規則を改正して対応）

・一部内容を改定し、**令和７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**及び**サイバーセキュリティ対策チェックリストマニュアル**を発出する予定。

主な修正点（案）

【追加項目】
- パスワードの桁数の規定、使い回しの禁止
- USBストレージ等の外部接続機器に対しての接続制限
- 二要素認証の実装（令和９年度実装に向けた対応）
- 運用管理規程等の整備

【その他修正】
- アクセス利用権限の設定について、管理者権限の対象者を明確化しているかを注記
- セキュリティパッチの項目等、端末PC・サーバ・ネットワーク機器等それぞれに求めていた項目を「医療情報システム全般」についての質問へ統合

※各項目の詳細についてはサイバーセキュリティ対策チェックリストマニュアル等を適宜修正記載する。

令和7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

令和７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

*立入検査時、本チェックリストを確認します。令和7年度中にすべての項目で「はい」にマルが付くよう取り組んで
*「いいえ」の場合、令和7年度中の対応目標日を記入してください。

	チェック項目	確認日	目標日
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)	はい・いいえ （　/　）	（　/　）
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**		
	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)	はい・いいえ （　/　）	（　/　）
	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等に確認した。(2-②) ※事業者と契約していない場合には、記入不要	はい・いいえ （　/　）	（　/　）
	事業者から製造業者/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）を提出してもらう。(2-③) ※事業者と契約していない場合には、記入不要	はい・いいえ （　/　）	（　/　）
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。※管理者権限対象者の明確化を行っている(2-④)	はい・いいえ （　/　）	（　/　）
	退職者や使用していないアカウント等、不要なアカウントを削除または無効化している。(2-⑤)	はい・いいえ （　/　）	（　/　）
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-⑥)	はい・いいえ （　/　）	（　/　）
	パスワードは英数字、記号が混在した8文字以上とし、定期的に変更している。※二要素認証、または13文字以上の場合は定期的な変更は不要(2-⑦)	はい・いいえ （　/　）	（　/　）
	パスワードの使い回しを禁止している。(2-⑧)	はい・いいえ （　/　）	（　/　）
	USBストレージ等の外部記録媒体や情報機器に対して接続を制限している。 (2-⑨)	はい・いいえ （　/　）	
	二要素認証を実装している。または令和９年度までに実装予定である。(2-⑩)	はい・いいえ （　/　）	（　/　）
	サーバについて、以下を実施している。		
	アクセスログを管理している。(2-⑪)	はい・いいえ （　/　）	
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-⑫)	はい・いいえ （　/　）	
	端末PCについて、以下を実施している。		
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-⑫)	はい・いいえ （　/　）	
	ネットワーク機器について、以下を実施している。		
	接続元制限を実施している。(2-⑬)	はい・いいえ （　/　）	
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）への連絡体制図がある。(3-①)	はい・いいえ （　/　）	
	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)	はい・いいえ （　/　）	
	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)	はい・いいえ （　/　）	
4 規程類の整備	上記1-3のすべての項目について、具体的な実施方法を運用管理規程等に定めている。(4-①)	はい・いいえ （　/　）	

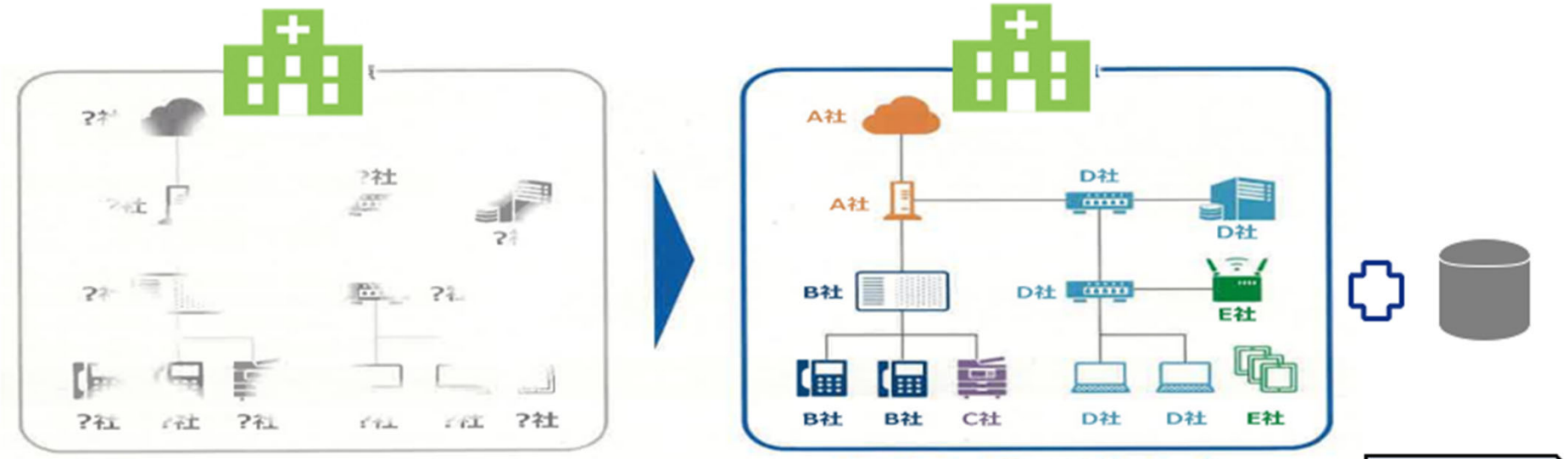
※薬局用・事業者確認用においても同様に改訂
※目標日・備考欄を省略して表示

医療機関におけるサイバーセキュリティ確保事業

令和5年度補正予算　36億円

- 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、診療の一部を長時間休止せざるを得なくなることから、医療機関等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。
- そのため、医療機関におけるサイバーセキュリティの更なる確保を行う。

- 厚生労働省では、全ての外部ネットワーク接続点を確認することを求めているが、中・大規模病院は多数の部門システムで構成されているため、各システムを提供する事業者と個別に連携しても、全てのネットワーク接続を俯瞰的に把握することは困難である可能性がある。
- また、ランサムウェア対策にはオフライン・バックアップが有効であることを踏まえ、厚生労働省ではオフライン・バックアップ整備を求めている。
- 医療機関におけるサイバーセキュリティの更なる確保のため、外部ネットワークとの接続の安全性の検証・検査や、オフライン・バックアップ体制の整備を支援する。



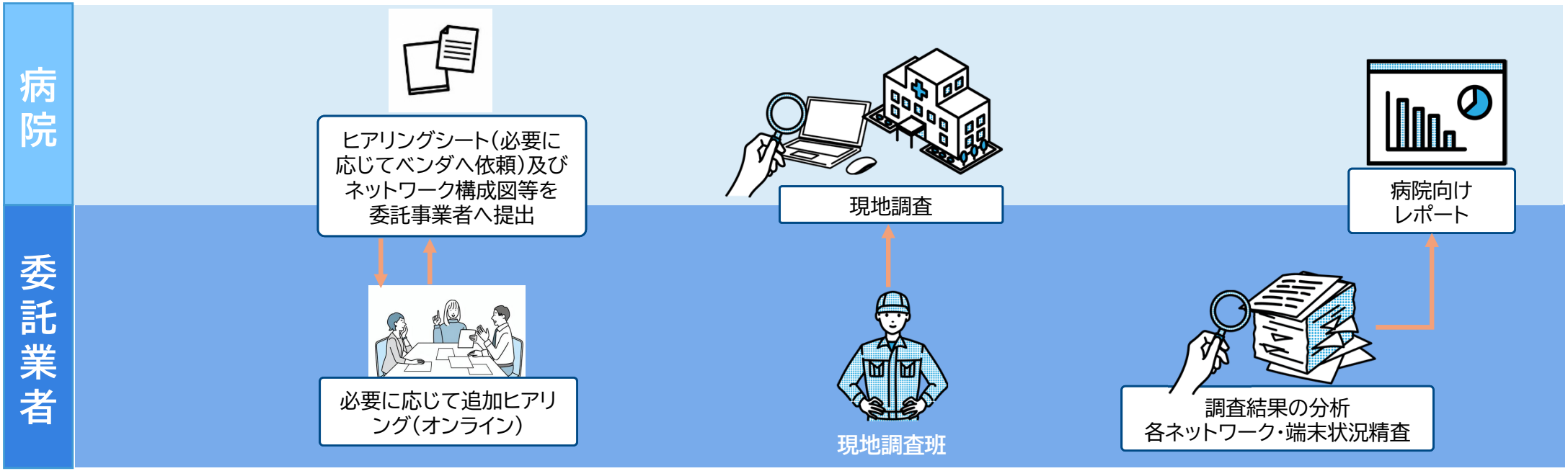
現状のネットワーク構成等が不明

ネットワーク構成等がみえる化

外部ネットワーク接続の俯瞰的把握、安全性の検証・調査（進め方）

事業概要

	①資料収集・ヒアリング	②現地調査・脆弱性診断	③レポート提出
現地調査	病院からネットワーク図、機器・回線一覧、端末情報等、調査に必要な情報をご提供いただく	外部接続拠点とその周辺機器の調査を実施いたします	現地調査報告
脆弱性診断	上記、機器・回線一覧で情報提供いただく	ご提供いただいたIPアドレス等に対して脆弱性診断を実施いたします	脆弱性診断・調査報告



オフラインバックアップの整備支援（全体像）

事業概要

- ランサムウェア対策において重要な対策手段となり得る「オフラインバックアップ」について、病院のバックアップ取得状況を適切に把握した上で、オフラインバックアップ計画書の策定、構築支援、構築後の継続的な運用・維持について、病院・電子カルテベンダーと協力しながら実施します。

オフラインバックアップ計画の策定

■対象病院の電子カルテバックアップ状況の把握

※ヒアリングシート等

・オンライン/オフラインバックアップの有無
・バックアップの目的、対象データ
・バックアップ方法、取得媒体　等

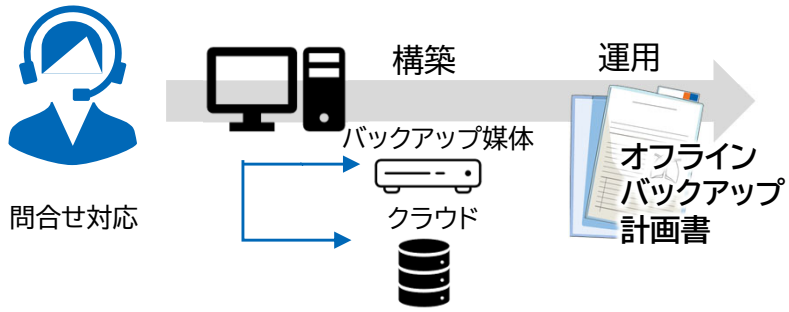
■オフラインバックアップ未実施病院の構築支援に向けた技術方式・実現方法、運用・維持の検討

・病院個々の現状を踏まえた適切な方式の検討、決定
・病院、電子カルテベンダとの役割（事前準備、構築、運用開始時）の明確化　等
⇒オフラインバックアップ計画の合意

オフラインバックアップ構築支援

■オフラインバックアップの円滑な実施に向けた現地構築支援作業

・病院での事前準備（必要経費、機器購入等）に関する支援
・事前検証済の推奨機器・構成で現地構築作業の実施
・構築後の円滑な運用・維持に向けた支援
（オフラインバックアップ計画書に反映）



必要な機器・サービスやそれらの調達にかかる費用、保守費用、電子カルテベンダーの設定費等は本事業の対象外。

取り組み事例集の紹介について

医療機関種別	急性期／回復期 200～400床未満（290床）	情シス体制	職員：5名体制 （全員常勤）	事例掲載区分	■ 医療情報システムに関する全体管理 □ 情報機器や端末、その他情報資産の整備・管理 ■ 保守契約、サービス利用契約の責任分界点、SLA整備
キーワード	システムや院内ネットワーク・回線数の集約、ベンダーの一元化、 電子カルテの更改タイミング				

区分	医療情報システムに関する全体管理	医療情報システムに関する全体管理	保守契約、サービス利用契約の責任分界点、SLA整備
課題	①情シスでシステムや機器、回線、保守契約などの情報を把握できていない Before　システム・回線が多数存在 After　可能な限り仮想化サーバ上へシステム集約し回線も一元化	② 部門独自でシステム導入・管理を実施 Before　部門ごとに独自にシステム導入 After　電子カルテ委員会を通じて情シス経由で導入	②医療情報システム全体の導入方針に一貫性がない Before　保守の取り決めや責任分解点が不明確 After　ベンダー管理（導入・保守）が可能な病院のルールを策定
取り組み内容	システムや機器、回線を一元化し管理対象を最小化した	電子カルテ委員会（月1回）を通じ、部門毎のシステム導入情報が共有できる体制を構築した	法人全体の医療情報システム全体を設計し、長期的な導入・運用計画を策定、実行した
取り組みの工夫点	• 電子カルテの**更改を契機**に法人全体で見直し • 電子カルテベンダー選定時に**サーバ仮想化による各システムを統合可能な**ベンダーを選定（可能な限り1社へ集約） • 院内LANも含めた**ネットワーク統合、保守・運用が実施できる**ネットワークベンダーを選定	• 新システムの企画・設計を情シスだけではなく、電子カルテ委員会のメンバーの意見を汲んで実施 • 電子カルテ委員会**メンバーにITに明るい各部門の医師も加え**、部門の意見・情報を集約	• 情シスが、部門から委員会に参画しているリーダーの意見を汲み取り、導入・運用の全体計画を策定 • 電子カルテの更改を契機に計画を実行、**部門システムも更改時に統合** • **長期計画の実現、運用が可能な**ベンダーを選定
効果（メリット）	• システム最小化に伴うトータルコストの縮小 **サーバ数55%減、導入コスト40%減（旧システム比）** • コミュニケーション対象のベンダー最小化 • 情報システム部の情報資産管理の稼働削減	• **部門毎の新たなシステムの導入状況の把握が可能**となる • **部門横断でセキュリティ対策等に関する情報の周知・展開が可能**となる • 部門間のコミュニケーションの醸成	• リモート接続も含めたシステムや回線集約の実現 • 医療情報システム全体の把握、管理が可能となる

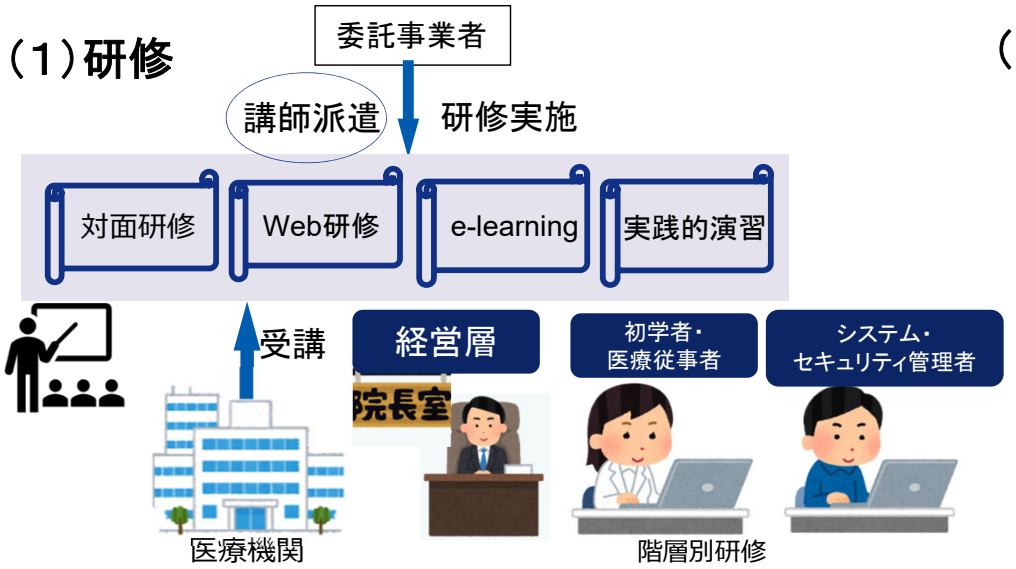
医療分野におけるサイバーセキュリティ対策調査事業

1 事業の目的

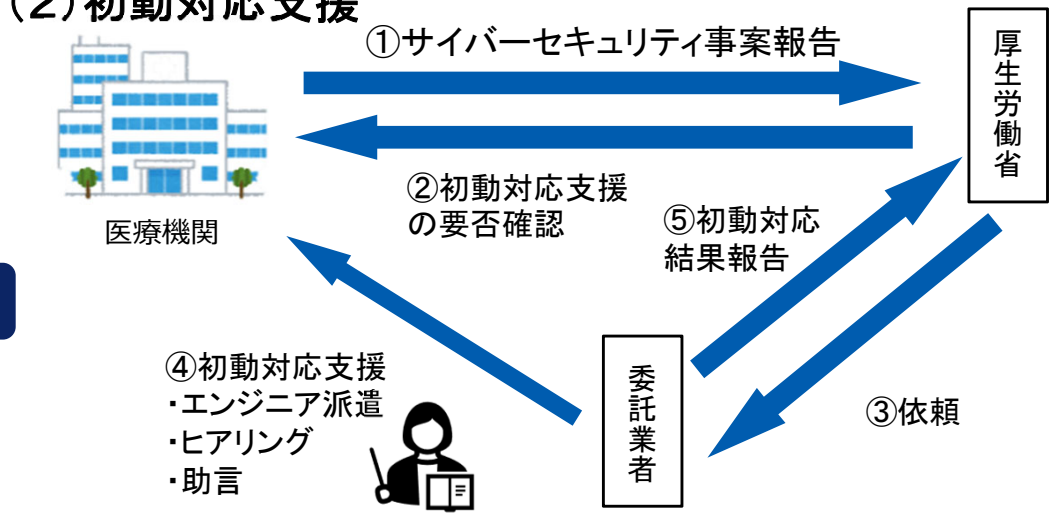
○医療機関のセキュリティ対策は、「医療情報システムの安全管理に関するガイドライン」に基づき、各医療機関が自主的に取組を進めてきているところである。昨今のサイバー攻撃の増加やサイバー攻撃により長期に診療が停止する事案が発生したことから実施した緊急的な病院への調査では、自主的な取組だけでは不十分と考えられる結果であった。
○医療機関の医療情報システムがランサムウェアに感染すると、保有するデータ等が暗号化され、電子カルテシステム等が利用できなくなることにより、診療を長時間休止せざるを得なくなることから、医療機関におけるサイバーセキュリティ対策の充実は喫緊の課題となっている。
○医療機関のサイバーセキ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

（1）研修



（2）初動対応支援



※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た、情報セキュリティ担当者向けの実践的演習の追加である。

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9500人（約9000人）
※ 令和６年度実績
括弧は令和５年度

◆ 初動対応支援数：４件（２件）
※令和６年度実績（随契期間含む）
括弧は令和５年度