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

医療情報セキュリティ等対策経費

厚生労働省 医政局 参事官（医療情報担当）
付医療情報室

Ministry of Health, Labour and Welfare of Japan

1

- 医療機関におけるサイバー攻撃の現状

「重要インフラのサイバーセキュリティに係る行動計画」の概要

「重要インフラのサイバーセキュリティに係る行動計画」の概要

官民連携による重要インフラ防護の推進

- 任務保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現
- 官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進

NISCによる総合調整

重要インフラ所管省庁

- 金融庁 ［金融］
- 総務省 ［情報通信、行政］
- 厚生労働省 ［医療］
- 経済産業省 ［電力、ガス、化学、クレジット、石油］
- 国土交通省 ［航空、空港、鉄道、水道、物流、港湾］

重要インフラ(全１５分野)

- 情報通信
- 金融
- 航空
- 空港
- 鉄道
- 電力
- ガス
- 政府・行政サービス
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油
- 港湾

関係機関等

- サイバーセキュリティ関係省庁 ［総務省、経済産業省等］
- 事案対処省庁 ［警察庁、防衛省等］
- 防災関係府省庁 ［内閣府、各省庁等］
- サイバーセキュリティ関係機関 ［NICT、IPA、JPCERT/CC等］
- サイバー空間関連事業者 ［サプライチェーン等に関わるベンダー等］

「重要インフラのサイバーセキュリティに係る行動計画」における主な取組

障害対応体制の強化

経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組となるよう、組織統治の一部としての障害対応体制の強化を推進

安全基準等の整備及び浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

情報共有体制の強化

官民間や分野内外間における情報共有体制の更なる強化

リスクマネジメントの活用

自組織の特性を明確化し、適した防護対策が継続的に実施されるようリスクマネジメントを活用

防護基盤の強化

分野横断的演習の推進、国際連携の推進、広報広聴活動の推進等の取組によるサイバーセキュリティ全体の底上げ

出典：内閣サイバーセキュリティセンターのウェブサイトより引用

医療機関におけるサイバー攻撃の現状

第12回健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ（令和４年５月27日）資料１抜粋

医療機関からの報告について

○　平成19年３月から、「医療情報システムの安全管理に関するガイドライン」に基づき、医療機関等においてサイバー攻撃等のインシデント事案が発生した場合は、当該医療機関等から厚生労働省等の所管官庁へ報告することを求めている。

○　また、都道府県等に対しては、平成30年10月に通知（「医療機関等におけるサイバーセキュリティ対策の強化について」（医政総発1029 第１号　医政地発1029 第３号　医政研発1029 第１号　平成30年10月29日））を発出し、必要に応じて管内の医療機関等における被害状況、対応状況等に係る調査及び指導を行うとともに、厚生労働省へ報告することを求めている。

診療に及ぼす影響について

１．一般に、ランサムウェアによるサイバー攻撃は**情報の暗号化**と**情報の詐取**と**金銭の要求**がセットとなっていることが多いが、**情報の詐取が確認された場合には個人情報漏洩事案となる**。

２．保存すべき診療録等が滅失・毀損する。また、患者の病歴等について再度の聴取等が必要となることによる**患者側も負担増加**。

３．過去の患者カルテと、来院した患者の氏名等といった基礎情報が電子的に突合できず、対面での指差し確認等の手作業で本人確認が必要。医療従事者が慣れない紙カルテでの運用に追われることになる**医療者側の負担増加**。

被害の状況により、診療報酬の請求事務に影響を及ぼすことがあるほか、診療データの継続的な提出を評価する「データ提出加算」の算定や、「データ提出加算」を前提とする入院料の届出に影響が生じる場合がある。

医療機関に対するランサムウェア攻撃の状況

○2022年10月31日に発生した大阪急性期･総合医療センターの事例においては、発生当日から5日間、三次救急と小児救急のほか予定手術も停止した。10日後から三次救急と小児救急の受け入れを一部再開している。一方、周辺医療機関との連携等により、患者の生命等への影響はなかった。

○2024年５月に地方独立行政法人岡山県精神科医療センターでもランサムウェア攻撃の事例が発生しているが、電子カルテを紙カルテ運用で代替し、発生当初より予約外来及び救急外来、入院診療を継続しており、地域医療提供体制は問題が生じていない。

○大阪急性期・総合医療センターの事例以降、厚生労働省からも専門家から構成される初動対応支援チームを派遣。

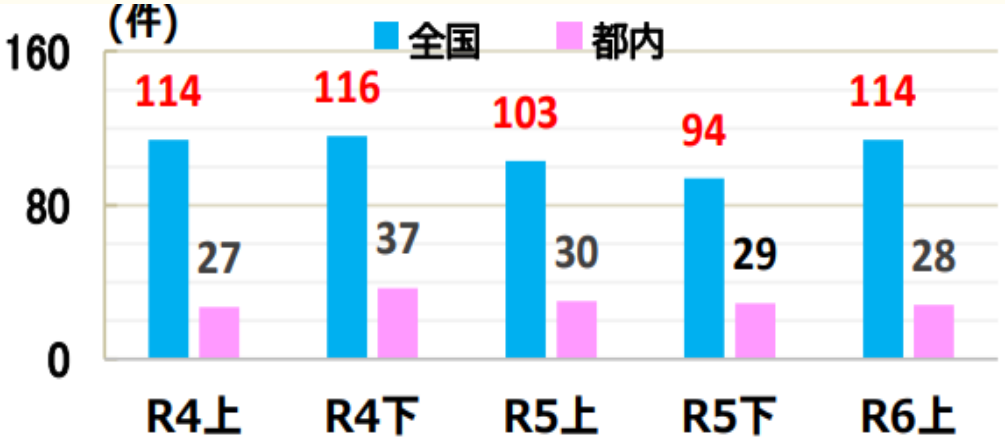
○散発的なサイバー攻撃事案は発生しているものの、長期にわたって診療が停止する事態は発生していない。

＜病院における主なランサムウェア攻撃の事例＞

発生	都道府県	医療機関名	病床	機能別区分	診療機能への影響、発生後の経過
2021.10	徳島県	つるぎ町立半田病院	120床	災害拠点病院 へき地医療拠点病院	三次救急受入と一般外来を停止。産科と小児科以外の治療行為を含む診療業務が**２か月に及んで滞った**。 **システム全面復旧までには２か月程度を要した**。
2022.10	大阪府	大阪急性期･総合医療センター	865床	高度急性期病院	三次救急と小児救急の受け入れを**10日間停止**。 発生から一か月後も一般外来を再開できなかった。 **システム全面復旧までには２か月程度を要した**。
2024.3	鹿児島県	鹿児島県医療生活協同組合 国分生協病院	129床	地域医療支援病院	救急と新規外来患者の受け入れ**10日間停止**。 （地区医師会等との連携で地域医療提供体制は維持） **システムの全面復旧までには１か月程度を要した**。
2024.5	岡山県	地方独立行政法人 岡山県精神科医療センター	252床	精神科救急医療施設 応急入院指定病院 ほか	発生当日から**一般及び救急外来、入院診療を継続**。 **システム全面復旧までには１か月程度を要した**。

ランサムウェア被害が高い水準で推移

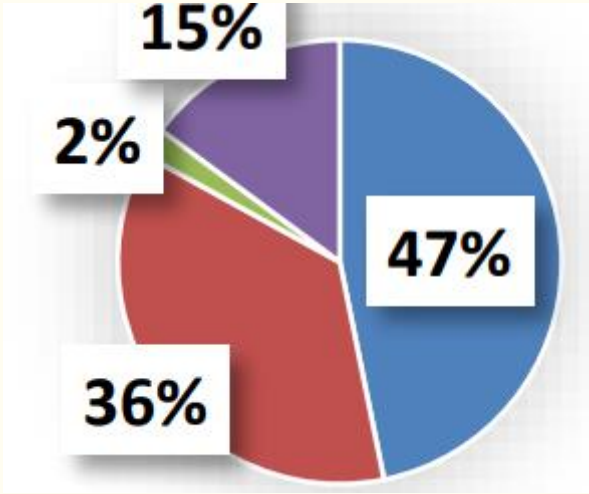
ランサムウェア被害の報告件数の推移



◆ ランサムウェア被害の特徴

- 令和６年上半期においても、被害は高水準で推移している。
- 手口としては、データの暗号化のみならず、データを窃取した上、「対価を支払わなければ当該データを公開する」などと対価を要求する「二重恐喝」による被害が多くを占める。

感染経路



出典：令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）
ランサムウェアの被害に係る統計
企業・団体等における被害の報告件数の推移（左図）
ランサムウェア被害にあった企業・団体等へのアンケート調査の回答（右図）

医療機関におけるサイバーセキュリティ対策に関する調査研究結果

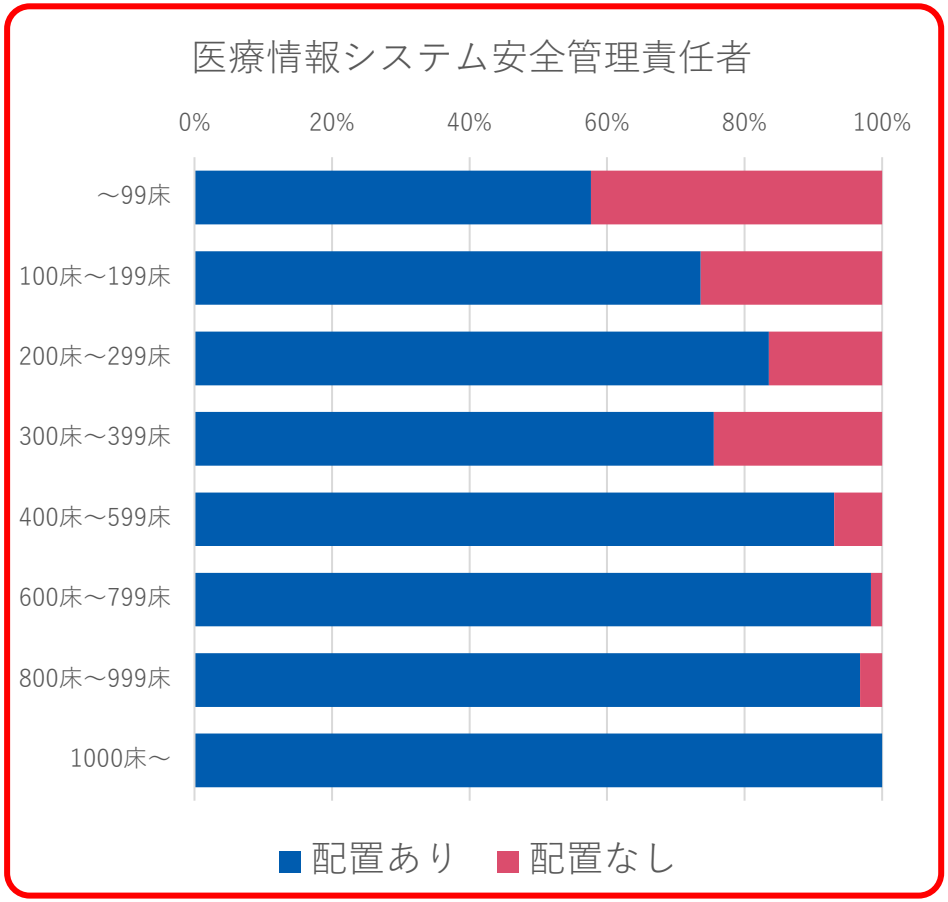
主な調査	調査内容	主な結果・課題
医療機関の サイバーセキュリティ 確保に関する現地調査	医療機関におけるネットワーク構成図等の 情報資産やバックアップ整備状況 に関する現地調査 ※実施期間：令和４年１月～３月 ※調査対象：11医療機関 ※各医療機関の病床規模 ~199床：3、200～399床：2、400床～：6	・情報資産台帳等で**把握されていない** 情報機器及び外部接続部が存在。 ・下記2パターンがあり ①外部接続部が数カ所に集約化 ②検査機器毎の保守回線等、 **外部接続点が多数** 医療機関ごとの状況は様々である。 （外部接続部：７～47カ所/医療機関）
医療機関の サイバーセキュリティ に関する意識調査	サイバーセキュリティ対策の実施状況や 施設内の運用規程の有無、 インシデント発生時の対応方法等 に関するアンケート調査 ※実施期間：令和４年9月～11月 ※調査対象：日本病院会会員2489会員 （回答数581会員、回答率23%）	・多くの院内ネットワークが異なった ベンダーにより形成されており **全体図を俯瞰的に把握できていない。** ・**バックアップ接続時の設定**が 適切になされていない。 ・ネットワークセキュリティのための 必要最低限の設定がなされていない。 ・インシデント発生時に対応できる 人材の不足。

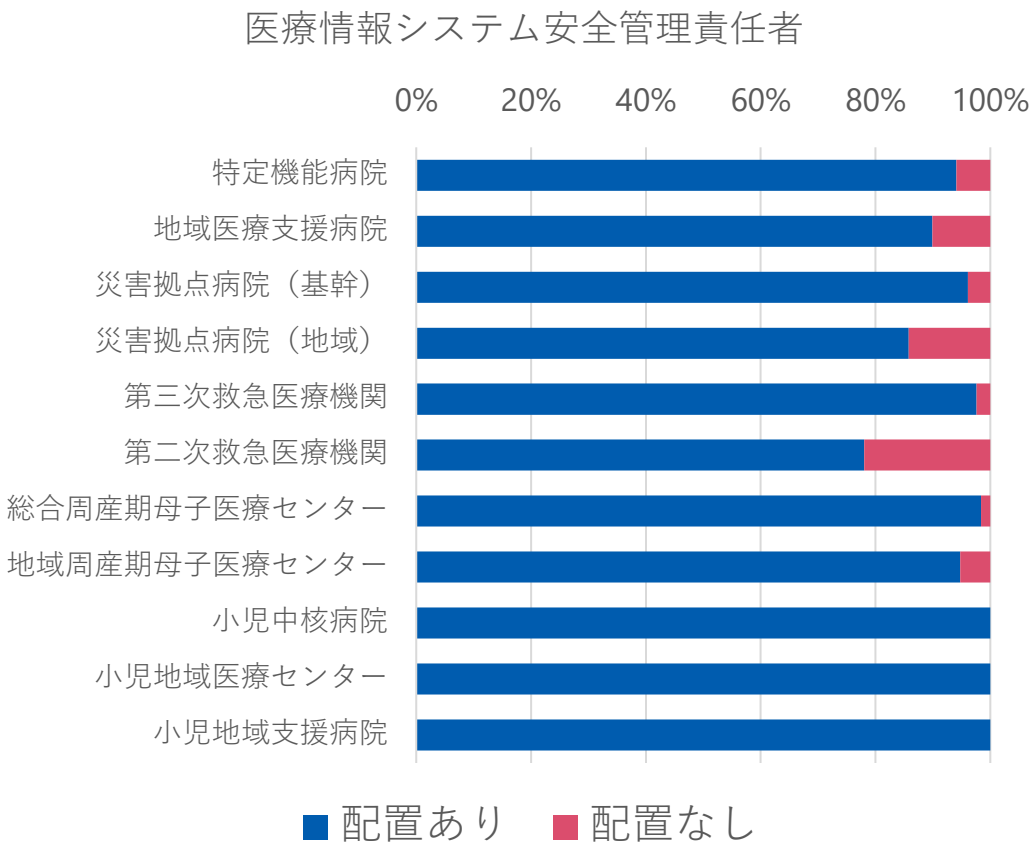
*厚生労働科学研究費補助金
「医療分野の情報化の推進に伴う医療機関等におけるサイバーセキュリティ対策のあり方に関する調査研究（令和3-4年度，研究代表者：近藤博史）」

医療情報システム安全管理責任者の配置状況

※令和5年度厚生労働行政推進調査地域医療基盤開発推進研究事業
「安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究」資料より

医療情報システム安全管理責任者
配置あり　521施設　配置なし　122施設





病床規模が小さい施設ほど、人材の配置がされない傾向にある

（参考）電子カルテシステムの普及状況の推移

出典：医療施設調査（厚生労働省）

	一般病院（※１）	病床規模別			一般診療所（※２）
		400床以上	200～399床	200床未満	
平成 20年	14.2 % (1,092／7,714)	38.8 % (279／720)	22.7 % (313／1,380)	8.9 % (500／5,614)	14.7 % (14,602／99,083)
平成 23年（※３）	21.9 % (1,620／7,410)	57.3 % (401／700)	33.4 % (440／1,317)	14.4 % (779／5,393)	21.2 % (20,797／98,004)
平成26年	34.2 % (2,542／7,426)	77.5 % (550／710)	50.9 % (682／1,340)	24.4 % (1,310／5,376)	35.0 % (35,178／100,461)
平成 29年	46.7 % (3,432／7,353)	85.4 % (603／706)	64.9 % (864／1,332)	37.0 % (1,965／5,315)	41.6 % (42,167／101,471)
令和 2年	57.2 % (4,109／7,179)	91.2 % (609／668)	74.8 % (928／1,241)	48.8 % (2,572／5,270)	49.9 % (51,199／102,612)
令和 5年	65.6 % (4,638／7,065)	93.7 % (609／650)	79.2 % (956／1,207)	59.0 % (3,073／5,208)	55.0 % (57,662／104,894)

【注　釈】
（※１）　一般病院とは、病院のうち、精神科病床のみを有する病院及び結核病床のみを有する病院を除いたものをいう。
（※２）　一般診療所とは、診療所のうち歯科医業のみを行う診療所を除いたものをいう。
（※３）　平成23年は、宮城県の石巻医療圏、気仙沼医療圏及び福島県の全域を除いた数値である。

医療情報セキュリティ等対策経費の事業概要（RSシート記載内容）

1 事業概要

〇昨今、国内の医療機関を標的としたランサムウェアによるサイバー攻撃被害が増加（ランサムウェアにより、長期にわたり診療が停止した複数の事例が発生）したことから、医療機関のサイバーセキュリティ対策の徹底を図る。

〇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等を実施する。

2 現状・課題

〇病院などの保健医療に関わる組織・団体でデジタルトランスフォーメーション(DX)を推進することは保健医療行政において急務とされており、その実務を担当しリーダーとして活躍する人材が求められている。

〇近年の医療機関を標的としたサイバー攻撃に対して、研修等を通じて平時からの対策徹底の周知や、実際に攻撃を受けた際の初動対応の支援が必要である。

〇厚生労働省では医療機関に全ての外部接続ネットワーク接続点を確認することを求めているが、特に中・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、そのネットワーク接続を俯瞰的に把握することが重要である。

〇サイバーセキュリティ事案が生じた際の速やかな復旧のためには、オフライン・バックアップが有効であり、医療機関においてオフライン・バックアップ環境を整備することが重要である。

2

- **医療分野におけるサイバーセキュリティ対策調査事業**

拡充

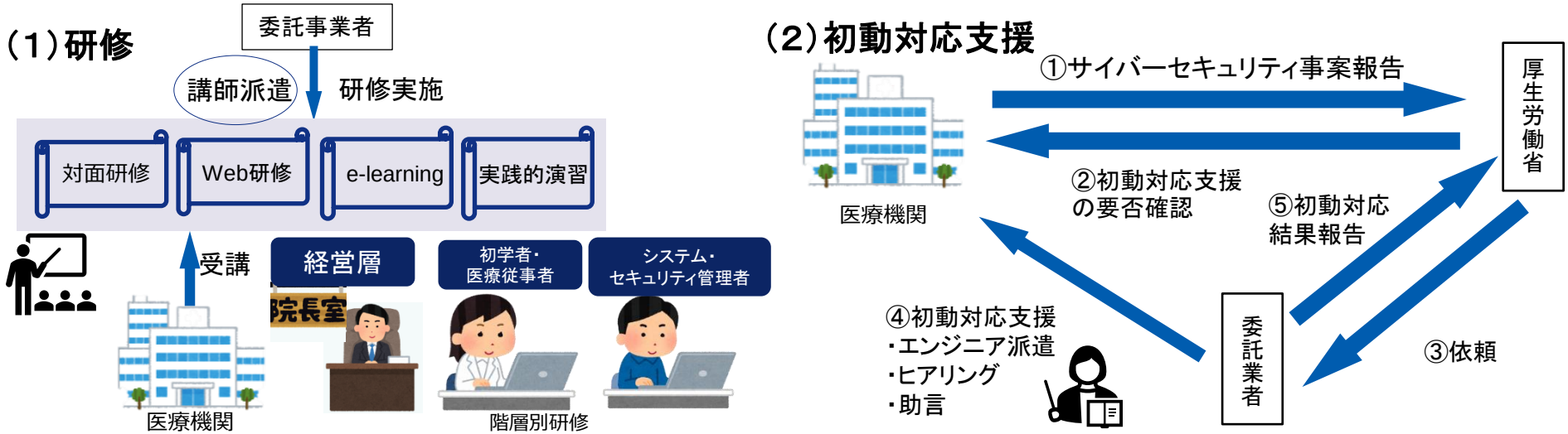
医療分野におけるサイバーセキュリティ対策調査事業

令和7年度予算額 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）

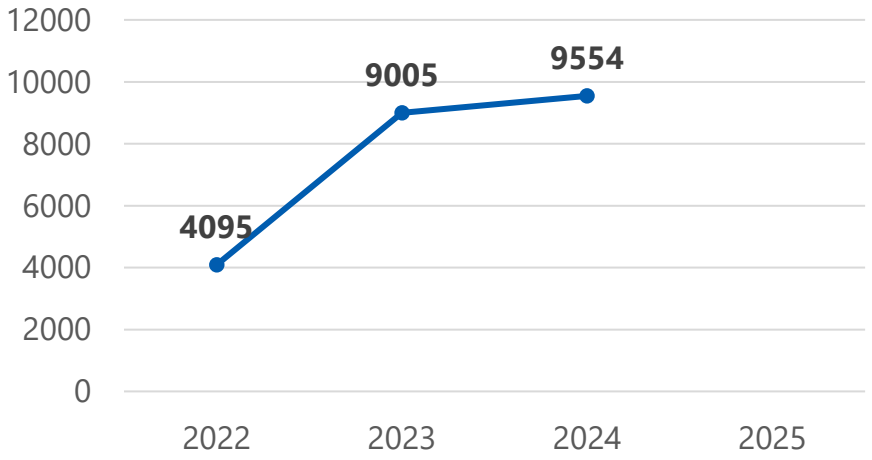
4 事業実績

◆ 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

医療分野におけるサイバーセキュリティ対策調査事業の実績

【医療機関向けサイバーセキュリティ研修参加者数の推移】（人）



参考/2024年度研修別の数

研修名	参加数
経営層向け	**1,073施設 1,175名**
システム・セキュリティ管理者向け	**1,738施設 1,876名**
初学者・医療従事者向け	**1,110施設 1,218名**
立入検査コース	**4,806施設 5,271名**
講師育成	**14施設 14名**

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。		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*		ワークショップ	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

3

- 医療機関におけるサイバーセキュリティ確保事業

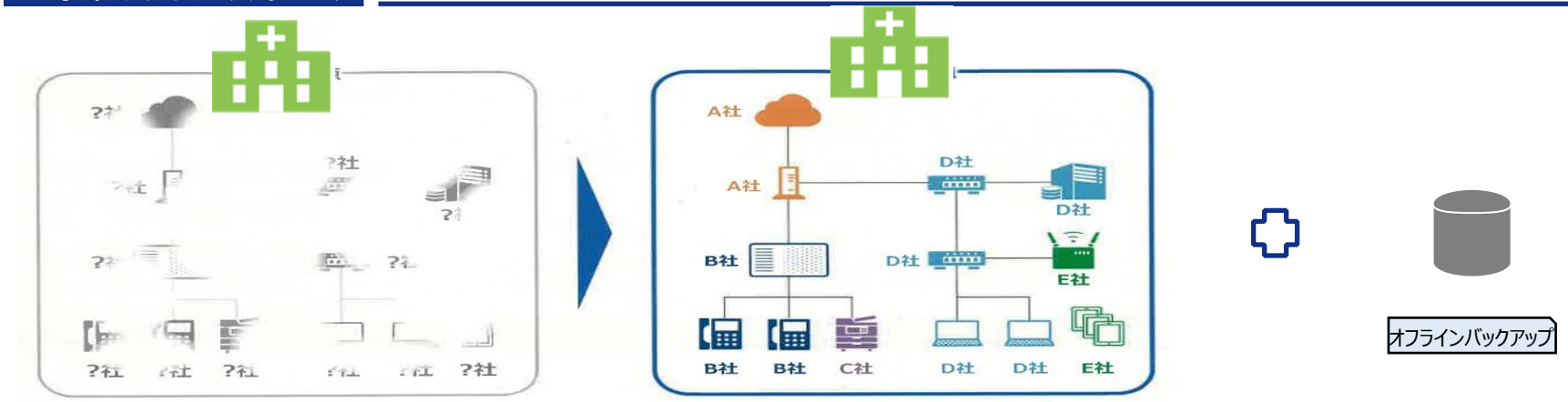
新規 医療機関におけるサイバーセキュリティ確保事業

令和７年度予算額　11.0億円（－）　※() 内は前年度当初予算額　※令和６年度補正予算額　13億円

1 事業の目的

○厚生労働省では、医療機関に対して委託先事業者と連携し、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ところ。
○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。
○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、医療機関に対して、オフラインでのバックアップデータの保存を求めている。
○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。

2 事業の概要・スキーム



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

3 実施主体等

委託先：委託事業（民間事業者）

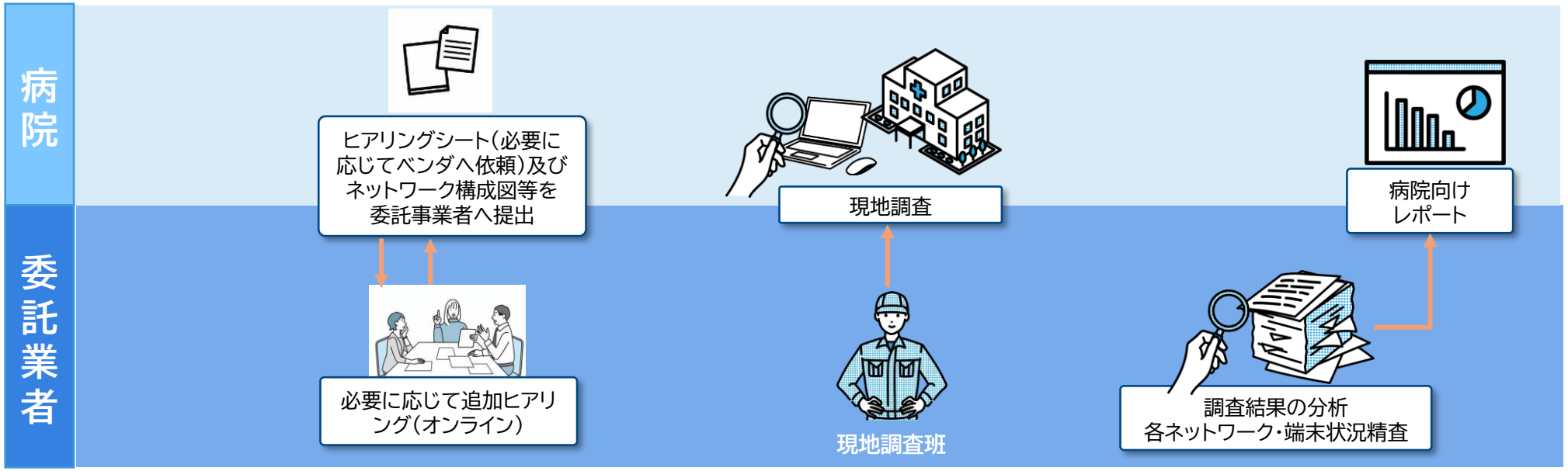
3 実施主体等

昨年度実績：1,363施設

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（R6年度事業）

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

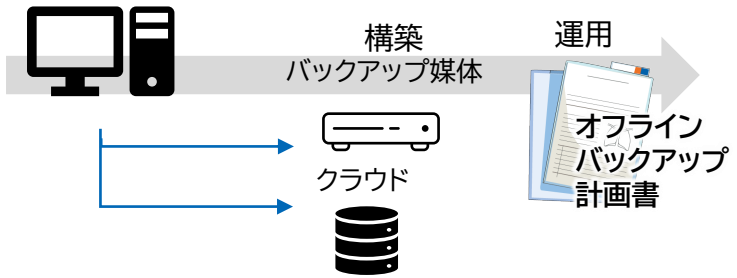
■オフラインバックアップ未実施病院の構築支援に向けた技術方式・実現方法、運用・維持の検討

・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）



オフラインバックアップ計画書
病院へ報告

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)
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		

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

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

4

- 医療情報セキュリティ等対策経費に関する論点

医療情報セキュリティ等対策経費に関する論点

1 論点

〇サイバーセキュリティインシデントが増加している昨今の事情を踏まえ、医療機関のサイバーセキュリティ対策をより一層充実していくための効果の検証及び成果をより適切に評価することができるアウトカムを検討する必要があるのではないか。

2 現在のアウトカム

〇医療分野におけるサイバーセキュリティ対策調査事業

長期アウトカム：前年の医療機関向けサイバーセキュリティ研修と同水準の受講者を確保する。

〇医療機関におけるサイバーセキュリティ確保事業

長期アウトカム：ネットワーク構成の見える化による、医療機関におけるサイバーセキュリティ対策の充実

3 見直しの方向性

〇サイバーセキュリティインシデントが起こるかどうかは極めて偶然的な事情に左右されることに加え、実際に防止したサイバー攻撃の件数を把握することは困難であるため、定量的なアウトカムを設定できていない。

〇代替案として、事業のKPI（Key Performance Indicator：重要業績評価指標）を設定する。

医療情報セキュリティ等対策経費に関するKPIの設定

医療分野におけるサイバーセキュリティ対策調査事業

〇KGI（Key Goal Indicator:重要目標達成指標）の設定

研修等を通じてセキュリティ人材の育成、医療機関を標的としたサイバー攻撃に対する平時からの対策徹底の周知や、実際に攻撃を受けた際の初動対応を行える体制を整える。

〇KPIの設定

1．医療機関向けサイバーセキュリティ研修の受講者（既存）・病院数

2．サイバー攻撃等によるシステム障害発生時に備えたBCPの策定している施設の割合

医療機関におけるサイバーセキュリティ確保事業

〇KGIの設定

電子カルテを導入しているすべての医療機関についてサイバーセキュリティ確保のため、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する。

〇KPIの設定

1．医療機関におけるサイバーセキュリティ確保事業を完遂した病院数

2．オフラインバックアップ体制を整備している病院の割合

医療機関におけるサイバーセキュリティ確保事業の見直しについて

ネットワーク構成図の作成について

○厚生労働省では、医療機関に対して委託先事業者と連携し、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。

○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。

○医療機関におけるサイバーセキュリティ確保事業の成果物としてネットワーク構成図等を作成することで、有効なセキュリティ対策を実施するための下地作りをする。

課題

○電子カルテシステムを導入している全国の病院を対象に都道府県にて選定、全国2,001病院が対象となった。その後、613施設が辞退となったため、最終的な本事業の参加医療機関は1,363施設。辞退の主な理由は、「人員不足のため（24%）」、「システム・NW更新・移転のため（１2%）」だった。(n=638)

見直し策

○事前提出書類等を公開し、事業参加前から準備に掛かる負担度、スケジュールを明示する。

○病院向け説明会実施を7月から5月へ前倒し、準備期間に余裕を持たせる。

○昨年度事業の調査結果を基に、事前提出書類等の見直しを行い書類作成の負担を軽減する。

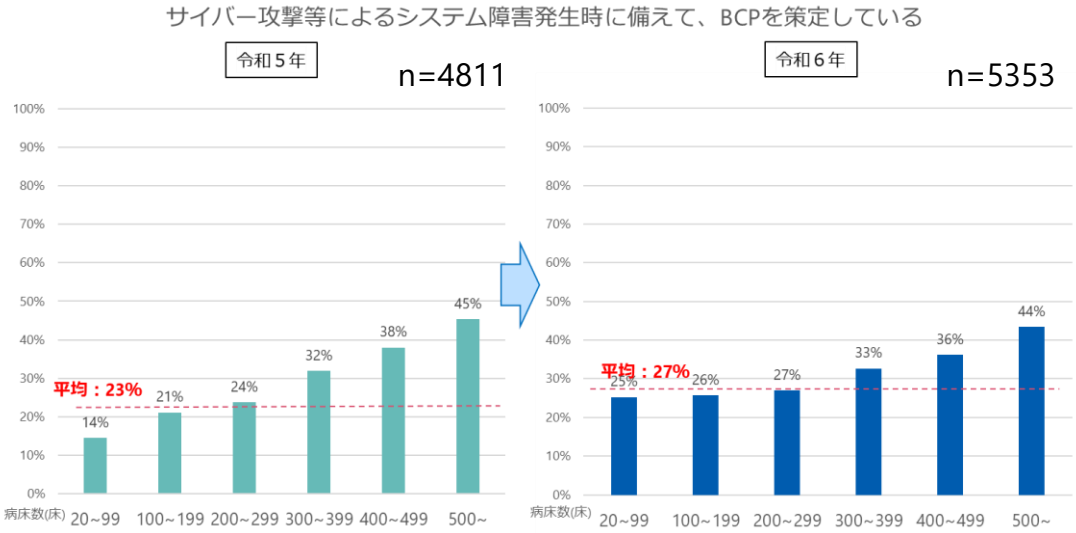
医療分野におけるサイバーセキュリティ対策調査事業のKPI設定

サイバー攻撃等によるシステム障害発生時に備えたBCP

○厚生労働省では、医療法第 25 条第１項に基づく立入検査でセキュリティ確保のために必要な取り組みの確認として「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５年６月）」を定め、その中で「サイバー攻撃を想定した事業継続計画（BCP）」を策定することとしており、非常時における組織全体のBCP策定を求めている。

○サイバー攻撃を想定したBCP策定を促進するため、医療機関向けサイバーセキュリティ研修「経営者向け研修 IT-BCPコース」を実施してる他、サイバー攻撃を想定した事業継続計画（BCP）策定の確認表等の公開を行っている。

○令和5年度「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」では、サイバーBCPの策定は全体平均で23%に留まり、令和6年度の同調査においても27%であった。



病床数（床）	20~99	100~199	200~299	300~399	400~499	500~	合計
調査対象医療機関数	2940	2810	1015	673	357	376	8171
有効回答数	1794	1816	698	474	270	301	5353

調査方法・対象

- G-MISを用いて、病院のサイバーセキュリティ対策の実態に関するアンケート調査を実施。（問数は24問）
- 調査対象は、G-MIS IDが付与されている、8,171の病院。（病院総数：8,205　※令和３年医療施設動態調査）

調査期間

・令和６年２月１日（木）～　令和６年３月８日（金）

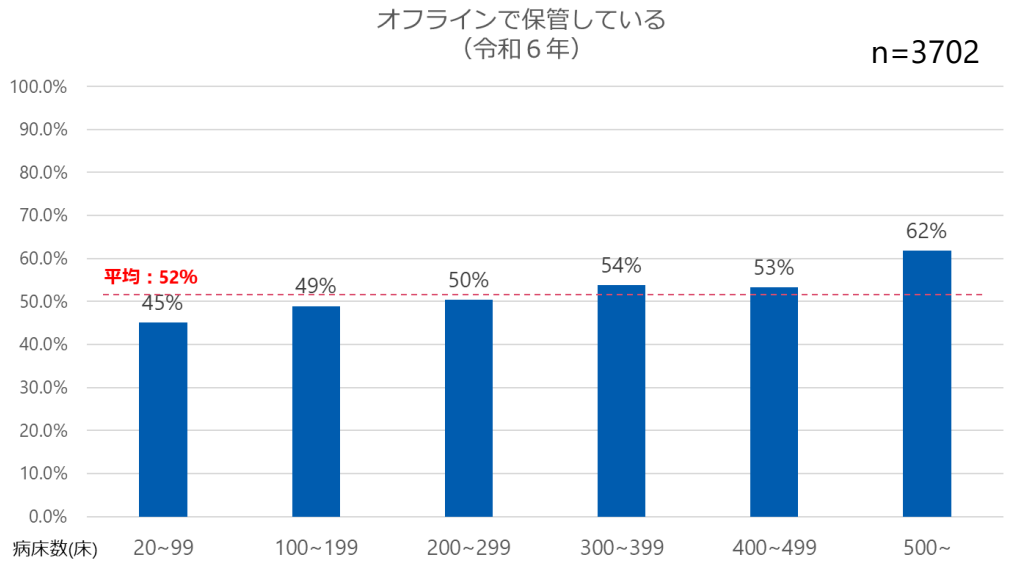
医療機関におけるサイバーセキュリティ確保事業のKPI設定

オフラインバックアップの整備について

○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、医療機関に対して、オフラインでのバックアップデータの保存を求めている。

○医療機関が平時から外部ネットワークとの接続の把握とオフライン・バックアップ体制の整備を行い、サイバーセキュリティの更なる確保を行う事で、医療DXの推進に繋がる。

○令和６年度「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」では、オフラインバックアップを保管している施設の割合は52%であった。



病床数（床）	20~99	100~199	200~299	300~399	400~499	500~	合計
有効回答数	1794	1816	698	474	270	301	5353
電子カルテのバックアップを作成している	988	1254	516	409	244	291	3702

調査方法・対象

- G-MISを用いて、病院のサイバーセキュリティ対策の実態に関するアンケート調査を実施。（問数は24問）
- 調査対象は、G-MIS IDが付与されている、8,171の病院。（病院総数：8,205　※令和３年医療施設動態調査）

調査期間

・令和６年２月１日（木）～　令和６年３月８日（金）

5

- 参考資料

大阪府立病院機構 大阪急性期・総合医療センターのランサムウェア感染に関して

事案概要

2022年10月31日(月) 早朝、地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター（以下、大阪急性期・総合医療センター）において、ランサムウェアを用いたサイバー攻撃によりファイルが暗号化され、電子カルテが使用不能となる事案が発生した。厚生労働省から派遣した初動対応支援チーム（一般社団法人ソフトウェア協会）の調査によると、感染経路は、院外の調理を委託していた**給食事業者のシステムを経由したものである可能性が高い**ことが判った。

新規外来患者の受入は引き続き停止しているが、緊急度の高い処置、手術は大阪急性期・総合医療センターにおいて継続して対応した。患者の生命等への影響はなかった。また、個人情報の漏洩も確認されていない。　（12月12日時点）

(参考)地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター
病床数：865床（一般病床831床、精神病床34床）
病院機能：基幹災害拠点病院、高度救命救急センター、地域周産期母子医療センター、小児地域医療センター、
地域医療支援病院、地域がん診療連携拠点病院　他

経過

10月31日(月)：インシデント発生。大阪急性期・総合医療センターからの初動対応支援の要請を受け、
厚生労働省より初動対応支援チームを派遣。同日夜、記者会見により当該事案を公表。
11月４日(金)：予定手術を一部再開。
11月７日(月)：発生後一週間経過。当該事案の現状と今後の復旧計画について記者会見を実施。感染経路は、給食事業者に設置されたVPN装置を経由した可能性が高いことを公表。
11月10日(木)：電子カルテの一部が仮設環境により参照可能となり、三次救急患者の受け入れと小児救急診療の一部を再開。
11月17日(木)：仮設環境による参照が救急外来において可能となり、一般救急患者の受け入れが再開。
12月12日(月)：電子カルテ再構築を完了させ本環境で順次稼働開始。各種オーダも順次再開予定。
1月11日(火)：システム全面復旧

厚生労働省の対応

１．要請を受けて、厚生労働省から専門家を派遣し、感染原因の特定や対応の指示等の初動対応の支援を行った。

２．11月10日に全国の医療機関に対して、サイバーセキュリティ対策の強化にかかる注意喚起を行った。

サイバー攻撃を想定した事業継続計画（BCP）

厚生労働省では、「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５年６月）」において「サイバー攻撃を想定した事業継続計画（BCP）」を策定することとしており、非常時における組織全体のBCP策定を求めている。その中で、医療情報システム部門のBCPを検討する場合には、「サイバー攻撃を想定した電子カルテシステム等障害時の医療情報システム部門における事業持続計画（BCP）策定の確認表」を参考にして、組織全体で策定されるBCPとの整合性を踏まえた内容になるように配慮する。

イメージ

2024年度診療報酬改定

【診療録管理体制加算1】（新設）140点

［施設基準］

・許可病床数**200床以上**の保健医療機関については、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。

・非常時に備えた**医療情報システムのバックアップを複数の方式で確保し、その一部はネットワークから切り離したオフラインで保管**していること。

・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。

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

確認表を元に策定することで各施設の負担が軽減

サイバー攻撃を想定した電子カルテシステム等障害時の医療情報システム部門における事業持続計画（BCP）策定の確認表を参考にする範囲

オフラインバックアップ体制の整備支援（全体像）

- 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」について導入を加速化するため、電子カルテのバックアップ取得状況をアンケートにて確認し、希望する病院に対して、構成相談、計画策定等の導入に向けた支援を行います。

オフラインバックアップの導入状況の確認

✓ 病院の電子カルテのバックアップ状況、オフラインバックアップの導入状況の把握
✓ 本事業で定義するオフライン化の要件を病院へ展開、適切な導入・運用ができているか確認を促す

Webアンケートにて確認

オフラインバックアップ未導入、かつ支援希望の病院へ
以下を実施

相談受付（Web打合せ等）

- 病院からのオフラインバックアップ導入・構築に向けた相談に対応
- 現状のバックアップ取得状況やシステム構成等をヒアリング
- 必要に応じて導入方式や機器等の情報、構築に向けた手順書等を提供

計画策定

- 現状のバックアップ取得状況やシステム構成等をヒアリングシートを用いてヒアリング
- ヒアリング内容をもとに、病院・電子カルテベンダー等と打合せを実施の上、報告書として取りまとめて納品

・本事業は、既に各病院で取得している電子カルテサーバのバックアップを適切にオフライン化することを目的としているため、病院におけるBCP計画の策定等は含みません。
・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、電子カルテベンダの設定費等は仕様書に記載のとおり、本事業の対象外です。

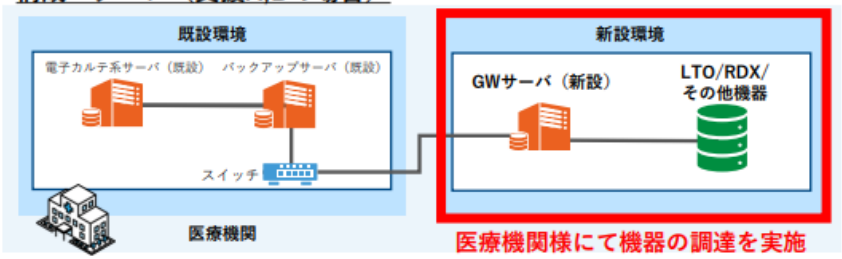
オフラインバックアップ支援の参考例

LTO保存・RDX保存・その他機器での保存の場合

- LTO/RDX/その他機器へオフラインバックアップを取得する構成を希望の医療機関様については、以下の構成にて支援を実施します。
  【支援A,B】　サーバを院内へ新設し、バックアップ媒体を接続する構成
  【支援C】　既設環境にバックアップ媒体を接続する構成

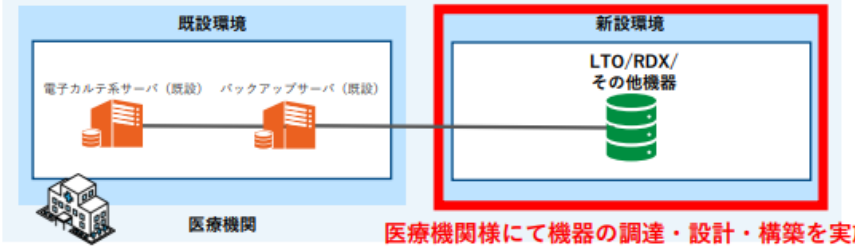
- いずれの支援パターンにおいても、バックアップ媒体、および新設サーバは医療機関様にて購入、保守手配をご対応いただく前提となります。
- 既設環境から新設環境へバックアップデータを転送するための既存機器の設計、設定変更、ケーブル等のご用意は医療機関様にてご対応いただく前提となります。

構成パターン（支援A,Bの場合）



医療機関様にて機器の調達を実施

構成パターン（支援Cの場合）



医療機関様にて機器の調達・設計・構築を実施

クラウド保存（MeISH）の場合

- クラウド環境へオフラインバックアップを取得する構成を希望の医療機関様については、当社指定のクラウドサービスを用いた支援を実施します。
  【支援A,B,C】
  クラウド接続装置を院内へ新設し、クラウドストレージへ接続する構成
  ※サーバの新設は不要となります。

- いずれの支援パターンにおいても、クラウド接続装置はクラウド事業者にて調達・設置します。医療機関様でのご対応は不要となります。
- 既設環境から新設環境へバックアップデータを転送するための既存機器の設計、設定変更、ケーブル等のご用意は医療機関様にてご対応いただく前提となります。

構成パターン（支援A,B,Cの場合）