資料５

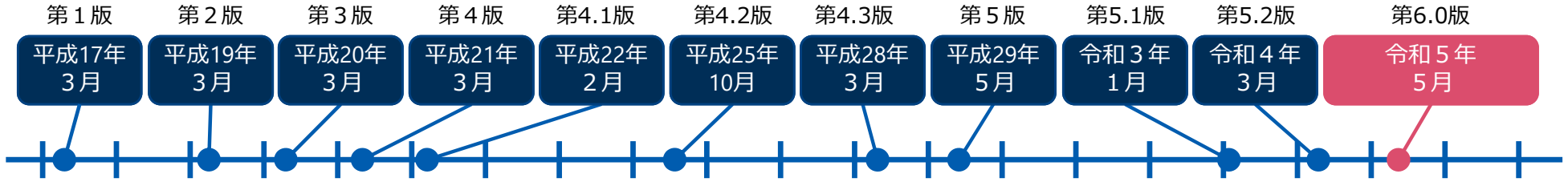
厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

医療分野におけるサイバーセキュリティ対策について

Ministry of Health, Labour and Welfare of Japan

医療情報システムの安全管理に関するガイドライン 策定の背景及び改定の経緯

- 医療情報システムの安全管理に関するガイドラインは、e-文書法、個人情報保護等への対応を行うための情報セキュリティ管理のガイドラインとして、平成17年3月に第１版を策定。
- 以降、各種制度の動向や情報システム技術の進展等に対応して改定。今般、**令和５年５月に第6.0版を策定。**



版	第１版、第２版、第３版	第４版（第4.1版、第4.2版、第4.3版）	第５版（第5.1版、第5.2版）	第6.0版
策定・改定概要	**第１版** • 医療情報システムのセキュリティ管理を目的とて策定 **第２版** • 重要インフラとしての医療情報システムという観点からの対応 **第３版** • 個人情報施策の議論およびモバイル端末普及への対応	**第4版** • 個人情報保護施策の議論およびモバイル端末普及への対応 **第4.1版** • 民間事業者のデータセンターにおける外部保存に関する対応 **第4.2版** • 調剤済み処方せん及び調剤録等の外部保存への対応 **第4.3版** • 「電子処方せんの運用ガイドライン」への対応	**第5版** • 医療機関等の範囲の明確化 • 改正個人情報保護法対応 • サイバー攻撃の動向への対応 **第5.1版** • クラウドサービスへの対応 • 認証・パスワードに関する対応 • サイバー攻撃等による対応 • 外部保存受託事業者の選定基準対応 **第5.2版** • ２省（総務省、経産省）GL等との整合性 • 改正個人情報保護法への対応 等 • 医療機関へのサイバー攻撃の多様化・巧妙化 • 「規制改革実施計画」等への対応 • 電子署名 • 外部ネットワーク 等	**第6.0版** <u>全体構成の見直し</u> • 概説編、経営管理編、企画管理編、システム運用編の４編に再構成 • Q&Aの充実 等 <u>技術的な動向</u> • 外部委託、外部サービスの利用に関する整理 • 情報セキュリティに関する考え方の整理 • 新技術、制度・規格の変更への対応 等

医療機関の管理者が遵守するべき事項への位置づけ

医療法施行規則を改正し、医療機関の管理者が遵守するべき事項にサイバーセキュリティの確保を位置づけるとともに、医療法第25条第１項に規定に基づく立入検査要綱の項目にサイバーセキュリティ確保のための取組状況を追加。

改正概要・対応の方向性

○　医療法施行規則第14条第２項を新設し、病院、診療所又は助産所の管理者が遵守すべき事項として、サイバーセキュリティの確保について必要な措置を講じることを追加する。

○　令和５年３月10日公布、４月１日施行済

○「必要な措置」としては、最新の「医療情報システムの安全管理に関するガイドライン」（以下「安全管理ガイドライン」という。）を参照の上、サイバー攻撃に対する対策を含めセキュリティ対策全般について適切な対応を行うこととする。

○　安全管理ガイドラインに記載されている内容のうち、優先的に取り組むべき事項については、厚生労働省においてチェックリストを作成し、各医療機関で確認できる仕組みとする。

○　また、医療法第25条第１項に規定に基づく立入検査要綱の項目に、サイバーセキュリティ確保のための取組状況を位置づける。

◎医療法施行規則（昭和二十三年厚生省令第五十号）

第十四条　（略）

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に、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。）を確保するために必要な措置を講じなければならない。

※　下線部を新設。

医療法に基づく立入検査の概要

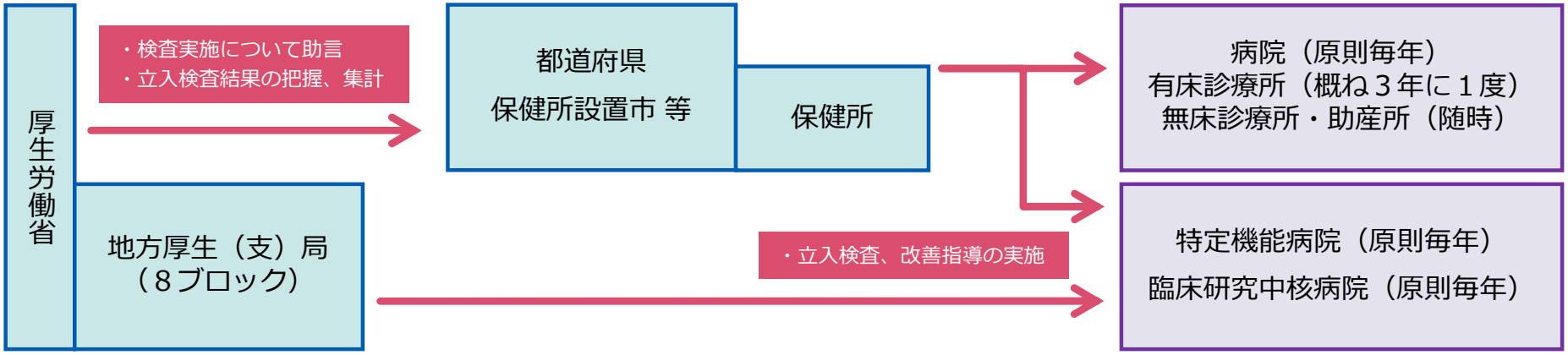
厚生労働省ホームページ

立入検査の目的

・病院、診療所等が法令により規定された人員及び構造設備を有し、かつ、適正な管理を行っているか否かについて検査し、不適正な場合は指導等を通じ改善を図ることにより、病院、診療所等を良質で適正な医療を行う場にふさわしいものとする。

立入検査の実施主体

・**医療法第２５条第１項による立入検査** ・・・ 各病院、診療所等に対し、都道府県等が実施
・**医療法第２５条第３項による立入検査** ・・・ 特定機能病院等に対し、国が実施



主な検査項目

○**病院管理状況**
➢カルテ、処方箋等の管理、保存　➢届出、許可事項等法令の遵守　➢患者入院状況、新生児管理等　➢医薬品等の管理、職員の健康管理
➢安全管理の体制確保　等
○**人員配置の状況**
➢医師、看護婦等について標準数と現員との不足をチェック
○**構造設備、清潔の状況**
➢診察室、手術室、検査施設等　➢給水施設、給食施設等　➢院内感染対策、防災対策　➢廃棄物処理、放射線管理　等

病院における主なランサム攻撃の事例

発生	都道府県	医療機関名	病床（発生時）	医療機関の役割等	攻撃経路等
2021年10月	徳島県	つるぎ町立半田病院	120床 (2021.10時点)	災害拠点病院 へき地医療拠点病院	外部ネットワークとの接続点（保守用VPN装置）の脆弱性の放置等
2022年10月	大阪府	大阪急性期・総合医療センター	865床	基幹災害拠点病院 高度救命救急センター ほか	外部委託業者（給食事業者）のシステム接続点（リモートデスクトップ）からの侵入等
2024年5月	岡山県	岡山県精神科医療センター	255床	精神科救急医療施設 応急入院指定病院 ほか	外部ネットワークとの接続点（保守用VPN装置）の脆弱性の放置等

✓ 中・大規模病院は多数の部門システムで構成されており、外部ネットワークとの接続点が網羅的に把握できていないことが研究*でも指摘されている。

＊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）」

✓ 外部ネットワークとの接続点が網羅的に把握できていないため、ネットワーク機器の脆弱性の管理や監視機器の効果的な導入が困難。

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

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

（目的）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

●結果等
- 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

（目的）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

●結果等
- 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**

医療機関におけるサイバーセキュリティ確保事業

R６年度～R7年度

✓　電子カルテ導入病院を中心に外部ネットワークとの接続点の安全性の検証・検査等を実施（厚労省から委託した専門業者が実施）。
（令和５年度補正予算　36億円・令和６年度補正予算　13億円・令和７年度当初予算　11億円）

✓　多くの医療機関において外部接続点が多数存在し、管理が困難となっている実情が明らかとなった。（R6年度：1363病院を実施）

R８年度～

✓　外部ネットワークとの接続点が多数存在する医療機関に対して、その適正化まで事業対象を拡充、接続点の維持管理体制づくり等の支援を実施。
（令和７年度補正予算　１４．７億円）

・厚生労働省委託業者によるネットワーク統合計画作成等の支援
・ネットワーク統合に必要な物品等に係る費用を医療機関に対して補助

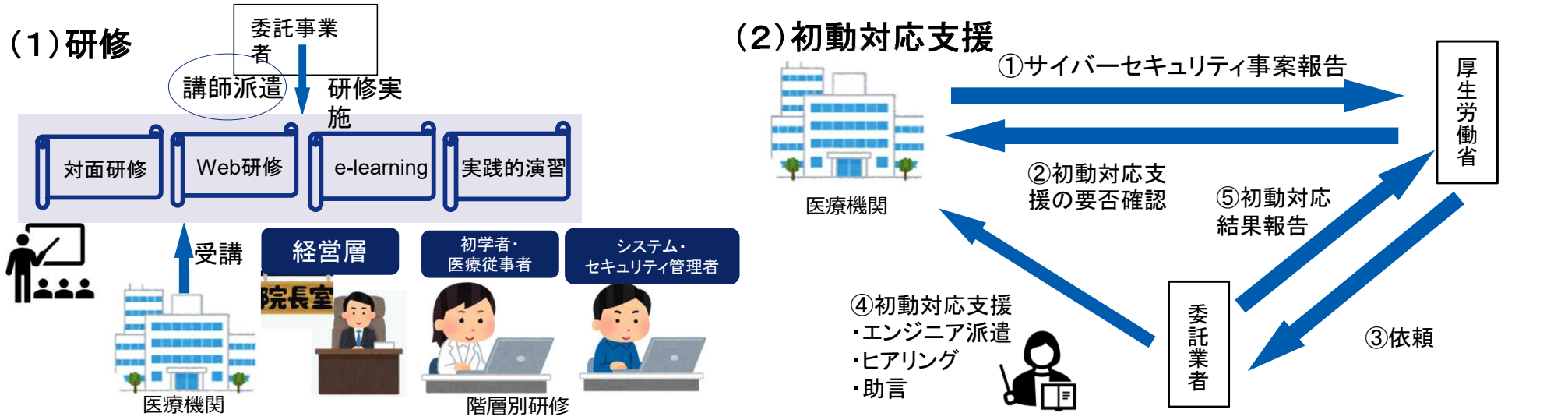
医療分野におけるサイバーセキュリティ対策調査事業

令和８年度予算案　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



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

医療機器のサイバーセキュリティ対応

○　医療機器のサイバーセキュリティ対策については、令和5年３月に薬機法第41条第3項に基づく基本要件基準を改正し、令和６年４月から義務化された。しかしながら、製造販売業者における取組状況には依然として差がある。

○　米国FDAでは製造販売業者に対し、製品の脆弱性評価に関する説明やソフトウェア部品表（SBOM）の提出等を求め、市販前・市販後を通した継続的なリスクマネジメントを前提とする規制が行われている。欧州においても同様の動きがあり、国際市場では「サイバーセキュリティ確保」が参入の前提条件となっている。

○　我が国においても、海外の制度を参照しながら、市販前及び市販後における医療機器のサイバーセキュリティ対応の妥当性を行政当局が確認する仕組みを構築することが必要。

【基本要件基準】
医療機器におけるサイバーセキュリティを確保するための設計及び製造にあたり、
① **製品の全ライフサイクルにわたって医療機器サイバーセキュリティを確保する計画を備えること**
② **サイバーリスクを低減する設計及び製造を行うこと**
③ **適切な動作環境に必要となるハードウェア、ネットワーク及びITセキュリティ対策の最低限の要件を設定すること**

設計・開発

・設計　・製造
・SBOM　・保守計画
・リスクマネジメント評価

市販前に確認

市販後

・脆弱性管理
・保守対応

・ソフトウェアアップデート

市販後に確認

医療機器の海外展開促進