資料３

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

# 医療機関等におけるサイバーセキュリティに関する取組について

医政局　医療情報担当参事官室

Ministry of Health, Labour and Welfare of Japan

# これまでの医療機関等におけるサイバーセキュリティ対策

## 2005年以降厚労省で進めている対応

**〇医療情報システムの安全管理に関するガイドラインの策定**

厚労省ではこれまで、医療機関等で起きたセキュリティ事案に対応するため、医療情報を扱う医療機関等に向けて「医療情報システムの安全管理に関するガイドライン」を発行。2005年3月の第1版発行以降、約10回の改定を重ね、都度、新しいセキュリティ事案への対応を取り込んできた。

**〇「サイバーセキュリティ対策チェックリスト」と立入検査における監査**

ガイドラインの中から最低限対応すべき項目をとして明確化し、医療法に基づく立ち入り検査の中でチェックリストの履行状況を確認してきた。

## 2024年以降厚労省で進めている対応

**〇医療機関等におけるサイバーセキュリティ対応の調査**

セキュリティ事案への対応強化が求められる中、2024年度から医療機関等における外部接続点やセキュリティの脆弱性について調査を行い、外部接続点が多すぎること、そもそも把握されていないことを確認。

**〇報酬改定における対応**

2024年度の診療報酬改定では、BCPの策定やオフラインバックアップの要件を盛り込んだ。

2026年度は、セキュリティ資格について言及した加算を新設した。

# 病院における主なランサム攻撃の事例

第１回デジタル・サイバーセキュリティWG（令和8年2月3日）
資料 3-2 一部改

| 発生 | 都道府県 | 医療機関名 | 病床 | 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<br>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<br>高度救命救急センター<br>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<br>応急入院指定病院<br>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 |
| 2026年2月 | 神奈川県 | 日本医科大学武蔵小杉病院 | 372床 | 災害拠点病院<br>救命救急センター<br>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。

✓ 推測しやすいパスワードやパスワードの使い回しによって、攻撃者がネットワークに侵入後容易に水平展開が可能となっている。

# 医療分野におけるサイバーセキュリティ対策調査事業

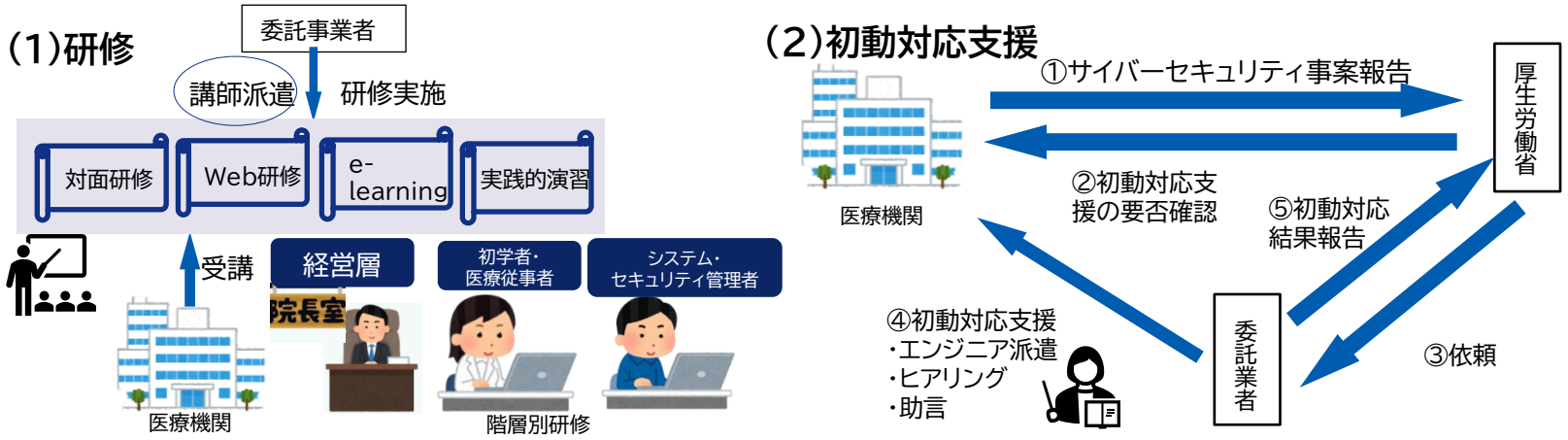
## 1 事業の目的

○ 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。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



# 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

# AI技術の進展と医療機関等における脅威認識

## AI技術の急速な進展

生成AIやフロンティアAIモデルなどの技術進展が社会の生産性向上に大きく寄与しています。

## サイバー攻撃の高度化リスク

高性能AIの悪用により攻撃の自動化や高速化が進み、短時間で容易に攻撃が行われるリスクが増大しています。

## 医療分野の脆弱性

医療機器や電子カルテに依存する医療機関はサイバー攻撃で診療継続に重大な影響を受ける可能性があります。

## 高水準なセキュリティ対策の必要性

医療機関等は重要インフラ分野として高いセキュリティ基準と組織的な対策の徹底が求められています。

# 医療機関等において改めてご確認いただきたい事項

**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」を用いて**
**皆様の医療機関等におけるサイバーセキュリティの取組をご確認ください。**

## 経営層の関与と意思決定体制の確立

**経営層の主体的関与**
サイバーセキュリティは経営課題。経営層の積極的関与が不可欠

**ガバナンス体制の確立**
ガバナンス体制を構築し、方針や資源配分を明確化

**責任者の任命と役割定義**
責任者を明確化→権限と責任範囲を定め→迅速な意思決定

**意思決定フローと訓練**
インシデント時の連絡系統や意思決定フロー整備→机上訓練

## インシデント対応体制と教育・訓練

**初動対応手順の明確化**（インシデント対応の基本）
感染端末の隔離や影響範囲の迅速な確認

**報告・連携体制の整備**
厚生労働省や関係機関への連絡先を事前に確認

**事後対応と再発防止**
原因分析と継続的な技術・運用・組織改善→再発防止

**教育・訓練の重要性**
全職員対象の定期的な教育やフィッシング訓練で対応力を強化

## リスク管理・脆弱性対策・ランサムウェア対策

**リスク管理の重要性**
医療情報システム全体を把握し、資産ごとのリスク評価を行う

**多層的な防御策**
ネットワーク分離、多要素認証、アクセス制御などの段階的防御で侵入と拡大を防ぐ

**脆弱性発見と更新管理**
脆弱性の早期発見と迅速なセキュリティパッチ適用が不可欠

**ランサムウェア対策**
オフラインバックアップや復旧訓練、不審メール対策→被害を最小化

## サプライチェーン対策とBCPの確保

**サプライチェーン全体の連携**
医療機器メーカーやシステムベンダーと連携し、脆弱性やインシデント情報を共有する体制の構築

**調達段階のセキュリティ要件**
調達時にセキュリティ要件を契約条件として明確化→リスクを未然に抑制

**事業継続計画（BCP）の策定と代替手段準備**
サイバー攻撃を想定したBCPを策定→紙運用等代替手段用意

**訓練と継続的改善**
「サイバー攻撃を想定したBCP策定のための確認表」を用いてBCPを策定→定期的な訓練で実行性を検証、改善