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

2023/06/06

公立病院経営強化に関する説明会

医療分野における サイバーセキュリティ対策の取組について

厚生労働省医政局

特定医薬品開発支援・医療情報担当参事官

岡本　潤　田中　彰子

Ministry of Health, Labour and Welfare of Japan

Ministry of Health, Labour and Welfare of Japan

1．サイバー攻撃に関する最近の動向

2．厚生労働省等における具体的な取組について

ひと、くらし、みらいのために

厚生労働省

Ministry of Health, Labour and Welfare

医療機関におけるランサムウェア被害（国内）

医療機関におけるサイバーセキュリティ対策セミナー
警察庁講演資料（令和５年２月15日）

日本経済新聞

ランサム攻撃でカルテ暗号化　徳島の病院、インフラ打撃

2021年11月12日 11:30

サイバー攻撃で電子カルテによる診療が中断されている半田病院（2日、徳島県つるぎ町）＝共同

徳島県つるぎ町の町立半田病院を10月末、サイバー攻撃が襲った。病院のシステムに侵入して情報を暗号化し、復旧と引き換えに金銭を要求するコンピューターウイルス「ランサムウエア」に感染した。約8万5千人分の電子カルテが閲覧できなくなり新規患者の受け入れを停止。復旧のめどは立っていない。命を守る地域の重要インフラは大打撃を受けた。

速報

- 10:32 雷雲観。左足痛め初場所休場　大関貴景勝しく
- 10:30 米国カリフォルニア州で銃撃、乳児ら6人死亡
- 10:30 外為10時　円、下げ幅拡大　一時128円台後半　実需の売り観測が重荷
- 10:30 ロシア・トルコ首脳、ウクライナとの捕虜交換を協議
- 10:20 リトビア、過去数十年で最悪の洪水発生　住民に避難要請

日経からのお知らせ

- 日経朝刊・電子版の購読数 247万
- キャリア採用の応募を受け付けています

あなたに合った電子版の使い方をご紹介

出典:日本経済新聞　https://www.nikkei.com/article/DGXZQOUE071OK0X01C21A1000000/

NHK NEWS WEB

関西 NEWS WEB

大阪急性期・総合医療センター サイバー攻撃で診療影響続く

11月01日　15時55分

「ランサムウエア」と呼ばれる身代金要求型のウイルスによるサイバー攻撃を受けた大阪急性期・総合医療センターでは、１１月１日も緊急以外の手術を停止するなど影響が続いています。
病院を訪れた患者からは「どこかに情報が流出してしまったら怖い」などと不安の声が聞かれました。

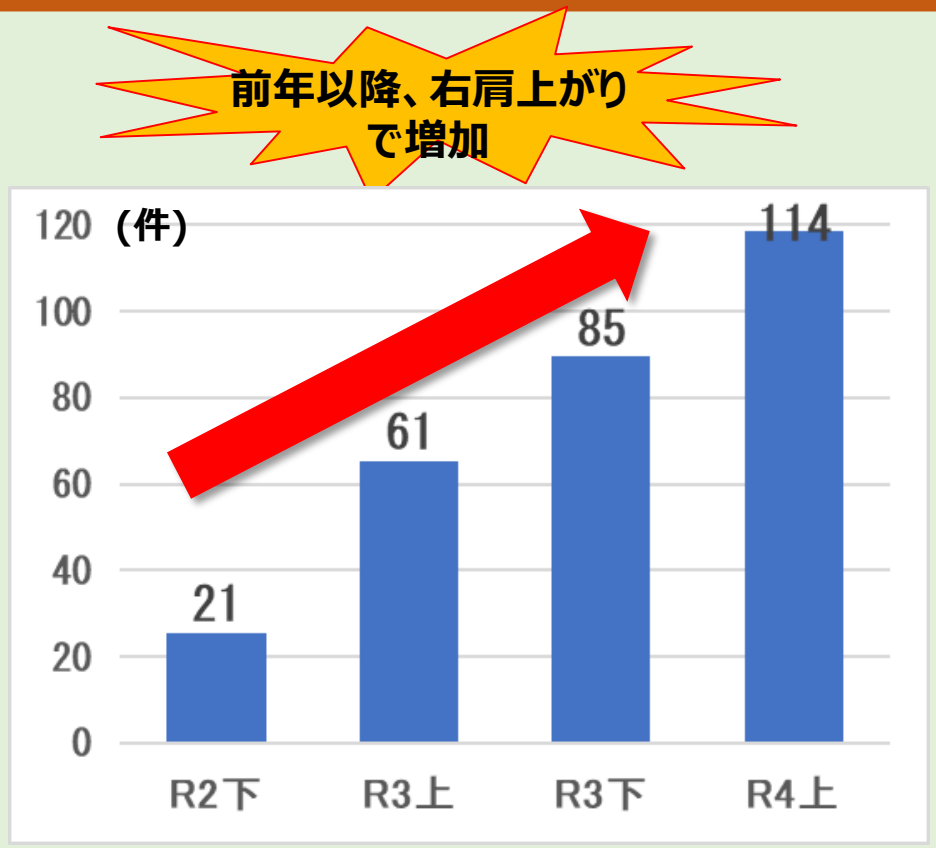
大阪・住吉区の大阪急性期・総合医療センターでは、１０月３１日、「ランサムウエア」とよばれる身代金要求型のウイルスによるサイバー攻撃を受け、電子カルテなどのシステムに障害が発生して閲覧などができなくなっています。
このため、病院では３１日に続き、１日も朝から通常の外来診療や緊急以外の手術を停止しているほか、救急患者の受け入れもできない状況だということです。

出典:NHK NES WEB　https://www3.nhk.or.jp/kansai-news/20221101/2000067859.html

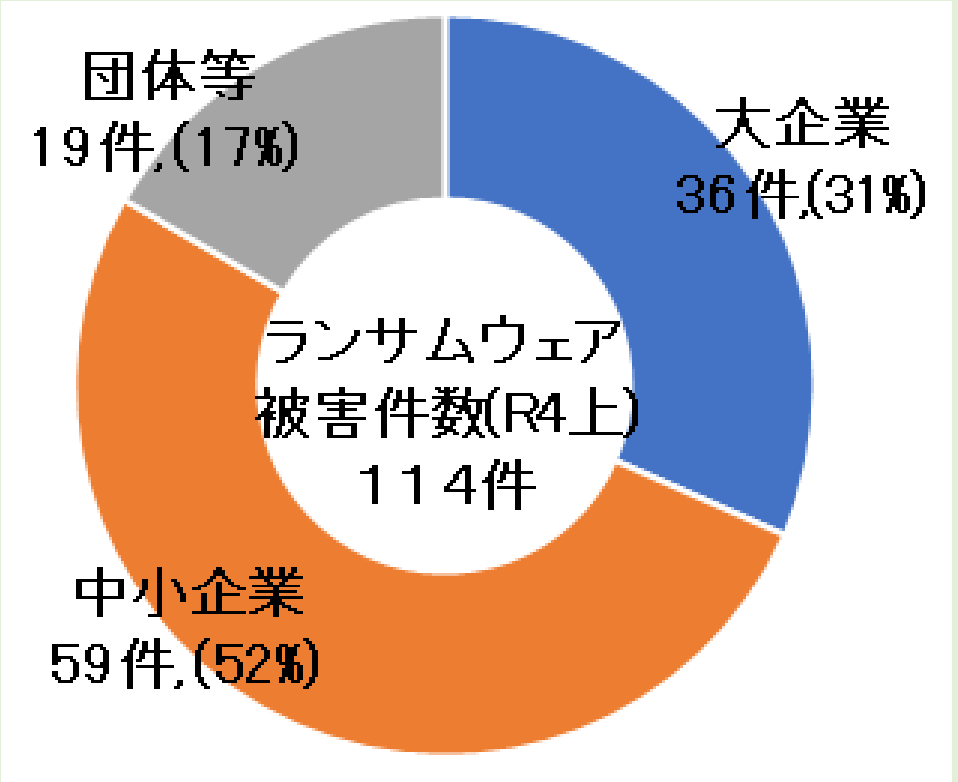
ランサムウェア被害が増加傾向（令和４年上期）

医療機関におけるサイバーセキュリティ対策セミナー
警察庁講演資料（令和５年２月15日）

ランサムウェア被害の報告件数の推移



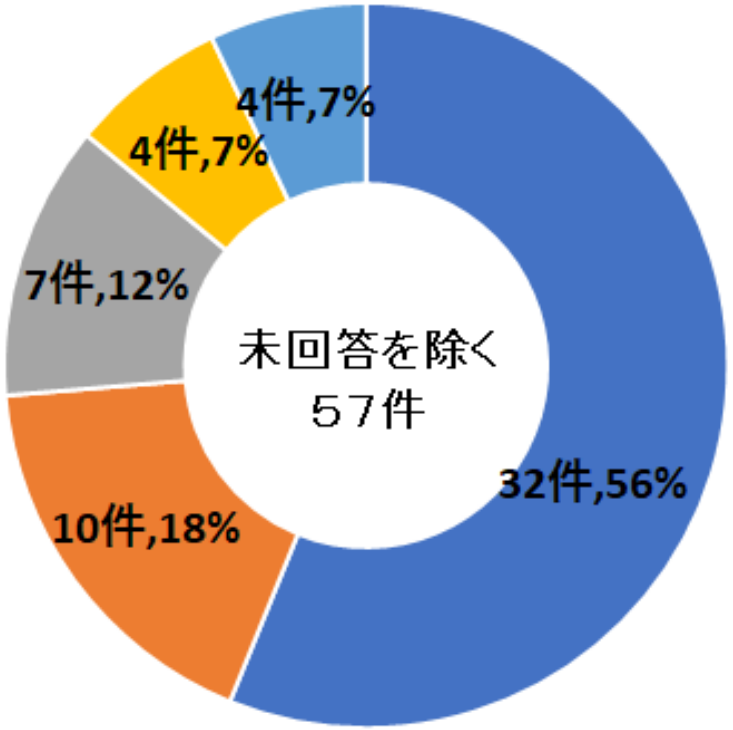
被害企業・団体等の規模別報告件数



VPN機器が侵入経路として狙われている傾向（令和４年上期）

医療機関におけるサイバーセキュリティ対策セミナー
警察庁講演資料（令和５年２月15日）

感染原因　（R4上期）



- VPN機器からの侵入
- 不明/調査中
- リモートデスクトップからの侵入
- 不審メールやその添付ファイル
- その他

我が国におけるサービス停止事案の最近の特徴

第８回健康・医療・介護情報利活用検討会 医療等情報利活用WG　資料２

統計上から得られる知見

- サービス停止の原因は、**自然災害、管理ミスが主流**
- **サイバー攻撃事案**といえるものは、**管理不十分**で発生したものが多い

管理を適切にすれば防止できる事案が毎年繰り返されている

- 「サービス停止」は重要インフラサービスの目的からの逸脱
  - 原因にかかわらず、「結果の保証」
- 「**組織全体のマネジメント**」と「**CSIRT**」の**連携が弱い**ようにみえる
  - サイバー事案は、サイバー部門だけで閉じていない
  - **総合的観点からのリスクが共有されていないのでは？**

組織に潜在するリスクをどのようにしたら組織内で共有できるのか

重要インフラ行動計画改定への提言（概要）

第８回健康・医療・介護情報利活用検討会
医療等情報利活用WG　資料２

現状認識

重要インフラを取り巻く環境は、予断を許さない状況まで来ている

- **第４次行動計画策定以降の状況変化**
  - ✓ サイバーセキュリティを取り巻く環境変化
  - ✓ 新たなサイバーセキュリティ戦略の策定
  - ✓ 近年のサービス障害の原因は、自然災害、管理ミスが主流、多くは管理不十分によって発生

課題の明確化

管理を適切にすれば防げた類似障害が繰り返し発生していることを踏まえ経営層を含め組織的対策が必要

- **第４次行動計画「本行動計画の検証」に基づく評価としては、一定の成果あり**
- **上記評価から直接導出されない課題が存在**
  - ✓ 経営層を含めた組織統治の在り方の検討
  - ✓ サイバーセキュリティ基本法に規定された責務等が認識されていない懸念
  - ✓ 将来を見据えた環境変化、新たなリスクへの対応

改定への提言

第４次行動計画における有効な取組は継続しつつ、特に以下の2点に留意すべき

- **（提言１）障害対応体制の強化の在り方の抜本的な見直し**
  - ✓ 現在の「経営層への働きかけ」から、組織統治の一部としてサイバーセキュリティを組み入れる方針を具体的に記載
  - ✓ サイバーセキュリティ基本法が公布・施行されたことを踏まえ、各関係主体の責務等を明確化
- **（提言２）将来の環境変化を先取りし、サプライチェーン等を含め包括的に対応**

重要インフラのサイバーセキュリティに係る行動計画

２０２２年６月１７日

サイバーセキュリティ戦略本部

			ムの不具合が引き起こす ンフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等 （サービス維持レベル(注2)）
			止 の安全運用に対する支障	・電気関係報告規則（事故報告）第3条 【サービス維持レベル】 ・システムの不具合により、供給支障電力が10万キロワット以上で、その支障時間が10分以上の供給支障事故が生じないこと
			停止 の安全運用に対する支障	・ガス関係報告規則第４条 【サービス維持レベル】 ・システムの不具合により、供給支障戸数が30以上の供給支障事故が生じないこと
政府・行政サービス	・地方公共団体の行政サービス	・地域における事務、その他の事務で法律又はこれに基づく政令により処理することとされるもの（地方自治法第2条第2項）	・政府・行政サービスに対する支障 ・住民等の権利利益保護に対する支障	・地方公共団体における情報セキュリティポリシーに関するガイドライン
医療	・診療	・診察や治療等の行為	・診療支援部門における業務への支障 ・生命に危機を及ぼす医療機器の誤作動	・医療情報システムの安全管理に関するガイドライン
水道	・水道による水の供給	・一般の需要に応じ、導管及びその他工作物により飲用水を供給する事業（水道法第３条及び第15条）	・水道による水の供給の停止 ・不適当な水質の水の供給	・健康危機管理の適正な実施並びに水道施設への被害情報及び水質事故等に関する情報の提供について」（平成25年10月25日付け厚生労働省健康局水道課長通知） ・水道分野における情報セキュリティガイドライン

1．サイバー攻撃に関する最近の動向

2．厚生労働省等における具体的な取組について

「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

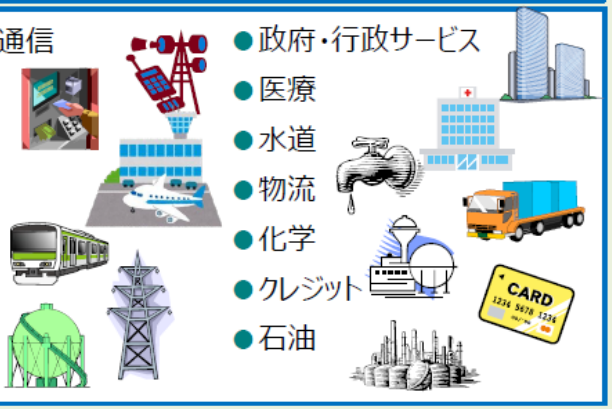
NISCによる総合調整

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、水道］
- 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、物流］

重要インフラ(全14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



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

厚生労働省所管の重要インフラ分野における主な取組

➢「重要インフラのサイバーセキュリティに係る行動計画」に基づき、内閣サイバーセキュリティセンター（NISC)と連携して、以下のとおりサイバーセキュリティ対策に取り組んでいる。

	障害対応体制の強化	安全基準等の整備及び浸透	情報共有体制の強化	リスクマネジメントの活用	防護基盤の強化
医療	➢ インシデント発生時の駆けつけ機能の確保	➢ 「医療情報システムの安全管理に関するガイドライン」を策定・周知	➢ 医療・水道事業者が、セプター※等を通じて、最新の情報セキュリティ動向を把握するための情報共有体制を整備 ➢ NISCが実施する情報共有の確認訓練（セプター※等における受信状況等を確認する訓練）に参加	➢ 医療機関のセキュリティ対策に関する調査事業を実施	➢ 医療機関向けサイバーセキュリティ対策研修 ➢ NISCが実施するサイバー攻撃による障害発生を想定した実践的な演習（分野横断的演習）に参加
水道	➢ 水道事業者等におけるサイバーセキュリティ対応マニュアルの作成の推進	➢ 水道施設の技術的基準を定める省令にサイバーセキュリティ対策を位置づけ ➢ 「水道分野における情報セキュリティガイドライン」を策定・周知			➢ リスクの評価、インシデント報告・対処体制の可視化及び訓練等について、事業者が自ら実施することができるようツールを作成中 ➢ 日本水道協会と連携したサイバーセキュリティ対策に係る講演等を実施

※セプター（CEPTOAR）　Capability for Engineering of Protection,Technical Operation,Analiysis and Response
・重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。
・重要インフラサービス障害の未然防止、発生時の被害拡大防止・迅速な復旧及び再発防止のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係者間で情報を共有。これにより、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資する活動を目指す。

医療情報システムの安全管理に関するガイドライン　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（以下「安全管理ガイドライン」）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年春に第6.0版を策定。

策定・改定時期	版	策定・改定概要
平成17年3月 第１版 平成19年3月 第２版 平成20年3月 第３版	第1版、第2版、第3版	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
平成21年3月 第４版 平成22年2月 4.1版 平成25年10月 4.2版 平成28年3月 4.3版	第4版（4.1、4.2、4.3）	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
平成29年5月 第５版 令和3年1月 5.1版 令和4年3月 5.2版	第5版（5.1、5.2）	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）ガイドライン等との整合性 ・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 等「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
令和５年　春	第6.0版	全体構成の見直し ・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 技術的な動向 ・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

第5.2版 から 第6.0版 への改定方針

2023年４月からの保険医療機関・薬局におけるオンライン資格確認導入の原則義務化により、概ねすべての医療機関等において、本ガイドラインに記載されているネットワーク関連のセキュリティ対策が必要となる。これを踏まえ、第6.0版への改定では、安全管理ガイドラインの読みやすさ向上の観点からの全体構成の見直しとともに、第5.2版で中長期的に検討を継続することとした論点を中心に内容の改定を図った。

○ 全体構成の見直し

・概説編、経営管理（Governance）編、企画管理（Management）編、システム運用（Control）編の４編構成

・Ｑ＆Ａや用語集、小規模医療機関（病院、診療所、薬局等）向けの特集、サイバーセキュリティ対策に関する特集等の作成。

○ 外部委託、外部サービスの利用に関する整理

・クラウドサービスの特徴を踏まえたリスクや対策の考え方

・医療機関等のシステム類型別に対応した責任等の整理　　等

○ 情報セキュリティに関する考え方の整理

・ネットワーク境界防御型思考／ゼロトラストネットワーク型思考

・災害、サイバー攻撃、システム障害等の非常時に対する対応や対策

・本人確認を要する場面での運用（認証に関する考え方の整理と認証技術）　　等

○ 新技術、制度・規格の変更への対応

・オンライン資格確認の導入に必要なネットワーク機器等の安全管理措置

・医療情報の共有・提供に関連する法令等の規定や技術・規格の動向

全体構成の見直し

医療機関等の様々な規模と多様なシステム構成・サービス提供形態を踏まえ、安全な情報資産管理を基礎とし、意思決定・方針策定・戦略立案（Governance）、企画管理・システム運営（Management）、管理方法・運用手段（Control）の３つの視点で整理した。

概説 編 Overview

ガイドラインの各編を読むに際して、まずはじめに、前提として必要な知識や各編の基本的な概要をまとめる。

- ガイドラインの目的
- 対象とする情報・文書・システム
- 関連する法令等の規定との関係や経緯
- 各編の位置付けと目次構成、概要 等

経営管理 編 Governance

組織の経営方針を策定し、情報化戦略を立案する経営管理層に必要な考え方や関連法制度等をまとめる。

- 取り扱う情報の重要性と関連法規
- 情報資産管理や情報システム運用に伴い生じる責任・責務
- 情報システムの有用性と安全管理 等

企画管理 編 Management

経営方針・情報化戦略に基づき、システム利用者・管理者・事業者で情報資産を運営、情報化を管理する考え方や方法論をまとめる。

- 情報資産管理体制と責任分界
- リスクアセスメントと対策
- 情報の種類に応じた管理・監査
- 非常時の対応と非常時への対策 等

システム運用 編 Control

安全な情報資産管理やシステム運用を実現するために、関連法制度を遵守した考え方とその実装手法、活用する技術等、具体的な考え方や技術をまとめる。

- 個人情報保護法、e-文書法、電子署名法等により求められる技術
- システム利用者、クライアント側/サーバ側/インフラ領域等それぞれで活用する安全管理対策・措置技術 等

別添 資料 Appendix

- 各編 概要
- 用語集
- Q＆A
- ガイドラインの改定と関連法規の遷移
- ガイドラインと関連法規との関係性
- 第5.2版から第6.0版への各項目の移行対応表
- 第6.0版の各編の各項目の相関表
- 診療所・小規模医療機関向けの特集
- 医療機関におけるサイバーセキュリティ・バックアップに関する特集
- サイバーセキュリティ対策チェックリスト
- システム障害発生時の対応フローチャート 等

令和３年度までの医療機関におけるサイバー攻撃への対応策

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。

取り組み

○　厚生労働省においては、「医療情報システムの安全管理に関するガイドライン」を定め、医療機関等に対し、技術的・運用管理上の観点から必要な対策を求めている。（R4.3月末の改定で医療機関へのサイバー攻撃の多様化・巧妙化等への対策を追加）

サイバー攻撃への具体的対策

【令和3年度の取組】

○病院へのサイバー攻撃により、診療が長期にわたって制限された事例（※）があったことから、令和3年11月、全国の医療機関に対し脆弱性が指摘されている機器の点検、バックアップの作成等について注意喚起を発出。

○令和4年1月21日に各都道府県・関係団体宛に通知し、全国の病院における、ランサムウェアを想定したリスクを把握するための実態調査を実施。

○　許可病床400床以上の保険医療機関について、①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、②当該責任者は、職員を対象として、少なくとも年１回程度、定期的に必要な情報セキュリティ研修を実施していること、③医療情報システムのバックアップ体制の確保状況を届け出ることを診療録体制加算の要件として追加。

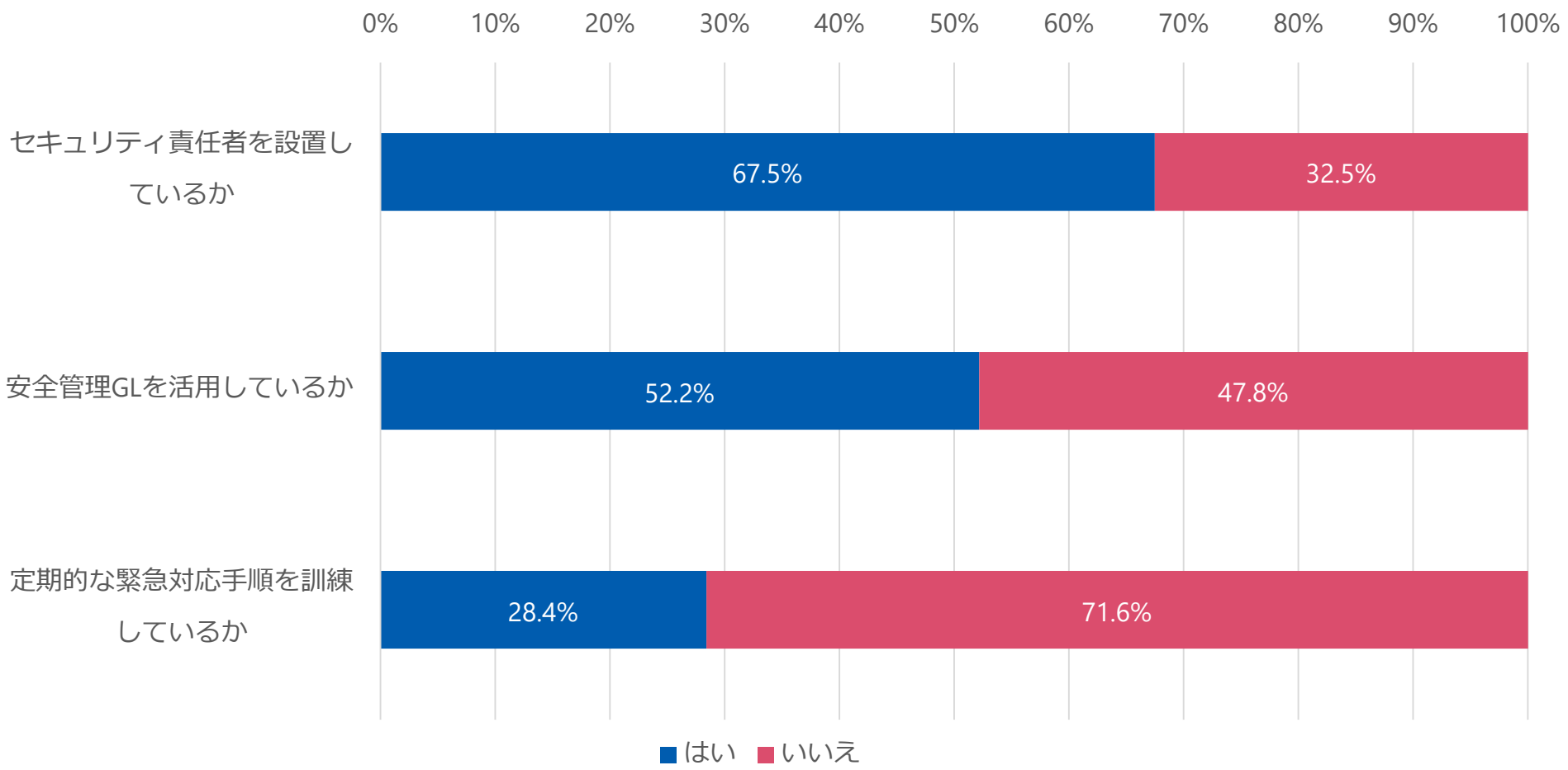
（※）徳島県つるぎ町立半田病院において、電子カルテシステムがランサムウェアに感染し、長期に渡り一部診療が停止した事案（R3.10）

調査結果について

第10回 健康・医療・介護情報利活用検討会
（令和４年３月30日）資料２

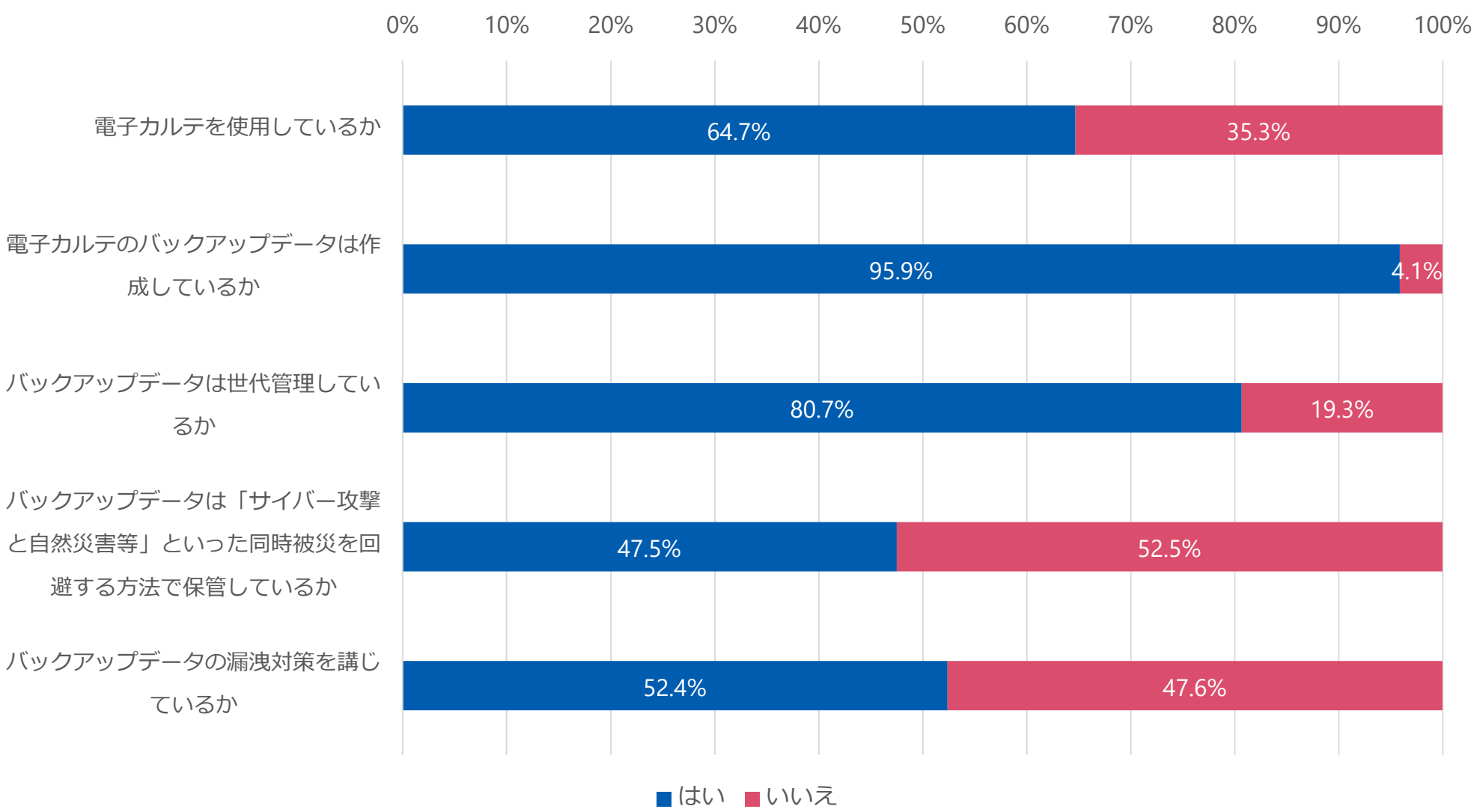
調査対象医療機関数：8,252施設

有効回答数　　：6,216施設（回答率：75.3%）



調査結果について（電子カルテシステムのバックアップについて）

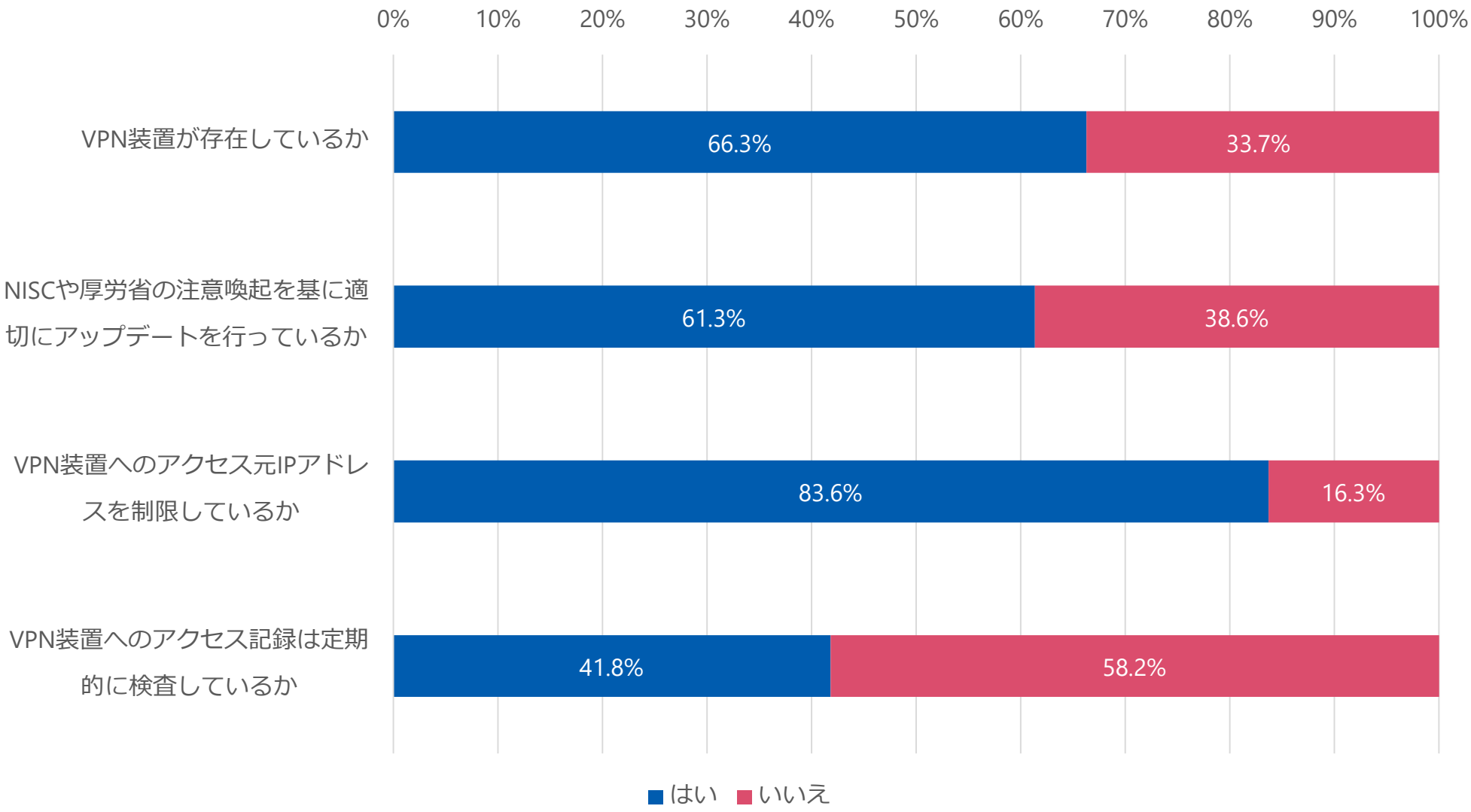
第10回 健康・医療・介護情報利活用検討会
（令和４年３月30日）資料２



※バックアップデータ作成に関する質問（2項目）以降ついては、電子カルテを導入している64.7%（4,020施設）が母数となっている。

調査結果について（リモートゲートウェイ装置について）

第10回 健康・医療・介護情報利活用検討会
（令和４年３月30日）資料２



※VPN装置のアップデートに関する質問（2項目）以降については、VPN装置が存在する66.3%（4,120施設）が母数となっている。

医療機関のサイバーセキュリティ対策の現状・課題

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

現状・課題

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たところ。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。

診療等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、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**。
   ※　令和２年改正個人情報保護法において、不正アクセス等による個人情報の漏えい（疑いを含む）については、件数に関わりなく個人情報保護委員会への報告を義務付け（令和４年４月施行）。 また、法人に対する罰金を最大1億円に引き上げ。

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**。
   ※　ランサムウェアによって、診療録をはじめとする診療に関する諸記録が暗号化され、バックアップファイルも含めて、完全には復号化できないことが判明した場合には、医療法第21 条等に抵触する恐れがある。

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**。

※　診療報酬との関係では、被害状況により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」届出を要件とする入院基本料の算定に影響が生じる場合がある。

医療機関におけるサイバーセキュリティ対策の更なる強化策
－　今後の医療機関におけるサイバーセキュリティ対策の基本方針　－

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９月５日）資料２-２

（１）短期的な医療機関におけるサイバーセキュリティ対策

１．平時の予防対応

①医療機関向けサイバーセキュリティ対策研修の充実　②脆弱性が指摘されている機器の確実なアップデートの実施
③医療分野におけるサイバーセキュリティに関する情報共有体制（ISAC）の構築　④検知機能の強化
⑤G-MIS用いた医療機関への調査実施

２．インシデント発生後の初動対応

①インシデント発生時の駆けつけ機能の確保　②行政機関等への報告の徹底

３．日常診療を取り戻すための復旧対応

①バックアップの作成・管理の徹底　②緊急対応手順の作成と訓練の実施

（２）中・長期的な医療機関におけるサイバーセキュリティ対策

１．バックアップデータの暗号化・秘匿化

２．保健医療分野におけるSOCの構築

医療分野におけるサイバーセキュリティ対策

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９月５日）資料２-２より一部改変

予防対応

① 医療機関向けサイバーセキュリティ対策研修の充実

– 「医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初動対応支援・調査事業一式」において、**医療従事者や経営層等へ階層別のサイバーセキュリティ対策に関する研修の実施**や、本事業において作成される**ポータルサイトを通じた研修資材の提供**により、医療従事者や経営層等のサイバーセキュリティ対策の意識の涵養を図る。

② 脆弱性が指摘されている機器・ソフトウェアの確実なアップデートの実施

– 医療法第25条第１項の規定に基づく**立入検査の実施により確認**を行う。また、例年発出している「医療法第25条第１項の規定に基づく立入検査の実施について」（医政局長通知）において、令和４年度は**サイバーセキュリティ対策の強化に関する事項について記載**した。**令和４年度中に医療機関等の管理者が遵守すべき事項に位置付けるための省令改正**を行う。

– NISCより情報提供のあった脆弱性情報について、医療セプターを通じた情報提供を引き続き行う。

③ 医療分野におけるサイバーセキュリティに関する情報共有体制（ISAC）の構築

– 他分野のISAC関係者の協力を得つつ、医療関係者数名のコアメンバーによる**検討**を行う。

④ 検知機能の強化

– **不正侵入検知・防止システム（IPS／IDS）の設置・活用を進める**よう、医療情報システムの安全管理に関するガイドライン**改定の検討**を行う。

⑤ G-MISを用いた医療機関への定期調査の実施

– 医療機関に対する**サイバーセキュリティ対策の実態調査**を実施する。

【質問項目（例示）】

・医療法に基づく立入検査の留意事項を認識し、必要な措置を講じているか。

・（許可病床数が400床以上の保険医療機関に対して）診療録管理体制加算の見直しを受けて、専任の医療情報システム安全管理責任者を配置しているか。

医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初動対応支援・調査事業(令和４年度)

第13回健康・医療・介護情報利活用検討会医療等情報利活用WG（令和４年12月15日）資料３（一部改変）

背景

医療分野のサイバーセキュリティについては、近年その脅威が高まっていることから、令和４年度厚生労働省事業において、医療機関向け研修やサイバーセキュリティインシデント発生時の初動対応の支援等を行う。

事業概要

（１）サイバーセキュリティ対策にかかる医療機関向け研修の実施
：医療機関職員の階層（初学者、経営層、システム･セキュリティ管理者等）に応じた研修の実施
（２）継続的な教育支援
：医療情報システム安全管理者が研修に活用できる教育コンテンツ作成･収集と公開
（３）平時のサイバーセキュリティインシデント対応手順の調査および既存BCPの見直し提案
：サイバーセキュリティインシデント発生時の適切な対応フローの整理、BCP（Business Continuity Plan）の提案
（４）サイバーセキュリティインシデントが発生した医療機関の初動対応支援
：サイバーセキュリティインシデントが発生した医療機関の原因究明や早期診療復帰を目的に、初動対応支援を実施

受託者

一般社団法人　ソフトウェア協会
：約700社のソフトウェア製品に係わる企業が集まり、ソフトウェア産業の発展に係わる事業を通じて、我が国産業の健全な発展と国民生活の向上に寄与することを目的とした一般社団法人

（サイバーセキュリティに関する主な活動内容）
・ソフトウェアやサイバーセキュリティに関連したセミナー、研修の実施　　・サイバーセキュリティに関する情報交換・周知
・サイバーセキュリティボランティア制度の創設・運用

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

【令和４年度医療機関向けサイバーセキュリティ研修】

研修名	研修参加者数
経営層向け	**第１回：約500名** **第２回：約400名**
システム・セキュリティ管理者向け	**第１回：約700名** **第２回：約600名** **第３回：約550名** **第４回：約500名**
初学者・医療従事者向け	**第１回：約400名** **第２回：約600名** **第３回：約500名** **第４回：約400名**
医療機関における サイバーセキュリティ対策セミナー	**約2000名**

（令和５年３月３日時点）

【研修資料】

○経営者向け研修資料：ポータルサイトに掲載
（どなたでも閲覧・ダウンロード可）

○システム管理者向け研修：ポータルサイト内の
e-learningサイトに掲載済み
（共通研修の申込者のみ閲覧・ダウンロード可）

○初学者・医療従事者向け研修：ポータルサイトに掲載
（どなたでも閲覧・ダウンロード可）

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

医療法に基づく立入検査の概要

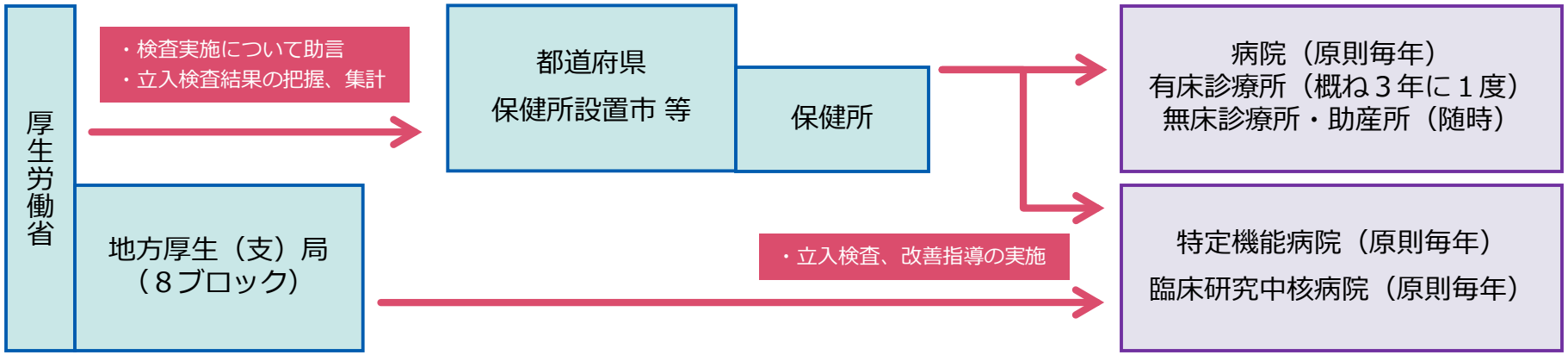
厚生労働省ホームページより引用
（https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/i-anzen/tachiirikensa.html）

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

医療機関の管理者が遵守するべき事項への位置づけ

これまでの本ＷＧでの議論を踏まえ、下記の通り、医療機関の管理者が遵守するべき事項に位置づけた。

これまでのＷＧでの議論

○　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たところ。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。平時の予防対応として、脆弱性が指摘されている機器の確実なアップデートの実施等が必要。（第11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））

○　医療機関がサイバーセキュリティを確保するための具体的な対策を明示し、ペナルティを課すのではなく、支援・助言を行うための検査になるような進め方が望ましい（（第11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））））

○　令和４年度中に医療機関等の管理者が遵守すべき事項に位置付けるための省令改正を行う。（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９月５日））

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（予定）

○　「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。

チェックリスト項目（案）

【医療機関において確認する項目】

大項目	項番	チェック項目
1 体制構築	1－1	医療機関に医療情報システム安全管理責任者を配置している。
2 情報システムの管理	2－1	医療機関において、以下について把握している。
		①　医療機関で用いる端末の一覧
		②　医療機関で用いるネットワーク機器の一覧
		③　医療機関で用いる記録媒体の一覧
		④　医療機関で用いるサーバーの一覧
	2－2	職員の私物や事業者所有の機器等について、診療に関する業務で使用する場合の許可や管理体制が明確になっている。
	2－3	医療機関は、既に報告されている脆弱性について、事業者から最新の安全性に関する確認結果の報告を受けている。
3 情報システムの運用	3－1	退職者のアカウント等、不要なアカウントを削除する管理体制ができている。
	3－2	利用者の職種・担当業務別の情報区分ごとのアクセス管理機能がある。
	3－3	ネットワーク機器（※）に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。 （※）VPN機器を含むインターネットとの接続を制御するルータ。
	3－4	サーバーでアクセス記録（アクセスログ）の管理をしている。
	3－5	ネットワーク機器にアクセス制限を実施している。
4 インシデント発生時の対応	4－1	サイバー攻撃を受ける等システムに重大な障害が発生したことを想定した事業継続計画（BCP）を策定済み、又は、令和５年度中に策定予定である。
	4－2	インシデント発生時に備えて、組織内連絡体制と外部関係機関（事業者、厚生労働省及び警察等）への連絡体制を整えている。
	4－3	医療機関において、診療継続の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。

【事業者において確認する項目】

大項目	項番	チェック項目
1 体制構築	1－1	事業者内に、医療情報システムの管理責任者がいる。
2 情報システムの管理	2－1	事業者は、提供するソフトウェア・機器等の脆弱性に関して、医療機関への導入時、以降適時、求められる安全性に関する状況（初期PWの変更、脆弱性の更新状況）を確認し、医療機関にその結果を報告し、対応している。
3 情報システムの運用	3－1	ネットワーク機器（※）に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。 （※）VPN機器を含むインターネットとの接続を制御するルータ。
	3－2	サーバーでアクセス記録（アクセスログ）の管理をしている。
	3－3	ネットワーク機器にアクセス制限を実施している。
4 インシデント発生時の対応	4－1	事業者は、インシデント発生時、事前に明確化している責任分界点に応じて対応できる体制を整えている。
	4－2	事業者は、バックアップについての保管及び取り扱いについて、医療機関に取り扱い説明書等の文書として提供している。

医療分野におけるサイバーセキュリティ対策

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９月５日）資料２-２

初動対応

① インシデント発生時の駆けつけ機能の確保

– 200床**以下**の医療機関に対し、**サイバーセキュリティお助け隊の活用を促進するための周知・広報**を行う

– 200床**以上**の医療機関に対し、「医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初動対応支援・調査事業一式」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医療機関の初動対応支援**を行う。

② 行政機関等への報告の徹底

– **医療情報セキュリティ研修およびG-MIS調査を通じ**、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いた**厚生労働省への報告の徹底**や、個人情報保護法改正に伴う**個人情報保護委員会への報告義務化の周知**を図る。

– 厚生労働省より、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いて医療機関より報告のあったサイバーインシデント事案について、攻撃先が同定されない程度に報告内容を適時情報提供し、攻撃手法や脅威について分析を行い、全国の医療機関へ情報発信・注意喚起を行う。

復旧対応

① バックアップの作成・管理の徹底

– 医療情報セキュリティ研修およびG-MIS調査を通じ、**バックアップの具体的な作成が明記**された医療情報システムの安全管理に関するガイドライン（５．２版）の周知を行う。

– 令和３年６月28日発出「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について(注意喚起)」の記載事項に留意し、データ・システムのバックアップを行う。

– 令和4年度診療報酬改定における診療録管理体制加算に係る報告書（７月報告）により、**バックアップ保管に係る体制等の確認**を行う。

② 緊急対応手順の作成と訓練の実施

– 「医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初動対応支援・調査事業一式」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対応手順の調査**を行い、**適切な対応フローの整理**を行う。また、整理した対応フローをもとに**サイバーセキュリティインシデントに備えたBCPの提案**を行う。

医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初動対応支援・調査事業(令和４年度)

第13回健康・医療・介護情報利活用検討会医療等情報利活用WG（令和４年12月15日）資料３（一部改変）

背景

医療分野のサイバーセキュリティについては、近年その脅威が高まっていることから、令和４年度厚生労働省事業において、医療機関向け研修やサイバーセキュリティインシデント発生時の初動対応の支援等を行う。

事業概要

（１）サイバーセキュリティ対策にかかる医療機関向け研修の実施
　：医療機関職員の階層（初学者、経営層、システム･セキュリティ管理者等）に応じた研修の実施
（２）継続的な教育支援
　：医療情報システム安全管理者が研修に活用できる教育コンテンツ作成･収集と公開
（３）平時のサイバーセキュリティインシデント対応手順の調査および既存BCPの見直し提案
　：サイバーセキュリティインシデント発生時の適切な対応フローの整理、BCP（Business Continuity Plan）の提案
（４）サイバーセキュリティインシデントが発生した医療機関の初動対応支援
　：サイバーセキュリティインシデントが発生した医療機関の原因究明や早期診療復帰を目的に、初動対応支援を実施

受託者

一般社団法人　ソフトウェア協会

：約700社のソフトウェア製品に係わる企業が集まり、ソフトウェア産業の発展に係わる事業を通じて、我が国産業の健全な発展と国民生活の向上に寄与することを目的とした一般社団法人

（サイバーセキュリティに関する主な活動内容）

・ソフトウェアやサイバーセキュリティに関連したセミナー、研修の実施　　・サイバーセキュリティに関する情報交換・周知
・サイバーセキュリティボランティア制度の創設・運用

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

第13回健康・医療・介護情報利活用検討会医療等情報利活用WG（令和４年12月15日）資料３（一部改変）

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ている。緊急度の低い患者については、一度自宅退院、周辺病院への転院を進めたので、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
延べ入院患者数：22.3万人（646人/日）
延べ外来患者数：29.5万人（1,268人/日）

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。
来年１月：システム全面復旧予定

厚生労働省の対応

１．医療機関から要請を受けて、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といった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。（参考資料 ３）

令和４年11月10日事務連絡
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(注意喚起)
(抜粋)

1 サプライチェーンリスク全体の確認

関係事業者のセキュリティ管理体制を確認した上で、関係事業者とのネットワーク接続点（特にインターネットとの接続点）をすべて管理下におき、脆弱性対策を実施する。

2 リスク低減のための措置

・パスワードを複雑なものに変更し、使い回しをしない。不要なアカウントを削除しアクセス権限を確認する。多要素認証を利用し本人認証を強化する。
・IoT 機器を含む情報資産の保有状況を把握する。
・VPN 装置を含むインターネットとの接続を制御するゲートウェイ装置の脆弱性は、攻撃に悪用される可能性があるので、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。
・悪用が既に報告されている脆弱性については、ログの確認やパスワードの変更など、開発元が推奨する対策が全て行われていることを確認する。
・VPN 機器に対する管理インターフェースのインターネット上の適切なアクセス制限を実施する。
・メールの添付ファイルを不用意に開かない、URL を不用意にクリックしないこと。不審メールは、連絡・相談を迅速に行い組織内に周知する。

3 インシデントの早期検知

・サーバ等における各種ログを確認する。（例：大量のログイン失敗の形跡の有無）
・通信の監視・分析やアクセスコントロールを再点検する。（例：不審なサイトへのアクセスの有無）

4 インシデント発生時の適切な対処・回復

・サイバー攻撃を受け、システムに重大な障害が発生したことを想定した事業継続計画が策定する。
・データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。
・インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、外部関係機関への連絡体制や組織内連絡体制等を準備する。
・インシデント発生時及びそのおそれがある場合には、速やかに厚生労働省等の関係機関に対し連絡する。

5 金銭の支払いに対する対応

サイバー攻撃をしてきた者の要求に応じて金銭を支払うことは、犯罪組織に対して支援を行うことと同義と認識しており、以下の観点により金銭の支払いは厳に慎むべきである。
・金銭を支払ったからと言って、不正に抜き取られたデータの公開や販売を止めることができたり、暗号化されたデータが必ず復元されたりする保証がないこと。
・一度、金銭を支払うと、再度、別の攻撃を受け、支払い要求を受ける可能性が増えること。

警察におけるランサムウェア事案の初動対応等

医療機関におけるサイバーセキュリティ対策セミナー
警察庁講演資料（令和５年２月15日）

【警察の方針】患者への対応やシステム復旧を優先
被害法人に過度の負担はかけない

■初動対応時における捜査活動

〇通信ログの保全依頼（外部接続機器を中心とした可能な範囲）
〇システム担当者からの事情聴取
（内容）・被害端末に関する情報
・インターネットにより接続可能な機器に関する情報
・業務への影響、復旧方針　等

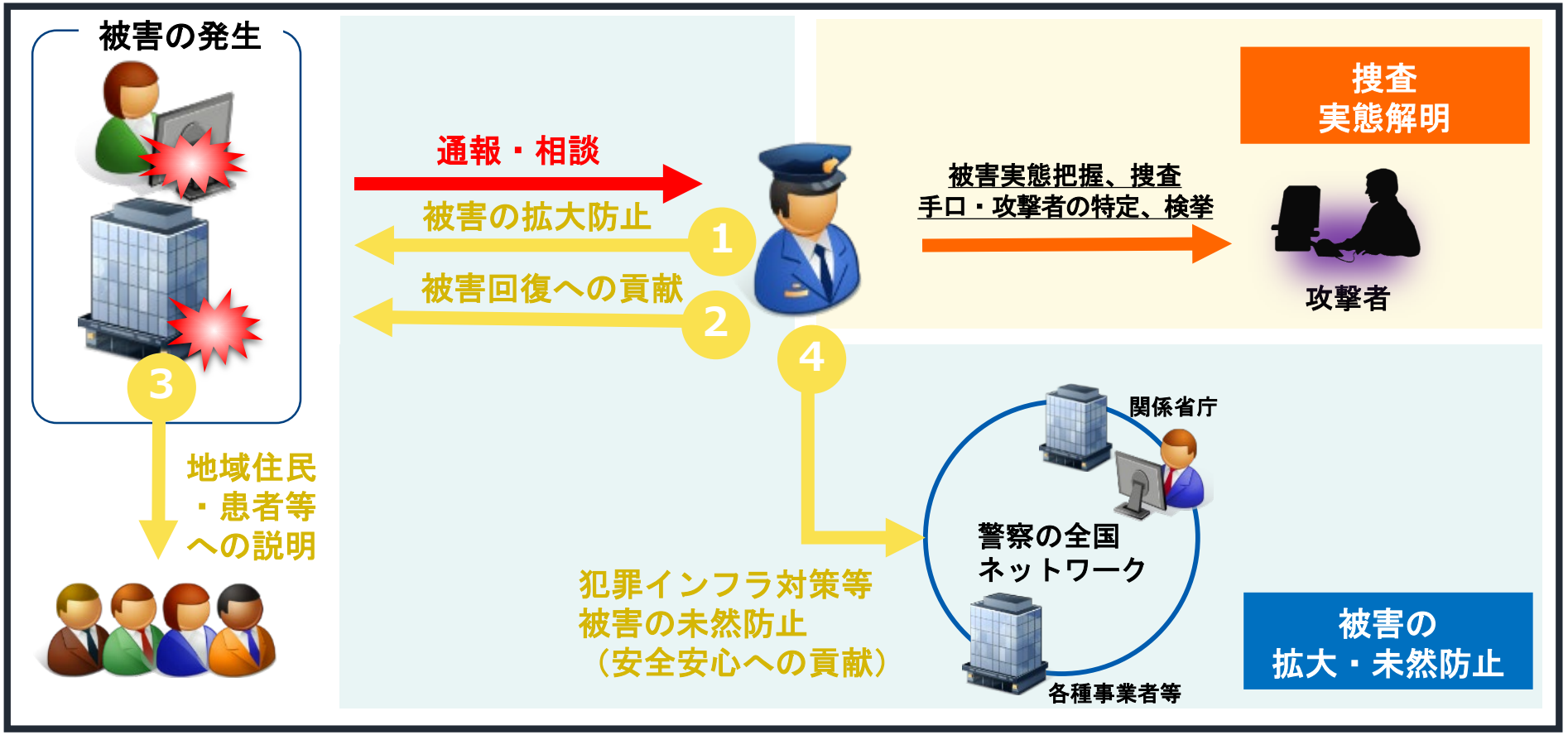
→被害原因（状況、手口、攻撃者情報等）の早期解明
→被害法人のシステムの早期復旧・被害回復の支援

※警察において対応が難しい内容
（医療機関の運営方針にかかる助言、直接の作業、機器の設定等）

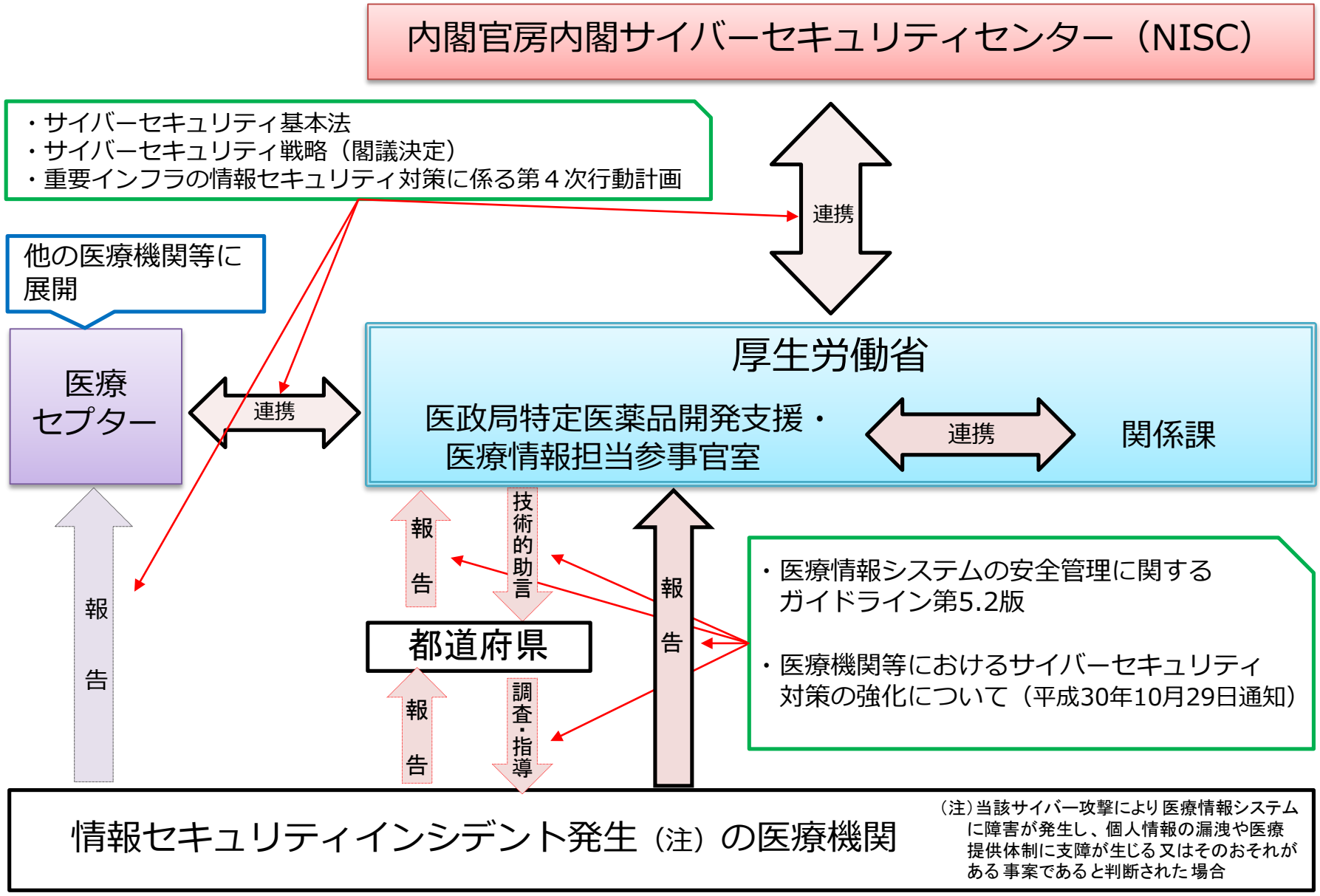
警察に通報することによる病院等におけるメリットについて

医療機関におけるサイバーセキュリティ対策セミナー
警察庁講演資料（令和５年２月15日）

① 被害医療機関等における被害の拡大防止（初動対応・再発防止等に関する助言等）
② 被害回復への貢献（被害回復制度等に関する助言、ランサムウェア被害時の被害回復に向けた支援）
③ 地域医療機関として社会的責任を果たしていることの説明（一般に犯罪に遭った際には警察に通報することが期待される）、犯罪の被害者であることの疎明
④ 社会全体の被害の未然防止（安全・安心なサイバー空間の確保に対する社会的貢献）



医療機関におけるサイバーセキュリティインシデント発生時の対応



情報共有の仕組み（セプターの概要）

名　称	**医療CEPTOAR**
事務局	**公益社団法人　日本医師会　情報システム課**
概　要	**１．機能** ＩＴ障害の未然防止、ＩＴ障害の拡大防止・迅速な復旧、ＩＴ障害の要因等の分析・検証による再発防止を図り、医療事業者のサービスの維持・復旧能力の向上に資するため、政府等から提供される情報を適切に医療事業者等の間で共有・分析することを目的に、医療分野の「情報共有・分析機能（セプター）」として、「医療CEPTOAR」を設置。 以下(1)～(3)の情報連絡体制等については現状の枠組みをもとに引き続き改善に向けて調整していく。 (1) 医療事業におけるＩＴ障害の未然防止、ＩＴ障害の拡大防止・迅速な復旧、ＩＴ障害の要因等の分析・検証による再発防止のための情報共有及び連携 (2) 政府、他のセプター等から提供される情報の構成員への連絡 (3) 政府、他のセプター等から提供される情報に関連する事項の情報共有 **２．構成** ● 日本医師会、日本歯科医師会、日本薬剤師会、日本看護協会（情報共有機能） ● 日本医療法人協会、日本精神科病院協会、日本病院会、全日本病院協会（情報共有機能） ● 全国自治体病院協議会、日本私立医科大学協会、日本慢性期医療協会、労働者健康安全機構、日本社会医療法人協議会、国立病院機構、地域医療機能推進機構、日本リハビリテーション病院・施設協会、地域包括ケア病棟協会、大学病院長会議（情報共有機能） ● オブザーバー（情報分析機能）として保健医療福祉情報システム工業会 **３．特色・特徴** ● これまでの活動・現行組織を基盤にした実効性のある体制。 ● 医療分野の特性として、医療提供体制の構築・維持は都道府県との情報共有体制が不可欠であることから、他の分野ではみられない都道府県との連携が必要。

中・長期的な医療機関におけるサイバーセキュリティ対策

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９月５日）資料２-２

【今後の検討事項】

バックアップデータの暗号化・秘匿化

・**最新技術を利用したバックアップの検討**
－医療情報のよりセキュアなバックアップを行うため、**バックアップデータの暗号化・秘匿化**に向けた検討を進める。

保健医療分野におけるSOC（Security Operation Center）の構築の検討

※ SOCとは、セキュリティ・サービス及びセキュリティ監視を提供するセンターのこと。（引用元：サイバーセキュリティ2022）

・ **24時間365日体制**で、プロキシサーバーを経由した医療機関に対する不審な通信やウェブサイトの稼働状況を監視することで、**サイバー攻撃の早期発見が可能**となる。

・保健医療分野を横断的に監視することで、医療機関に対して**多く使われる攻撃手法**・**昨今のサイバー攻撃の傾向**を**観測**することができ、その観測データを医療機関内のCSIRTや情報共有体制（ISAC）へ提供することにより、**分析および対策に資することが可能**となる。ただし、セキュリティ対策にかける費用と損害のバランスには留意が必要。

・厚生労働省において、令和４年度事業として「保険医療機関等へのセキュリティ監視環境検証事業」を実施予定。医療機関へ情報資産の実地調査等を行い、**セキュリティ監視システムの全体構成の検討**や**保健医療分野において望ましいSOC構築に向けた検討**を行っていく。

その他

・「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」の対象事業者と医療機関等の合意形成の項目及び、HELICS協議会において医療情報化指針として採択した（令和4年8月）「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）の遵守を業界団体及び医療機関に徹底する。

医療分野のサイバーセキュリティに関する検討状況

第7回サイバーセキュリティ研究会
（令和４年４月11日）資料３より抜粋

- 医療機関における外部ネットワーク接続の拡大等を踏まえ、厚生労働省において、サイバーセキュリティ対策の在り方を検討中。

医療機関等のサイバーセキュリティ対策

厚生労働省において、医療機関における外部ネットワーク接続の拡大や、国内の医療機関を標的にしたサイバー攻撃の増加を踏まえ、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を実施。
本調査研究事業では、

- ✓ 国内外における医療情報セキュリティ動向調査
- ✓ 医療情報システムのクラウド化における現状調査
- ✓ よりわかりやすいチェックリストの提案
- ✓ 有効なモデルセキュリティポリシー案の策定
- ✓ **医療機関における「サイバーセキュリティお助け隊」の活用可能性・追加すべきオプション等の検討**

を実施予定。

医療機関の規模やネットワーク構成等により、お助け隊をそのまま活用できるもの、特殊事情に合わせたオプションを必要とするものなどが存在する可能性。これらを**経済産業省と厚生労働省とで連携し、精査・検討していく**。

サイバーセキュリティお助け隊サービス

- 2019年度・2020年度実証事業で得られた知見に基づき、実証参加事業者がサービスを開発。
- サービス普及に向け、2021年度よりサービスブランドを設立。現時点で12サービスが登録。サービス審査登録制度の運営とともに、中小企業の意識啓発・サプライチェーンによる普及などの施策と一体となった普及施策の展開を開始。

中小企業のサイバーセキュリティ対策に不可欠な各種サービス

サイバーセキュリティお助け隊サービスウェブページ（11/10公開）
〈https://www.ipa.go.jp/security/otasuketai-pr/〉

- EDR・UTMによる異常監視
- 緊急時の対応支援・駆け付けサービス
- 相談窓口
- 簡易サイバー保険
- 簡単な導入・運用

中小企業でも導入・維持できる価格でワンパッケージで提供

お助け隊サービス審査登録制度：
一定の基準を満たすサービスにお助け隊マークの商標利用権を付与

お助け隊サービスA
お助け隊サービスB
お助け隊サービスC

サービス提供 → 中小企業 → 自社の信頼性をアピール → 取引先（大企業等）

サイバーセキュリティ お助け隊

お助け隊サービス利用の推奨等の中小企業の取組支援

SC3(サプライチェーン・サイバーセキュリティ・コンソーシアム)

→SC3（業種別業界団体が参加）で利用推奨を行うことで、より多くの中小企業がお助け隊サービスを活用し、万が一の際に早急に正しい対処が行える状態を目指す。

IT導入補助金による「サイバーセキュリティお助け隊サービス」の導入支援

- 「通常枠」及び「デジタル化基盤導入枠」において、オプションとして「サイバーセキュリティお助け隊サービス」をメインツールと組み合わせて申請することが可能。この際、「サイバーセキュリティお助け隊サービス」を申請する事業者については、申請採択における審査時に加点対象に。
- また、コロナ禍における「原油価格・物価高騰等 総合緊急対策」（4月26日決定）に関連し、新たに「セキュリティ対策推進枠」を設置。「サイバーセキュリティお助け隊サービス」の単品での申請が可能に。

オプションとして「サイバーセキュリティお助け隊サービス」をメインツールと組み合わせて申請可能。

「サイバーセキュリティお助け隊サービス」を単品で申請可能。

	通常枠		デジタル化基盤導入枠					セキュリティ対策推進枠 新設
	A類型	B類型	デジタル化基盤導入類型				複数社連携IT導入類型	
補助額	30万円～150万円未満	150万円～450万円以下	会計・受発注・決済・ECソフト：5万円～50万円以下	会計・受発注・決済・ECソフト：50万円超～350万円	PC・タブレット等：～10万円	レジ・券売機等：～20万円	(1)デジタル化基盤導入類型の対象経費（左記同様） (2)消費動向等分析経費（上記(1)以外の経費）※1 50万円×参画事業者数 補助上限：(1)+(2)で3,000万円 (3)事務費・専門家費 補助上限：200万円	5万円～100万円
補助率	1/2以内		3/4以内	2/3以内（※2）	1/2以内		(1)デジタル化基盤導入類型と同様 (2)・(3) 2/3以内	1/2
補助対象経費	ソフトウェア購入費、クラウド利用料（最大1年分）、導入関連費		ソフトウェア購入費、クラウド利用料**（最大2年分）**、導入関連費、**ハードウェア購入費**					ｻｲﾊﾞｰｾｷｭﾘﾃｨｻｰﾋﾞｽ利用料（最大2年分）（※3）

(※1)消費動向等分析経費のクラウド利用料は、１年分が補助対象となります。
(※2)交付の額が50万円超の場合の補助率は、当該交付の額のうち50万円以下の金額については3/4、50万円超の金額については2/3。
(※3)（独）情報処理推進機構（IPA）「ｻｲﾊﾞｰｾｷｭﾘﾃｨお助け隊ｻｰﾋﾞｽﾘｽﾄ」に掲載されたサービス

Ministry of Health, Labour and Welfare of Japan

ご静聴ありがとうございました。

ひと、くらし、みらいのために

厚生労働省

Ministry of Health, Labour and Welfare

（参考）お助け隊サービスの提供イメージ

第11回健康・医療・介護情報利活用検討会
医療等情報利活用WG　資料３

- 中小企業にUTM、EDR等のセキュリティ監視ツールを設置し常時の異常監視を行うとともに、①相談窓口による導入・運用に関するユーザーからの各種相談の受け付け、必要に応じて②リモートでの支援や③駆けつけ支援などを実施。