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

2023/2/15

医療機関におけるサイバーセキュリティ対策セミナー

厚生労働省における医療機関のサイバーセキュリティ対策にかかる取組について

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室室長補佐

岡本　潤

Ministry of Health, Labour and Welfare of Japan

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期対応支援・調査事業

目次

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。

GL5.2版への改定について

○　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・巧妙化への対策等を追加）

サイバー攻撃への具体的対策について

【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）

医療機関がサイバー攻撃（疑い含む）を受けた場合の対応

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

各　都道府県 保健所設置市 特別区　医政主管部（局）長　殿

厚生労働省医政局総務課長
厚生労働省医政局地域医療計画課長
厚生労働省医政局研究開発振興課長
（　公　印　省　略　）

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

日頃より医療分野の情報化に関し、格別のご配慮を賜り、厚く御礼申し上げます。

医療分野における情報化につきましては、近年、電子カルテシステムや地域医療情報連携ネットワーク等の普及が進み、情報通信技術は医療現場の多くで活用されています。

一方で、昨年５月に発生した世界的なランサムウェア「WannaCry」による被害をはじめ、我が国の医療機関においても相次いでコンピュータウイルスの感染事案が報告され、医療提供体制に支障が生じる事例も発生するなど、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おります。

厚生労働省におきましては、内閣サイバーセキュリティセンター（NISC）及び医療関係団体等と連携して、医療機関等（医療法（昭和 23 年法律第 205 号）に規定する医療提供施設のほか、地域医療情報連携ネットワーク等を含む。以下同じ。）におけるサイバーセキュリティ対策に取り組んできたところですが、今後は都道府県、保健所設置市及び特別区とも連携を強化し、対策のさらなる充実を図ってまいりたいと考えておりますので、貴職におかれましては、下記についてご協力方よろしくお願いいたします。

なお、本通知は、地方自治法（昭和 22 年法律第 67 号）第 245 条の４第１項の規定に基づく技術的助言であることを申し添えます。

記

１　「医療情報システムの安全管理に関するガイドライン」の周知徹底について

医療機関等においてサイバー攻撃を受けた際の非常時の対応については、「医療情報システムの安全管理に関するガイドライン　第５版」（平成 29 年５月 30 日政統発 0530 第１号。以下「ガイドライン」という。）に定められているところです。

医療機関等に対するサイバー攻撃の危険性がさらに高まっていることに鑑み、貴職におかれましては、管内の医療機関等に対して、ガイドラインの更なる周知徹底を図るとともに、医療機関等においてコンピュータウイルスの感染などによるサイバー攻撃を受けた疑いがある場合にあっては、別紙を活用して直ちに医療情報システムの保守会社等に連絡の上、当該サイバー攻撃により医療情報システムに障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、速やかに当該医療機関等から厚生労働省医政局研究開発振興課医療技術情報推進室（以下「医療技術情報推進室」という。）に連絡を行うよう、注意喚起をお願いいたします。

２　情報セキュリティインシデント発生時の国への報告について

管内の医療機関等において、コンピュータウイルスの感染などによるサイバー攻撃を受け医療情報システムに障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案を貴自治体が把握した場合（医療機関等からの報告により把握した場合のほか、報道発表又はマスコミ報道等により把握した場合を含む。）にあっては、事実把握後速やかに貴自治体から医療技術情報推進室に報告いただくようお願いいたします。特に自治体立病院につきましては、自治体立病院運営部署（団体）又は都道府県におかれては、自治体立病院を有する市区町村と連携し、国との情報共有に万全を期していただきますようお願いいたします。

３　情報セキュリティインシデントが発生した医療機関等に対する調査及び指導について

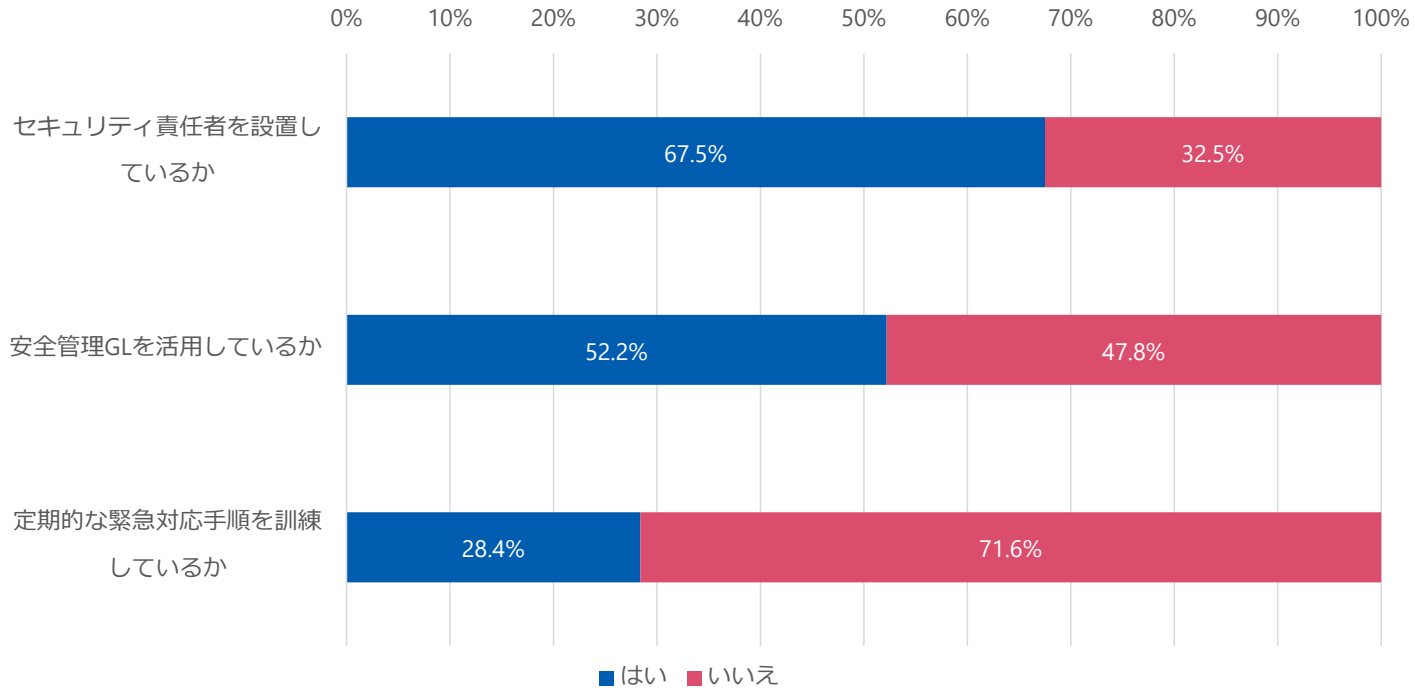
貴自治体においては、コンピュータウイルスの感染などによるサイバー攻撃を受けた医療機関等に対し、必要に応じて、被害状況、対応状況、復旧状況、再発防止策等に係る調査及び指導を行い、医療技術情報推進室に報告いただくようお願いいたします。なお、事案発生時には厚生労働省より情報収集・調査・指導等の依頼があり得ることを申し添えます。

また、病院、診療所又は助産所に対する情報セキュリティインシデントに係る調査及び指導につきましては、医療法第 25 条及び第 26 条並びに医療法施行規則（昭和 23 年厚生省令第 50 号）第 42 条に基づく立入検査等を行うことが可能です。当該立入検査等の実施にあたっては、サイバーセキュリティに係る技術的事項等につ

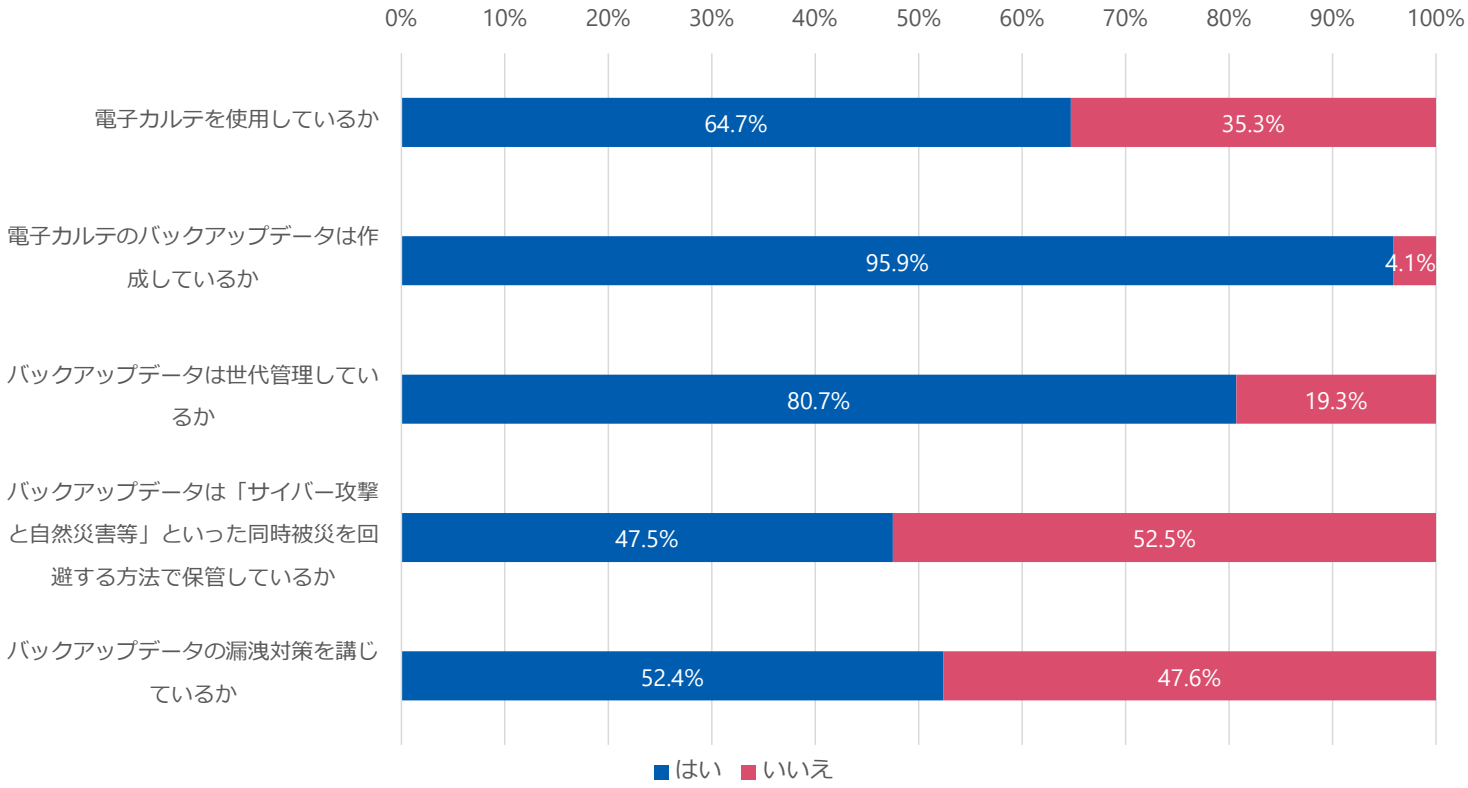
調査結果について

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%）



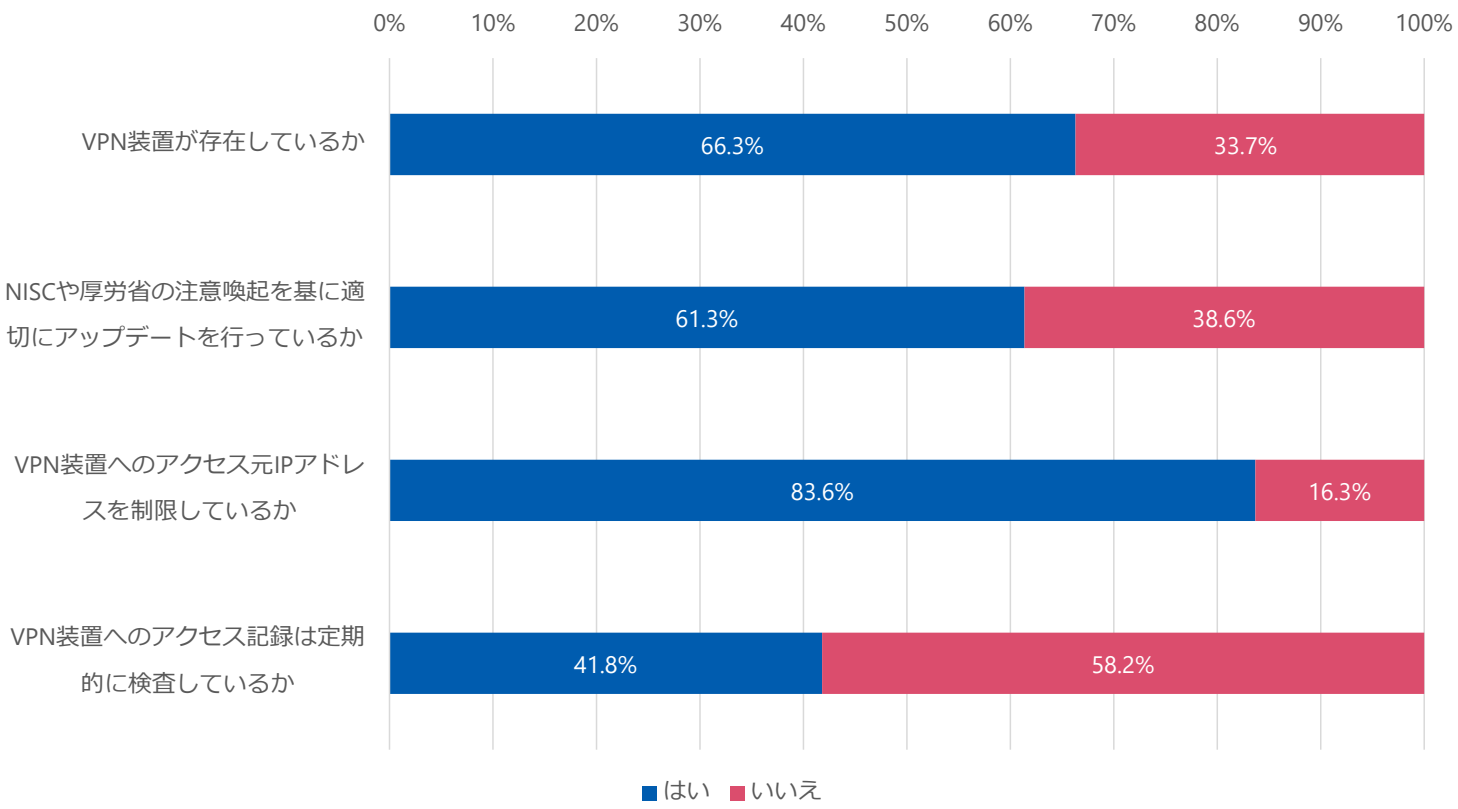
調査結果について（電子カルテシステムのバックアップについて）



※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。

今年の調査について

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を開始します

厚生労働省は、昨年に引き続き、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を、本日より実施します。

本調査は、病院におけるランサムウェアなどのサイバー攻撃被害のリスクを把握するとともに、早急に有効な対策の実施を促すため、病院が保有する電子カルテシステム等の医療情報システムにおけるサイバーセキュリティ対策の実態を把握することを目的としております。

調査方法については、別紙「調査項目一覧」の内容を、医療機関等情報支援システム（G-MIS）を用いて行います。

厚生労働省では、引き続き、医療機関に必要なサイバーセキュリティ対策を適切に進めてまいります。

■調査概要
・調査名：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
・スケジュール：令和５年１月27日（金）～２月17日（金）
・調査対象施設：医療機関等情報支援システム（G-MIS）を利用している病院（8,238病院）※令和５年１月19日時点
・調査方法：医療機関等情報支援システム（G-MIS）　を用いた電子調査方式
・調査項目：別紙のとおり

技術的な質問・用語等については、院内担当者だけでなく、システム設置事業者や保守ベンダーへ照会等を行い、質問内容を理解した上で、回答してください。

〇主な調査項目
・バックアップデータの作成方法等詳細に関して
・VPN機器の詳細に関して
・事業継続計画（BCP）に関して（サイバー攻撃等によるシステム障害発生時に備えた）

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**。
4. 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期対応支援・調査事業

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期対応支援・調査事業

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。**（令和５年１月27日より調査開始）**
【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期対応支援・調査事業

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

（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

【取組事項】

① 医療機関向けサイバーセキュリティ対策研修の充実 ——▶**今年度のセキュリティ研修事業者（(一社)ソフトウェア協会）に委託**
– 「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」を８月19日より公示開始。本事業により、**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。

予防対応

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**検討グループを年内に立ち上げる。**

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。

出典元：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資料より抜粋

【令和４年度の医療機関向けサイバーセキュリティ研修】

ポータルサイトを設置し、医療機関向けの研修実施内容や予定に関してお知らせ

12月から順次サイバーセキュリティ研修を開始

- **経営者、システム・セキュリティ管理者・初学者**のそれぞれの立場にあった**３階層の教育コンテンツ**を提供
- **オンライン型の研修**実施による遠隔地で参加可能な体制
- **e-learningでのセキュリティ基礎研修**の提供

※詳細は受託事業者でポータルサイトを作成し、Webページの新規作成や更新を行います。

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期対応支援・調査事業

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

https://mhlw-training.saj.or.jp/

研修名	研修参加者数
経営者向け	約500名
システム・セキュリティ管理者向け（計4回）	1回目　約700名 2回目　約600名
第1回 初学者・医療従事者向け	約400名
第２回 初学者・医療従事者向け	約600名

（2月14日時点）

医療法第25条第１項の規定に基づく立入検査にかかる省令改正施行に関して

経緯・概要

○　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が必要。（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））

○　**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４月１日施行予定）**

◎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、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。）の確保のために必要な措置を講じなければならない。

※　下線部を新設する。

（参照条文）
◎医療法（昭和二十三年法律第二百五号）
第十七条　第六条の十から第六条の十二まで及び第十三条から前条までに定めるもののほか、病院、診療所又は助産所の管理者が、その構造設備、医薬品その他の物品の管理並びに患者、妊婦、産婦及びじよく婦の入院又は入所につき遵守すべき事項については、厚生労働省令で定める。

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

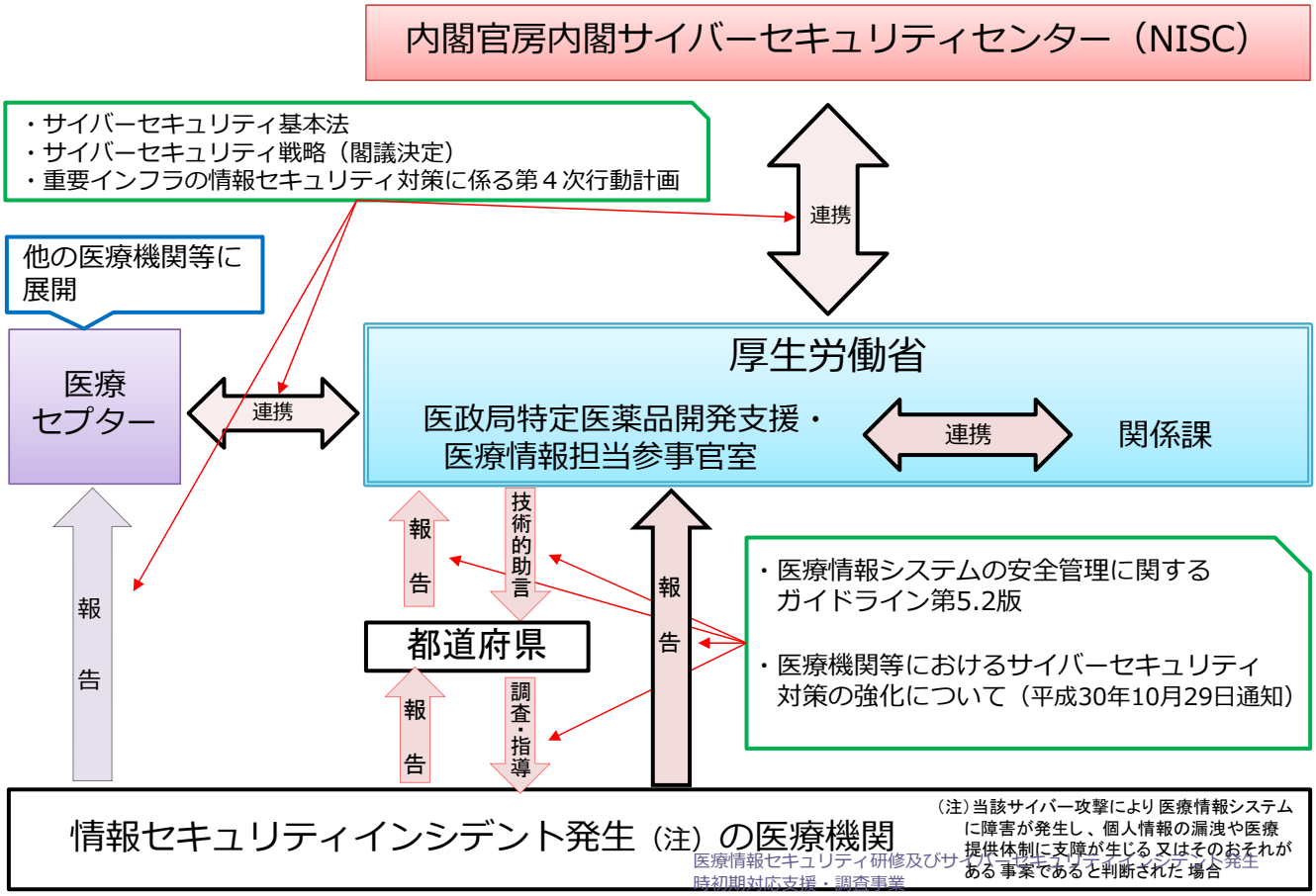
（１）サイバーセキュリティ対策にかかる医療機関向け研修の実施
：医療機関職員の階層（初学者、経営層、システム･セキュリティ管理者等）に応じた研修の実施
（２）継続的な教育支援
：医療情報システム安全管理者が研修に活用できる教育コンテンツ作成･収集と公開
（３）平時のサイバーセキュリティインシデント対応手順の調査および既存BCPの見直し提案
：サイバーセキュリティインシデント発生時の適切な対応フローの整理、BCP（Business Continuity Plan）の提案
（４）サイバーセキュリティインシデントが発生した医療機関の初動対応支援
：サイバーセキュリティインシデントが発生した医療機関の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

医療機関における情報セキュリティインシデント発生時の対応



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期対応支援・調査事業

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。

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期対応支援・調査事業

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事案に関して

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3一部抜粋

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。

(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。

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。

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

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。

中・長期的な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

【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**。

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期対応支援・調査事業

Ministry of Health, Labour and Welfare of Japan

皆様へのお願い

- G-MIS調査に関するご協力のお願い
- サイバーインシデント（疑い）事案時の厚生労働省等へのご報告
- 医療機関等に求めているサイバーセキュリティ対策の徹底

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