情報提供

那医発第271号
令和8年7月16日

施設長　各位

那覇市医師会
会　　長　玉井　修
担当理事　小禄 雅人

平素より医師会事業へのご支援ご協力賜り感謝申し上げます。
沖縄県医師会より「令和８年度 診療所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について（周知依頼）」の通知が届きましたのでご案内申し上げます。
☆ 問合せ先（那覇市医師会　事務局：宮城・前泊　／電話 ０９８－８６８－７５７９）

・・・・・・・・・・・・・・・・・・・・・・・・記・・・・・・・・・・・・・・・・・・・・・・

沖医発第562号
令和８年７月６日

地区医師会情報システム担当理事　殿

沖縄県医師会
理事　富名腰　亮
（公印省略）

令和８年度 診療所における
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について（周知依頼）

時下ますますご清祥のこととお慶び申し上げます。
さて、日本医師会よりみだしの件について、別紙のとおり通知があります。
本件は、診療所におけるサイバーセキュリティ対策の実態把握及び今後の効果的な支援につなげることを目的として、厚生労働省が調査を実施する旨の案内となっております。
同調査は、医療機関用情報支援システム(G-MIS)を利用している診療所を対象として実施されるものであり、調査対象の診療所に対しては、G-MIS により通知される予定となっておりますので、内容をご確認の上、調査へのご協力をお願いいたします。
つきましては、貴会におかれましても、本件についてご了知いただくとともに、貴会会員への周知方につきご高配を賜りますようよろしくお願い申し上げます。

記

●令和８年度 診療所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について　（令和８年６月22日 日医発第576号(情シ)）

調査名　：診療所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
調査対象：医療機関等情報支援システム（G-MIS）を利用している診療所
※調査対象の診療所に対して、G-MIS により通知される予定。
調査期間：令和８年７月６日（月）～令和８年８月21日（金）
回答方法：回答要領に基づき、G-MIS 上で回答。
※詳細につきましては、別添資料をご確認ください。

※関係文書は文書管理システムへ掲載致します。

沖縄県医師会事務局業務２課：宮良
TEL：098-888-0087
FAX：098-888-0089
g2@okinawa.med.or.jp

16

日医発第576号(情シ)
令和 8 年 6 月 22 日

都道府県医師会　担当理事　殿

日本医師会　常任理事
長 島　公 之
(公 印 省 略)

令和８年度 診療所における
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について

平素より本会会務の運営に特段のご理解・ご支援を賜り厚く御礼申し上げます。

近年、国内外の医療機関を標的とした、ランサムウェア（情報システムを使用不可の状態にした上で身代金を要求するウイルス）を利用したサイバー攻撃による被害が増加している状況にあり、日本医師会においても注意喚起を行ってまいりました。

例年、厚生労働省において、病院を対象としたサイバーセキュリティ対策の実態調査が行われておりますが、この度、診療所でのランサムウェア被害のリスクを把握や、実態を踏まえて今後の効果的な支援につなげることを目的として、診療所を対象とした実態調査を行う旨が通知され、協力依頼が参りました。

調査方法については、下記期間において別紙回答要領に基づき「医療機関等情報支援システム（G-MIS)」を用いて行われるとのことです。また、調査の設問内容は「医療機関・薬局におけるサイバーセキュリティ対策チェックリスト」の項目に含まれているため、チェックリストや同マニュアルを確認しながら、調査に協力ください。

なお、「日本医師会サーバーセキュリティ支援制度」では、厚生労働省の「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」への対応として、実践ガイドやセミナー動画の提供、相談窓口の開設を行っておりますので、適宜ご活用ください。

つきましては、貴会におかれましても、本件についてご了知いただくと共に、貴会管下の郡市区等医師会ならびに会員への周知方につき、是非、ご高配を賜りますようお願い申し上げます。

記

【調査名】診療所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
【調査対象】医療機関等情報支援システム（G-MIS）を利用している診療所
※調査対象の診療所に対して、G-MIS により通知される予定。
【調査期間】令和８年７月６日（月）～令和８年８月 21 日（金）
【回答方法】回答要領に基づき、G-MIS 上で回答。

【照会先】
①G-MIS のログインや操作に関すること
○ログイン画面(https://www.med-login.mhlw.go.jp/s/login/)

○ユーザ名（ログイン ID）が不明などのログインに関するお問い合わせ「よくあるお問い合わせ」
（https://www.mhlw.go.jp/content/001698266.pdf）
厚生労働省 G-MIS 事務局
TEL：050-3355-8230　応対時間：平日 9 時～17 時

②調査の内容に関すること
厚生労働省 医政局 医療情報担当参事官室
担当者：橋本、安藤、東、上村
TEL：03-6812-7837
応対時間：平日 10 時～17 時（12 時 15 分～13 時 15 分を除く）

【別添資料】
・令和 8 年 6 月 15 日付事務連絡「令和 8 年度診療所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について(依頼)」
・別紙「診療所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」回答要領（調査項目）

【参考】
・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
https://www.mhlw.go.jp/content/10808000/001253950.pdf

・令和 7 年度版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マニュアル
https://www.mhlw.go.jp/content/10808000/001490741.pdf

・日本医師会サイバーセキュリティ支援制度（日医メンバーズルーム）
https://www.med.or.jp/japanese/members/info/cyber_shien.html
④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の実践ガイドおよびセミナー動画の提供
⑤日本医師会セキュリティガイドライン相談窓口
TEL：0120-339-199　運営時間　平日 9 時～18 時
チェックリスト、ガイドラインの各種相談に対応。
日本医師会 A①会員が開設・管理する医療機関等が利用可能。（A①会員本人に加え、職員からのお問合せ、都道府県医師会、郡市区等医師会の事務局からのお問合せも可能）

以上

事　務　連　絡
令和８年６月15日

公益社団法人　日本医師会　御中

厚生労働省医政局
医療情報担当参事官室

令和８年度 診療所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
調査について（依頼）

日頃より厚生労働行政に対しご協力を賜り、厚く御礼申し上げます。

近年、サイバー攻撃は増加の一途をたどり、医療機関を標的としたサイバー事案が続いております。

これまで、厚生労働省では、病院におけるサイバーセキュリティに係る調査を行っておりました。

この度、調査の範囲を広げ、診療所におけるランサムウェア被害のリスクを把握するとともに、その実態を踏まえて今後の効果的な支援につなげるため、診療所におけるサイバーセキュリティ対策の実態を調査することといたしました。

つきまして、貴会におかれては、貴会関係者に本調査についてご周知いただくとともに、対象医療機関への円滑かつ正確な報告の促進をお願い申し上げます。

また、ご周知いただく際には、今回の調査の設問内容が「医療機関・薬局におけるサイバーセキュリティ対策チェックリスト」の項目に含まれているため、この機会に「医療機関・薬局におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・薬局・事業者向け～」とチェックリストを改めてご確認いただき、調査にご対応いただけるよう、ご周知いただきますようお願いいたします（※）。

（※）チェックリスト及びチェックリストマニュアルは回答日時点での、最新のものを利用するようご留意ください。

なお、本調査は、別紙回答要領に基づき、G-MIS を用いて行うこととしておりますので、合わせて、以下の通り、ご周知をお願いいたします。

【調査名】
診療所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

【調査対象】
医療機関等情報支援システム（G-MIS）を利用している診療所
※調査対象の診療所に対して、G-MIS により通知される予定です。

【調査期間】
令和８年７月６日（月）～令和８年８月２１日（金）

【回答方法】
別紙回答要領に基づき、G-MIS 上で回答。

【照会先】
① G-MIS のログインや操作に関すること
ログイン画面（https://www.med-login.mhlw.go.jp/s/login/）はこちら

ユーザ名（ログイン ID）が不明などのログイン等に関するお問い合わせは、
「よくあるお問い合わせ」（https://www.mhlw.go.jp/content/001698266.pdf）をご参照ください。

厚生労働省 G-MIS 事務局
TEL：050-3355-8230
応対可能時間：9 時～17 時（土日祝日を除く）

② 調査の内容に関すること
厚生労働省 医政局 医療情報担当参事官室
担当者：橋本、安藤、東、上村
TEL：03-6812-7837
応対可能時間：10 時～17 時（土日祝日及び平日 12 時 15 分～13 時 15 分を除く）

別紙

「診療所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」
回答要領

依頼事項

- 本回答要領に基づき、診療所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（以下「本調査」という。）について回答をお願いします。

- 回答にあたっては、必ず本回答要領を確認してください。

- 本調査は「医療情報システムの安全管理に関するガイドライン」・「医療機関・薬局におけるサイバーセキュリティ対策チェックリスト」及び厚生労働省等から発出された通知・事務連絡等の内容を基に調査します。これらの文書について確認の上、回答してください。

  参考：

  「医療情報システムの安全管理に関するガイドライン」および「医療機関・薬局におけるサイバーセキュリティ対策チェックリスト」については、以下のＵＲＬより最新版をご参照ください。調査票回答画面からもアクセスできるようにしておりますのでご活用ください。

  https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

- 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、回答してください。

- 回答は、令和８年６月末時点の状況についてお答えください。

（※）医療情報システムとは、オーダリングシステム、電子カルテシステム、レセプト電算システム（審査請求受付も含む）、画像・検査等の各部門システム、地域医療ネットワークシステム、PHR 等、診療所における診療を補助するためのシステム全般を指します。

【調査項目について】

Ｑ１　回答者の氏名

回答者の氏名を記載してください。

Ｑ２　医療情報システム安全管理責任者を設置している

医療情報システム安全管理責任者とは情報セキュリティ対策に関する統制の実効性を確保するために、安全管理を直接実行する者を指します。医療情報システム安全管理責任者としての職務は、経営層が担うことを想定していますが、医療機関等の規模・組織等を考慮して、企画管理者が医療情報システム安全管理責任者を兼務することは可能です。

参考：「医療情報システムの安全管理に関するガイドライン」
経営管理編　3.安全管理全般【遵守事項】
③ 安全管理を直接実行する医療情報システム安全管理責任者及び
企画管理者を設置すること。

Ｑ３－１　サイバー攻撃等によるシステム障害発生時に備え、事業継続計画（BCP）を策定している

「医療情報システムの安全管理に関するガイドライン」では、情報セキュリティインシデントが発生し、医療情報システムの可用性が損なわれる事態に備えて、通常時から、非常時における医療情報システムの運用に関する対応を整理することが重要である、と求めています。自組織において、サイバー攻撃等に備えた事業継続計画（BCP）を策定している場合は「はい」を選択してください。サイバー攻撃等とは、医療情報システムの稼働（可用性）が損なわれる、災害、サイバー攻撃、システム障害等が想定されます。

参考：「医療情報システムの安全管理に関するガイドライン」
経営管理編 3.安全管理全般【遵守事項】
⑬ 情報セキュリティインシデントの発生に備え、非常時における業務継続の可否の
判断基準、継続する業務内容の選定等に係る意思決定プロセスを検討し、BCP 等を整備すること。

Ｑ３－２　Ｑ３－１に対して「はい」を選択した方が対象となる質問です。
事業継続計画（BCP)において策定された対処手順が適切に機能するか、訓練等により確認している

「医療情報システムの安全管理に関するガイドライン」では、自組織において定められているサイバー攻撃を想定した事業継続計画（BCP）が適切に機能することを訓練等により確認することが重要であるとされています。自組織の事業継続計画（BCP）において策定された対処手順が適切に機能することを、訓練等により確認している場合は「はい」を選択してください。

参考：「医療情報システムの安全管理に関するガイドライン」
経営管理編 3.安全管理全般【遵守事項】
⑮ 通常時に整備していたBCPが、非常時において迅速かつ的確に実施できるよう、通常時から定期的に訓練・演習を実施し、その結果を踏まえ、必要に応じて改善に向けた対応を企画管理者やシステム運用担当者に指示すること。

Ｑ４　サーバ、端末、ネットワーク機器の台帳管理を行っている

医療情報システムで用いる情報機器等の安全性を確保するために、情報機器等の所在と、それらの使用可否の状態を適切に管理する必要があります。そのため、企画管理者（医療機関の危機管理を行う責任者のこと）に対して診療所で所有する医療情報を扱うシステムで用いる情報機器等について機器台帳を作成して管理を行い、情報機器等が利用に適した状況にあることを確認可能な状態とすることを求めています。

これを満たしている場合は「行っている」を選択してください。紙媒体であっても電子媒体であっても構いません。台帳で管理する内容としては情報機器等の所在や利用者、ソフトウェアやサービスのバージョンなどが想定されます。

参考：「医療情報システムの安全管理に関するガイドライン」
企画管理編　9.医療情報システムに用いる情報機器等の資産管理【遵守事項】
① 医療情報システムにおいて用いる情報機器等の資産管理を行うのに必要な規程その他の資料を整備し、その管理を行うこと。

Ｑ５　少なくとも年１回程度、職員を対象として、情報セキュリティに関する研修を行っている

「医療情報システムの安全管理責任者が、職員向けに実施する情報セキュリティに関する研修を指します。研修を実施している場合は「はい」を選択してください。

医療機関向けセキュリティ教育支援ポータルサイト：MIST（https://mist.mhlw.go.jp/）で提供される e-learning 研修等も該当します。

参考：「医療情報システムの安全管理に関するガイドライン」

企画管理編　7.安全管理のための人的管理【遵守事項】

② 個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施すること。また、教育・訓練の実施状況について定期的に経営層に報告すること。

Ｑ６　自組織において、電子カルテシステムを使用している

診療録の記載・保存を電子カルテシステムで行っている場合は「はい」を選択してください。

なお、本問でいう電子カルテシステムとは、以下を指します。

- オーダリング機能、画像管理等の部門システム及び診療録を電子的に記録する機能を備えた統合的な医療情報システム