令和 3 年 11 月 5 日

郡市区等医師会　御中

一般社団法人 大阪府医師会
（公印省略）

医療機関を標的としたサイバー攻撃への対応について（注意喚起）

平素は、本会事業の推進に格別のご高配を賜り、厚く御礼申し上げます。

標記の件について、このたび別添 1、2 の通り、日本医師会から通知がありました。

別添 1 は、平成 17 年 3 月 31 日「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」（医政発第 0331009 号薬食発第 0331020 号保発第 0331005 号厚生労働省医政局長厚生労働省医薬食品局長厚生労働省保険局長連名通知）の別添として示された「医療情報システムの安全管理に関するガイドライン」の第 5.1 版につきまして、「『医療情報システムの安全管理に関するガイドライン 第 5.1 版』の策定について」（日医発第 1104 号（情シ 53）令和 3 年 2 月 8 日）にてお知らせしたところでありますが、追加資料が策定・発出された旨の通知であります。

別添 2 は、サイバーセキュリティについて医療機関の注意を喚起するものであります。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、日本医師会では、令和 3 年 7 月 6 日「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関する注意喚起を行っております。昨今の状況を受けて、改めての周知でございます。使用不可改めて安全点検を行い、必要に応じて技術的安全対策等を実施するなどし、サイバーセキュリティ対策の強化を図るよう依頼がなされております。

本件につきまして、貴会におかれましてもご了知いただき、会員医療機関へご周知賜りますようお願い申し上げます。

【担当】坂井・西川・広野
大阪府医師会　総務課企画室
TEL:06-6763-7021

（情シ　42）
令和 3 年 10 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）

「医療情報システムの安全管理に関するガイドライン」に関する
追加資料（チェックリスト、フローチャート）について

平素より本会会務の運営に対しましてご高配を賜り深く感謝申し上げます。

さて今般、厚生労働省医政局研究開発振興課より、本会に対して標記に関する周知方依頼がありました。

本件は、平成 17 年 3 月 31 日「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」（医政発第 0331009 号薬食発第 0331020 号保発第 0331005 号厚生労働省医政局長厚生労働省医薬食品局長厚生労働省保険局長連名通知）の別添として示された「医療情報システムの安全管理に関するガイドライン」の第 5.1 版につきまして、「『医療情報システムの安全管理に関するガイドライン 第 5.1 版』の策定について」（日医発第 1104 号（情シ 53）令和 3 年 2 月 8 日）にてお知らせしたところでありますが、追加資料が策定・発出された旨の通知であります。

「医療機関のサイバーセキュリティ対策チェックリスト」

本チェックリストは、医療機関のサイバーセキュリティ対策の現状を把握することを目的に、そのチェック項目を整理したものであり、幅広くサイバーセキュリティ対策に対応した内容となっております。

チェックリストは、（1）経営層向けチェックリスト、（2）システム管理者向けチェックリスト、（3）医療従事者・一般のシステム利用者向けチェックリスト―の 3 種類から構成されており、医療機関のどの部分に弱みがあるのか把握し優先的に必要な対策を検討する一助となるものです。

「医療情報システム等の障害発生時の対応フローチャート」

本チャートは、医療機関がサイバーセキュリティの体制整備を行うにあたり、平時の備えや障害発生時に各担当者が行う対応について、フローチャートでまとめられております。体制整備や障害発生時の対応の確認を検討する一助となるものです。

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、貴会管下郡市区医師会及び会員への周知方につき、ご高配賜りますようよろしくお願い申し上げます。

なお、ガイドラインの PDF 形式並びに本追加資料の PDF 形式は下記厚生労働省ホームページにて公開されており、ホームページ内には、医療機関の個別状況に応じて加工可能なようにエクセル形式ファイルも掲載されております。

「医療情報システムの安全管理に関するガイドライン第 5.1 版（令和 3 年 1 月）」
https://www.mhlw.go.jp/stf/shingi/0000516275.html
「医療機関のサイバーセキュリティ対策チェックリスト」及び「医療情報システム等の障害発生時の対応フローチャート」の項目

以上

【(情シ 42) 添付書類／資料】

■「医療情報システムの安全管理に関するガイドライン」のチェックリスト、フローチャートの策定について（厚生労働省事務連絡／R3.10.20）
・「医療機関のサイバーセキュリティ対策チェックリスト」
・「医療情報システム等の障害発生時の対応フローチャート」

（情シ　４３）
令和３年11月２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）

医療機関を標的としたサイバー攻撃への対応について(注意喚起)

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、日本医師会では、令和３年７月６日「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)」(情シ 22 号)において、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関する注意喚起を行っております。昨今の状況を受けて改めて周知いたします。

各医療機関に置かれましては、「医療情報システムの安全管理に関するガイドライン　第5.1版」(https://www.mhlw.go.jp/stf/shingi/0000516275.html）の追加資料として発出されました、令和３年10月22日「『医療情報システムの安全管理に関するガイドライン』に関する追加資料（チェックリスト、フローチャート）について」（情シ42号）にてご案内いたしました、「医療機関のサイバーセキュリティ対策チェックリスト」「医療情報システム等の障害発生時の対応フローチャート」等をご活用いただき、自施設の対応状況をチェックいただければと考えます。

もし、サイバー攻撃(コンピュータウイルスの感染等)を受けた疑いがある場合は、被害の拡大を防ぐため、直ちに医療情報システムの保守会社等に連絡し、指示を仰いでください。
さらに、診療系情報システムの停止や個人情報の流出等の被害等が発生した場合は、
厚生労働省医政局研究開発振興課医療情報技術推進室　(03-3595-2430)
へご連絡いただきますようよろしくお願い致します。
また、一般的な情報セキュリティ（主にウイルスや不正アクセス）に関する技術的な相談に対してアドバイスを受けたい場合は、
情報処理推進機構(IPA) 情報セキュリティ安心相談窓口
電話　03-5978-7509（平日日中のみ）　メール　anshin@ipa.go.jp
等をご活用ください。

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。

以上