令和 3 年 12 月 3 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（ランサムウェア）への対応について
（再注意喚起）

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。

標記の件について、このたび別添の通り、日本医師会から通知がありました。

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、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。今回の事務連絡は、昨今の状況を受けて厚生労働省からの改めての周知依頼となります。

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。

今回の事務連絡の内容は以下の 4 点です。

１）リモート接続等に利用される、SSL-VPN 装置（特に FORTINET 社製）の脆弱性が悪用される事例が増えていくことから、機器を納品した事業者等への確認や機器の内容に更新がないか点検して早期に対応してください。

２）ランサムウェアを利用したサイバー攻撃により情報が失われる事案が発生していることから、「医療情報システムの安全管理に関するガイドライン第 5.1 版」の「7.2 章 見読性の確保について」（バックアップの作成、バックアップからの閲覧の確保）及び「7.3 章 保存性の確保について」（バックアップおよび履歴の保存）を参考に、バックアップを作成してください。

３）サイバー攻撃により医療情報システムに障害が発生した場合は、厚生労働省（下記連絡先）に連絡してください。

■厚生労働省 医政局研究開発振興課医療情報技術推進室 TEL:03-3595-2430 MAIL: igishitsu@mhlw.go.jp 標的型メールを受信した場合等は、情報処理推進機構（IPA）に相談してください。

■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

４）「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」を活用いただき、対策に役立ててください。
「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

本内容は、基本的に医療機関従事者ならびに医療機関と守秘義務契約を結んだベンダーのみに見せることができます。ホームページの一般に公開されている部分には掲載しないようお願いいたします。

【参考資料】
・令和 3 年 11 月 26 日付日医宛て厚生労働省医政局研究開発振興課名事務連絡
「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」
・別添：「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 抜粋」

また、必要に応じて、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)も参照ください。

＜ランサムウェア対策に参考となるサイトや資料＞
■IPA のランサムウェア対策特設ページ
https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html

■IPA ランサムウェアの脅威と対策～ランサムウェアによる被害を低減するために
https://www.ipa.go.jp/files/000057314.pdf
特に、6 ページ 1.5.ランサムウェアの感染経路
8 ページ 3.1.ランサムウェアに感染しないための対策
9 ページ 3.2.ランサムウェアの感染に備えた対策

■IPA 事業継続を脅かす 新たなランサムウェア攻撃について
～「人手によるランサムウェア攻撃」と「二重の脅迫」～
https://www.ipa.go.jp/files/000084974.pdf
特に、5. 対策

一般社団法人大阪府医師会総務課企画室
ＴＥＬ06-6763-7021 ＦＡＸ06-6764-0267