

事 務 連 絡
令和 3 年 11 月 26 日

各 $\left[\begin{array}{l} \text{各 都 道 府 県 衛 生 主 管 部 (局) 長} \\ \text{地 方 厚 生 (支) 局 医 事 課 長} \end{array} \right]$ 殿

厚生労働省医政局研究開発振興課
医療情報技術推進室

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
(再注意喚起)

近年、国内外の医療機関を標的とした、ランサムウェアを利用したサイバー攻撃による被害が増加していることから、令和 3 年 6 月 28 日付け「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)」(厚生労働省政策統括官付サイバーセキュリティ担当参事官室、厚生労働省医政局研究開発振興課医療情報技術推進室、厚生労働省医薬・生活衛生局医療機器審査管理課、厚生労働省医薬・生活衛生局医薬安全対策課事務連絡)をもって注意喚起するとともに、令和 3 年 10 月 20 日付け「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「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」について(厚生労働省医政局研究開発振興課事務連絡)をもって「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」の別添として、「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」を策定した旨通知いたしました。その後、医療機関に対するサイバー攻撃の事例が複数あり、医療機関の診療体制に大きな影響が出ているところ。

つきましては、再度、貴管内の市町村(特別区を含む。)、関係機関及び関係団体等に注意喚起いただきますよう、よろしくお願いいたします。

特に、医療機関において、下記の点に注意いただくよう併せて周知をお願い申し上げます。

なお、参考までに、NISC から提供された FORTINET 社製品の脆弱性情報及び同ガイドラインの抜粋を添付いたします。

記

1. リモート接続するために利用される、SSL-VPN 装置（特に FORTINET 社製）の脆弱性を悪用し、医療機関のネットワークに不正侵入し、ランサムウェアに感染させる事例が複数発生していることから、対応策として、ソフトウェア、機器等に脆弱性がないか点検し、脆弱性を発見した場合は早急に対処すること。
2. 最近、国内外の医療機関を標的とし、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、このような場合に備えて、「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「7.2 章 見読性の確保について」及び「7.3 章 保存性の確保について」を参考に、バックアップを作成すること。
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、「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 6.10 章 C. 最低限のガイドライン 5」を参照して所管省庁等に連絡すること。また、標的型メールを受信した場合等は、情報処理推進機構（IPA）に相談されたい。
なお、医療機関等がサイバー攻撃を受けた際の厚生労働省の連絡先は、次のとおりである。

(医療機関等がサイバー攻撃を受けた際の厚生労働省連絡先)
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
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、対策に役立てていただくこと。