2023 年 2 月 13 日

総務大臣　松本 剛明　殿
厚生労働大臣　加藤　勝信　殿

全国保険医団体連合会
会長　住江 憲勇

【要望書】政府・厚生労働省としてセキュリティ対策の強化を求める

前略　国民医療の確保に関するご尽力に敬意を表します。

さて、昨今、複数の病院・診療所で電子カルテ等のシステムがランサムウェアに感染し、診療に大きな影響が発生しました。

医療機関のサイバーセキュリティは、内閣サイバーセキュリティセンター(NISC)が指定する重要インフラに位置付けられ、一般的なセキュリティ以上の対策が求められています。

2022 年４月診療報酬改定では、診療録管理体制加算の施設基準において、許可病床数 400 床以上の病院に専任の医療情報システム安全管理責任者の配置と職員研修等を義務付けましたが、診療報酬上の加算評価はありません。

このような中で、全国保険医団体連合会では医療 ISAC が実施する「FortiNet 社製 VPN 装置の導入実態に関する緊急調査」に協力し、協会・医会の会員 897 医療機関（病院 264、医科診療所 427、歯科診療所 206）から回答頂きました。

（https://hodanren.doc-net.or.jp/info/investigation/230120_scr_svy/）

院内システムにリモートメンテナンス環境を導入している医療機関は全体の７割に達していますが、院内でどのようなリモートメンテナンス機器が利用されているかについて正確に把握している医療機関はそのうち３割程度であることが判明した。

昨年 10 月に深刻な脆弱性の報告のあった Fortinet 社製品か否かを問わず、リモートメンテナンス用機器には外部からの悪意あるアクセスを可能にしかねない脆弱性が継続的に発生していることから、適時の対応が求められます。

また、ベンダーとセキュリティ対応を含めた契約上の役割・責任を定めた契約を取り交わしている医療機関は全体の１割強にとどまりました。医療機関はベンダーとの間で明確なセキュリティも含めた契約関係を合意し、協力を仰げる態勢を整備することが重要です。

また、医療機関が安全管理措置を講じるためのサポート役として、医療機関と同じ目線に立ち、ベンダーが医療セキュリティの改善に向けたリスクコミュニケーションの工夫を凝らすとともに、医療機関側のセキュリティリテラシーの向上も重要課題の一つです。

現在の診療報酬はこうしたセキュリティ対策に必要な費用を全く評価していませんが、そもそもこうしたセキュリティ対策は患者負担を伴う診療報酬で評価すべきではなく、公的資金を投入して実施すべきです。

医療機関は、国民の命と健康を守る砦です。またサイバー攻撃は、病床の大きさや医療機関の種別を選ぶとは限らず、医科・歯科ともセキュリティ対策の強化が必要です。

国におかれては、セキュリティ対策の重要性に鑑み、公的補助金を創設し、診療の継続性・安全性を担保していただけますよう、強く要望いたします。

記

一. 政府・厚生労働省として、セキュリティ対策の一層の強化を図ること。
一. 政府・厚生労働省は、公的・民間を問わず全ての医療機関等がサイバーセキュリティ対策を講じられるよう、公的補助金を創設すること。
一. 医療機関等のサイバーセキュリティ対策を担う会社の質が確保できるよう、行政として必要な対策を行うこと。
一. サイバーセキュリティについて厚生労働省で進めている「情報システムの安全管理に関するガイドライン」（第６版）については、わかりやすく表現し、医療現場の対応が進みやすくなるよう改善すること。
一. サイバー攻撃を受け、電子カルテや診療報酬請求システム等が損害を受けた場合は、概算請求を認めること。また、データ提出加算を含めた施設基準要件についても特例的な対応を行い、要件を満たすものとすること。