医第 3382 号
令和４年 12 月 27 日

各関係団体会長　殿

神奈川県健康医療局保健医療部医療課長
（公　　印　　省　　略）

医療機関における年末年始の情報セキュリティに関する注意喚起（依頼）

本県の保健医療行政の推進につきましては、日頃からご理解、ご協力をいただきお礼申し上げます。

標記のことについて、令和４年 12 月 21 日付けで、厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室から事務連絡がありました。

つきましては、貴会会員に周知くださいますようお願いします。

問合せ先
法人指導グループ　田邉
電　話　(045)210-1111　内線 4870

事　務　連　絡
令和４年 12 月 21 日

各 (都道府県 / 保健所設置市 / 特別区) 衛生主管部（局）　御中

厚生労働省医政局
特定医薬品開発支援・医療情報担当参事官室

医療機関における年末年始の情報セキュリティに関する注意喚起

日頃より医療分野の情報化に関し、格別のご配慮を賜り、厚く御礼申し上げます。

年末年始の長期休暇の時期は、システム管理者が長期間不在になる等、普段の業務体制とは異なる状況になりやすく、情報セキュリティ対策について特別の注意が必要となります。

昨今、医療機関へのサイバー攻撃が増加しており、医療提供体制への影響も生じた事案が確認されております。厚生労働省では、医療情報システムの安全管理に関するガイドラインや関連する通知に基づいた対応を求めており、また同様のサイバー攻撃が他の医療機関にも行われる恐れがあることから、その対策の共有等のため、医療機関がサイバー攻撃を受けた等の場合には厚生労働省に連絡するよう求めております。

そこで、平成 29 年度より医療機関からのサイバーセキュリティインシデントに関する厚生労働省への緊急連絡先を設けております。つきましては、別紙のとおり、管内の医療機関に周知願います。

なお、本内容は医療セプターを通じて日本医師会等の医療団体から地方支部にも周知するよう並行して連絡しております。

医療団体等には周知されますが、その他医療機関宛ての連絡方法がありましたら周知頂くようお願いいたします。

別　紙

○　近年、国内外の医療機関を標的とした、ランサムウェアを使用したサイバー攻撃による被害が増加しております。今般の大阪急性期・総合医療センターで発生した事案を踏まえると、ランサムウェアの侵入口が取引先のシステムであった可能性が高いことから、令和４年 11 月 10 付事務連絡「医療機関におけるサイバーセキュリティ対策の強化について（注意喚起）」を参考にして、医療機関自身のシステムにおけるサイバーセキュリティ対策に加え、サプライチェーンとの接続状況や、取引先システムのサイバーセキュリティ対策をも俯瞰しつつ、必要な対策を講じていただきますようお願いいたします。

　また、これらのランサムウェアによるサイバー攻撃は、共通して、医療機関と外部機関（主にベンダーや取引事業者等）を接続する通信機器とそのソフトウェア（以下「リモートゲートウェイ装置」という。）の脆弱性を通じて行われていることが指摘されています。特に、Fortinet 社製の SSL-VPN 装置については、その脆弱性を悪用し、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確認されており、令和４年 12 月 16 日付事務連絡「FortiOS に関する脆弱性情報への対応について（注意喚起）」を発出しておりますので、速やかにご対応をお願いします。

　なお、内閣サイバーセキュリティセンター（NISC）からも「年末年始休暇等に伴うセキュリティ上の留意点について（注意喚起）」（令和４年 12 月 20 日付内閣官房内閣サイバーセキュリティセンター）が発出されておりますので、参考にしていただくようお願いいたします。

○　独立行政法人 情報処理推進機構（IPA）は「年末年始における情報セキュリティに関する注意喚起」として、年末年始の長期休暇期間における情報セキュリティ対策を発表しています。重要インフラ事業者各位においても、年末年始における対策を実施して頂きたく情報提供いたします。

年末年始における情報セキュリティに関する注意喚起－IPA セキュリティセンター
https://www.ipa.go.jp/security/topics/alert20221213.html

　長期休暇の時期は、「システム管理者が長期間不在になる」等、いつもとは違う状況になりやすく、不正ソフトウェアや不正アクセス等の被害が発生した場合に対処が遅れてしまうなど、場合によっては組織を越えて被害が及ぶ可能性があります。このような事態とならないよう、上記リンク先を参考にして、長期休暇前の対策として、「緊急連絡体制の確認」、「院内ネットワークへの機器接続ルールの確認と遵守」、長期休暇明けの対策として「不審なメールに注意」等を実施していただきますようお願いいたします。

○　サイバー攻撃を受けた疑いがある場合

- 保守会社等へ直ちに連絡
  ・保守会社等へ直ちに連絡し、指示に従って必要な対策を講じてください。
- 厚生労働省へ連絡
  ・サイバー攻撃においては、攻撃者は不正アクセスを行った組織から別の組織へ、又は同種の攻撃を別の組織に行い、感染を拡大させていきます。こうした被害の拡大を防ぐための情報共有はサイバーセキュリティ対策では重要です。
  サイバー攻撃を受けた疑いがある場合には、下記の厚生労働省の連絡先に御連絡ください。※なお、いたずら防止のため、184 発信、公衆電話発信は受信不可としますので、医療機関の電話で御連絡願います。

【連絡先】厚生労働省医政局厚生労働省医政局
特定医薬品開発支援・医療情報担当参事官室
０８０－２０７３－０７６８

○　（参考）医療機関等におけるサイバーセキュリティ対策の強化について

過去の通知ファイルについて以下の URL で公表しています。
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

（参考）テレワークを行う際のセキュリティ上の注意事項
https://www.ipa.go.jp/security/announce/telework.html

（参考）Web 会議サービスを使用する際のセキュリティ上の注意事項
https://www.ipa.go.jp/security/announce/webmeeting.html