日医発第803号（情シ）
令和6年8月2日

都道府県医師会　担当理事　殿

公益社団法人　日本医師会
常任理事　長島　公之
（公印省略）

医療機関等におけるサイバーセキュリティ対策の取組みについて（周知依頼）

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。

医療機関等のサイバーセキュリティ対策については、日医発第361号（情シ）『令和6年度版「医療機関におけるサイバーセキュリティ対策チェックリスト」及び「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」について』（令和6年5月17日）にて、医療法に基づく立入検査への対応として、対策に取り組んでいただいているかと存じます。

一方、令和6年5月に岡山県精神科医療センターで発生したサイバー攻撃事案において、電子カルテの閲覧・利用ができなくなる等により、一部診療に影響が生じるとともに、個人情報の流出も確認されています。

こうした状況を踏まえて、厚生労働省では、チェックリストの中でも特に迅速に対応いただきたい事項を「サイバー攻撃リスク低減のための最低限の措置」としてとりまとめたとして、本会宛に周知依頼がありました。

内容としては、最低限取り組んでいただきたい事項として、

○パスワードを強固なものに変更し、使い回しをしない

○IoT機器を含む情報資産の通信制御を確認する

○ネットワーク機器の脆弱性に、ファームウェア等の更新を迅速に適用する

を呼びかけるものとなっております。

なお、日本医師会サイバーセキュリティ支援制度では、同チェックリストに対応するため、「日本医師会セキュリティガイドライン相談窓口」を設けております。本件やチェックリストにご対応いただく中で、不明点等がございましたら、是非ご活用ください。

【日本医師会セキュリティガイドライン相談窓口】
TEL：0120-339-199 平日 9 時～18 時（土日、祝日、年末年始は休業）
※詳細は日本医師会メンバーズルーム内専用ページをご確認ください。
https://www.med.or.jp/japanese/members/info/cyber_shien.html

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、ご高配を賜りますようお願い申し上げます。

【別添資料】
・【事務連絡】医療機関等におけるサイバーセキュリティ対策の取組みについて（周知依頼）

以上

事　務　連　絡
令和６年８月１日

公益社団法人 日本医師会 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
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

医療機関等におけるサイバーセキュリティ対策の取組みについて（周知依頼）

日頃から厚生労働行政に対して御協力を賜り、厚く御礼申し上げます。

医療機関等のサイバーセキュリティ対策については、「令和６年度版「医療機関におけるサイバーセキュリティ対策チェックリスト」及び「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」について」（令和６年５月 13 日医政参発 0513 第６号。以下「チェックリスト等」という。）等をお示し、各医療機関等において対策に取り組んでいただいているところです。

他方、令和６年５月 19 日に岡山県精神科医療センターで発生したサイバー攻撃事案において、電子カルテの閲覧・利用ができなくなる等により、一部診療に影響が生じました。また、今回の事案においては個人情報の流出も確認されています。医療機関等を対象とするサイバー攻撃は後を絶たず、その脅威は日増しに高まっています。

こうした状況を踏まえて、立入検査に用いられるチェックリスト等の内容を含んだ、特に迅速に対応いただきたい事項を「サイバー攻撃リスク低減のための最低限の措置」として（別添）のとおりまとめました。貴団体におかれましては、内容について御了知の上、管内及び管下の医療機関等に対して周知徹底を図るとともに、その運用に遺漏なきようお願いいたします。

■医療機関等がサイバー攻撃を受けた場合等の厚生労働省連絡先
医政局特定医薬品開発支援・医療情報担当参事官室
TEL ： 03-6812-7837
MAIL: igishitsu×mhlw.go.jp
※迷惑メール防止のため、メールアドレスの一部を変えています。
「×」を「@」に置き換えてください。
URL： https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

別添

【サイバー攻撃リスク低減のための最低限の措置】

○パスワードを強固なものに変更し、使い回しをしない

VPN 装置等の ID・パスワードの漏洩は、システムへの侵入に直結し、医療機関等にとって重大なリスクとなります。実際にこれまで攻撃を受けた医療機関では、パスワードが容易に推測可能なものであったり、4 桁と短かった例が確認されています。被害を未然に防ぐためには、強固な ID・パスワード設定の徹底が必要です。

また、複数の機器や外部サービス等で、同一のパスワードを設定しないことも重要です。パスワードの使い回しは漏えいリスクを高め、一度の漏えいにより被害範囲が拡大しうるため、非常に危険です。

〈危険な ID/パスワードの例〉

- Administrator（工場出荷時の設定等）
- 12345678（単純な羅列）
- pa$$w0rd、i234567&9（単純な置換、流出済）
- qwerty、7410（キーボードの配列）
- KoroHospital、KoroTaro(予測可能、施設の名称、代表者名など)

〈強固なパスワードとは〉

長く、複雑で、推測困難なものが推奨されます。

-13 桁以上（桁数が多いほど、機械的な総当たりでの解析が困難）

-英数字、大文字・小文字、記号が混在（組み合わせが多いほど解析が困難）

-ランダムな文字列（単語等の組み合わせによる解析を回避）

○IoT 機器を含む情報資産の通信制御を確認する

医療機関等のネットワークについて、通信網を正確に把握し、適切に対策が講じられているか、確認が必要です。

ネットワークが閉域網と認識されている場合においても、医療機関等が把握できていない VPN 装置等の外部接続点が設置されている場合があるため、関係事業者と協力してネットワーク接続点を確認し、アクセス制御等が適切に実施されているかを確認してください。

また、各種システムや通信制御を行っている機器のログが適切に保存され、運用されていることを確認してください。

〇ネットワーク機器の脆弱性に、ファームウェア等の更新を迅速に適用する

サイバー攻撃の被害を受けた医療機関では、ネットワーク機器のバージョンアップやパッチ適用、ファームウェアアップデートが適切に行われていない事例が多く確認されています。更新作業を実施するまでの間、サイバー攻撃の標的となる可能性があり、対象機器に深刻な脆弱性がある場合には、システムへの侵入等に悪用されるおそれがあります。

適切な頻度で脆弱性情報の確認及び更新（あるいはメーカより示されているリスク低減措置）が行われているか、事業者と連携して今一度確認をお願いします。

併せて、セキュリティ対策ソフトの稼働状況（最新の定義ファイルが適用されるようになっているか等）についても確認してください。

（参考）

■医療機関に対するサイバーセキュリティ対策リーフレット（令和５年 10 月）

URL：https://www.mhlw.go.jp/content/10808000/001180153.pdf

■医療機関におけるサイバーセキュリティ対策チェックリスト（令和６年５月）

URL：https://www.mhlw.go.jp/content/10808000/001253950.pdf

■薬局におけるサイバーセキュリティ対策チェックリスト（令和６年５月）

URL：https://www.mhlw.go.jp/content/10808000/001253958.pdf

■医療情報システムの安全管理に関するガイドライン　第 6.0 版（令和５年５月）

URL：https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html