日医発第 1609 号（情シ）
令 和 4 年 11 月 16 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強化について（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。
サイバー攻撃による被害は増加し、直近では、医療機関を標的としたランサムウェア攻撃により、地域の医療提供体制に影響を及ぼすケースも発生しております。

ランサムウェアへの対応におきましては、日本医師会としてもこの事態を深刻に受け止め、2022 年 11 月 2 日に日本医師会 CEPTOAR 通信（FAX 版）を発出いたしました。今般、厚生労働省では、添付のとおり医政局並びにサイバーセキュリティ担当参事官室との連名で、各都道府県衛生主管部（局）宛に注意喚起が行われました。
内容としては、昨今の被害を受けて、「関係事業者とのネットワーク接続点の確認」「リスク低減のための措置」「インシデントの早期検知」「インシデント発生時の適切な対処・回復」「金銭の支払いに対する対応」などの注意喚起が行われております。

日本医師会では、サイバーセキュリティに関連する日常の些細なものから今回のランサムウェアへの感染トラブルまで幅広く相談できる相談窓口（年中無休・受付時間：9 時～21 時）を設置し本年 6 月から稼働しております。

日本医師会サイバーセキュリティ支援制度　対応相談窓口
TEL：0120-179-066　年中無休　9 時～21 時
A①会員のいる医療機関であれば、勤務医の方、事務員も相談可能です。
医師会も利用可能です。

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】
・令和 4 年 11 月 10 日付都道府県衛生主管部(局)宛て文書「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（注意喚起）」
同文書が参照している、令和 3 年 6 月 28 日付事務連絡「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（注意喚起）」については、令和 3 年 7 月 6 日（情シ 22 号）「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（注意喚起）」を参照ください。
・2022 年 11 月 2 日発行、日本医師会 CEPTOAR 通信　FAX 版

写

事　務　連　絡
令和４年 11 月 10 日

各都道府県衛生主管部（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
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強化について（注意喚起）

今般、大阪急性期・総合医療センター（以下「センター」という。）において、ランサムウェアによるサイバー攻撃事案が発生し、電子カルテの閲覧・利用ができなくなる等により、地域の医療提供体制に影響が出ているところです。医療機関を攻撃対象とする同種攻撃は近年増加傾向にあり、その脅威は日増しに高まっています。

厚生労働省では、センターに専門家チームを派遣して、原因の調査と復旧支援を行っていますが、攻撃の侵入経路は、医療機関自身のシステムではなく、院外の調理を委託していた事業者のシステムを経由したものである可能性が高いことが判っています。

医療機関においては、保有する医療情報の安全を確保するため、「医療情報システムの安全管理に関するガイドライン」（以下「ガイドライン」という。）等に基づき、必要な対策を講じていただいているところですが、今般のセンターにおける事案も踏まえると、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等をも俯瞰しつつ、必要な対策を講じていくことが求められています。

こうした状況を踏まえ、管内、管下の医療機関に対し、同種のサイバー攻撃に備え、令和３年６月 28 日付事務連絡「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（注意喚起）」（参考）に加え、下記の対策が適切に講じられているか確認を要請するとともに、万が一、サイバー攻撃を受けた場合にも事業継続計画等により地域住民への医療提供体制に支障が出来ることのないよう注意喚起をお願いします。

また、内閣サイバーセキュリティセンターにおいて、ランサムウェア対策に関する特設サイトを作成しているので、必要に応じてご活用下さい。

記

１　サプライチェーンリスク全体の確認

上記の通り、自組織のみならずサプライチェーン全体を俯瞰し、発生が予見されるリスクを医療機関等自身でコントロールできるようにする必要があることから、関係事業者のセキュリティ管理体制を確認した上で、関係事業者とのネットワーク接続点（特にインターネットとの接続点）をすべて管理下におき、脆弱性対策を実施する。

２　リスク低減のための措置

〇パスワードを複雑なものに変更し、使い回しをしない。不要なアカウントを削除しアクセス権限を確認する。多要素認証を利用し本人認証を強化する。

〇IoT 機器を含む情報資産の保有状況を把握する。

〇VPN 装置を含むインターネットとの接続を制御するゲートウェイ装置の脆弱性は、攻撃に悪用される可能性があるので、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。

〇悪用が既に報告されている脆弱性については、ログの確認やパスワードの変更など、開発元が推奨する対策が全て行われていることを確認する。

〇VPN 機器に対する管理インターフェースのインターネット上の適切なアクセス制限を実施する。

〇メールの添付ファイルを不用意に開かない、URL を不用意にクリックしないこと。不審メールは、連絡・相談を迅速に行い組織内に周知する。

３　インシデントの早期検知

〇サーバ等における各種ログを確認する。(例:大量のログイン失敗の形跡の有無)

〇通信の監視・分析やアクセスコントロールを再点検する。(例：不審なサイトへのアクセスの有無)

４　インシデント発生時の適切な対処・回復

〇サイバー攻撃を受け、システムに重大な障害が発生したことを想定した事業継続計画が策定する。

〇データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。

〇インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、外部関係機関への連絡体制や組織内連絡体制等を準備する。

〇インシデント発生時及びそのおそれがある場合には、速やかに厚生労働省等の関係機関に対し連絡する。

５　金銭の支払いに対する対応

厚生労働省としては、サイバー攻撃をしてきた者の要求に応じて金銭を支払うこ

とは、犯罪組織に対して支援を行うことと同義と認識しており、以下の観点により金銭の支払いは厳に慎むべきである。

〇金銭を支払ったからと言って、不正に抜き取られたデータの公開や販売を止めることができたり、暗号化されたデータが必ず復元されたりする保証がないこと。

〇一度、金銭を支払うと、再度、別の攻撃を受け、支払い要求を受ける可能性が増えること。

６　ランサムウェア特設ページ

https://security-portal.nisc.go.jp/stopransomware/

■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。

都道府県医師会・郡市区等医師会御中

発行：公益社団法人日本医師会
発行日：2022 年 11 月 2 日号

日本医師会 CEPTOAR 通信 FAX 版

サイバーセキュリティに関する情報を速報します。必要なものを掲載していますのでぜひお読みください。

ランサムウエアに関する注意喚起

昨今、報道でもあるとおり医療機関でのランサムウエアによる被害が発生しています。

ランサムウエアに感染するとパソコン等に保存されているデータが暗号化され使用できない状態にされてしまいます。その上で、情報漏洩の脅迫やデータを戻す対価として金銭が要求されます。医療機関の対策をご確認ください。

■ 対策

「インターネットにつながる機器の対応」

インターネットに接続している機器（VPN 装置、ルーター）の脆弱性を悪用して侵入するケースもあります。機器にセキュリティ等の更新がないかメーカーの Web ページなどで情報を得るかもしくは、機器を納品した事業者に点検を依頼しましょう。

「電子メールへの基本的な対応」

外部とやり取りする電子メールが侵入の入り口になることもあります。下記を心がけてください。

◆身に覚えのないメールの添付ファイルは開かない。URL をクリックしない。

◆自分が送信したメールに対する返信に見えても、不審な場合は添付ファイルを開かない

◆信頼できるメール以外では添付ファイルを開いても、「マクロを有効化する」や「コンテンツの有効化」ボタンはクリックしない

◆職場 PC で不自然なメールの添付ファイルや URL を開いた場合は、すぐにシステム管理部門などに連絡する

「ID パスワードの管理をしっかり行う」

パスワードをモニター横などに貼り付けたりせず、他者がログインできないように注意する。

・他には「パソコンの OS およびソフトウェアを常に最新の状態に保つ」「セキュリティソフトを導入し、常に最新の状態に保つ」等の日頃の心がけも必要です。

■ 感染に備えた 321 ルールのバックアップ

ランサム被害からの復旧にはバックアップからの復元も大切になります。

バックアップデータを 3 個作成したうえで、外付けハードディスクやブルーレイディスクなど 2 種類の媒体に保存。もう 1 つは利用しているネットワークからはアクセスできない場所への保管「クラウドサービス利用」「バックアップ取得時以外はオフラインで保管」「別のネットワークや場所に保管」など対策を検討しましょう。

また、バックアップデータから実際に復旧できることを確認しておくことも重要です。

■ 日本医師会サイバーセキュリティ支援制度 対応相談窓口

サイバーセキュリティに関連する日常の些細なものから今回のランサムウエアへの感染トラブルまで幅広く相談できる相談窓口(年中無休・受付時間：9 時～21 時)。無料で何度でも利用が可能です。

対応相談窓口（緊急相談窓口）

TEL：0120-179-066　年中無休　9 時～21 時

A①会員のいる医療機関であれば、勤務医の方、事務員も相談可能です。医師会も可能です。

もし、医療機関がサイバー攻撃（コンピュータウイルス感染等）を受けた疑いがある場合は、直ちに医療情報システムの保守会社等に連絡し指示を仰いでください。わからない場合は日本医師会対応相談窓口(0120-179-066)をご活用ください。さらに、診療系情報システムの停止や個人情報の流出等の被害等が発生した場合は、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(03-6812-7837)へ連絡をお願い致します。

問い合わせ窓口　情報システム課　josys@po.med.or.jp