日医発第 1192 号（情シ）
令 和 6 年 10 月 8 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）

セプター通信（CEPTOAR 通信）の発出について（ランサム詐欺 FAX）

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。

日本におけるサイバーセキュリティ対策として、重要インフラ「情報通信」「金融」「航空」等分野の内の１つに「医療」があります。その中で、日本医師会は医療セプター（CEPTOAR:情報共有組織）事務局を務めております。

先般の医療機関へのサイバー攻撃被害を受け、日本医師会では、対策をより強化するため、医療機関に見てほしいセキュリティ情報をセプター通信（CEPTOAR 通信）として、FAX および「日医君」だよりにて都道府県、郡市区医師会にお送りしております。

各医師会からデジタルデータを求める声もいただいていることから、従来の周知に加え、発出文書としてお送りすることといたしました。

今回の内容は、
最近、医療機関宛てにランサムウェアに感染したとの偽の FAX を送り、
身代金を取ろうとする詐欺が発生していることへの注意喚起
になります。

今までの周知情報につきましては、
日医ホームページ　メンバーズルーム
サイバーセキュリティ・医療セプターについて
https://www.med.or.jp/japanese/members/info/ceptoar/
をご覧ください。

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。

以上

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：2024年10月8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いたします。必要なものを掲載してますのでぜひお読みください。

医療機関に送信される ランサム攻撃を装う詐欺ＦＡＸへの注意喚起

※本注意喚起(特に添付の脅迫文)については、公開情報ではないため、会員等関係者限りとして周知をお願いいたします。

令和６年９月 30 日より、医療機関の FAX 宛に、ランサムウェアの感染による金銭の支払いを命じる旨の文書が届いていると複数の医療機関より厚生労働省へ報告が寄せられています。

FAX にはランサムウェアに感染させた旨の記載がありますが、現時点では実際に攻撃を受けたという報告は受けておりません。

医療機関で同文書を受け取った場合には、金銭の支払い等、文書の命令に安易に応じることなく、施設のネットワーク環境、医療情報システムを調査頂き、次の警察、厚生労働省等にご報告・ご相談頂くようお願い申し上げます。

（参考）医療機関に届いた脅迫文（２例）

■脅迫文１

First of all, we have infected all your computers, all your electronic devices with ransomware.

We have all the information in our possession and have hidden some of the logs.

We have manipulated, destroyed, and rendered inoperable your devices.

We are also capable of leaking other information.

～省略～

We control the lives of our patients, the business life of our hospitals, the careers of our doctors, and even confidential information.

We do not want to harm even a finger to our friendly friends who are willing to pay us.

But anyone who doesn't pay is our enemy. We will show no mercy.

In the unlikely event that we do not receive a deposit from you, we will not be held responsible.

■警察へ連絡：最寄りの警察署又は都道府県警察本部のサイバー犯罪相談窓口
https://www.npa.go.jp/bureau/cyber/soudan.html

■都道府県へ連絡:最寄りの道府県所管部局(医療政策課等)

■厚生労働省へ連絡：医政局特定医薬品開発支援・医療情報担当参事官室
MAIL:　igishitsu@mhlw.go.jp

※身代金の支払いに対する考え方について

サイバー攻撃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して、厚生労働省は次の観点からも金銭の支払いは厳に慎むべきしております。

〇金銭を支払ったからと言って、データの公開や販売を止めたり、データが必ず復元される保証がないこと。

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。

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。

本内容は、医療機関従事者ならびに医療機関と守秘義務契約を結んだベンダーのみに見せることができます。ホームページなど、一般の方への公開はご遠慮ください。

問い合わせ窓口　情報システム課　josys@po.med.or.jp

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いたします。必要なものを掲載してますのでぜひお読みください。

■脅迫文２

We have successfully used ransomware to obtain your personnel information, patient information, and other documents with your business partners.

We are trying to shut you out of business, but your computer can be encrypted and rendered unusable at any time.

No correspondence is required. We are not going to argue with you guys.

We are just waiting for a great choice from you.

We will not take payment as a declaration of war. We will give you time to discuss. Patient lives and money, employees and money, facilities and money. Think about what is important to you.

If you send 0.5 BTC to the BTC address below within a week, I will stop releasing your information and you will stop destroying medical equipment.

I await your excellent choice!

We have successfully used ransomware to obtain your personnel information, patient information, and other documents with your business partners.

We are trying to shut you out of business, but your computer can be encrypted and rendered unusable at any time.

No correspondence is required. We are not going to argue with you guys.

We are just waiting for a great choice from you.

We will not take payment as a declaration of war. We will give you time to discuss. Patient lives and money, employees and money, facilities and money. Think about what is important to you.

If you send 0.5 BTC to the BTC address below within a week, I will stop releasing your information and you will stop destroying medical equipment.

I await your excellent choice!

■対応のご相談には、

日本医師会サイバーセキュリティ対応相談窓口も併せてご活用ください。

年中無休　6 時～21 時
TEL：0120-179-066

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。

本内容は、医療機関従事者ならびに医療機関と守秘義務契約を結んだベンダーのみに見せることができます。ホームページなど、一般の方への公開はご遠慮ください。

問い合わせ窓口　情報システム課　josys@po.med.or.jp