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：2021年12月1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。

1．ランサムウエアに関する注意喚起

報道されております通り、医療機関にてランサムウエアによる被害が発生しております。

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搾取され、暗号化して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。

■ランサムウエアの侵入経路

・インターネットに接続している機器（VPN装置、ルーター）の対策されていない脆弱性を悪用した侵入

・院内のパソコンに不正なメールを送り付けて、ウイルス感染させて端末を遠隔操作する

・ウェブサイトに掲載されている広告から、正規のサイトによく似た偽サイトへ誘導しプログラムをダウンロードさせて感染させる

■対策

・「VPN機器の点検」機器を納品した事業者等に設定の確認を依頼する。もしくは、機器の内容に更新がないかメーカーのWebページなどで情報を得ましょう。

・「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張り付けたりせず、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。

■ランサムウエアの感染に備えた対策

機器の故障に備えた定常的なバックアップに加えて、外付けハードディスクやブルーレイディスクなどの外部媒体に定期的なバックアップを行うなど複数の保存を用意する。

[参考]IPA ランサムウエア対策特設ページ
https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html

[参考]IPA ランサムウエアの脅威と対策～ランサムウエアによる被害を低減するために
https://www.ipa.go.jp/files/000057314.pdf

[参考]IPA 事業継続を脅かす 新たなランサムウエア攻撃について～「人手によるランサムウエア攻撃」と「二重の脅迫」～
https://www.ipa.go.jp/files/000084974.pdf

2．Emotetの活動再開の注意喚起

2021年1月末に活動が収束したとみられていたマルウエアEmotetについて、11月中旬に活動再開し、国内でも不審メールが確認された

もし、医療機関がサイバー攻撃（コンピュータウイルスの感染等）を受けた疑いがある場合は、直ちにご利用の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。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　医政局研究開発振興課医療情報技術推進室(03-3595-2430)へご連絡いただきますよう、よろしくお願い致します。

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：2021年12月1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。

とのことです。

Emotetに感染するとパソコン内の電子メール情報が搾取され、以前にメールでやり取りした相手に対し、過去のメール本文にウイルス付きファイルを添付した形のメールが送信され、被害が拡大していきます。

さらに、ランサムウエアをはじめとした他のマルウエアの被害に繋がる可能性もあります。

■対策

「1．ランサムウエアに関する注意喚起」で記載してます「電子メールへの基本的な対応」を心がけてください。

[参考]IPA「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメール
https://www.ipa.go.jp/security/announce/20191202.html

また、感染が疑われる場合には、JPCERT/CCが公開している検査プログラムをご利用ください。対処法も掲載されております。

[参考]JPCERT/CCマルウエアEmotetへの対応
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

3．ホームページCMSシステムの脆弱性に対する注意喚起

ホームページの更新を便利に行うコンテンツ管理システム(CMS)である「Movable Type」「Power CMS」等につきまして、深刻な脆弱性が発見されました。本脆弱性を悪用した攻撃が確認されています。

本攻撃を受けて侵入されると、不審ファイルの設置や情報窃取、悪意のあるサイトへの転送、ホームページ機能の停止が行われる可能性があります。

各メーカーより修正プログラムが出ておりますので、アップデート等対策をご検討ください。

アップデートを適用できない場合には、設定ファイルの書き換え等の回避策にて、本脆弱性の影響を軽減することが可能とのことですので、下記リンクをご参照ください。

[参考]IPA更新：「Movable Type」のXMLRPC APIにおけるOSコマンド・インジェクションの脆弱性について（JVN#41119755）
https://www.ipa.go.jp/security/ciadr/vul/20211020-jvn.html

＜本通信について＞

医療は、日本を支える重要インフラ（全14分野）の一つとして位置づけられており、各分野にはサイバーセキュリティ情報の共有、連絡を行うための機能として、セプターの事務局が置かれております。日本医師会は、2018年3月に医療セプター事務局の業務を厚生労働省から引き継ぎ、内閣サイバーセキュリティセンター（NISC）や厚生労働省からもたらされる関連情報を、医療機関に提供しております。

随時提供される情報を下記ホームページに掲載するとともに、速報性が高いものについては、「日医君」だよりや本FAXを用いて会員の皆様にお知らせいたしますので、是非ご一読ください。

過去の情報につきましては、随時こちらに掲載しております。併せてご活用ください。

日本医師会ホームページ医療セプターについて
https://www1.med.or.jp/japanese/members/info/ceptoar.html

もし、医療機関がサイバー攻撃（コンピュータウイルスの感染等）を受けた疑いがある場合は、直ちにご利用の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。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　医政局研究開発振興課医療情報技術推進室(03-3595-2430)へご連絡いただきますよう、よろしくお願い致します。