文書の種類	連絡書	文書レベル	－
決裁	運営会議	通知範囲	全施設
有効期限	2023.6.30	照会先	コンプライアンス推進室

人事・第 2023-22 号

2023 年 6 月 7 日

事務長 各位

総務責任者 各位

ＴＭＧ本部　コンプライアンス推進室

マルウェア等への対応・対策研修実施について（連絡）

標記について、グループ病院におけるマルウェア感染疑いの事故発生を受け、マルウェア等への対応・対策について下記の通り研修を実施していただきますようお願いいたします。

記

1. 事故概要：研修資料「マルウェア等への対応・対策」をご確認ください。
2. 研修対象：全職員（非常勤を含む）
3. 研修方法：下記の通り。
   1）部署単位での回覧
      (1) 各所属長に研修資料を配布（研修資料 1～3）
      (2) 各部署にて回覧
      (3) 職員は各自で研修資料を熟読の上、閲覧後に押印やサイン
      (4) 所属長が全員の閲覧・押印等を確認
   2）注意喚起ポスターの掲示（研修資料 2）
      今回の事象に関する注意喚起ポスターを作成しておりますので、必要に応じて、職員から見えるところに掲示してください。
4. 研修期間等：2023 年 6 月 30 日までに全員が閲覧および押印等を完了させ、GoogleForm から施設単位で完了報告を行ってください。（回答 URL はメールにて配信）
5. 研修資料：下記の通り。
   資料 1)「マルウェア等への対応・対策」
      マルウェア等への一般的な対応・対策についてまとめた資料です。今回の事故概要に関する記載を含みます。
   資料 2)「偽警告にご注意ください」
      偽警告に関する注意喚起ポスターです。
   資料 3)「偽警告とは」
      偽警告の特徴や対応方法を記した資料です。
6. 担当：TMG 本部　コンプライアンス推進室　大橋

以上

事故防止研修資料：マルウェアへの対応・対策

◆実際にあった事例◆

ニュースサイトの閲覧中に「トロイの木馬に感染しました」という画面になり、大音量でアラームが鳴り響いた。ブラウザの×ボタンを押しても消すことができなかった為、電源ボタンを押しＰＣを強制終了させ、再度ＰＣを起動したがアラームが鳴りやまず、「トロイの木馬に感染したため画面上の番号に電話」するよう警告音で指示された。

携帯でその番号に電話をかけ、マイクロソフト職員を名乗る電話相手の指示に従っていると、リモートコントロールを許可してしまいそのままましばらく画面を操作された。最終的に「セキュリティの為」と称し金銭を要求されたが、その段階で総務課へ報告し、総務課担当者からＰＣを触らないよう指示。その後、本当にウイルスに感染していないか調査を行った。

本事例では「トロイの木馬」という有名なプログラムの名前が出されたものの、調査の結果、実際には感染していませんでした。

つまりこれは「偽警告（フェイクアラート）」を通じた、いわゆる「サポート詐欺」のようです。ただし、ＰＣをリモートコントロールされていた事実があるため、慎重な確認が必要でした。

実際にはトロイの木馬に感染していなかったものの、**もし実際にトロイの木馬に感染していたとしたら、どうするべきだったでしょうか。**

またトロイの木馬だけでなく、悪意のあるプログラム全般に遭遇したら、どのように対応すべきでしょうか。

＜＜　なお、偽警告については別途資料を用意しておりますので、そちらをご覧ください　＞＞

1.マルウェアとは

マルウェアとは、コンピュータウイルス、トロイの木馬、ランサムウェア等を含む、悪意のあるソフトウェアの総称で、ネットワークに害を与えたり、悪用したりすることなどを目的としています。

マルウェアに感染すると、大切な情報資産が破壊されたり、目に見えないところで情報漏えいを引き起こしたり、盗まれた情報を悪用されたりする等さまざまな被害を受けてしまうだけでなく、他のPC等への攻撃の踏み台にされることもあります。

2.マルウェアの感染経路

マルウェアの感染経路は様々で、WEBサイトの閲覧、ファイルやプログラムのダウンロード・インストール、メールの添付ファイルのオープン、USBメモリ等の外部記録媒体からの感染、クラウドストレージを介した感染、特定のネットワークからの感染等、非常に多様で巧妙化しています。

実在する組織や人物を装っている場合もあるため、怪しいURLやメールを開かないといった当たり前の対応だけでなく、不明なものについては先方に一度確認をとるなど感染させない工夫が必要です。また定期的なバックアップも重要になります。

★なお、TMG内の主なPCにはEDR（マルウェアの検知・隔離・封じ込めを行うエンドポイントセキュリティ対策ソフトウェア）が実装されており、マルウェア感染後の被害を最小限に抑制する働きをしています。

3.マルウェア感染後の対応：初期動作→報告

◆一般的な初期動作◆

- すべてのネットワークから遮断
- 電源は落とさない（強制終了しない）
- ウイルススキャン、ウイルス等の特定
- 感染したマルウェアごとに対応

◆グループ内 報告相談先◆

- 各施設内 システム担当部署
- TMG本部 コンプライアンス推進室
- TMG本部 総務部総務課
- TMソリューション

その他、必要に応じて、個人情報保護委員会／警察／IPA等へ連絡・相談します。
※個人情報の漏えい等またはその疑いがある場合には、個人情報保護委員会への報告が必須です（速報：3～5日以内／確報：内容により30～60日以内）

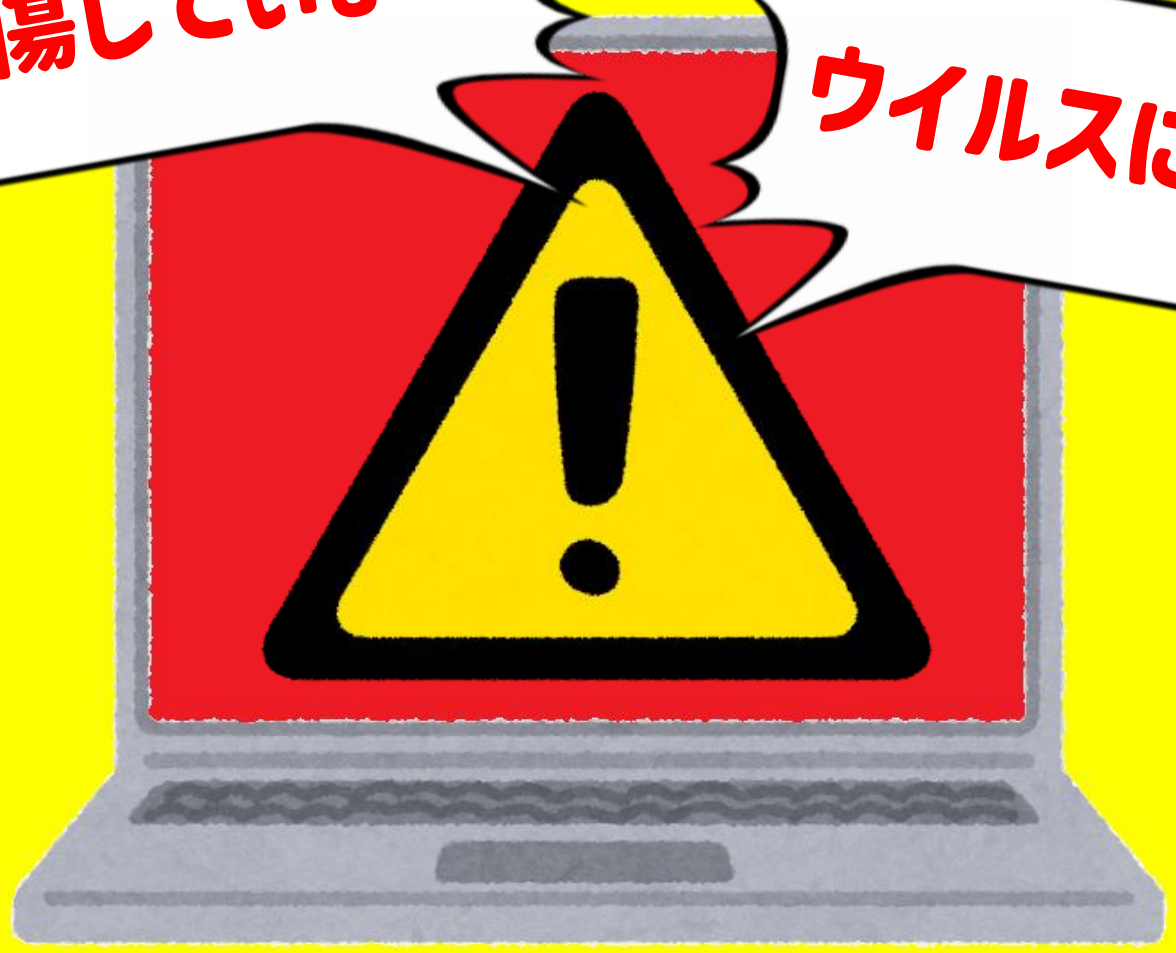
4.情報セキュリティ関連研修の実施について

今回の事例は、セキュリティリテラシーが備わっていれば防げた事態でしたので、対策として情報セキュリティに関する研修を実施予定です。詳細は別途ご案内します。

（TMG本部　コンプライアンス推進室）

システムが損傷しています

ウイルスに感染しました

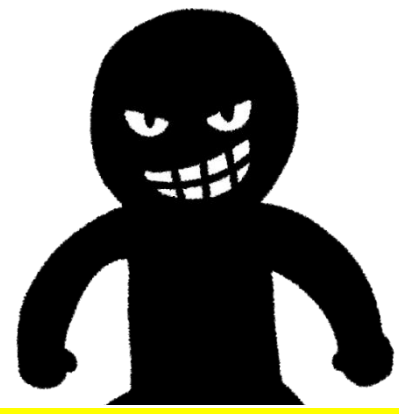


フェイクアラート

それ、偽警告です！

偽警告は、あなたに対して、こんなことを求めてきます

「いますぐここをクリックして回復！」
「このサポート番号に電話して！」
「修復用アプリ・ソフトをダウンロード！」



すべて詐欺です！

あわてずに**ブラウザを閉じ、**すぐに報告してください！

偽警告(フェイクアラート)とは？

「お使いのデバイスがウイルスに感染しました」
「トロイの木馬に感染しています」
「ファイルの消滅まであと◯秒…」
「システムの損傷度◯%…」

といった文言とともに表示される警告画面で、
ときに大音量でアラーム音が鳴り響くこともあり、
利用者の不安をあおり判断力を鈍らせます。

特徴は
“ブラウザ上に警告が表示される”
“不安をあおり、何らかの操作・行動を促す”
という点です。

画面の指示に従ってソフトやアプリをダウンロードしたり、
サポートセンターとされる番号に電話したり、
個人情報を入力・提供してしまったりすると、
以下のような事態が起こります。

- 端末の乗っ取り
- 高額請求
- 個人情報やパスワード等の機密情報の流出
- 実際にウイルスに感染

PCのみならず、 最近はスマートフォンでも
同様に偽警告が表示されることがありますので
個人使用の端末でも注意が必要です。

偽警告(フェイクアラート)の対策は？

【偽警告に遭遇しないために】

●メールやSMSで送られてきた不審なURLにアクセスしない

※URLをWEBブラウザの検索窓で検索するのも見破る為の一つの手段です。
ただしブラウザ上部のアドレス欄には入力しないでください！

●信頼できないサイトにアクセスしない

●開発元や提供元が不明なソフト・アプリをダウンロードしない

【偽警告に遭遇したら】

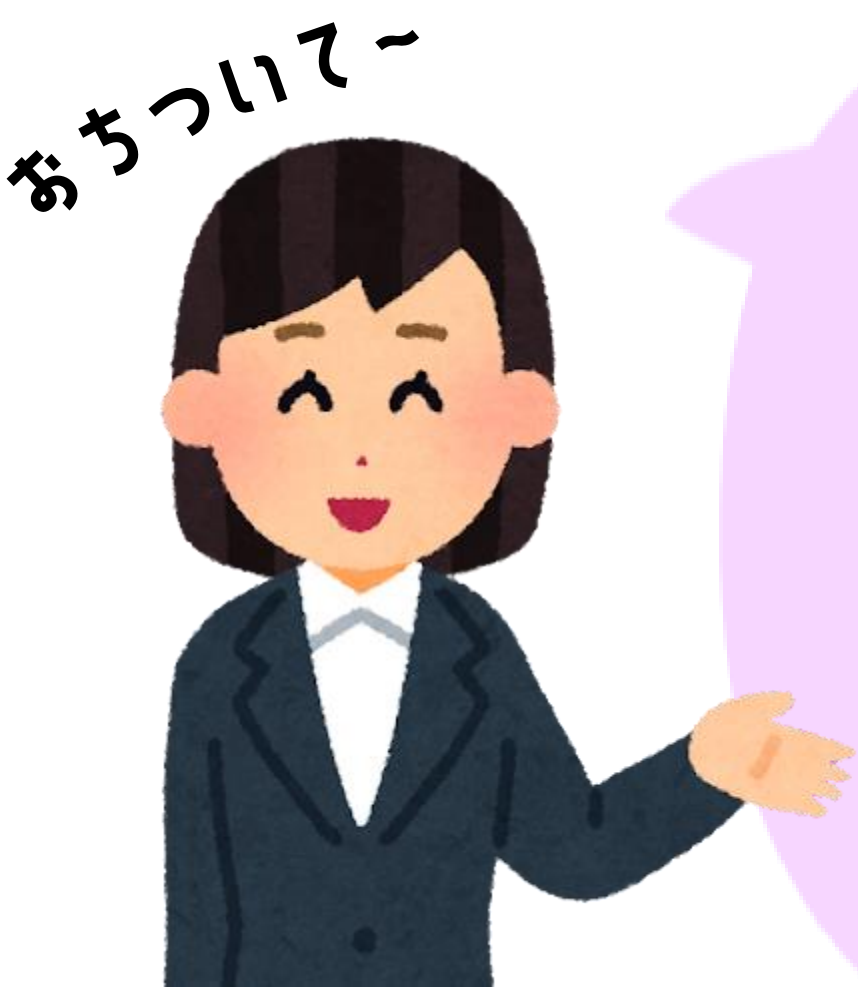
●ブラウザを閉じる（Alt+F4 同時押し等）、端末の再起動

●ブラウザの閲覧履歴・キャッシュ・cookieを削除する

●正規のウイルス対策ソフトを使用してマルウェアスキャンを実行

※感染を知らせるHPに誘導されてオンラインでのウイルススキャンを実行してはいけません！

●所属長に報告し、TMソリューションに対応を相談する



上記の通りに行動できない場合や、
どうしたらよいか分からない場合でも、
まずはひと呼吸。落ち着いて対応しましょう！

自分ひとりで対処や判断ができないときは、
所属長や周りの方に相談してください！

もし偽警告の指示に従ってしまったら…？

【アプリ・ソフトをダウンロードしてしまったら】

●アプリ・ソフトのアンインストール

●念のため、ウィルス対策ソフトでスキャン

●サブスクリプション（継続課金）を契約した場合は、解除

【個人情報やパスワード等を入力・提供してしまったら】

●どんな情報を入力・提供してしまったか整理

●銀行口座・クレジットカードの情報を教えてしまった場合は、
お使いの銀行・カード会社に連絡

●金銭被害がある場合は警察へ

【ウイルス感染の疑いがあったら】

●動作がおかしいと思った時点で報告

●ウイルス対策ソフトで状況を確認

●スマホの場合は、公式サポートに連絡し指示を仰ぐ

初期対応が大事！
冷静に行動しましょうね♪