マルウェア・ランサムウェアに感染しないために

□ **身に覚えのない、または不審なメールやスパムのリンクをクリックしない**

・知らない人からのメールの添付ファイルは絶対に開かないでください。サイバー犯罪者は、オンラインストア、銀行、警察、裁判所、または税務署等になりすましメールや SMS を送信します。受信者に、システムがマルウェアに感染する不正なリンクをクリックするように誘導します。

・どんなアカウントでも感染のおそれがあり、友人、同僚のメールやソーシャルメディアのアカウントからのなりすましメールに不正なリンクが添付されていることもあります。

□ **インターネットの閲覧中は、疑わしいリンク、ポップアップ、またはダイアログボックスをクリックしない**

・それらをクリックすると、マルウェアがシステムにダウンロードされる可能性があります。そうしたリンクからは目的の Web サイトに到達せず、マルウェアに感染してしまうかもしれません。気になる情報は、自ら検索エンジンで Web サイトを検索するようにしてください。

□ **ソフトウェアは、信頼できる Web サイトから公式バージョンのみをダウンロードする**

・携帯電話やタブレットに何かをダウンロードする場合は App Store（Apple）や Google Play ストア（Android）などの信頼できるソースやストアを使用してください。Web サイトが不正であるかどうかを判断する最良の方法は、URL に細心の注意を払うことです（ただし、昨今では被害者を騙すために似たようなドメインを使用しているケースが多く、ドメイン名での判別は難しいことも多くあります）。URL のドメイン名は、Web サイトの名前と一致している必要があります。HTTPS 接続と南京錠のアイコンの表示は安全な接続のサインですが、これは信頼できるという意味ではありません。

□ **PC に保存されているデータを定期的にバックアップする。**

・PC に保存されているデータを定期的にバックアップすれば、ランサムウェアに感染しても個人のデータが完全に破壊されることはありません。

□ **堅牢なセキュリティ製品を使用し、ソフトウェアと OS を確実に最新のものにする**

・Mac ユーザーは全学ソフトウェアライセンスの McAfee Endpoint Security for Mac、Windows ユーザーは Windows Defender の使用をお勧めます。

・マルウェア・ランサムウェアを検出するための各種機能はオフにしないでください。

・オペレーティングシステム（OS）またはアプリケーションは、新しいバージョンが発表

されたらインストールしてください。ソフトウェアがアップデートを自動的にインストールするオプションを提供している場合は、それを利用してください。

□ **ローカルファイアウォールを有効にする**

・不正アクセスから保護するため、ローカルファイアウォールを有効にしてください。

- Apple の場合：[システム環境設定] > [セキュリティとプライバシー]
- Windows の場合：[スタート] > [設定] > [プライバシーとセキュリティ] > [Windows セキュリティ] > [ファイアウォールとネットワーク保護]

□ **大学のネットワークで不正不審な通信又はウイルスを検知した場合、**

・情報基盤センターからまず GSICS 情報処理委員会に連絡があります。その後担当者よりウイルスが検知された端末の使用者に連絡いたしますので、担当者の指示に従って対応してください。

・まずパソコンをネットワークから切り離します。無線 LAN の場合は、無線の機能をオフにしてください。その後証拠保存のため、できるだけ電源を切らずに保存しておいてください。

・一旦ウイルスに感染した場合、コンピュータ内の情報が抜き取られて送信されている可能性が高いので、そのパソコンの Web ブラウザやアプリに登録してある（利用したことがある）ID のパスワードをすべて変更してください、特に銀行やクレジットカード関連の場合は、すぐに連絡して利用を一旦止めましょう。

・GSICS 情報処理委員会の指示に従い，復旧作業を行いましょう。ウイルス感染が疑われる場合，ウイルス対策ソフトにおける調査および結果に基づく作業の指示があります。

・GSICS 情報処理委員会の許可が出ないうちは，ネットワークに接続しないようにしてください。

引用元

- NO MORE RANSOM ＞ 一般ユーザーへのアドバイス
  https://www.nomoreransom.org/ja/prevention-advice-for-users.html
- 神戸大学 LMS BEEF ＞ Venture 情報基礎 2022 ＞ ３．インターネットの利用
  https://venture.center.kobe-u.ac.jp/pluginfile.php/95820/mod_resource/content/0/johokiso3.pdf

国際協力研究科情報処理委員会