基本的な IT セキュリティ対策の徹底について

生研電子計算機室 2020 年 4 月 1 日

今日、インターネットにアクセスできる PC はすべて悪意のある人々からの攻撃対象となっています。「自分のメールやファイルは見られたら困るようなものはない」という方もおられますが、迷惑メールの送信元にする、他の PC を攻撃するための踏み台として利用するなどのかたちで悪用される可能性があります。そのような事態が発生すれば、あなたも加害者の一員にされてしまう恐れがあります。つきましては、利用中の PC やスマートフォンなどの IT デバイスについて以下の基本的なセキュリティ対策の徹底をお願いいたします。

セキュリティアップデートは速やかに適用する

OS やアプリケーションのセキュリティアップデートは自動更新する設定にしてください。アップデートが存在することを通知するポップアップが表示された場合、後回しにしないで速やかに実行してください。Windows は、米国日付の毎月第二火曜日(日本時刻では翌日の水曜日)にまとめてセキュリティ更新プログラムが公開されます。この日には PC を使用する前に必ず Windows Update を実施してください。

サポート切れのソフトウェアや機器類は使用しない

OS、アプリケーション等のソフトウェアや、機器自体のサポートが切れたものは使用しないでください。どうしても使用する必要がある場合は、ネットワークに接続せず、スタンドアロンで使用してください。スタンドアロン環境であっても、専用ツール[1]等を用いて必ず定期的に最新のウイルス対策ソフトでスキャンを実施してください。スタンドアロン環境の PC 等とデータのやり取りを行う場合は、データ交換専用のメディア（USB メモリや外付け HDD 等）を用意してください。また、スタンドアロン環境から取得したファイルを開く前に、必ずインターネットに接続された別の PC にてウイルスチェックを実施してください。

ウイルス対策ソフトを最新版に保つ

多くの方は、東大で契約しているトレンドマイクロ社のウイルスバスタークラウドを PC にインストールされていますが、一度インストールしたまま放置されていることが少なくないようです。ウイルスバスタークラウドは毎年新しいバージョンが公開されていますが、自動的にはバージョンアップされません。これは新種のウイルスに対応するための日常的な自動アップデートとは別です。また、ひとつのバージョンは約 2 年でサポートが終了し、その後は自動アップデートが止まり、新種のウイルスに対応できなくなってしまいます。現時点で旧バージョンのまま使用している場合はすぐにバージョンアップしてください[2]。その後は年に 1 回はバージョンアップしてください。

（裏面へつづきます）

---

[1] 例えば、トレンドマイクロ社の「Portable Security」といった製品があります。電子計算機室でも貸出を実施しています。
（2020 年 3 月末時点での URL）
https://www.trendmicro.com/ja_jp/business/products/user-protection/sps/endpoint/portable-security-2.html

[2] ウイルスバスタークラウドのバージョンとサポート期限については以下の URL を参照してください。
https://helpcenter.trendmicro.com/ja-jp/article/TMKA-01074

不審なメールの添付ファイルやリンク先を安易に開かない

メールサーバ管理者や学会の案内などを装った「標的型攻撃メール」が送られてくることがあります。そのようなメールはよくみると送信元のメールアドレスがおかしい(大学のメールサーバ管理者を名乗りながら、送信元は@yahoo.com になっている)など、なにかしら不自然な点があるはずです。そのようなメールの添付ファイルやリンク先の web ページを開かないでください。添付ファイルはウイルスで、特定の宛先向けに改変されており、ウイルス対策ソフトが検知できない場合が少なくありません。

パスワードを厳重に管理する

PC へのログイン、メールサーバへのアクセス、Google などのインターネットサービス利用などで、複数のユーザアカウントをお持ちだと思います。ユーザアカウントの管理について以下の点を厳守してください。

- パスワードは十分複雑なものにする(適当なフレーズを組み合わせ、部分的に数字や記号に置き換える)
- 同じパスワードを複数のユーザアカウントで使いまわさない
- パスワードは他人に知られないように十分注意し、漏洩した可能性がある場合は直ちに変更する

重要なファイルは定期的にバックアップをとる

最近は、PC 上のファイルを勝手に暗号化し、元に戻すための「身代金」を要求する、いわゆるランサムウェアによる攻撃も少なくありません。対策として重要なファイルはバックアップを取り、PC から切り離された状態もしくは書き込み不可の状態で保管して、もしランサムウェアに感染しても復元できるようにしてください。

以上