不審メールの添付ファイル／URLをクリックしてしまった！そんな時...

2019 年
8 月

自己判断していませんか？

NG
クリックしたけど、
すぐに閉じたから
大丈夫！

NG
変なサイトが開いたけど、
PCにおかしな
動きはないから、OK！

NG
クリックしてしまったから
ウイルス対策ソフトでスキャンしたよ。
何も検出されなかったから
これで安心！

NG
まずいなぁ（；´Д｀）
けど上司や周りには
言いづらいし、
黙っとこう ...

検出がなくても...

- ウイルス対策ソフトで検出できるのは50%未満といわれています
- 感染未遂だったり、感染しても被害が出ていないだけということもあります
- たとえ何も検出されなくても安心はできません

すぐに閉じても...

- 人間の感覚の「すぐ」は、コンピュータには通用しません
- 開いたファイルを仮に「すぐ」閉じたとしても、とっくに不正な通信は発生しているものと考えましょう

言いづらくても...

- すぐに上司とCERT（事務職員*は事務情報支援G）に報告しましょう
- 上司の方は、何事も報告しやすい風通しのよい環境整備を心がけましょう
- 不審メールが届いたら、グループ、研究室等内で積極的に声がけをしましょう

*事務ネットワーク使用者（事務用レンタルPC使用者）

PCが通常どおりでも...

- 通常、ウイルスは利用者から見えない様に活動し、感染拡大や情報の窃取を試みます
- 数日から数週間程度PC内で潜伏してから、ウイルスが活動を開始するケースもあります

これらを放置すると最悪の場合...

個人情報や研究データなどの情報漏洩に繋がります。
その結果、大学の社会的信用が失墜したり、金銭的損害が発生する可能性があります。

インシデント対応は時間との勝負です
対応が遅れるほど、業務復帰にも時間がかかります

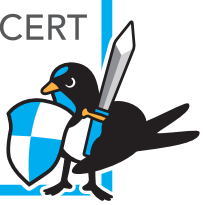
もし、開いてしまったら...

1. ネットワークから切りはなす。
2. 上司とCERTに報告しましょう。（事務職員の方は事務情報支援グループ【内3274】）

困ったときは
1人で悩まず
まず相談を！

[問い合わせ]
MAIL：contact@cert.titech.ac.jp
TEL　：3272（内線）

東工大CERT
TokyoTech
Computer
Emergency
Response
Team



日頃から気をつけること4 箇条

1. OSとソフトウェアは 常に最新の状態に
2. ウイルス対策ソフトも 常に最新に
3. 不審なメールは 開かないように
4. バックアップは 定期的に※

※ ウイルスによるデータの乗っ取り(不正なハードディスクの暗号化)を防ぐためにバックアップデータはネットワークから切り離すなど利用中のPCからアクセス出来ない所に保存することをお勧めします。

最近のセキュリティ情報

■ NAS*の運用／セキュリティ設定に注意

本学でも、NASの設定が不適切だったために、不正ログインされた事案があります

*NAS：Network Attached Storage。ネットワークに直接接続して使用する外部記憶装置。
バッファロー製Link StationやQNAP社製のものなどがある

✓ アカウント管理に細心の注意を払う

初期パスワードは必ず変更! 不要なアカウントは作らず、年に一度は全アカウントをチェックしましょう

✓ できるだけグローバルIPアドレスは使用しない

共同研究で学外とのやり取りがどうしても発生する等の場合を除き、グローバルIPアドレスは使用せず
プライベートIPアドレスを割り当てましょう

✓ 使用する最低限のポートのみ開け、不要なポートは閉じる

SSH、VPN、FTP、HTTP、telnet etc. 様々なポートがありますが、不要なものは無効化しましょう
開けっ放しのポートから不正侵入されるおそれがあります。最悪の場合、重要なデータや情報が漏洩してしまいます

✓ ログを保存する

万が一インシデントが発生した場合、不審なログイン履歴やアクセス履歴がないか調査することができます

万が一インシデントが起こってしまったら、一人で解決しようとせず、
『組織』として対応し、今後の方針を決めるようにしましょう

東工大CERTについて

CERTは情報セキュリティ専門チームです。東工大における研究/教育/事務活動等を促進させるため、安全な計算機環境が構築できるようサポートする事がCERTの役割です。セキュリティ事案発生時における緊急対応を行うほか、セキュリティ情報の発信、学内の脆弱性調査など事前対応に重きを置いた情報セキュリティに関わる活動を行っています。

■ 東工大CERTの体制

■ WEBおよび問い合わせ

WEB ： http://cert.titech.ac.jp
MAIL ： contact@cert.titech.ac.jp
TEL ： 3272（内線）
twitter ： @T2CERT