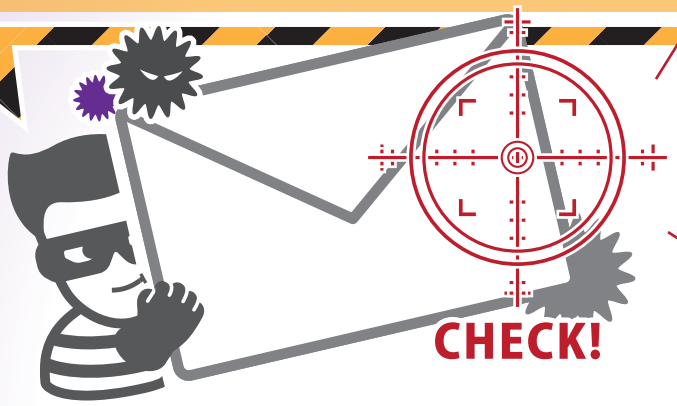
2021年
4月

そのクリック ちょっと待って！ 危険なメールかも？

WARNING!!

**知人や取引業者がマルウェアに感染し、
攻撃メールを送信する事案が頻発しています！**



CHECK! 差出人

実際にやり取りをした業者、学内組織、
自分自身が差出人として使われます

CHECK! 件名

実際にやり取りをしたメール件名が
RE:(返信)で使われる場合があります

CHECK! 本文　CHECK! ファイル

実際にやり取りをした本文やファイルが
盗まれ、引用される場合があります

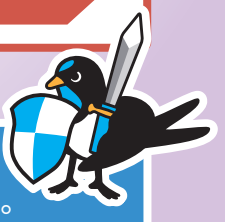
あなたのPCがウイルスに感染すると…こんな可能性が！

- 重要、機密情報が盗み取られます（ID、パスワード、送受信メール、アドレス等）
- データが暗号化、破壊されます 復旧の代償に金銭的要求をされる場合もあります
- 学内の他端末や学外へも感染が広がり、取引先や共同研究先でも被害が発生します
- 結果として、大学の社会的信用の失墜や金銭的な被害をもたらします

**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、添付ファイルやURLを間違えてクリックしてしまったら…

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】）



効果的な対策

- 添付ファイルやURLを反射的にクリックせず、必ず一呼吸おいて確認しましょう。
  一人で判断せず送信元に直接確認するか東工大CERTへ連絡を！
- OSやウイルス対策ソフトウェアは常に最新の状態にアップデートしましょう。
- 添付ファイル開封時に不審なマクロが立ち上がったら、無効化して周りの人に確認を！

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

■在宅、リモート勤務時の情報セキュリティ事案が多発しています

一定の防御態勢が整った大学のネットワークや、適切に管理された常時最新のＰＣ環境が使えなくなるため、データの保護機能が弱まります。より一層自分自身で注意してデータを守る必要があります。上記を踏まえて以下のようなポイントに注意して対策を行いましょう。

✓ 情報漏洩対策

・機密情報、重要な情報を扱う業務は大学出勤時に、それ以外を在宅勤務時に行うなど、取り扱う情報の重要性に応じた業務の見直し／切り分けを行いましょう。
・やむを得ず、重要な情報を学外へ持ち出す必要がある場合は上長等に相談すると共に、所属部局で定められている情報の持ち出しの可否や必要な手続きを確認しましょう。

✓ ウイルス対策

・PCへは必ずウイルス対策ソフトをインストールし、OS、ソフトウェアは常に最新の状態にアップデートしましょう。
・メールの添付ファイルやURLはすぐにクリックせず、一旦確認することを習慣にしましょう。判断に迷ったら周りの方に電話やメール等で相談しましょう。

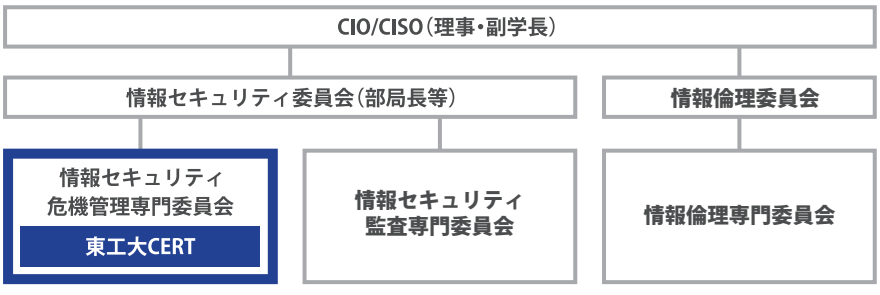
✓ 紛失、盗難対策

・持ち運びしやすいノートPCやUSB等は、本体やデータに必要に応じて適切なパスワードを設定しましょう。
・データは定期的にバックアップを行いましょう。

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