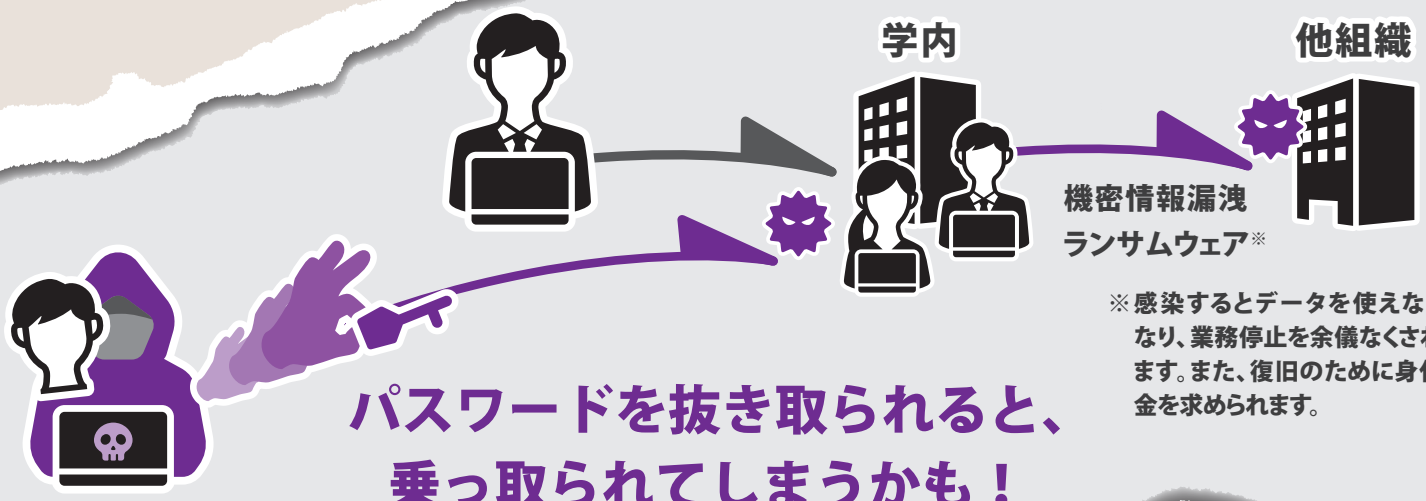
2023 年
4 月

そのリモート接続、安全ですか？



※感染するとデータを使えなくなり、業務停止を余儀なくされます。また、復旧のために身代金を求められます。

パスワードを抜き取られると、乗っ取られてしまうかも！

見直しポイント

POINT 1 組織のルール

- 管理者権限を誰が持つべきか確認しましょう
- 端末の持ち出しやリモート接続のルールを組織内で明確にしましょう

POINT 2 リモート接続（VPN・リモートデスクトップ等）の設定

- パスワードを複雑で推測されづらいものにしましょう
  （例）　英字と数字を両方含む12文字以上
- 二要素認証を取り入れましょう
  （例）パスワードとソフトトークンでログイン
- 定期的にアップデートし、より安全性の高い状態を保ちましょう

「不審なメールを開かない」など、基本的なルールに関しても見直しを！

詳しくは裏面へ

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

■ ランサムウェアによる被害が多発しています

◎ ランサムウェアとは

コンピューターウイルスの一種で、データを暗号化し使用できない状態にしてしまいます。データ復元のために身代金を要求する他、最近では、金銭を支払わなかった場合暗号化したデータを漏洩させると脅迫する「二重脅迫」のケースも増加しています。日本では2021年に平均して約5億8600万円の身代金が支払われています。

◎ 最近の事例

医療機関がランサムウェアに感染しました。電子カルテのデータが暗号化され、閲覧できなくなったことで、診療や手術を一時的に中断する事態となりました。また、完全な業務再開までには2か月程度の時間を要しました。ランサムウェアは医療機関が委託していた給食サービスから侵入したと考えられています。更に、給食サービスのVPNが攻撃されていたことが分かっています。

◎ 大学での事例

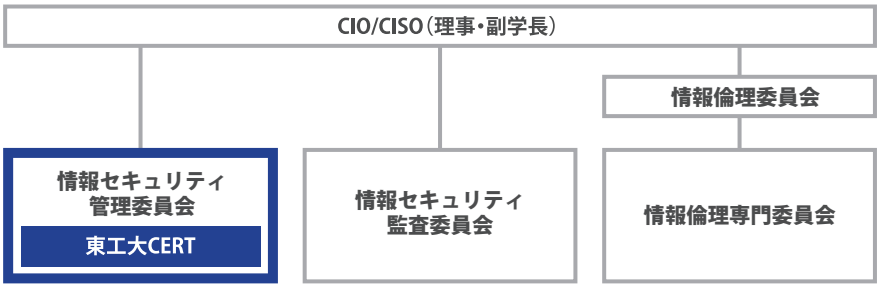
東海国立大学機構がランサム被害 - ログに総当り攻撃の痕跡
https://www.security-next.com/141573

歴史ある米私立大学、コロナとランサムウェア攻撃の影響で閉校
https://www.itmedia.co.jp/news/articles/2205/10/news096.html

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