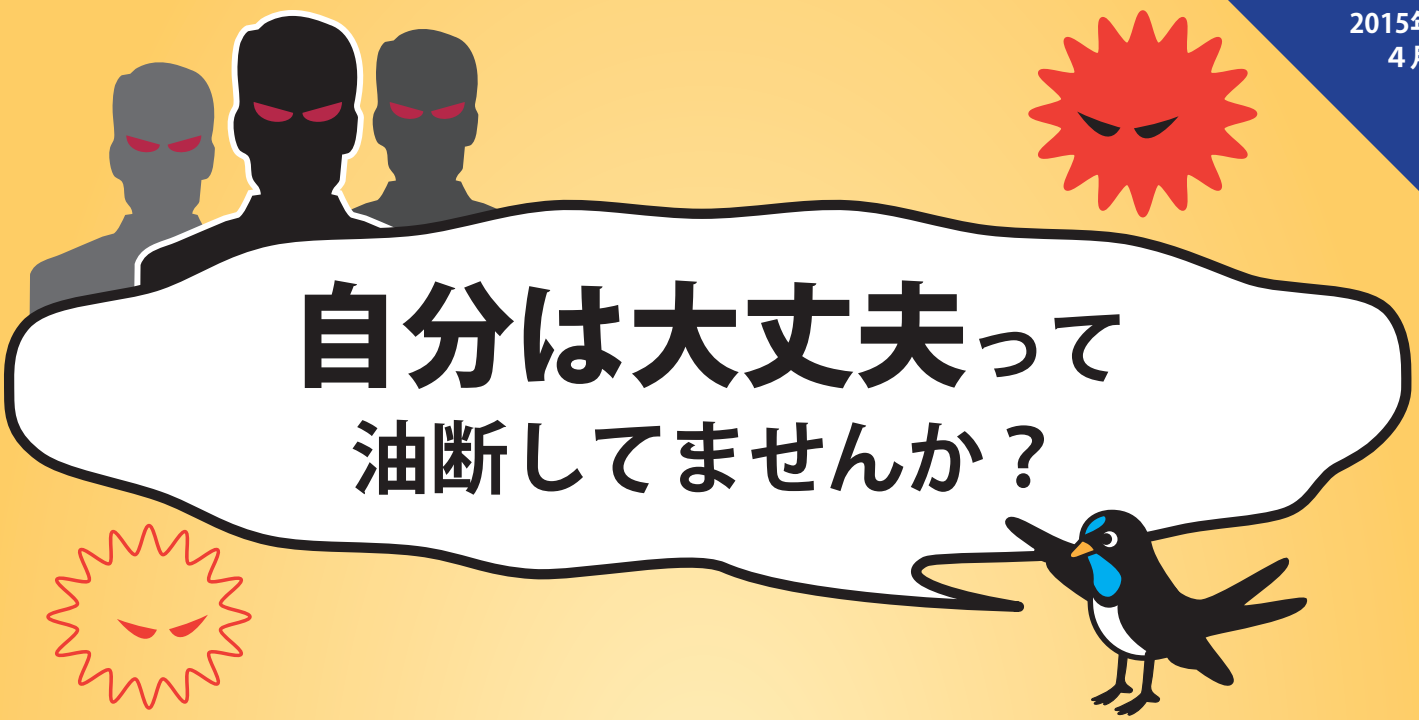
2015年
4月



自分は大丈夫って油断してませんか？

OSとソフトウェアは
常に最新の状態に

ウイルス対策ソフトも
最新に

不審なメールは
開かないように

学内での最近の被害例

身代金を要求する脅迫ウイルス（ランサムウェア）に感染。

Q. どこで感染したの？

A. メールに添付されていたファイルを開いたら急にパソコンが使えなくなりました。

Q. 感染するとどうなるの？

A. パソコンに保存されてる特定の拡張子を持ったファイルを暗号化して人質にとり、暗号化解除ツールの購入と引き換えに身代金を要求します。その暗号化ツールでないと暗号化されたファイルは元に戻せません。パソコンは再インストールするしかありません。

Q. 被害にあわないためにはどうすればいいの？

A. 別のパソコンやNAS（ネットワーク接続用ディスク）などにバックアップをしておいてください。
OSとソフトウェアは最新の状態にしておいてください。
ウイルス対策ソフトウェアを使用してください。

おかしいと思ったら

1. ネットワークから切りはなす。
2. 直ぐにCERTへ連絡を。3272（内線）

困ったときは
1人で悩まず
まず相談を！

[問い合わせ]

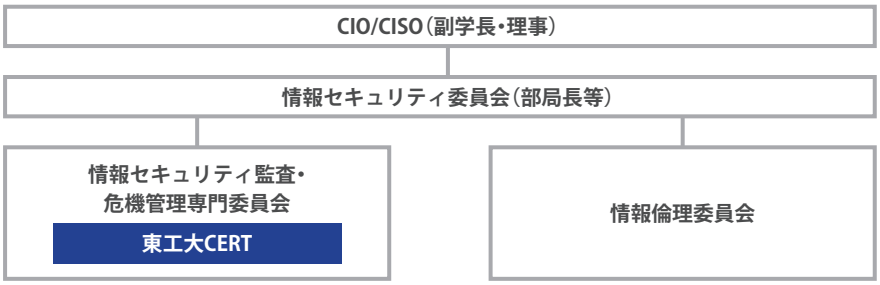
MAIL：contact@cert.titech.ac.jp
TEL　：3272（内線）

東工大CERT
Tokyo Tech Computer Emergency Response Team
http://cert.titech.ac.jp

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、取り締まることではなく安全な計算機環境を提供する事が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



■ CERT構成員

統括責任者　：松浦知史（学術国際情報センター 准教授）
　　友石正彦（大学マネージメントセンター 教授）
CERTメンバー：情報基盤課長
　　情報企画グループ
　　技術職員（ネットワーク担当、認証基盤担当）

■ 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）

日頃から気をつけること3 箇条

◎ **セキュリティアップデートはチェックしましょう。**
◎ **安全なパスワードを使いましょう。**
◎ **見覚えのないメールの添付ファイルには注意しましょう。**

セキュリティ情報

■ 身代金を要求する脅迫ウイルス（ランサムウェア）について

ファイルを不正に暗号化し、復元のために金銭を要求する脅迫ウイルス（ランサムウェア）について、トレンドマイクロから最近の傾向を踏まえた解説記事が出ています。実際、学内でも感染事例が確認されています。出所の特定できないメールの 添付ファイルには触れない、OSやソフトウェアのアップデートは欠かさないと言った 当たり前の事をまずは徹底する事が重要と考えられます。加えて下記の 3点が記事で指摘されています。

1. **決して身代金を支払わない**
2. **セキュリティ製品をインストールする（ウイルス対策ソフトウェア等）**
3. **重要なファイルはバックアップを取る**

ファイルが暗号化され元に戻らないと研究/教育/事務活動等に多大な 影響が生じる可能性があります。セキュリティやバックアップの体制を 見直しましょう。

> 多様化するランサムウェア、その手口を解説
> http://blog.trendmicro.co.jp/archives/9922