2018 年
12 月

IoT機器・ネットワーク機器 ちゃんと管理していますか？

初期設定のまま
運用していると …

不正アクセスや遠隔操作されるかも！

管理者パスワードが
適切に設定されていないと …

不正ログインされる危険が！

ソフトウェア／ファームウェアの
アップデートをしていないと …

脆弱性を悪用される可能性が！

適切に管理しないと、会議内容等を盗み見されたり、マルウェアに感染して乗っ取られ、外部サーバや外部サイトなどへの攻撃の踏み台となる可能性があります

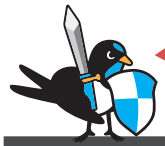
Q. 被害に遭わない／加害者にならないようにするには、どうすればいいの？

A.1
適切なアクセス権等の設定や
定期的なアップデートを行う
機器管理担当者を決める

A.2
設定を見直す
（使用しないプロトコル
やインタフェースを
無効化しましょう）

A.3
管理者パスワードを
複雑なものに変更する

A.4
最新のソフトウェア／
ファームウェアを利用する



ネットワークに接続されるあらゆる機器の管理に注意し、運用を適切に行いましょう

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

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

■ビットコインなど仮装通貨に関する不正なマイニング（発掘）について

✓ 大学の資産を不当に利用し個人が金銭等の対価を得ることは禁じられています

大学は資産として多くの計算機を有しています。その計算機を不当に利用し、個人が対価を得ることは規則的にも倫理的にも許されない行為です。ビットコインに代表される仮想通貨の一部にはマイニング（発掘）と呼ばれる過程が組み込まれおり、多くの計算機資源を消費する対価として、仮想通貨を得られる仕組みが存在します。大学におけるマイニングが社会的にも大きな問題として取り上げられています。マイニングに限らず、個人が不当に対価を得るような行為を行わないようお願いします。

✓ 意図せずマイニングを行わないために、アップデートの徹底を

2018年現在、脆弱性を抱えた多数のWebサイトにマイニングツールが不正に埋め込まれており、Webサイトを閲覧しただけでマイニングを行ってしまうケースが多発しています。これは広範囲に渡る個人の計算機資源を浪費させ、その対価に不正に仮想通貨を得ようという目的の下に、多くは犯罪組織などによって行われています。意図的ではないにせよ、大学の計算機資源を利用し、犯罪組織など反社会的な集団に対価を与えるような行為は慎むべきです。基本的なことですが、OSやソフトウェア、アンチウイルスソフトのアップデートを徹底してください。PCだけでなく、Androidなどモバイル端末にも注意が必要です。

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