# 情報セキュリティチェックシート　基礎編（保存用）

このチェックシートには、近頃急増しているコンピュータウイルスへの感染や情報漏えいなどの被害に遭わないために必ず知っておいて欲しいことをまとめています。大学内でパソコンやインターネットを使う前に,「インターネットの安全・安心ハンドブック(情報セキュリティハンドブック)」を一読するとともに, これらの項目について確認しましょう。そして別紙の「情報セキュリティチェックシート基礎編(提出用)」にチェックの上で指定の提出先までご提出ください。

※ なお, 本紙は各自保管の上で必要に応じて確認してください。

NISC「インターネットの安全・安心ハンドブック」

パスワード
### パスワードの使い回しはやめましょう
特に Twitter や Facebook など個人的に使用しているアカウントのパスワードを業務 ( 学内メールや業務システムなど ) では絶対に使ってはいけません。

パスワード
### なるべく長いパスワードを使用しましょう
最低でも英大文字や数字，記号を含めた 10 文字以上のパスワードを設定しましょう。

パスワード
### パスワードのメモは他人に見られないように保管しましょう
パスワードが書かれたメモなどをディスプレイや机には貼ってはいけません。

ソフトウェア
### パソコンには必ずウイルス対策ソフトをインストールしましょう
東工大では学生・職員が 無償で利用可能なウイルス対策ソフトを用意しています。

ソフトウェア
### ソフトウェアやOSは常に最新バージョンへ更新しましょう
サポートの終了しているソフトウェア・OS の業務での利用は禁止されています。ソフトウェアのバージョンが古いとウイルス感染する可能性が増加します。

メール
### 添付ファイルやURLリンク付きのメールには十分注意しましょう
不審に感じたら，まずは開かずに周りの人に相談しましょう。

データの管理
### 業務に必要不可欠なデータは必ずバックアップをとりましょう
特に重要なデータのバックアップはネットワークから切り離して保管しましょう。

データの管理
### 個人情報を含むデータにはパスワードをかけましょう
職員番号や氏名など個人を特定できるような情報は，業務で触る必要のある人のみで共有しましょう。

緊急対応
### ウイルス感染が疑われる場合にはパソコンをネットワークから切り離しましょう
パソコンの電源を入れたまま，LAN ケーブルを抜くもしくは無線 LAN 接続を切断しましょう。

緊急対応
### ウイルス感染が疑われる場合には速やかに報告/連絡/相談しましょう
直属の上司および東工大 CERT あるいは事務情報支援グループへの連絡が必要です。

研究推進部 情報基盤課 情報セキュリティ対策グループ E2-5 e-mail: kib.sec@jim.titech.ac.jp 内線 : 3272 （2019.04）

## 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

ＯＳやソフトウェアのセキュリティアップデートは必ず行いましょう。ＰＣ起動時に確認する習慣を身に付けたり、可能な場合は自動アップデートの設定を行うことをお勧めします。

### 2 ウイルス対策ソフトも 常に最新に

ウイルス対策ソフトを導入しているだけで安心してはいけません。サポートが有効な対策ソフトを利用すると同時にウイルス定義ファイルも最新に保つことが必要です。

### 3 不審なメールは 開かないように

受け取ったメールに不審な点がないか注意する癖をつけましょう。
「なりすましメール」による攻撃は，いくつかのポイントを確認することで多くの被害を避けることができます。

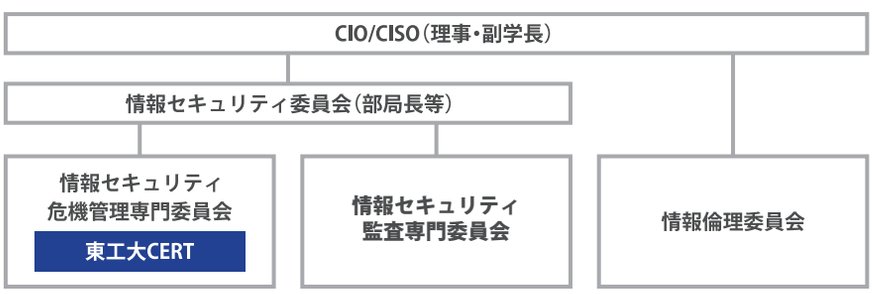
### 4 バックアップは 定期的に

ウイルスによってファイルが暗号化され元に戻せなくなることを防ぐため、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。

## 東工大 CERT とは

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

**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

# 情報セキュリティチェックシート　基礎編　（提出用）

記入日：＿＿＿＿/＿＿＿＿/＿＿＿＿　所属部署：＿＿＿＿＿＿＿＿＿＿＿＿　回答者氏名：＿＿＿＿＿＿＿＿＿＿＿＿

**下記の項目をチェックしてご提出ください。もし分からない用語などがあれば，**
**その部分を蛍光マーカーでマークのうえで周囲の人に相談してみましょう。**

☐ パスワード
**パスワードの使い回しはやめましょう**
特に Twitter や Facebook など個人的に使用しているアカウントのパスワードを業務 ( 学内メールや業務システムなど ) では絶対に使ってはいけません。

☐ パスワード
**なるべく長いパスワードを使用しましょう**
最低でも英大文字や数字，記号を含めた 10 文字以上のパスワードを設定しましょう。

☐ パスワード
**パスワードのメモは他人に見られないように保管しましょう**
パスワードが書かれたメモなどをディスプレイや机には貼ってはいけません。

☐ ソフトウェア
**パソコンには必ずウイルス対策ソフトをインストールしましょう**
東工大では学生・職員が 無償で利用可能なウイルス対策ソフトを用意しています。

☐ ソフトウェア
**ソフトウェアやOSは常に最新バージョンへ更新しましょう**
サポートの終了しているソフトウェア・OS の業務での利用は禁止されています。ソフトウェアのバージョンが古いとウイルス感染する可能性が増加します。

☐ メール
**添付ファイルやURLリンク付きのメールには十分注意しましょう**
不審に感じたら，まずは開かずに周りの人に相談しましょう。

☐ データの管理
**業務に必要不可欠なデータは必ずバックアップをとりましょう**
特に重要なデータのバックアップはネットワークから切り離して保管しましょう。

☐ データの管理
**個人情報を含むデータにはパスワードをかけましょう**
職員番号や氏名など個人を特定できるような情報は，業務で触る必要のある人のみで共有しましょう。

☐ 緊急対応
**ウイルス感染が疑われる場合にはパソコンをネットワークから切り離しましょう**
パソコンの電源を入れたまま，LAN ケーブルを抜くもしくは無線 LAN 接続を切断しましょう。

☐ 緊急対応
**ウイルス感染が疑われる場合には速やかに報告/連絡/相談しましょう**
直属の上司および東工大 CERT あるいは事務情報支援グループへの連絡が必要です。

[ チェックシート提出先 ]

**研究推進部 情報基盤課 情報セキュリティ対策グループ E2-5**