

Online で授業を受けるときはセキュリティに気を付けてください。

1. Teams や Zoom で授業を受けるとき

- ① システムのアップデートの知らせが来たらすぐアップデートしてください。
- ② LMS(授業支援システム)にある、授業で使うミーティング URL や ID、パスワードはほかの人には絶対教えないでください。
- ③ 授業のときに、先生が名前、ビデオやマイクのルールについて説明します。そのルールに従ってください。
- ④ 授業の録画をしたり、写真を撮ったりしてはいけません。また、授業の資料や動画を勝手に共有したり、SNS などにアップしたりしてはいけません。

※ 「横浜国立大学情報格付け基準」及び「情報格付けに係る取扱いガイドライン」による。

2. パソコンのセキュリティについて

(1) Apex One はいつも新しいバージョンにしておきましょう。キャンパスの Wifi が使えるときは、情報基盤センターの HP から無料の Apex One をダウンロードできます。

https://www.itsc.ynu.ac.jp/security/vb_haifu.html

- ① Apex One の「予約検索」を「有効」にして、スキャンしておくようにしてください。
- ② 毎月の 10 日、20 日、30 日はマルウェア (Malware) をチェックする日 (CheckDay) です。その日は、パソコンをフルスキャンしてください。
- ③ 海外から授業を受ける場合など、キャンパスに入れない学生は、自分でセキュリティソフトを準備して、使ってください。

(2) パスワードについて

- ① パスワードは、大文字、小文字、数字や記号を使って作ってください。
- ② 少なくとも 10 文字以上してください。
- ③ パスワードを変えるときは、前のパスワードと似たものにしないでください。
- ④ 使ったことがあるパスワードをまた使ってはいけません。

(3) OS・ソフトウェアについて

- ① OS/ソフトウェアをアップデートして、いつも新しいバージョンにしておいてください。
- ② アップデートができない古いバージョンの OS やソフトウェアは使わないでください。
- ③ 使わないソフトウェアは消してください。
- ④ 信頼できないフリーソフトウェアはなるべくパソコンに入れないようにしてください。