

# 情報セキュリティ対策再確認のお願い

2022年2月2日  
情報メディアセンター

教育機関の教育、研究、運営などの活動における情報化の進展、特に昨今の新型コロナウイルス感染症の対応の一環として、オンライン授業の取り組みをはじめ、様々なウェブシステムの利用が広がっています。

それに伴い、インターネットに接続されたシステムとデータの不正使用や損害から保護するための継続的な取り組みとしての情報セキュリティの重要性はさらに増しています。

改めまして情報システムを利用の際の心構えとして情報セキュリティ対策の再確認をお願いいたします。

(参考) 青山学院大学附置情報メディアセンター利用上の注意  
<https://www.aim.aoyama.ac.jp/about/attention/>

## 1) ログイン ID とパスワードの管理の徹底

ログイン ID とパスワードの管理においては、以下の点に注意してください

- 大文字小文字・記号・数字などを組み合わせたり、誕生日や辞書にある単語人名などは使わないフレーズにしたりして、他人に容易に推測されにくいものにする
  - (参考) 教育研究システムで用いる LDAP パスワードは下記資料に掲載されているルールに従ってください  
CoursePower > HOME > 学内資料 (教員向け) > 新入生向け IT オリエンテーション資料 > 情報システムの利用について > P18  
<https://cp.aim.aoyama.ac.jp/lms/lginLgir/index?target=b7MI9mGN>
- パスワードは紙に書いたりせずに管理する
- 親族、友人、学外者を問わず人に教えたり、人から借りたりしない
- パスワードを入力するときは他人に見られないようにする。また、人がパスワードを入力しているときは見ないようにする
- 複数のサービスで同じパスワードを使いまわさない

## 2) フィッシングサイトへの注意

銀行・クレジットカード会社・公的機関などからの重要な通知は、通常はメールではなく書面で行われます。重要と思われる通知がメールで届いた場合は、メール本文中の URL にアクセスするのではなく、検索や電話や窓口へ直接出向くなど別の手段で確認するようにしましょう。個人情報やクレジットカード番号等の入力を促す電子メールには注意しましょう。

## 3) コンピュータウイルスへの対策

インターネットには多くのウイルスが蔓延しており、無防備な PC は数分インターネットにアクセスしただけで、何らかのウイルスに感染すると言われています。以下のような対策が効果的です。自分の パソコン は必ずウイルス対策をするようにしましょう。

- ウィルス対策ソフトのインストール、アップデートを行う
- OS やアプリケーションソフトのアップデートを行う
- ダウンロードするファイルやメールの添付ファイルに対して注意し不審なファイルは開かない
- データのバックアップを定期的に行う

また感染が疑われる場合には、LAN ケーブルを抜く、無線 LAN を切断するなどして、ネットワークから切り離してください。

(参考) ウィルス感染の対処について

<https://www.aim.aoyama.ac.jp/security/virus-infect/>

以上