新宿キャンパス　八王子キャンパス　附属中学校・高等学校

学園生活と情報セキュリティ

Information Security for School Life

工学院大学
KOGAKUIN UNIVERSITY

はじめに

皆さんの学生生活では、情報機器（パソコン、タブレット、スマートフォン等）や情報サービス・システム（ホームページ、KUPORT、メール等）を利用する機会がたくさんあります。これらは非常に便利ですが、皆さんが利用方法を一歩間違うとトラブルや事件に巻き込まれたり、逆に自分自身が攻撃側となり周囲に迷惑をかけたりする可能性もあります。

このようなトラブルを防ぎ、正しく情報機器やシステムを使える状態のことを、情報セキュリティが守られている状態と言います。

情報セキュリティを守るためには、技術的な対応も必要ですが、もう一つ必要なのは、利用者の意識です。利用者である皆さん一人ひとりの日常の注意とマナーによって、情報機器や情報サービス・システムを活用して、充実した学園生活を送りましょう。

ルールを遵守すること

皆さんが大学で情報機器や情報サービス・システムを利用する際には、学内のルールを必ず守らなくてはなりません。情報機器やシステムの利用に関する学内のルールとしては、学則や情報科学研究教育センターの演習室利用規約などがあります。加えて、授業や研究活動などで利用する際には、必ず担当の教職員の指示を遵守しましょう。
また、学外・学内に関わらず、やってはいけないことが法律で決められています。例えば、無断で情報をコピーしたり（著作権法違反）、他人に成りすましてアクセスしたり（不正アクセス禁止法違反）するようなことはしてはいけません。
このようなルールや法律については、「知らなかった」では済まされません。最悪、処分を受ける可能性もあります。

情報セキュリティ対策を実施しましょう

皆さんが、学内の情報機器や情報サービス・システムを利用する場合、または、自分の機器を学内ネットワークに接続して利用する場合には、情報セキュリティ対策を必ず実施しましょう。

◆情報セキュリティ対策の具体例

①情報機器にセキュリティ対策ソフトを導入しましょう

皆さんが個人所有や研究室所有の情報機器を利用する場合には、必ずセキュリティ対策ソフト（情報機器に侵入・感染しようとする有害ソフトウェアを検出・駆除する機能をもったソフト）を導入しましょう。
セキュリティ対策ソフトを導入していないと、情報機器は、いわゆるコンピュータウイルスのような有害ソフトウェアに感染させられてしまうことがあります。
その結果、有害ソフトウェアによって、情報機器内のデータを破壊されたり、重要な情報を不正に取得されたりする等、様々な被害を受けることになります。また、周囲に対する攻撃に利用され、意図せず不正行為に加担してしまうことがあります。

◆情報セキュリティ対策の具体例【続き】

②情報機器のOSやソフトウェアを随時更新し、最新の状態を保つようにしましょう

皆さんが利用している情報機器に関連する OS やアプリケーションソフトウェアの更新やパッチ配布があった場合には、速やかに適用しましょう。
このような更新やパッチは、該当のプログラムの不具合を修正するもので、それを放置しておくことは、その不具合を利用した有害ソフトウェアの感染の可能性が高いまま放置しておくことなります。

③パスワードやIDを設定し、適切に管理しましょう

必要に応じて、皆さんが利用する情報機器や情報サービス・システムには、パスワードを設定しましょう。そして、その ID やパスワードは他者に知られないように管理しましょう。
ID やパスワードを他者に知られると、皆さんが知らないところで、不正に情報機器や情報サービス･システムにアクセスされ、自分になりすまされる可能性があります。
このため、皆さんには、ID やパスワードを厳正に管理することが求められているのと同時に、自分の都合でその ID やパスワードを他者に教えることも禁止されています。
学内のルールによると、演習室のパソコンに友人の ID でログインして使用したり、自分の KUPORT を友人に使用させたりする等の場合には、処分の対象となります。

④疑わしい対象へはアクセスしないように注意しましょう

疑わしい対象へのアクセス（セキュリティが担保されていないと考えられるサイトへ接続する、不審なメールの URL をクリックする、内容の分からない添付ファイルをクリックする 等）しないようにしましょう。
有害ソフトウェアの感染や、個人情報やパスワードの不正取得については、殆どの場合、不正なファイルをクリックしたり、不正なサイトへ接続したりすることによって、発生していますので、十分に注意をしてください。

⑤情報機器の盗難や紛失を防ぐため、対策を講じましょう

残念ながら、学内でも情報機器の盗難事案が発生しています。また、情報機器をうっかり紛失して他者に利用されてしまったという事案もあります。情報機器は、必ず自分自身で管理しましょう。

⑥情報の不用意な開示・発信は避けましょう

個人情報や認証情報（ID・パスワード等）は、信頼できる相手のみに開示しましょう。
例えば、疑わしいサイトに皆さんの住所・氏名・電話番号等を入力することは危険です。ID/ パスワードについても、いつもの入力画面と違う（画面のデザインが違う。画面の URL が違う　等）場合には、偽装サイトの可能性もありますので、入力は一旦思いとどまり、URL を確認する、企業の公式ホームページからやり直す等の対応が必要です。
また､SNS で個人が特定できるような情報を書き込むことも避けた方がいいでしょう。もちろん､皆さん自身の情報だけでなく､友人や周囲の情報についても同じです。不用意な書き込みよって、自分だけでなく、周囲の人にも危害が発生する可能性があります。

⑦公衆無線LANの使用には注意を払いましょう

公衆無線LANは非常に便利な仕組みですが､セキュリティ対策が十分でない場合もあります。通信が暗号化されていないため､他者によって通信中の情報が傍受されてしまう場合もあります。皆さんが公衆無線 LAN を使用する際には、大切な情報は取り扱わないように注意を払いましょう。

ソフトウェアライセンスや著作権を順守しましょう

海賊版や違法コピーされたソフトウェアは、著作権の侵害やソフトウェアライセンス使用許諾等のルールに違反しているものです。従って、「個人で使用するから」「商用目的ではないから」という勝手な理屈で利用することはできません。このような違法行為は、絶対に行ってはいけません。
ソフトウェアに限らず、映画や音楽、各種の情報等のコンテンツも著作権で守られているものが多く、これらをネットに無断でアップすること自体、違法であることは知っていると思います。さらに、そのようなものをたまたまネットで見つけ、軽い気持ちでダウンロードすることも著作権法上の違法行為となり、処罰されることになります。

◆おかしいな？と思ったら（連絡・相談先）

情報セキュリティインシデント通報窓口（Point of Contact / 略称 PoC）
poc@kogakuin.ac.jp

皆さんが情報機器や情報システムを利用する上で、情報セキュリティ上の問題が発生した場合には、学園の情報セキュリティインシデント通報窓口へ連絡して下さい。
また、周囲で情報セキュリティ上「おかしいな」「気になるな」というできごとを目撃・発見した場合にも、ぜひ窓口へ連絡して下さい。