

静岡県立大学情報ネットワーク利用上の遵守事項ガイドライン（学生向け）

本学の情報ネットワークを利用するに当たっては、必ず、「静岡県立大学情報ネットワーク利用規程（以下「利用規程」という。）」とこのガイドラインを熟読し、利用規程を遵守することに同意の上、適正にネットワークを利用してください。ネットワークを利用する者がその管理責任を負うことになります。

また、このガイドラインは、「静岡県立大学情報ネットワーク利用規程」第6条に定める遵守事項やインターネット等の利用上の注意について、事例を示し、わかりやすく説明するものです。ガイドラインを十分に理解し、静岡県立大学の一員としてネットワークの良識ある利用を心がけてください。

学内ネットワークを利用するには（接続する端末について）

- ・ウイルス対策（セキュリティソフトのインストール等）を行っていること。
- ・OS（Windows、macOS等）やソフトウェア（Microsoft Edge、Google Chrome、Zoom、Acrobat Reader等）のアップデートを行っていること。

※持込PC（タブレット等を含む）を使用する際は、原則、学内無線LANへ接続してください。
有線LAN利用については、教職員の許可なく接続することは認められません。

1 利用の目的（利用規程第3条）

「①教育」、「②研究」、「③大学事務」、「④図書館事務及び図書検索」のために利用する他、「⑤その他学長が認めたもの」以外の目的の利用を禁止しています（遵守事項：利用規程第6条第1号）。まずこれが、一般のプロバイダ等でのネットワーク利用とは異なるところです。

例えば、本学ネットワークを利用して次のようなことを行う場合は、目的外利用に当たりますので、注意しましょう。

- ・本学のメールアドレスを利用したネットショップやネットオークション等の利用
- ・オンラインゲームの利用
- ・出会い系サイト等の不適切なサービスの利用
- ・個人用途における楽曲や画像、動画ファイル、商用ソフトウェアのダウンロードやアップロード
- ・ネットショッピングサイト開設等、営利目的の活動や商業活動
- ・政治や宗教活動
- ・ギャンブル等の賭博行為

この他、ネットワーク上の迷惑行為、例えば商業的な広告宣伝の目的で不特定多数の人に電子メールを送りつける行為等も許されません。

2 不正行為

(1) ユーザ ID 及びパスワードの貸与、販売、譲渡等

学内システム（ユニバーサルパスポートや学内情報ポータルサイト等）は、ID とパスワードによる認証を前提として運用されています。ID とパスワードの貸借は、その詐称行為に相当し、ネットワーク及びネットワークで接続されているシステムの適正かつ正常な運用を妨げる不正行為です。貸した人も借りた人も不正利用となります。他者へのなりすましと何ら変わりはありません。

(2) ユーザ ID やパスワードは、各自が責任を持って管理すること

悪意のある人に ID やパスワードを知られた場合、不正利用が行われ、情報の漏えい等の大きな問題に発展することもあり得ます。自分が被害を受けるばかりでなく、自分を踏み台にして被害を拡散・拡大させることもあります。

パスワードは定期的に変更し、数字だけの組み合わせや名前等、解読されやすいものをパスワードとして使用することのないようにして、適切に管理しましょう。

(3) 本学が所有又は管理する情報ネットワークやコンピュータのシステムを変更しないこと

システムを勝手に書き換えたり壊したりすることは犯罪にもなりかねません。本学所有のシステムに限られたことではなく、他の大学や機関、企業等のシステムを変更することも同様です。

(4) 本学が所有又は管理するソフトウェアを複製しないこと

安易にコピーやダウンロードすると、著作権や特許権等知的所有権の侵害に当たりますので、注意しましょう。このことについても、本学所有のソフトウェアに限られたことではなく、他の大学や機関、企業等のソフトウェアを複製することも同様です。

(5) 情報ネットワーク管理・運営に重大な支障を与える行為をしないこと

他の利用者の存在やシステムの負荷を考慮せず、自分の都合だけで大量の電子メールを送受信することもシステムの円滑な利用を阻害します。

また、目的に関わらず、ファイル共有ソフトの使用は禁止しています。

(6) 情報ネットワークを利用して第三者に迷惑又は損害を与える行為をしないこと

- ・通信の秘密とプライバシー、個人情報の保護

無断で他人のメールの内容を見る、本人の承諾を得ないまま電子メールの内容を他人に知らせること。また、メール等のやり取りの中で知り得た個人情報を許可なく公開することは許されるものではありません。

- ・ネットワーク上での誹謗中傷や名誉毀損行為、感情にまかせた個人攻撃や差別行為、ストーカー行為やセクハラ行為等も、決して許されるものではありません。

ネットワークの世界と言っても、一般の社会、その中の人間関係と全く同じなのです。

- ・公序良俗に反するわいせつな画像や文章をホームページに掲載する等の行為。

(7) コンピュータウイルス対策等のセキュリティ保持に責任を持って努めること

学内ネットワークは多数のユーザが利用しているものであり、たった一人の不注意等によることから、様々な脅威となる影響を広範囲にばらまくことが考えられます。セキュリティ対策を実施していないパソコン等によって、他の学内ユーザのパソコン等にウイルスの感染が広まり学内ネットワークに障害を招いたり、個人情報の流出や不正ユーザの踏み

台にされ学外のネットワークに不正接続をする等の被害の可能性があります。

また、「出所不明のプログラムや電子メールの転送」、「知らない人から送られてきた添付ファイルを安易に開くこと」は、とても危険なことです。

このようなことから、以下の項目については、基本的なセキュリティ対策として、常にチェックをしてください。

前段でも記述しましたが、本学ネットワークを利用する上での最低条件です。

【重要】

- ・ウイルス対策ソフトをインストールし、定義ファイルを最新に保つこと。
- ・OS (Windows、macOS 等) やソフトウェア (Microsoft Edge、Google Chrome、Zoom、Acrobat Reader 等) のアップデートを行うこと。
- ・パスワードは定期的に変更し、簡単なパスワードを使用しない等、管理を徹底すること。

ネットワークが安全かつ円滑に機能し、運営されるためには、利用するユーザがルールを遵守し、使用するパソコン等が安全に保たれていることが不可欠です。

それが、(5)や(6)を未然に防止することにもつながっていきます。

3 遵守事項違反行為に対する措置

利用規程の遵守事項を守らない利用者に対しては、利用登録の取り消しや一定期間の利用停止といった措置を取ることがあります。

このような措置が取られた場合、措置が解除されるまでの間は、本学のネットワークを利用することができません。その結果、これらの措置を受けた場合は、次のような大変な状況に陥ってしまいます。

- ・学務情報システム（ユニバーサルパスポート）を利用できなくなり、履修登録やレポート提出を Web 上で実施できない。
- ・講義に必要な課題や資料を Web 上で受け取ることができない。
- ・大学の電子メールを利用できない。
- ・講義や研究等で必要な場合であっても、学内のネットワークへ接続できない。
- ・実習室に設置しているパソコンを利用できない。
- ・図書館の情報検索用パソコンを利用できない。
- ・学内の無線 LAN (Wi-Fi) を利用できない。

※このようなことにならないよう、大学の情報ネットワーク・システムを利用する上でのルールを守り、有効に活用しましょう。