こういうことは…情報倫理違反です

The Following Activities Violate Information Ethics:

ファイル交換ソフトウェアで違法に配信されていた映画や音楽ファイルを、ダウンロードするだけなら大して悪くないと思って、自分もダウンロードした。
Downloading film or music files that have been transmitted illegally by file-sharing software even if you thought the illegality of downloading itself was insignificant.

(2010 年 1 月から、こうしたダウンロードも著作権法違反です)
(Such downloading has become illegal under the Copyright Law since January 2010)

全員の了承を得ることなく、住所の入ったクラス名簿をホームページで一般公開した。
Making public on a homepage a class list including addresses without obtaining prior consent from each individual listed.

インターネット掲示板に他人を脅すような文句を書いた。
Posting intimidating or threatening contents on an Internet bulletin board.

パスワードを紙に書いてコンピュータの画面の脇に貼っている。
Writing your password on a piece of paper attached to the side of your computer display.

電子ジャーナルやデータベースの利用契約で禁じられているのに、大量に資料をダウンロードした。
Even though it is prohibited by contract, downloading large quantities of material from electronic journals or databases.

インターネットで見つけた他人の文章の全部または一部を、出典を明示することなく流用して，授業の自分のレポートとして提出した。
Handing in a document containing the whole or a part of another person's file that you found on the Internet as your own report for a class, without citing the source.

面倒なので、コンピュータにウィルス対策ソフトウェアをインストールしていない。
Virus checking is tiresome, so your computer is not protected by antivirus software.

情報倫理・コンピュータ利用ガイドライン

Guidelines for Information Ethics and Computer Use

情報ネットワークとコンピュータを適切・安全に利用するために

Using the University Information Network and Computers in a Safe and Proper Manner

発行者　Issued by

東京大学情報倫理委員会
(Committee for Information Ethics, The University of Tokyo)
http://www.cie.u-tokyo.ac.jp/
office@cie.u-tokyo.ac.jp

東京大学情報システム緊急対応チーム
(University of Tokyo Computer Emergency Response Team)
http://park.itc.u-tokyo.ac.jp/ut-cert/
ut-cert@nc.u-tokyo.ac.jp

関連規則・情報　Related Rules and Infomation

東京大学情報倫理規則
(University of Tokyo Rules Pertaining to Information Ethics)
東京大学情報倫理運用規程
(University of Tokyo Operational Rules Pertaining to Information Ethics)
http://www.cie.u-tokyo.ac.jp/

東京大学情報ネットワークシステム運用規則
(University of Tokyo Rules Pertaining to the Operation of the Information Network System)
東京大学情報ネットワークシステム利用ガイドライン
(University of Tokyo Guidelines for Use of the Information Network System)
https://www.nc.u-tokyo.ac.jp/

電子ジャーナル
(Electronic journals to which The University of Tokyo subscribes)
http://ejournal.dl.itc.u-tokyo.ac.jp/

学内の計算機資源（情報ネットワークとコンピュータ等）の利用に当たっては、以下の点に注意を払い、利用者としての自覚と責任を持って行動して下さい。これらに違反した場合、注意や処罰の対象になります。

①教育・研究目的に限定

学内の計算機資源の利用は、教育・研究に関する目的に限定されています。この目的に沿わない不適切な行為、違法行為、倫理に反する行為を禁じます。

②不適切な情報発信の禁止

学内の計算機資源から、以下のような情報を発信することは禁止されています。

(1) 本名以外による情報
(2) 知的財産権・肖像権を侵害する情報
(3) 差別・誹謗中傷にあたる情報
(4) プライバシーを侵害する情報
(5) わいせつな情報
(6) 教育・研究を妨害する情報
(7) 他者の業務・作業を妨害する情報
(8) 虚偽情報
(9) 守秘義務のある情報

③違法コピーの禁止・違法コンテンツのダウンロード禁止

音楽、映像、本、ソフトウェアなどの著作物を、違法にコピーして配布したり、ライセンス規約を守らずに利用してはいけません。これらを、P2P 型ファイル共有ソフトウェア等を用いて、見知らぬ他人に配布できる状態にすることは違法です。また、著作権法改正により、2010 年 1 月から、違法に配信されている音楽・映像コンテンツを、それと知りながらダウンロードすることも違法となりました。P2P型ファイル共有ソフトウェアは教育・研究上どうしても必要である場合以外は使用しないようにしましょう。本学では違法行為や不適切な利用の可能性がある通信を監視しており、疑わしい場合は調査しています。

④大量ダウンロードの禁止

学内から「自由に」使って良いように見えるサービスでも、東京大学とサービス提供元との間で利用条件が定められているのが普通です。例えば、多くの電子ジャーナルやデータベースでは、コンピュータプログラムなどを利用して一度に大量のコンテンツをダウンロードすることは禁じられています。利用条件を守らない者がいると、東京大学全体に対するサービスが停止される可能性がありますので注意して下さい。

⑤アカウントの盗用・貸与の禁止

パスワードを推測するなどして、他人のアカウントを盗用することは犯罪となります。また、全ての利用者には、自分が保持するアカウント、パスワード、情報機器、ソフトウェア等を安全に管理する義務があります。他人に自分のアカウントやコンピュータを悪用されると、所有者自身が困るだけでなく、見知らぬ第三者や大学全体に迷惑がかかります。また、自分の代わ

When using the University computer resources (information network and computers), be sure to follow these guidelines. Everyone should be a responsible user. Breaking the rules will lead to warnings or disciplinary action.

① Use Limited to Educational and Research Purposes

The use of the University computer resources is limited to educational and research purposes only. Any and all use of the University computer resources for inappropriate, illegal or unlawful, and/or unethical purposes is strictly prohibited.

② Limitations on Information Transmission

University computer resources users are prohibited from sending information that . . .

(1) is not sent under your own name,
(2) infringes on the intellectual property rights of others,
(3) is discriminatory, slanderous, or libelous,
(4) infringes on the privacy of others,
(5) is obscene,
(6) disrupts education or research,
(7) disrupts the work of any individual,
(8) is false, and
(9) is confidential.

③ Illegal Copying and Downloading is Prohibited

Users are prohibited from reproducing or distributing copyrighted materials (such as music, movies, books, or software) in an illegal manner; and you must not infringe on their licenses. Making such data accessible to a third party by P2P (Peer-to-Peer) file-sharing software or other similar means is illegal. In addition, even downloading illegally distributed music or movies has become illegal since January 2010, if you are aware that such distribution is illegal. P2P file-sharing software may be used only when it is absolutely necessary for educational or research purposes. The University monitors for possible illegal or inappropriate uses, and investigates suspicious cases.

④ Excessive Access and Downloading is Prohibited

Some electronic services may appear to be free on campus, but usually there are usage-limit agreements between the University and the providers. For example, excessive access by using computer programs or downloading tools are prohibited by most electronic journals or databases. If a person violates such agreements, the service may be terminated for the entire University, so be careful on the manner.

⑤ Stealing an Account and Letting Someone Else Use Your Account is Prohibited

Stealing computer system accounts by guessing or decoding passwords is a criminal offense. All users shall be held accountable and must assume full responsibility for their own computers, system accounts, passwords, memory devices, software, etc. Misuse of your computer or system account by a third party will inconvenience you, others, and the University as a whole. And never let anyone use your system account for any reason whatsoever such as asking somebody else to submit a report or to do partial work on your behalf.

⑥ Protect Your Password

Easy-to-guess passwords lead to computer abuse. Avoid passwords that are easy to guess, those created from names, words, only numbers, birthdates, and/or the combinations thereof. Passwords based on keyboard layouts or short in nature should be avoided as well. Choose a combination of letters (a mixture of upper and lower cases), numerals, and special characters; and ensure that your passwords represent a random combination. Memorize your passwords and closely guard any written records of passwords.

⑦ Be Cautious about Loss or Theft of Your Information Assets

Strict care must be taken at all times concerning loss or theft of your laptops, hard disk drives, USB memory sticks, or any memory devices that contain important information. Thefts occur even on the University campus particularly in classrooms, cafeterias, and other public areas accessible to everyone. In the event that you should lose an item which contains a system account or a password, you should report this to your System Administrator immediately.

⑧ Antivirus Software is Mandatory

Antivirus software must be installed on all computers. Ensure that the automatic updating of your antivirus software is functioning properly, thereby keeping your virus definition files current; and routinely scan all files on your computers. One major means of virus infection is exchanging files via memory devices such as USB memory sticks, as well as file exchanging over networks. Before you use a device or a media that is not yours, run a virus scan on it immediately. Some operating systems have default features that automatically run programs or open files in CD-ROMs or USB memory sticks upon connection, but these should be disabled.

Antivirus software is available at a very low price through the University. Licenses are distributed by the Information Technology Center to departments and laboratories, and to every unit within the University. Please consult the person in charge of your unit for a license.

⑨ Keep Your Software Updated

Always keep your OS and software updated. Be sure to enable automatic update functions. Computer virus infections and other security problems develop easily with old versions of software. In addition, please refrain from using unsupported software because security fix patches are generally unavailable.

⑩ Turn off Your Computer during Long Absences

If you plan not to use your computer for a long period of time such as consecutive holidays or business trips, turn it off for energy-saving reasons and to prevent computer security risks. When you return, be sure to update your software and virus definition files before using them.

⑪ In Case You Get a Warning

When professors, staff, or system administrators warn you of inappropriate use of the University computer resources, you must follow their instructions immediately. Continued use of computers infected by viruses or any and all other inappropriate use of computers is strictly prohibited.

りにレポートを提出してもらう、または業務を一時的に代行してもらうなどの目的で、自分のアカウントを他人に貸与することは決してしないで下さい。

⑥簡単なパスワードを使用しない

コンピュータが悪用される原因のひとつはパスワードが推測されてしまうことです。特に危険なものは、名称、単語、数、それらの組み合わせ、キーボードの配列、短いものなどです。アルファベット大文字、小文字、数字などを組み合わせた意味のない文字列を利用して下さい。パスワードは記憶するか、それができない場合は他人に盗まれない工夫をして厳重に保管して下さい。

⑦情報機器の盗難や紛失に注意

ノートパソコン、ハードディスク、USBメモリなど、重要な情報が入った情報機器の紛失と盗難に注意して下さい。盗難による被害は学内でも数多く発生しています。教室や食堂など不特定多数が出入りする場所は特に危険です。学内システムのアカウントやパスワードが入った情報機器を失った場合、速やかにその発行元に連絡して下さい。

⑧ウィルス対策の徹底

全てのマシンにウィルス対策ソフトウェアをインストールして下さい。ソフトウェアを導入したら、ウィルスのパターンファイルを自動更新して最新版に保ち、定期的にコンピュータ内の全ファイルにウィルスチェックを行って下さい。ネットワークのほか、USBメモリなどの物理メディアによる情報の受け渡しも重大な感染経路です。他人から渡された「何か」をマシンに接続したら、最初にウィルスチェックを行って下さい。オペレーティングシステムには、CD-ROM やUSBメモリなどの挿入時に中身を自動再生する機能がありますが、設定によりオフにして下さい。

なお、学内ではウィルス対策ソフトウェアが非常に安価に利用できます。ソフトウェアライセンスは情報基盤センターから各組織（部局や研究室など）に配布されています。利用者は自分が所属する組織からライセンスを入手してください。

⑨ソフトウェアを最新の状態に

オペレーティングシステムやアプリケーションは常に最新版にアップデートして下さい。自動更新ができるソフトウェアは、その機能をオンにして下さい。最新でないソフトウェアを利用していると、ウィルス感染等のセキュリティ問題が容易に発生します。また、製造者のサポートが切れたソフトウェアは、セキュリティ問題が発見されても修正されないため使用を控えて下さい。

⑩長期間不在にする場合は端末の電源をオフにする

長期休暇や出張などにより数日間以上コンピュータを利用しない場合、セキュリティならびに省エネの観点から、必ず電源をオフにして下さい。再び利用する場合、作業を開始する前にソフトウェアやウィルス対策ソフトウェアのパターンファイルを最新版に更新して下さい。

⑪もしも注意を受けたら

教職員やシステム管理者から注意や指示を受けた場合、その内容に速やかに従って下さい。ウィルスに感染したままコンピュータを利用し続けたり、不適切な利用を継続してはいけません。