The University of Tokyo Computer Use Guidelines

Using the University information network and computers in a safe and proper manner

University of Tokyo Computer Emergency Response Team

http://park.itc.u-tokyo.ac.jp/ut-cert/
ut-cert@nc.u-tokyo.ac.jp

2009.4
10,000

東京大学コンピュータ利用ガイドライン

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

東京大学情報システム緊急対応チーム

http://park.itc.u-tokyo.ac.jp/ut-cert/
ut-cert@nc.u-tokyo.ac.jp

学内の情報ネットワークとコンピュータは、教育と研究を目的としています。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。例えば、不適切なウェブサイトの閲覧、不適切な情報の発信、著作権の侵害、悪戯、いやがらせ、不正アクセスなどは注意や処罰の対象になります。また、すべての利用者には、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。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ください。

①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ください。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ください。

②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ください。パスワードは記憶するか、それが出来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ください。

③ソフトウェアをアップデート

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ください。自動更新が出来るソフトウェアは、その機能をオンにしてください。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ください。

④ウィルス対策

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ください。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ください。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ください。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ください。

The purpose of the information network and computers in the University of Tokyo is for educational, research, and administrative use only. Any and all use of the University information network and computers for inappropriate, illegal or unlawful, and/or unethical acts is strictly prohibited. Accessing inappropriate websites, sending out unsuitable information, violating copyright privacies, causing annoyance or any other form of harassment, and accessing networks and computers illegally will lead to warnings or disciplinary action. All users will be held accountable and must assume full responsibility for their own computers, system accounts, passwords, memory devices, software, and etc. Misuse of your computers or system accounts by a third party will inconvenience you, others, and the University as a whole. Be sure to follow these guidelines, and act as a responsible user.

(1) Be cautious about misplacing or theft of your information assets

Strict care must be taken at all time concerning misplacing or theft of your laptops, hard disk drives, USB memory sticks, or any memory devices that include 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 includes a system account or a password, you should report this to your Network Administrator immediately.

(2) Guard your password

Intuitive passwords lead to computer abuse. Avoid passwords that are easy to guess, those created from names, words, digits, and/or their combinations. 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 or closely-guard any written records of them.

(3) Keep your software updated

Always keep your OS and software current. 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.

(4) Measures for computer viruses

Antivirus software must be installed on all computers. Ensure that the automatic updating of your antivirus software is functioning properly, thereby keep your virus definition file 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 companion features that run programs or open files in CD-ROMs or USB memory sticks automatically upon connection, but these should be disabled.

Antivirus software is available at a very low price for University property. The Licenses are distributed by the Information Technology Center to departments and laboratories, and to every unit within the University. Please consult the unit that you belong to for a license.

(5) Turn off your computers during long absences

Turn off your computers if you anticipate not using them for a long period of time such as consecutive holidays, graduation, business trips, and other similar reasons. When you return, ensure that your software and virus definition files are current before using them.

(6) Inappropriate file sharing is strictly prohibited

Using file sharing programs to share music, movies, books, software, and other copyrighted data with a third party is illegal. Regarding a P2P file sharing program, you must take cautionary measures about the data you download, because such programs generally enable or cause unintentional or inadvertent transmission of messages or files. Moreover, inappropriate file sharing may possibly cause virus infections and information leaks. Nowadays illegal copying and security fears caused by file sharing have become social problems. The university monitors network use in the event of possible illegal or inappropriate use, and investigates suspicious cases.

(7) Excessive access or downloading is prohibited

Excessive access or downloading of online journals or databases that breach terms of service is prohibited. Particularly, excessive access to a database using downloading tools that consume an unreasonable amount of network or computer resources inconveniences other users, and may lead to disciplinary action.

(8) In case you are warned

When professors, staff, or network administrators warn you of inappropriate use of the University network or computers, 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.

Related WWW sites

University of Tokyo Computer Emergency Response Team
http://park.itc.u-tokyo.ac.jp/ut-cert/

University of Tokyo Rules Pertaining to Information Ethics
http://www.cie.u-tokyo.ac.jp/

Electronic Journals University of Tokyo subscribes to
http://ejournal.dl.itc.u-tokyo.ac.jp/

Copyright Research and Information Center
http://www.cric.or.jp/

なお、学内ではウィルス対策ソフト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。

⑤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、卒業、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、必ず電源をオフにしてください。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ください。

⑥不適切なファイル共有は厳禁

音楽、映像、本、ソフトウェアなどの著作権が存在するデータ（著作物）を、P2P型ファイル共有ソフトウェア等により見知らぬ他人がダウンロードできる状態にすることは違法です。多くのP2P型ファイル共有ソフトウェアでは、データをダウンロードした端末が自動的にそのデータの発信者になるため、ダウンロードするにも注意が必要です。また、不適切な共有はウィルス感染や情報漏洩の危険性も高めます。著作物の違法コピーや、ファイル共有による情報セキュリティの低下は社会問題になっています。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。

⑦大量ダウンロードの禁止

電子ジャーナルやデータベースの利用にあたり、利用規約に違反するような大量のダウンロードを行わないでください。特に、ダウンロードプログラム等を利用して集中的にデータベースにアクセスすると、ほかの利用者の迷惑になり、違反者はサービスを利用できなくなる可能性があります。

⑧もしも注意を受けたら

教職員やネットワーク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ください。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。

関連情報（Related WWW sites）

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/

東京大学情報倫理ガイドライン
（University of Tokyo Rules Pertaining to Information Ethics）
http://www.cie.u-tokyo.ac.jp/

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

著作権情報センター
（Copyright Research and Information Center）
http://www.cric.or.jp