情報倫理・コンピュータ利用ガイドライン

本学の計算機資源(情報ネットワークとコンピュータ等)の利用に当たって、注意を払い、利用者として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。また、学外活動や私生活においても、本学の学生や教職員として良識と節度ある行動をお願いします。

言語選択
日本語P2

情報倫理・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

Please select your language.
English P4

Guidelines for Information Ethics and Computer Use

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

请选择语言
簡体字P6

信息伦理及计算机利用指南

正确、安全地利用信息网络和计算机　*原文为日文。

언어를 선택해 주세요
한국어 P8

정보윤리・컴퓨터 이용 가이드라인

정보 네트워크와 컴퓨터를 적절하고 안전하게 이용하기 위하여 *원본은 일본어입니다.

言語を選んでください。

2019.3

P2 日本語
P4 English
P6 簡体字
P8 한국어

東京大学　情報倫理・コンピュータ利用ガイドライン

本学の計算機資源（情報ネットワークとコンピュータ等）の利用に当たって、以下の点に注意を払い、利用者として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。また、学外活動や私生活においても、本学の学生や教職員として良識と節度ある行動をお願いします。

①教育・研究目的に限定

本学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・公開の禁止

本学の計算機資源から、以下のような情報を発信または公開することは禁止されています。

(1) 本名以外（匿名・偽名）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) 虚偽の情報
(9) 守秘義務違反にあたる情報

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、他人に配布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**注意が必要です。また、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は違法であり、**刑事罰の対象**となる場合もあります。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。

④大量ダウンロードの禁止

本学から「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。また、**パスワードは使い回しをせず**、システムやソフトウェアごとに使い分けて、慎重な管理に努めて下さい。

⑦情報機器の盗難や紛失に注意

ノートパソコン、スマートフォン、タブレット、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。盗難による被害は本学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。本学の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ウイルス対策の徹底

全てのコンピュータでは、適切なウイルス対策をして下さい。本学では、ウイルス対策ソフトのライセンスが情報基盤センターから各組織（部局や研究室など）に有償配布されています。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。ウイルスのパターンファイルは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のウイルスチェックを行って下さい。しかし、ウイルス対策ソフトを導入しても、それだけで全てのウイルスを完全に防げるわけではありません。安心せずに常に感染の危険を避けることを心がけてください。USBメモリなどをコンピュータに接続した際には、最初にウイルスチェックを行って下さい。学内連絡や取材申し込みなど、**正当な内容を装った悪意のあるウイルスメール**が増えています（標的型攻撃）。メールの添付ファイルやメール本文の外部リンクから、ウイルスに侵入されないよう注意して下さい。

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、ウイ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イ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下さい。ウイ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。本学では、通信内容に情報セキュリティ上の問題がないかについて、機械的な検知や遮断を行うことがあります。

こういうことは…情報倫理違反です。

★友人に勧められてP2P型ファイル共有ソフトウェアをインストールしたら、売られているはずの音楽や映画の海賊版を発見し、怪しいと思いつつダウンロードした（2012年10月から、こうしたダウンロードは**刑事罰**の対象となりました）。
★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。本人から了承を得ずに、ブログに他人の顔写真を掲載した（不適切な情報発信の禁止：プライバシーを侵害する情報）。
★ツイッターやインターネット掲示板に他人の誹謗中傷や、差別的な書き込みをした（不適切な情報発信の禁止：差別・誹謗中傷にあたる情報）。
★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。
★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。
★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。

P2日本語
P4 English
P6簡体字
P8 한국어

UTokyo Guidelines for Information Ethics and Computer Use

When using the University's 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 actions. Furthermore, we would request that as students or members of staff of the University you will act with common sense and moderation even in activities outside of the University and in private life.

①Use Limited to Educational and Research Purposes

The use of the University's 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.

②Prohibition on Transmission or Release of Information

Users of the University 's network and computer resources are prohibited from sending or releasing information that:
(1)is not sent under your own name (sending anonymously or using aliases),
(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, or (9) violates confidentiality.

③Illegal Copying and Downloading

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. Care needs to be taken when using P2P file sharing software to download data, as many of these types of software will **automatically make the terminal that downloaded the data its originator**. In addition, knowingly downloading illegally distributed music or movies is unlawful and **subject to criminal punishment**. P2P file-sharing software may be used only when it is absolutely necessary for educational or research purposes.

④Excessive Access and/or Downloading is Prohibited

It may appear that some electronic services may be "freely used" within the University, but usually there are usage-limit agreements between the University and the providers. For example, excessive accesses 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 in this respect.

⑤Stealing an Account or Letting Someone Else Use Your Account

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.

⑥Protect Your Passwords

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. Also please maintain a high sense of security by **using different passwords for each system or software rather than using the same password for all.**

⑦Be Cautious about Loss or Theft of Your Information Assets

Strict care must be taken at all times concerning loss or theft of your laptops, smartphone, tablet terminal, hard disk drives, USB memory sticks, or any memory devices that contain important information. Thefts have occurred even within the University, particularly in classrooms, cafeterias, and other public areas accessible to everyone. In the event that you should lose an item that contains accounts or passwords for the University's system, you should report this to your Network Administrator immediately.

⑧Use of antivirus software is mandatory

Take appropriate anti-virus measures on all computers. The University distributes antivirus software licenses for a fee through the Information Technology Center to all departments, laboratories, and units within the University. Please consult the person in charge of your section for a license. The automatic update function of your antivirus software must be set correctly in order to keep the virus definition files current. Similarly all files on your computers must be routinely scanned. However, even if antivirus software is installed, that alone is not sufficient to fully prevent all viruses. Therefore, do not feel too complacent, and always try to avoid the risk of infection. If USB memory devices or other devices are being connected to your computer, make sure to run a virus scan on it immediately.
There has been an increase in **emails with malicious viruses made to look like legitimate emails** (targeted attacks), such as contacts from within the University and request for interviews by the media. Please be careful so that viruses do not come in through emails attachments or external links included as part of actual email messages.

⑨Keep 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.

⑩Turn 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.

⑪In Case You Get a Warning

In the event professors, staff, or network 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. Please be aware that The University of Tokyo may carry out automatic technical checks to ensure there are no problems security-wise and may block contents of communications when necessary.

The Following Activities Violate Information Ethics:

★Having installed a P2P (peer-to-peer) file sharing software on suggestion of a friend, you found pirate copies of music and movies that are on sale. You downloaded them knowing it to be questionable (such downloads became subject to **criminal punishment** from October 2012).
★Making public on a homepage a class list including addresses without obtaining prior consent from each individual listed. Uploading photographs showing other people's faces on blogs etc. without their prior consent (prohibition of sending inappropriate information: information which infringes on privacy).
★Writing discriminatory or libelous contents on an Internet bulletin board, Twitter or other SNS sites (prohibition of sending inappropriate information: discriminatory or libelous information).
★Writing your password on a piece of paper attached to the side of your computer display.
★Even though it is prohibited by contract, downloading large quantities of material from electronic journals or databases.
★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.

P2 日本語
P4 English
P6 簡体字
P8 한국어

东京大学 信息伦理及计算机利用指南

在利用本校的计算机资源（信息网络和计算机等）时，请注意以下各项内容。作为使用者应提高认识并承担起责任。如有违反，将受到警告和处罚。并且，在校外的活动以及私人生活中，也请以作为本校的学生或教职员工的意识为基准掌握好各自行动的分寸。

①仅限于教育及研究目的

本校计算机资源的使用，**仅限于教育和研究目的**。对于违背这一目的的不正当行为、违法行为及违反伦理道德的行为均严令禁止。

②禁止发送、公开不正当信息

不得使用本校计算机资源发送或公开下列信息：
(1) 署有非真实姓名（匿名、假名）的信息
(2) 侵犯知识产权、肖像权的信息
(3) **涉及歧视、诽谤中伤的信息**
(4) 侵犯隐私权的信息
(5) 有猥亵内容的信息
(6) 妨碍教育、研究的信息
(7) 妨碍他人业务、工作的信息
(8) 虚假的信息
(9) 涉及违反保密义务的信息

③严禁非法拷贝及下载违法内容

严禁非法拷贝和公开音乐、影像、书刊、软件等著作物的行为，以及不遵守版权规定的行为。使用P2P型文件共享软件，将以上著作物等置于可以向他人传播的状态属于违法行为。由于在多数的P2P型文件共享软件下，下载了数据的终端会**自动地成为该数据的发信者**，所以需要注意。此外，在知情的情况下下载违法公开的音乐、影像内容是违法的，**可能会被处以刑罚**。除因教育和研究目的必须使用的情况外，请不要使用P2P型文件共享软件。

④严禁大量下载

本校的一些互联网服务看上去可以“自由”使用，但通常在东京大学与服务提供商之间都签订了使用规约。例如：许多电子期刊和数据库都禁止使用计算机程序等一次性大量下载数据。如果有人不能遵守使用规约，可能会停止对整个东京大学提供服务，敬请注意。

⑤不得盗用和借用帐号

通过猜测密码等盗用他人帐号属于犯罪行为。另外，所有用户对自己保有的帐号、密码、信息设备、软件等负有安全管理义务。个人的帐号和计算机被他人不当使用，不仅会给本人同时也会给不相关的第三者乃至整个大学造成困扰。此外，绝对不要出于让他人帮自己代交课业报告或临时代理业务等目的，将自己的帐号借给他人使用。

⑥不要使用过于简单的密码

计算机被他人恶意利用的一个原因是密码遭到破译。尤其危险的是，使用名字、单词、数字以及它们的组合，或者键盘上的字符排列、过短的密码等。请使用大小写字母和数字组合而成的无意义字符串做密码。请记住密码，如果记不住的话，请注意以他人无法盗取的方式妥善保管。此外，**不要重复使用密码**，针对不同系统和软件区别使用密码，谨慎地做好保管工作。

⑦防止信息设备的被盗和遗失

要注意防止笔记本电脑、智能手机、平板电脑、硬盘、USB存储设备等载有重要信息的信息设备被盗和遗失。本校已发生多起因信息设备被盗而造成严重损失的案例。尤其是教室、食堂等公共场所危险因素很多。如果丢失了带有本校计算机系统帐号及密码的信息设备，请尽快与相关发行方联系。

⑧彻底实施防病毒对策

请在所有的计算机上做好适当的防病毒措施。在校内防病毒软件的使用许可已通过信息中心有偿配发给各部门（院系、机构、研究室等）。请通过所属部门获取软件使用许可。请自动更新病毒库文件，保持最新状态，并定期扫描计算机内全部文档以防止病毒感染。但是，即使安装了防病毒软件也不能完全阻挡所有病毒。为了避免被病毒感染，在平时使用中要多加注意，不得掉以轻心。将USB存储设备等连接到计算机上时，请首先进行病毒扫描检查。进行校内联系、申请采访等**伪装成普通正常内容的恶意病毒邮**件有所增加（锁定目标攻击）。请一定注意避免通过邮件的附件、邮件正文中的外部链接遭遇病毒的入侵。

⑨使软件保持最新状态

请定时将操作系统和应用软件等升级为最新版本。对于具有自动更新功能的软件应开启该功能。使用没有更新为最新版本的软件容易发生计算机病毒感染等安全问题。同时，尽可能不要使用那些厂家技术支持服务已经过期的软件，因为这些软件即使发现安全漏洞也无法修复。

⑩长期不在时请关闭终端电源

由于休长假或出差等数日不使用计算机时，为了信息安全和节约能源，请务必关闭电源。重新使用计算机时，在开始工作之前请将应用软件及防病毒软件的病毒库文件更新为最新版。

⑪如果受到警告

在受到教职员、系统管理员的警告或得到指示时，请尽快遵从其指示。不得在计算机受到病毒感染的情况下继续使用，或持续不正当地使用计算机。请注意，东京大学会在信息安全的角度对通信内容进行技术监控，在必要的时候还会切断通信。

以下行为……都是违反信息伦理的行为。

★安装了朋友推荐的P2P型文件共享软件后，发现了本来应该是在市面上出售的音乐或者电影的盗版，虽然认为可疑，还是下载了(自2012年10月起，这种下载成为了**刑罚的对象**)。
★未经全体人员同意，在网页上公布记载有住址信息的班级名册。没有征得当事人的同意，在博客上传带有他人面容的照片（不当信息发送的禁止：侵害个人隐私的信息）。
★在微博，互联网公告板上书写诽谤中伤、歧视他人的语句(不当信息发送的禁止：歧视、诽谤中伤之类的信息）。
★把密码写在纸上并张贴在电脑画面旁边。
★尽管在电子期刊、数据库的使用协议中被明确禁止，仍然大批量地下载资料。
★把从网上找来的别人的文章，不明确标明出处地挪用全部或部分内容，当作自己的课业报告提交。

P2日本語
P4 English
P6簡体字
P8 한국어

도쿄대학 정보윤리・컴퓨터 이용 가이드라인

본교의 계산기 자원(정보 네트워크와 컴퓨터 등)을 이용할 때는 다음 사항에 주의하여 이용자로서의 자각과 책임을 가지고 행동해 주십시오. 이를 위반한 경우, 주의나 처벌의 대상이 됩니다. 또한 교외활동이나 사생활에 있어서도 본 대학의 학생 혹은 교직원으로서 모범이 되는 행동을 부탁드립니다.

①교육・연구 목적에 한정

본교의 계산기 자원의 이용은 **교육・연구에 관한 목적에 한정되어 있습니다**. 이 목적에 맞지 않는 부적절한 행위, 불법 행위, 윤리에 반하는 행위를 금합니다.

②부적절한 정보 발신・공개의 금지

본교의 계산기 자원을 통해 다음과 같은 정보를 발신 또는 공개하는 것은 금지되어 있습니다.

(1)본명 이외(익명・위명)에 의한 정보
(2)지적 재산권・초상권을 침해하는 정보
(3)**차별・비방 중상에 해당하는 정보**
(4)프라이버시를 침해하는 정보
(5)외설적인 정보
(6)교육・연구를 방해하는 정보
(7)타인의 업무・작업을 방해하는 정보
(8)허위 정보
(9)비밀유지의무위반에 해당하는 정보

③불법 복제의 금지・불법 콘텐츠의 다운로드 금지

음악, 영상, 책, 소프트웨어 등의 저작물을 불법 복사하여 배포하거나 라이센스 계약을 지키지 않고 이용해서는 안 됩니다. 이를 P2P형 파일 공유 소프트웨어 등을 사용하여, 모르는 타인에게 배포 가능한 상태로 만드는 것은 불법입니다. 대부분의 P2P프로그램의 경우, 데이터를 다운로드한 컴퓨터가 **자동으로 그 데이터의 배포자가 되기 때문에** 주의가 필요합니다. 또한 불법 공유되고 있는 음악・영상 콘텐츠를 불법인 줄 알면서 다운로드하는 것도은 불법이며 **형사처벌의 대상이** 되는 경우도 있습니다. P2P형 파일 공유 소프트웨어는 교육・연구상 꼭 필요한 경우 이외에는 사용하지 않도록 합시다.

④대량 다운로드의 금지

본교에서 '자유롭게' 사용해도 괜찮아 보이는 서비스라도 도쿄대학과 서비스 제공자 간에 이용조건이 정해져 있는 것이 보통입니다. 예를 들어, 대부분의 전자저널이나 데이터베이스에서는 컴퓨터 프로그램 등을 이용하여 한번에 대량의 콘텐츠를 다운로드하는 것은 금지되어 있습니다. 이용조건을 지키지 않는 사람이 있으면 도쿄대학 전체에 대한 서비스가 정지될 가능성이 있으므로 주의해 주십시오.

⑤계정 도용・대여의 금지

패스워드를 추측하는 등의 방법으로 타인의 계정을 도용하는 것은 범죄입니다. 또한 모든 이용자에게는 자신이 보유한 계정, 패스워드, 정보기기, 소프트웨어 등을 안전하게 관리할 의무가 있습니다. 타인이 자신의 계정이나 컴퓨터를 악용하면 소유자 자신이 곤란할 뿐만 아니라 모르는 제삼자나 대학 전체에 피해를 주게 됩니다. 또한 자기 대신에 리포트를 제출하게 하거나 업무를 일시적으로 대행하게 하는 등의 목적으로 자신의 계정을 타인에게 대여하는 일은 절대로 하지 마십시오.

⑥간단한 패스워드는 사용하지 말 것

컴퓨터가 악용되는 원인 중 하나는 추측 가능한 패스워드의 사용입니다. 특히 위험한 패스워드는 명칭, 단어, 숫자 또는 그것들을 조합한 것, 키보드의 배열, 짧은 패스워드 등입니다. 알파벳의 대문자, 소문자, 숫자 등을 조합한, 의미 없는 문자열을 이용해 주십시오. 패스워드는 기억하거나 그럴 수 없는 경우에는 다른 사람이 도용할 수 없도록 엄중하게 보관해 주십시오. **또한 패스워드는 동일한 것을 여러 곳에 사용하지 말고**, 시스템이나 소프트웨어별로 구분해서 사용하고 신중하게 관리해 주십시오.

⑦정보기기의 도난 및 분실에 주의할 것

노트북 컴퓨터, 스마트폰, 태블릿, 하드 디스크, USB 메모리 등, 중요한 정보가 들어 있는 정보기기의 분실 및 도난에 주의해 주십시오. 도난에 의한 피해는 본교에서도 많이 발생하고 있습니다. 교실이나 식당 등불특정 다수가 드나드는 장소는 특히 위험합니다. 본교의 시스템 계정이나 패스워드가 들어 있는 정보기기를 분실했을 경우 신속히 그 계정을 발행한 기관에 연락해 주십시오.

⑧철저한 바이러스 대책

모든 컴퓨터에 올바른 바이러스 백신을 실행하십시오. 본 대학에서는 바이러스 백신 소프트웨어의 라이센스를 정보기반 센터에서 각 조직(부국과 연구실 등)에 유상 배포하고 있습니다. 이용자는 자신이 소속된 조직에서 라이센스를 취득해 주십시오. 바이러스의 패턴 파일은 자동업데이트하여 최신 버전을 유지하고, 정기적으로 컴퓨터 내의 모든 파일의 바이러스 검사를 해 십시오. 그러나 바이러스 백신 소프트웨어를 도입하는 것만으로 모든 바이러스를 완전히 막을 수 있는 것이 아닙니다. 안심하지 마시고 항상 감염의 위험을 피할 수 있도록 유의해 주십시오. USB 메모리 등을 컴퓨터에 연결할 때는 먼저 바이러스 검사를 해 주십시오.
교내 연락이나 취재 신청 등, **합법적 내용으로 가장한 악성 바이러스 메일**이 증가하고 있습니다(표적 공격). 메일에 첨부된 파일과 메일 본문의 외부 링크에서 바이러스가 침입하지 못하도록 주의해 주십시오.

⑨소프트웨어를 최신 상태로

운영체제(OS)와 컴퓨터 소프트웨어는 항상 최신 버전으로 업데이트해 주십시오. 자동 업데이트가 가능한 소프트웨어는 그 기능을 ON으로 설정해 주십시오. 최신 버전이 아닌 소프트웨어를 이용하면 바이러스 감염 등의 보안문제가 쉽게 발생합니다. 또한 제조자의 기술지원이 만료된 소프트웨어는 보안문제가 발견되어도 수정되지 않으므로 사용을 자제해 주십시오.

⑩장기간 부재 중인 경우는 단말기의 전원을 끈다

장기휴가나 출장 등으로 며칠 이상 컴퓨터를 이용하지 않는 경우, 보안 및 에너지 절약 차원에서 반드시 전원을 꺼 주십시오. 다시 이용할 경우에는 작업을 시작하기 전에 소프트웨어와 바이러스 백신의 패턴 파일을 최신 버전으로 업데이트해 주십시오.

⑪만약 주의를 받으면

교직원이나 시스템 관리자로부터 주의나 지시를 받은 경우, 그 내용을 신속하게 따라 주십시오. 바이러스에 감염된 채로 컴퓨터를 계속 이용하거나 부적절한 이용을 계속해서는 안 됩니다. 본교에서는, 정보 보안상 통신 내용에 문제가 없는지 자동으로 감지하고 차단할 수도 있습니다.

이런 경우는…정보윤리 위반입니다

★친구의 권유로 P2P프로그램을 인스톨하여 시판중인 음원과 영화 등의 해적판으로 의심되는 파일을 다운로드하였다. (2012년 10월부터 이러한 다운로드도 **저작권법 위반**입니다.)
★전원의 승낙을 받지 않고 주소가 포함된 클래스의 명단을 홈페이지에 일반 공개하였다. 본인의 승낙을 받지 않고 블로그 등에 타인의 얼굴이 찍힌 사진을 게재하였다 (부적절한 정보유포 금지: 사생활을 침해하는 정보).
★트위터를 비롯한 각종 SNS사이트와 인터넷 게시판에 타인을 비방하거나 차별하는내용의 글을 썼다 (부적절한 정보유포 금지: 비방 혹은 차별에 해당하는 정보).
★패스워드를 종이에 적어 컴퓨터 모니터 옆에 붙여 놓았다.
★전자저널이나 데이터베이스의 이용계약에 금지되어 있는데 대량으로 자료를 다운로드하였다.
★인터넷에서 찾은 다른 사람의 문장 전부 또는 일부를, 출처를 명시하지 않고 자신의 리포트에 유용하여제출하였다.

関連規則・情報　currently available only in Japanese
Related Rules and Information
相关规则及信息
관련 규칙.정보

東京大学情報倫理規則／東京大学情報倫理運用規程

The University of Tokyo Rules Pertaining to Information Ethics／The University of Tokyo Operational Rules Pertaining to Information Ethics

东京大学信息伦理规则 / 东京大学信息伦理运用规程

도쿄대학 정보윤리규칙 / 도쿄대학 정보윤리 운영규정

https://www.u-tokyo.ac.jp/adm/cie/ja/

東京大学情報ネットワークシステム運用規則/東京大学情報ネットワークシステム利用ガイドライン

The University of Tokyo Rules Pertaining to the Operation of the Information Network System／The University of Tokyo Guidelines for Use of the Information Network System

东京大学信息网络系统运用规则 / 东京大学信息网络系统利用指南

도쿄대학 정보 네트워크 시스템 운영규칙 / 도쿄대학 정보 네트워크 시스템 이용 가이드라인

https://www.nc.u-tokyo.ac.jp/guide/rule_001
https://www.nc.u-tokyo.ac.jp/guide

電子ジャーナル

Electronic journals to which The University of Tokyo subscribes

电子期刊

전자저널

https://www.dl.itc.u-tokyo.ac.jp/ej/notice_new.html

When using the University's 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 actions. Furthermore, we would request that as students or members of staff of the University you will act with common sense and moderation even in activities outside of the University and in private life.

発行者　Issued by 发行者　발행자

東京大学情報システム部
Information Systems Department, The University of Tokyo
东京大学信息系统部
도쿄대학 정보 시스템 부
https://www.u-tokyo.ac.jp/adm/cie/ja/index.html
office.adm@gs.mail.u-tokyo.ac.jp

東京大学情報システム緊急対応チーム(UTokyo-CERT)
The University of Tokyo Computer Emergency Response Team (UTokyo-CERT)
东京大学信息系统紧急对策小组(UTokyo-CERT)
도쿄대학 정보시스템 긴급대응팀(UTokyo-CERT)
https://cert.u-tokyo.ac.jp/
office@cert.u-tokyo.ac.jp