

2021年度版

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

English
P4

Guidelines for Information Ethics and Computer Use

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

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。

한국어
P8

정보윤리·컴퓨터 이용 가이드라인

정보 네트워크와 컴퓨터를 적절하고 안전하게 이용하기 위하여
*원본은 일본어입니다.

大学の施設や研究室の情報機器だけでなく、
個人のスマートフォンやタブレット、PCを使う
ときも、東京大学の情報システムにアクセスし
ていることをご存じですか？

学内で情報機器を使うときには、本学構成員と
しての自覚と責任を持ち、情報倫理と情報セ
キュリティのルールを守って情報システムを利
用してください。



I 東京大学の情報倫理ルールの基礎知識

①本学の情報システムの利用は「教育・研究目的」に限定されています。

本学の情報システムの利用は、**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・公開は禁止されています。

本学の情報システムを利用して以下のような情報を発信・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 | (6) 教育・研究を妨害する情報 |
| (2) 知的財産権・肖像権を侵害する情報 | (7) 他者の業務・作業を妨害する情報 |
| (3) 差別・誹謗中傷にあたる情報 | (8) 虚偽の情報 |
| (4) プライバシーを侵害する情報 | (9) 守秘義務違反にあたる情報 |
| (5) わいせつな情報 | (10) 教育・研究活動における機微情報 |

例) SNSに他人の誹謗中傷や差別的な書き込みをした。

個人情報、成績情報、研究情報を書き込みした、または漏洩させてしまった。

③情報、著作物の不正利用は禁止されています。

他人の情報を盗用・改ざんしたり、音楽、映像、書籍、論文、ソフトウェア等の著作物を無断でコピーして配布する等の著作権を侵害する行為は犯罪です。また、違法に配信されている音楽、映像、書籍、論文、ソフトウェアのプログラム等を、ダウンロードすることは違法であり、**刑事罰の対象**になります。

④大量ダウンロードは禁止されています。

多くの電子ジャーナルやデータベースでは、一度に大量のコンテンツをダウンロードすることは禁止されています。本学とサービス提供元との間でデータ利用条件が定められており、利用条件を守らない者がいると、本学に対するサービスが停止される可能性があります。

⑤アカウントID・パスワードの盗用・貸与は禁止されています。

他人のアカウントID・パスワードを盗用することは犯罪です。また、全ての利用者には、自分が保持するアカウントID・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。本学が提供しているアカウントID・パスワードは責任をもって管理してください。

⑥情報機器の盗難や紛失に注意してください。

ノートPC、タブレット等の重要情報が入った情報機器の紛失と盗難が学内でも発生し、情報漏洩が起きています。本学のシステムのアカウントID・パスワードが入った情報機器を失った場合、すぐに部局の担当窓口ご連絡してください。

II 東京大学の情報セキュリティルールの基礎知識

①推測されやすいパスワードを使用しないでください。

パスワードを設定する際には推測されやすいもの（名称、単語、誕生日、キーボードの配列等）は使用せず、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使用してください。**2要素認証**などが提供されている場合には積極的に活用しましょう。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ください。

②ウイルス対策とソフトウェアの脆弱性対策を徹底してください。

使用者が管理権限をもつ全てのコンピュータでは、適切なウイルス対策をしてください。ウイルスのパターンファイルは最新版に保ち、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ください。常に感染の危険を避けることを心がけてください。また本学では、大学所有の機器を対象に、情報基盤センターから各組織（部局や研究室）にウイルス対策ソフトが有償配付されています。使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。

関連して、**OSやアプリケーションも常に最新版に更新**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、ウイルス感染等のセキュリティリスクが高まります。

③ウイルスメールによるサイバー攻撃に警戒してください。

本学でも**正当な内容を装った巧妙な悪意のあるウイルスメール（フィッシングメール、標的型攻撃メールなど）**が増えています。添付ファイルやURLを開くとウイルス感染したり、ID・パスワードが漏洩したりします。ウイルス感染すると、金銭を脅迫されたり自身のPCが他者へウイルスメールを発信し始めるものもあります。少しでも怪しいと思ったメールは開かず、すぐに部局の担当部署に連絡してください。

④セキュリティ対策が行われていないWiFiは利用しないでください。

セキュリティ対策が行われていないWiFiを利用すると、通信内容を盗聴され、ID・パスワード等を窃取される危険性が高まります。**Free WiFiや暗号化に対応していないアクセスポイントには接続しないでください。**

⑤長期間利用しない端末は電源をオフにしてください。

長期間利用しない端末の電源はオフにしてください。長期休暇明けは、PC起動後の一番最初にソフトウェアの更新を行ってください。

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、速やかに従ってください。他者をサイバー攻撃したり情報漏洩が起きる危険性がありますので、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。

I Fundamentals of UTokyo Information Ethics

① Use Limited to Educational and Research Purposes

The University's information system is **restricted to educational and research purposes** only. Use of the information system for inappropriate, illegal, unlawful, or unethical purposes is strictly prohibited.

② Prohibition on Transmission or Release of Information

Users of the University's information system are prohibited from sending or releasing information that:

- | | |
|--|---|
| (1) is not sent under your own name
(i.e., sending anonymously or using aliases), | (5) is obscene, |
| (2) infringes on the intellectual property rights or
portrait right of others, | (6) disrupts education or research, |
| (3) is discriminatory, slanderous, or libelous, | (7) disrupts the work of any individual, |
| (4) infringes on the privacy of others. | (8) is false, (9) violates confidentiality, or |
| | (10) provides subtle information related to
educational and research activities. |

For example, posting slanderous, libelous, or discriminatory content about others on the SNS or leaking personal information, grades, or research information is strictly prohibited.

③ Prohibition on Illegal Use of Copyrighted Materials and Information

Copyright violation is a criminal offence. Such acts include stealing or altering information of others, and reproducing and distributing copyrighted material (such as music, movies, books, academic literature, or software) without consent. In addition, knowingly downloading illegally distributed music, movies, books, academic literature, or software is unlawful and **subject to criminal punishment**.

④ Prohibition on Excessive Downloading

Most electronic journals and databases prohibit excessive downloading all at once. There are usage-limit agreements between the University and the providers. If a person violates such an agreement, the service may be terminated for the entire University.

⑤ Prohibition on Stealing or Lending an Account

Stealing another's account ID and password is a criminal offense. All users must safely maintain their account ID, password, information assets, software, etc. Please responsibly maintain your account ID and password provided by the University.

⑥ Be Cautious about Loss and Theft of Your Information Assets

Loss and theft of information assets such as laptops and tablets containing important information have occurred within the University, resulting in an information leak. If you lose an item that contains accounts or passwords for the University's system, report the loss to your Network Administrator immediately.

II Fundamentals of UTokyo Information Security Rules

① Avoid Easy-to-Guess Passwords

When creating a password, avoid an easy-to-guess password (such as names, words, birthdates, or letters lining up on the keyboard). Instead, choose a combination of letters (a mixture of upper and lower cases) and numerals, which represents a random combination. If **two-factor authentication** is available, actively embrace it. Passwords must not be reused. Use a different password for each system and software.

② Pay Attention to Antivirus Measures and Mitigation Strategies for Software Vulnerability

Employ appropriate antivirus measures on all computers that you manage. Update to the latest antivirus definition files and routinely run a virus scan on all files to avoid the risk of infection. The University distributes antivirus software licenses for a fee through the Information Technology Center for all departments (or laboratories). Individuals must obtain a license from their department. Additionally, you must **maintain the latest version of OS and software applications** by constantly updating. Not using the latest version increases the security risk.

③ Be Cautious with Cyber Attacks Originating from Virus Emails

There has been an increase in **emails with malicious viruses, which look like legitimate emails (phishing emails, targeted attacks, etc.)** within the University. Opening an attachment or accessing the URL can infect your computer with a virus or steal your personal information such as passwords. If your computer is infected with a virus, the attacker may demand a ransom or your computer may send virus emails to others. If you find an email to be even slightly suspicious, don't open it. Instead, immediately report it to the person in charge of your department.

④ Avoid Unsecured WiFi

If you use unsecured WiFi, the risk that your communication content is tapped to steal your ID and password greatly increases. **Don't connect to free WiFi or an access point without security encryption.**

⑤ Power Down Your Terminal during Long Absences

If you plan not to use your terminal for a long period of time, please power it down. When you return, update your software and virus definition files.

If You Receive a Warning...

If a professor, staff, or network administrator warns you of inappropriate use of computer resources, you must follow the instructions immediately. Continued use of computers infected by viruses or any other inappropriate use is strictly prohibited due to risks associated with cyberattacks and information leaks.

I 东京大学信息伦理规定的基础知识

①本校的信息网络系统仅限于“教育及研究目的”。

本校的信息网络系统仅限于教育、研究相关的目的。凡是不符合该目的的不正当行为、违法行为、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。

不得使用本校的信息网络系统发送或公开下列信息。

- | | |
|-----------------------|--------------------|
| (1) 署有非真实姓名（匿名、假名）的信息 | (6) 妨碍教育、研究的信息 |
| (2) 侵犯知识产权、肖像权的信息 | (7) 妨碍他人业务、工作的信息 |
| (3) 涉及歧视、诽谤中伤的信息 | (8) 虚假信息 |
| (4) 侵犯隐私权的信息 | (9) 涉及违反保密义务的信息 |
| (5) 有猥亵内容的信息 | (10) 教育、研究活动中的敏感信息 |
- 例) 在社交媒体上上传了涉及对他人构成诽谤中伤或歧视的内容。
上传了个人信息、成绩信息、研究信息，或使之泄漏。

③严禁信息、著作物的不正当使用。

盗用、篡改他人的信息，随意复制、散布音乐、影像、书籍、论文、软件等侵犯著作权的行为属于犯罪行为。此外，下载违法散布的音乐、影像、书籍、论文、软件的程序等行为也是犯罪行为，**将受到刑事处罚**。

④严禁大量下载。

许多电子期刊和数据库都禁止一次性大量下载数据。本校和服务提供商之间规定了数据使用条件，如果有人不遵守使用条件，则可能会停止对本校提供服务。

⑤不得盗用或借用他人ID账号、密码。

盗用他人ID账号、密码属于犯罪行为。此外，所有用户对自己保有的ID账号、密码、信息设备、软件等都负有安全管理义务。请妥善管理本校提供的ID账号、密码。

⑥注意防范信息设备的失窃、遗失。

笔记本电脑、平板电脑等内有重要信息的信息设备的遗失、失窃在本校内也有发生，并导致了信息的泄漏。如内有本校系统ID账号、密码的信息设备遗失、失窃，请立即报于各部门负责窗口知晓。

II 东京大学信息安全规定的基础知识

①请勿使用容易被猜到的密码。

在设定密码时，请勿使用容易被猜到的组合（名称、单词、生日、键盘上的排列等），请使用大小写字母、数字等混合的无意义的字符串。如提供了**双重验证**等时，请积极使用。此外，请勿使用相同密码，请根据系统、软件等设定不同的密码。

②请做好反病毒和软件漏洞的防护对策。

用户须在所有具有管理权限的计算机上做好反病毒防护对策。请始终保持病毒库文件为最新版本，并定期对计算机中的所有文件进行病毒扫描检查。在使用计算机时，请时刻注意避免被病毒感染。此外，本校信息中心已针对校园内的所有设备向各部门（院系、研究室等）有偿发放防病毒软件。请用户向自己所属的部门获取软件使用许可。

此外，请始终保持**操作系统、应用程序**为最新版本。如使用非最新版本的软件，则感染病毒的危险几率会增高。

③谨防基于病毒邮件的网络攻击。

本校中，**伪装成正常内容的恶意病毒邮件（钓鱼邮件、针对性攻击邮件等）**正在增加。一旦打开了这些邮件中附件或URL网址，就会感染病毒并导致ID账号、密码等泄漏。感染病毒后，可能会被威胁索要钱财，或是从自己的PC向其他人发送病毒邮件。如发现可疑的邮件，请勿打开并立即与各负责部门取得联系。

④请勿连接无安全对策的WiFi。

连接无安全对策的WiFi，会被窃听通信内容，ID密码等被盗取的风险增加。请勿连接**Free WiFi**或**没有加密的接入点**。

⑤终端长期不使用时，请关闭电源。

请关闭长期不使用的终端的电源。长假结束后首次启动PC时，请第一时间更新升级软件。

如果接到了提醒警告……

如果接到了来自教职员工或网络管理人员的提醒警告或指示时，请立即听从指示。如在感染了病毒的情况下继续使用计算机，或不正确的使用，都可能会导致对他人造成网络攻击，并存在致使信息外泄的风险。因此，如遇此种情况，请立即停止使用计算机。

I 도쿄대학의 정보윤리 룰의 기초 지식

① 본교의 정보 시스템의 이용은 '교육·연구 목적'으로 한정되어 있습니다.

본교의 정보 시스템의 이용은 **교육·연구에 관한 목적으로 한정되어 있습니다**. 이 목적에 맞지 않는 부적절한 행위, 불법 행위, 윤리에 어긋나는 행위를 금지합니다.

② 부적절한 정보 발신·공개는 금지되어 있습니다.

본교의 정보 시스템을 이용하여 아래와 같은 정보를 발신·공개하는 것은 금지되어 있습니다.

- | | |
|-----------------------------|-----------------------|
| (1)본명 이외(익명·위명)에 의한 정보 | (6)교육·연구를 방해하는 정보 |
| (2)지적 재산권·초상권을 침해하는 정보 | (7)타인의 업무·작업을 방해하는 정보 |
| (3) 차별·중상모략에 해당하는 정보 | (8)허위 정보 |
| (4)개인정보를 침해하는 정보 | (9)비밀유지의무위반에 해당하는 정보 |
| (5)외설적인 정보 | (10)교육·연구 활동에 민감한 정보 |

예) SNS에 타인의 중상모략이나 차별적인 글을 적었다.
개인정보, 성적 정보, 연구 정보를 적었거나 누설해버렸다.

③ 정보, 저작물의 부정 이용은 금지되어 있습니다.

타인의 정보를 도용·조작하거나 음악, 영상, 서적, 논문, 소프트웨어 등의 저작물을 무단으로 복사하여 배부하는 등의 저작권을 침해하는 행위는 범죄입니다. 또한 불법으로 배포되고 있는 음악, 영상, 서적, 논문, 소프트웨어의 프로그램 등을 다운로드하는 것은 불법이며 **형사 처벌의 대상**이 됩니다.

④ 대량 다운로드는 금지되어 있습니다.

많은 전자저널이나 데이터베이스에서는 한 번에 대량의 콘텐츠를 다운로드하는 것은 금지되어 있습니다. 본교의 서비스 제공처와의 사이에 데이터 이용 조건이 정해져 있으며, 이용 조건을 지키지 않는 자가 있으면 본교에 대한 서비스가 정지될 가능성이 있습니다.

⑤ 계정 ID·패스워드의 도용, 대여는 금지되어 있습니다.

타인의 계정 ID·패스워드를 도용하는 것은 범죄입니다. 또, 모든 이용자에게는 자신이 보유하고 있는 계정 ID·패스워드, 정보 기기, 소프트웨어 등을 안전하게 관리할 의무가 있습니다. 본교가 제공하고 있는 계정 ID·패스워드는 책임지고 관리해 주십시오.

⑥ 정보 기기의 도난이나 분실에 주의해 주십시오.

노트북, 태블릿 등의 중요 정보가 들어있는 정보 기기의 분실과 도난이 학교 내에서도 발생하여 정보 누설이 발생하고 있습니다. 본교의 시스템 계정 ID·패스워드가 들어있는 정보 기기를 분실한 경우, 즉시 부국의 담당 창구로 연락해 주십시오.

Ⅱ 도쿄대학의 정보 보안 룰의 기초 지식

① 추측하기 쉬운 패스워드를 사용하지 말아 주십시오.

패스워드를 설정할 때는 추측하기 쉬운 것(명칭, 단어, 생일, 키보드의 배열 등)은 사용하지 말고, 알파벳 대문자, 소문자, 숫자 등을 조합한 의미가 없는 문자열을 사용해 주십시오.
2 요소 인증 등이 제공되고 있는 경우에는 적극적으로 활용합니다. 또한 패스워드는 공통으로 사용하지 말고 시스템이나 소프트웨어 별로 나눠서 사용해 주십시오.

② 바이러스 대책과 소프트웨어의 취약성 대책을 철저히 해 주십시오.

사용자가 관리 권한을 가지는 모든 컴퓨터에서는 적절한 바이러스 대책을 해 주십시오. 바이러스의 패턴 파일은 최신판을 유지하고, 정기적으로 컴퓨터 내 모든 파일의 바이러스 체크를 해 주십시오. 항상 감염의 위험을 피하기 위해 주의해 주십시오. 또한 본교에서는 대학이 소유하는 기기를 대상으로 정보 기반 센터에서 각 조직(부국이나 연구실)으로 바이러스 대책 소프트웨어를 유상 배부하고 있습니다. 사용자는 자신이 소속된 조직으로부터 라이선스를 입수해 주십시오.
관련하여, **OS나 애플리케이션도 항상 최신판으로 갱신**해 주십시오. 최신이 아닌 소프트웨어를 이용하면 바이러스 감염 등의 보안 리스크가 커집니다.

③ 바이러스 메일에 의한 사이버 공격을 경계해 주십시오.

본교에서도 **정당한 내용을 위장해서 교묘한 악의를 가진 바이러스 메일(피싱 메일, 표적형 공격 메일 등)**이 증가하고 있습니다. 첨부 파일이나 URL을 열면 바이러스에 감염되거나 ID·패스워드가 누설됩니다. 바이러스에 감염되면 금전적으로 협박을 당하거나 자신의 PC가 타인에게 바이러스 메일을 발신하기 시작하는 것도 있습니다. 조금이라도 의심스럽다고 생각되는 메일은 열지 말고 즉시 부국의 담당 부서로 연락해 주십시오.

④ 보안 대책이 실시되지 않은 WiFi는 이용하지 말아 주십시오.

보안 대책이 실시되지 않은 WiFi를 이용하면 통신 내용을 도청당해, ID·패스워드 등이 도취될 위험성이 커집니다. **Free WiFi나 암호화에 대응하지 않는 액세스 포인트에는 접속하지 말아 주십시오.**

⑤ 장기간 이용하지 않는 단말은 전원을 꺼 주십시오.

장기간 이용하지 않는 단말의 전원은 꺼 주십시오. 장기 휴가가 끝난 뒤에는 PC 기동 후 제일 먼저 소프트웨어 갱신을 해 주십시오.

만약 주의를 받으면...

직원이나 네트워크 관리자로부터 주의나 지시를 받은 경우 신속하게 따라 주십시오. 타인을 사이버 공격하거나 정보가 누설될 위험성이 있으므로 바이러스에 감염된 채로 컴퓨터를 계속해서 이용하거나 부적절한 이용을 계속해서 안 됩니다.

関連規則・情報 currently available only in Japanese

Related Rules and Information

- 東京大学情報倫理ガイドライン
- The University of Tokyo Information Ethics Guidelines
- <https://www.u-tokyo.ac.jp/adm/cie/ja/index.html>



- 東京大学情報セキュリティ・ポリシー
- UTokyo Basic Policy for Information Security
- <https://www.u-tokyo.ac.jp/ja/about/rules/public16.html>



- 東京大学情報セキュリティ教育
- UTokyo Information Security Education
- <https://www.u-tokyo.ac.jp/adm/dics/ja/securityeducationvideo.html>



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



Did you know that you are accessing the University of Tokyo's information system even when you use your personal smartphone, tablets or PCs on campus in addition to the information equipment of the university facilities and laboratories?

Please be aware and responsible as a member of the University, and follow these rules of information ethics and information security whenever you use any information equipment on campus.



< 発行元 Issued by >

- 東京大学情報システム部
- Information Systems Department, The University of Tokyo
- 東京大学信息系统部
- 도쿄대학 정보 시스템 부

E-mail : office.cie.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)
- 東京大学信息系统緊急対策小组(UTokyo-CERT)
- 도쿄대학 정보시스템 긴급대응팀(UTokyo-CERT)

Website : <https://cert.u-tokyo.ac.jp/>

E-mail : office@cert.u-tokyo.ac.jp

