東京大学
THE UNIVERSITY OF TOKYO

2025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.

本学の情報システムを利用する際には、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ください。

本学の情報システムには学内ネットワークや大学で契約するクラウドサービスが含まれます。こうしたシステムを学内の施設や研究室の情報機器から利用する時だけでなく、本学構成員の所有する情報機器（スマートフォン、タブレットやPC）で利用する場合でも情報倫理と情報セキュリティのルールに従う必要があります。

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。

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。

本学の提供する情報システム（ネットワーク含む）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
(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
(10) 教育・研究活動における機微情報

違反となる例）SNSに他人の誹謗中傷や差別的な書き込み、虚偽の書き込みをする。
SNSなどに試験問題や解答など業務を妨害する書き込みをする。
SNSの書き込みやAIが生成した文章を、真偽を確認せずに拡散する。
個人情報、成績情報、研究情報を書き込みする、または漏洩させる。

③著作物の不正利用は禁止されています。

音楽、映像、書籍、論文、ソフトウェア等の著作物を権利者に無断でコピーして配布する等の行為は著作権侵害に当たり犯罪になり得ます。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**の対象になるほか、権利者に損害を与えた場合は賠償を求められることもあります。

④大量ダウンロードは禁止されています。

本学で契約している電子ジャーナルやデータベースは、一度に大量のコンテンツをダウンロードすることが禁止されています。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、本学全体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)を勝手に使用することは犯罪です。アカウントを共用したり、ログイン後の情報機器を別の者に操作させることはアカウントの貸与となります。全ての利用者には、自分が保持するアカウント、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は責任をもって適切に管理してください。

Ⅱ　東京大学の情報セキュリティルールの基礎知識

①推測しづらいパスワードを設定し、多要素認証を活用してください。

パスワードを盗まれないように、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、数字などを混在した意味のない文字列を使用してください。パスワード認証のみでは、不正アクセスの被害にあう可能性が高いため、**多要素認証**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、本学のウイルス対策ソフトウェア提供サービスなどを利用してソフトウェアをインストールしてください。関連して、**ＯＳやアプリケーション**もサポートされている最新の修正プログラム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。なお、サポートが終了しているOSやアプリケーションは修正が行われないため、原則として使用しないでください。

③メールによるサイバー攻撃に警戒してください。

コンピュータウイルスやそのダウンロードURLが添付されているメール、あるいはフィッシングや標的型攻撃を行うなどの悪意のあるメールが多くなっています。メールに添付されたファイルやURLへのアクセスには十分に注意してください。フィッシングや標的型攻撃メールの多くは一見不審ではありません。すべてのメールに警戒してください。

④提供者が信頼できないWi-Fiの利用は避けてください。

Wi-Fi提供者や他の利用者に悪意があると、ID・パスワードなどを含む通信内容が盗み見られる可能性があります。信頼できる運営者が提供するWi-Fi以外への接続は避けてください。秘密の情報を送る場合は、UTokyo VPNを利用する等の対策を取ってください。

⑤オンライン授業やテレワークをする「場所」に気をつけてください。

ファミレスやカフェなどパブリックな場所で、ビデオ会議やオンライン授業に参加したり、ファイルを見たりすると、周りに情報漏洩する危険性があります。自室など安全な場所で行ってください。

⑥メールの「送り方」に気をつけてください。

「BCC」で送信するべきメールを、「TO」や「CC」で送信すると、同報している宛先（メールアドレス、名前）が情報漏洩します。情報漏洩が起こらないよう、同報メール送信時は細心の注意を払いましょう。

⑦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、USBメモリ、ポータブルハードディスク等の重要情報が入った情報機器の紛失と盗難が本学でも発生し、情報漏洩が起きています。本学のシステムのアカウントが入った情報機器を失った場合を含め、すぐに部局窓口部署に連絡してください。

不審な状況を見たら・感じたら…
自分のアカウントを誰かに使われているかもしれない・コンピュータウイルスに感染したかもしれない・不審なメールを受け取ったなどの不審な状況を見かけたら・感じたら、速やかに部局窓口部署へ連絡してください。

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。

UTokyo Guidelines for Information Ethics and Computer Use

When using the UTokyo information systems, you must be aware and responsible as a member of UTokyo by following the information ethics and security rules.
The UTokyo information systems include the University network and contracted cloud services. You must follow the information ethics and security rules not only while using the systems on information equipment located in the University facilities and laboratories, but also while using the systems on your personally owned information equipment (smartphones, tablets, and PCs).
In addition, as a student, faculty or staff member at UTokyo, please exercise good judgement and self-discipline even in activities conducted outside UTokyo and in your private life.

I Fundamentals of the UTokyo Information Ethics

① Use Limited to Educational and Research Purposes.

The use of the information systems (including networks) provided by the University is limited to **educational and research purposes**. Any inappropriate, illegal or unethical conduct that is inconsistent with these purposes is prohibited.

② Prohibition 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 the intellectual property rights or portrait rights of others,
(3) is discriminatory, slanderous, or libelous,
(4) infringes the privacy of others,
(5) is obscene,
(6) disrupts education or research,
(7) disrupts the work of any individual,
(8) is false,
(9) violates confidentiality, or
(10) provides subtle information related to educational and research activities.

Examples of violations:
Posting defamatory, discriminatory, or false content about others on social media.
Posting examination questions, answers, or any posts that disrupt university operations on social media.
Spreading posts or AI-generated content on social media without verifying their authenticity.
Posting or leaking personal, grade, or research information.

③ Unauthorized use of copyrighted materials is prohibited.

Copyright violation is a criminal offence. Such acts include stealing or altering information of others, as well as the reproduction and distribution of 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.

Downloading a large volume of contents from electronic journals and databases contracted by UTokyo is prohibited. UTokyo has a signed usage agreement with service providers; thus, if a member of UTokyo violates the terms of the agreement, it could result in suspension of the service.

⑤ Prohibition on Stealing or Lending of an Account.

Using another person's account information (ID and password) without permission is a crime. Sharing accounts or allowing others to operate logged-in information equipment constitutes account lending. All users have an obligation to safely maintain their own accounts, information equipment, and software. Please be responsible in maintaining your accounts provided by UTokyo.

II Fundamentals of the UTokyo Information Security Rules

① Use Hard-to-Guess Passwords and Multifactor Authentication.

To prevent someone from stealing your passwords, do not use easy-to-guess passwords (names, words, birthdates, a sequence of letters aligned on the keyboard, etc.); use a random alphanumeric string that mixes upper- and lower-case letters, numbers, and other elements. Since authentication using a password alone is prone to unauthorized accesses vulnerabilities, please actively use **multifactor authentication** if it is available. Do not use the same password for all of your accounts; use different ones for each system and software.

② Use of antivirus software is mandatory.

Please install appropriate antivirus software on all the computers you administrate. Keep the virus definition files up-to-date, and routinely run virus checks on entire files stored on the computer. Please be vigilant to avoid risks of infection. Install software using the UTokyo antivirus software provision service. Similarly, you must also update and maintain the latest versions of the **OS and other software**. Computers running outdated versions of software are exposed to greater risks of virus infection.
Please do not use an OS or software that has reached its end of support (EOS) date because security patches will no longer be issued.

③ Be Wary of Cyber Attacks Via Emails.

Malicious emails containing computer viruses, download links, phishing attempts, or targeted attacks are becoming increasingly common. Exercise extreme caution when accessing attachments or links in emails. Many phishing or targeted attack emails may appear legitimate. Be wary of all emails.

④ Avoid using Wi-Fi of untrustworthy providers.

If a Wi-Fi provider or other users have malicious intent, your communications, including IDs and passwords, may be intercepted. Please avoid connecting to anything other than Wi-Fi provided by a reliable operator. Use protective measures, such as UTokyo VPN, when sending confidential information.

⑤ Please be Careful about “Where” You Attend Online Classes and Conduct Remote Work.

If you participate in video conferences or online classes, or view files in a public location such as restaurants or cafes, information may be divulged to the people around you. Conduct these activities at a safe place, such as your room.

⑥ Please be Careful with “How” You Send an Emails.

If you add recipient email addresses to the “TO” or “CC” fields when the “BCC” is more appropriate, the recipients’ information (email addresses and names) will be divulged to the other recipients.
To prevent information leaks when sending email to multiple recipients, pay particular attention to these fields.

⑦ Be Cautious about Loss or Theft of Your Information Assets.

UTokyo is experiencing incidents of information leakage related to loss or theft of information equipment (such as laptops, tablets, USB memory sticks, and portable hard disks) containing important information. If you lose any information device containing the university system account, immediately contact the departmental contact.

If you see or feel something suspicious...

If you feel or suspect that your account may be being used by someone else, that your computer may have been infected with a virus, or that you have received a suspicious email, immediately contact the departmental contact.

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 cyber attacks and information leaks.

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

在使用本校的信息系统时，应具备身为本校成员的自觉与责任感，遵守信息伦理与信息安全方面的规则。
本校的信息系统包含了校园网和与高校签约的云服务。有鉴于此，除了在校内设施和研究室的信息设备上使用外，在本校成员拥有的信息设备（智能手机、平板电脑和PC机）上该使用信息系统时也必须遵守信息伦理和信息安全规则。
此外，在校外活动和私生活方面，作为本校的学生和教职人员，也请保持良知和节制。

Ⅰ 东京大学信息伦理规定的基础知识

①仅限于教育及研究目的。

本校提供的信息系统（包括网络）**仅限用于教育和研究的目的**。禁止不符合这一目的的不当行为、违法行为和不道德行为。

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
(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
(10) 教育、研究活动中的敏感信息

（违规示例）在SNS上发布诽谤他人、带有歧视性或虚假的帖子。
在SNS等上发布试题和答案等妨碍本校业务的帖子。
在未确认真伪的情况下传播SNS上的帖子和AI生成的文章。
发布或泄露个人信息、成绩信息、研究信息的帖子。

③禁止非法使用受版权保护的作品。

未经版权所有者许可复制和分发音乐、视频、书籍、论文、软件等受版权保护的作品可能构成侵犯版权的犯罪行为。此外，下载非法传播的音乐、视频、书籍、论文、软件程序等属于违法行为。这些行为将受到**刑事处罚**。如果给版权所有者造成损害，可能被要求赔偿。

④严禁大量下载。

本校签约的电子期刊和数据库禁止一次性下载大量内容。本校与服务提供商之间规定了数据使用条件，任何人若不遵守使用条件，可能导致暂停向整所大学提供服务。

⑤不得盗用或借用他人ID账号、密码。

盗用他人账号（ID、密码）属于犯罪行为。另外，在不告知密码的情况下允许他人操作信息设备的行为属于租借账号。此外，所有用户对自己保有的账号、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账号。

Ⅱ 东京大学信息安全规定的基础知识

①请设定较难被猜到的密码，并积极使用多重要素验证。

为避免密码被窃盗，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），请使用较难被猜到的大小写字母、数字等混合的无意义的字符串。仅使用密码验证时容易遭到非法访问，因此如提供了**多重要素验证**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，请使用本校的反病毒软件提供服务等安装软件。同时，请始终保持**操作系统**、**应用程序**为受支持的最新版本。如使用非最新版本的软件，则感染病毒的危险几率会增高。
另外，已经停止支持的操作系统和应用程序不会得到修正，原则上请勿使用。

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。很多情况下，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PC等设备中存储的个人信息、机密信息和ID、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。如发现有可疑的邮件，请勿打开并立即与各负责部门取得联络。

④请避免使用不可信供应商提供的Wi-Fi。

如果Wi-Fi供应商或其他用户有恶意，则包括ID和密码在内的通信内容可能会被窃取。请避免连接不可靠的运营商提供的Wi-Fi。发送机密信息时，请采取使用UTokyo VPN等对策。

⑤请注意线上课堂及远程办公等的“场所”。

在餐厅、咖啡厅等公共场所参加视频会议、在线课程或查看文件等，都存在向周围泄露信息的危险。请在自己的房间等安全的场所进行上述操作。

⑥请注意邮件的“发送方式”。

应该通过“BCC”发送的邮件，但却以“TO”或“CC”的方式发送时，其中的其他收件人（邮件地址、姓名）等信息将会泄露。
为了避免发生信息泄露的问题，在发送具有多个收件人的邮件时，请务必充分小心。

⑦注意防范信息设备的失窃、遗失。

本校也曾发生过笔记本电脑、平板电脑、USB存储器、移动硬盘等包含重要信息的信息设备的丢失和被盗事件，导致信息泄露。如发生丢失含有本校系统账户的信息设备的情况时，请立即联系所属部门的窗口所属学部的窗口部门。

当您看到或感到有可疑情况时……

如果您看到或感到有任何可疑情况，例如自己的帐户可能被某人使用、可能感染了计算机病毒、可能收到了可疑电子邮件，请立即联系所属部门的窗口。

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。

P2 日本語
P4 English
P6 簡体字
P8 한국어

도쿄대학 정보윤리・컴퓨터 이용 가이드라인

본교의 정보 시스템을 이용할 때는 본교 구성원으로서의 자각과 책임을 가지고 정보윤리와 정보 보안 룰을 지켜주십시오.
본교 정보 시스템에는 교내 네트워크 및 대학이 계약한 클라우드 서비스가 포함되어 있습니다. 이 시스템을 교내 시설이나 연구실 정보기기로 이용할 때뿐만 아니라 본교 구성원이 소유하는 정보기기(스마트폰, 태블릿 및 PC)로 이용하는 경우에도 정보윤리와 정보 보안 룰을 따를 필요가 있습니다.
또, 학외 활동이나 사생활에 있어서도 본교의 학생이나 교직원으로서의 양식과 절도 있는 행동을 부탁드립니다.

Ⅰ 도쿄대학의 정보윤리 룰의 기초 지식

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

본교에서 제공하는 정보 시스템(네트워크 포함)은 **교육 및 연구와 관련된 목적으로만** 이용할 수 있습니다. 이 목적에 부합하지 않는 부적절한 행위, 위법 행위, 비윤리적인 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・가명)에 의한 정보
(2) 지적 재산권・초상권을 침해하는 정보
(3) 차별・중상모략에 해당하는 정보
(4) 개인정보를 침해하는 정보
(5) 외설적인 정보
(6) 교육・연구를 방해하는 정보
(7) 타인의 업무・작업을 방해하는 정보
(8) 허위 정보
(9) 비밀유지 의무 위반에 해당하는 정보
(10) 교육・연구 활동에 민감한 정보

위반 사례) SNS에 타인을 비방하거나 차별적인 내용, 허위 사실을 올리는 행위.
SNS 등에 시험문제나 답안 등 업무를 방해하는 글을 올리는 행위.
SNS의 글이나 AI가 생성한 문장의 진위를 확인하지 않고 확산하는 행위.
개인 정보, 성적 정보, 연구 정보를 작성하거나 유출하는 행위.

③저작물의 부정 이용은 금지되어 있습니다.

음악, 영상, 서적, 논문, 소프트웨어 등의 저작물을 권리자에게서 무단으로 복사하여 배포하는 등의 행위는 저작권 침해에 해당하여 범죄가 될 수 있습니다. 또한 위법으로 배포된 음악, 영상, 서적, 논문, 소프트웨어 프로그램 등을 다운로드하는 행위도 위법이며, **형사 처벌**의 대상이 될 뿐만 아니라 권리자에게 손해를 끼친 경우 배상을 요구받을 수 있습니다.

④ 대량 다운로드는 금지되어 있습니다.

본교에서 계약한 전자 저널 및 데이터베이스는 한 번에 많은 콘텐츠를 다운로드하는 행위가 금지되어 있습니다. 본교와 서비스 제공처 간에 데이터 이용 조건이 정해져 있으며, 이용 조건을 지키지 않는 사람이 있으면 본교 전체의 서비스가 정지될 수 있습니다.

⑤ 계정 ID・패스워드의 도용, 대여는 금지되어 있습니다.

타인의 계정(아이디 및 비밀번호)을 무단으로 사용하는 것은 범죄입니다. 계정을 공유하거나 로그인 후 다른 사람이 정보 기기를 조작할 수 있도록 하는 것은 계정 대여에 해당합니다. 모든 이용자는 자신이 보유한 계정, 정보 기기, 소프트웨어 등을 안전하게 관리할 의무가 있습니다. 본교에서 제공하는 계정을 책임감 있고 올바르게 관리해 주시기 바랍니다.

Ⅱ 도쿄대학의 정보 보안 룰의 기초 지식

①추측하기 어려운 패스워드를 설정하고 다요소 인증을 활용하십시오.

패스워드가 도용되지 않도록 추측하기 쉬운 것(명칭, 단어, 생일, 키보드 배열 등)은 사용하지 말고 알파벳 대문자, 소문자, 숫자 등을 조합한 의미 없는 문자열을 사용해 주십시오. 패스워드 인증만으로는 부정 접속의 피해를 볼 가능성이 높기 때문에 **다요소 인증**이 제공되는 경우에는 적극적으로 활용합시다. 또, 패스워드는 공통으로 사용하지 말고 시스템이나 소프트웨어 별로 나눠서 사용해 주십시오.

②바이러스 대책과 소프트웨어의 취약성 대책을 철저히 해 주십시오.

사용자가 관리 권한을 가진 모든 컴퓨터에서는 적절한 바이러스 대책을 세워 주십시오. 바이러스의 패턴 파일은 최신판을 유지하고 정기적으로 컴퓨터 내 모든 파일의 바이러스 체크를 해 주십시오. 항상 감염의 위험을 피하기 위해 주의해 주십시오. 또한 본교에서의 바이러스 대책 소프트웨어 제공 서비스 등을 이용하여 소프트웨어를 설치해 주십시오. 관련하여 **OS나 애플리케이션**도 지원되고 있는 최신 수정 프로그램으로 갱신해 주십시오. 특히 장기 휴가 후에는 주의해 주십시오. 최신이 아닌 소프트웨어를 이용하고 있으면 바이러스 감염 등의 보안 리스크가 커집니다.
또, 지원이 종료된 OS나 애플리케이션은 수정이 되지 않기 때문에 원칙적으로는 사용하지 말아 주십시오.

③이메일을 통한 사이버 공격에 주의하시기 바랍니다.

컴퓨터 바이러스나 다운로드 URL이 첨부된 메일, 혹은 피싱 메일과 표적형 공격 메일 등의 악성 메일이 늘고 있습니다. 메일에 첨부된 파일이나 URL을 열 때는 충분히 주의하시기 바랍니다. 대부분의 피싱 메일과 표적형 공격 메일은 언뜻 보면 수상하지 않습니다. 모든 메일을 경계하시기 바랍니다.

④제공자를 신뢰할 수 없는 Wi-Fi 이용은 삼가주시기 바랍니다.

Wi-Fi 제공자나 다른 이용자에게 악의가 있다면 아이디 및 비밀번호 등을 포함한 통신 내용을 훔쳐볼 수 있습니다. 신뢰할 수 있는 운영자가 제공하는 Wi-Fi 외에는 연결하지 마시기 바랍니다. 비밀 정보를 전송할 때는 UTokyo VPN을 이용하는 등의 조치를 취하시기 바랍니다.

⑤온라인 수업이나 재택근무를 하는 '장소'에 주의해 주십시오.

패밀리 레스토랑이나 카페 등 공공장소에서 화상 회의나 온라인 수업에 참여하거나 파일을 열람하면 주변에 정보가 유출될 위험이 있습니다.자택 등 안전한 장소에서 진행해 주시기 바랍니다.

⑥메일의 '송신 방법'에 주의해 주십시오.

'BCC'로 송신해야 할 메일을 'TO'나 'CC'로 송신하면 같이 수신되는 연락처(메일 주소, 이름) 정보가 누설됩니다.
정보가 누설되지 않도록 같이 수신되는 메일 송신 시에는 세심한 주의를 기울입시다.

⑦ 정보 기기의 도난이나 분실에 주의해 주십시오.

본교에서도 노트북, 태블릿, USB 메모리, 휴대용 하드디스크 등 중요 정보가 담긴 정보 기기의 분실 및 도난이 발생하여 정보 유출이 일어나고 있습니다. 본교 시스템 계정이 저장된 정보 기기를 분실한 경우 등, 즉시 담당 창구 부서에 연락하시기 바랍니다.

수상한 상황을 발견하거나 느꼈다면…

자신의 계정이 누군가에게 이용되고 있을지도 모른다, 컴퓨터 바이러스에 감염되었을지도 모른다, 수상한 메일을 받았다는 등 수상한 상황을 발견하거나 느꼈다면 즉시 담당 창구 부서에 연락하시기 바랍니다.

만약 주의를 받으면……

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

- 東京大学の情報セキュリティ(UTokyo Accountでの認証が必要)
- Information Security at UTokyo（Authentication with your UTokyo Account is required.）
- https://univtokyo.sharepoint.com/sites/Security

- 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.u-tokyo.ac.jp/gen01/reiki_int/reiki_naiki/utnik-001.pdf
- https://www.nc.u-tokyo.ac.jp/guide

- 電子リソース利用上の注意
- Electronic Resources Usage Policy
- https://www.lib.u-tokyo.ac.jp/ja/library/literacy/user-guide/campus/caution

＜発行元　Issued by＞

- 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

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)
- 东京大学信息系统紧急对策小组(UTokyo-CERT)
- 도쿄대학 정보시스템 긴급대응팀(UTokyo-CERT)

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