東京大学
THE UNIVERSITY OF TOKYO

2026年度版

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

Guidelines for Information Ethics and Computer Use

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

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。

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。

P2日本語
P4 English
P6 簡体字
P8 한국어

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。その他の注意点もありますので、10ページ目の「電子リソース利用上の注意」を必ず読んでください。

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。

パスワードのみの認証はリスクがあります。**多要素認証**が設定可能な場合は必ず有効にしましょう。パスワードは名前・単語・生年月日・キーボード配列など推測されやすいものを避け、複数の単語を記号や数字でつなげる等、十分な長さの文字列を使ってください。パスワードはシステム毎に異なるものを使用してください。パスワード漏洩時は速やかにパスワード変更をしてください。

多数のパスワード を管理する方法として、紙に記録して厳重に保管する方法や、暗号化機能を備えたパスワード管理アプリ等の利用があります。バックアップを作成して保管してください。記録自体が漏れてもすぐ悪用されない工夫（例：記録時に実際のパスワードに含めない数文字を前後に付け、利用時に外して使う）をするとさらに安全です。

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。

管理権限をもつ全てのコンピュータで、ウイルス定義ファイルを最新版に保ち、定期的に全ファイルのウイルスチェックをしてください。**ＯＳやアプリケーション**は最新の修正プログラムを適用し、古いソフトウェアの利用は避けましょう。サポート終了製品は修正が行われないため、原則使用禁止です。本学提供のウイルス対策ソフトウェアの利用も検討してください。

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、スマートフォン、ポータブルストレージ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(10ページ目参照)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。

P2 日本語
P4 English
P6 簡体字
P8 한국어

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 The use of UTokyo information systems is 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 The dissemination or publication of inappropriate information is prohibited.

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) sensitive 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 The unauthorized use of copyrighted works 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 The excessive downloading is prohibited.

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. Please be sure to read the "Electronic Resources Usage Policy" on page 10.

⑤ The theft or lending of accounts (ID and password) is prohibited.

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 Set a password that is hard to guess and make use of multi-factor authentication.

Password-only authentication carries significant risks. If **multi-factor authentication** is available, always enable it. Avoid passwords that are easy to predict, such as names, common words, birth dates, or keyboard patterns.

Instead, use a sufficiently long string by combining multiple words with symbols or numbers. Make sure each system has a unique password. If a password is compromised, change it immediately.
To manage multiple passwords, you may record them on paper and store it securely, or use a password manager with encryption features. Always create and keep a backup. For added security, consider techniques that prevent immediate misuse even if the record is leaked (e.g., adding extra characters before or after the actual password when recording it, and removing them when using the password).

② Ensure thorough virus protection and software vulnerability mitigation.

Keep virus definition files up to date on all computers with administrative privileges, and perform regular virus scans on all files. Apply the latest patches to your **operating system and applications**, and avoid using outdated software. Products that are no longer supported do not receive security updates and must not be used as a rule. Consider using the antivirus software provided by the university.

③ Be alert to cyberattacks delivered via email.

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 from untrusted 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 Pay attention to where you take online classes and work remotely.

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 how you send 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 careful about the loss or theft of your information devices.

UTokyo is experiencing incidents of information leakage related to loss or theft of information devices(such as laptops, tablets, smartphones, and portable storage devices) containing important information. If you lose any information device containing the university system account, immediately contact the departmental contact. (Refer to page 10).

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则基础知识

①本校的信息系统使用仅限于“教育与研究目的”。

本校提供的信息系统（包括网络）的使用仅限于**与教育和研究相关的目的**。禁止任何不符合该目的的不当行为、违法行为以及违反伦理的行为。

②禁止发布或公开不当信息。

禁止利用本校的信息系统发布或公开以下类型的信息：

(1) 非实名（匿名、假名）信息
(2) 侵犯知识产权或肖像权的信息
(3) 属于歧视、诽谤中伤的信息
(4) 侵犯隐私的信息
(5) 淫秽信息
(6) 妨碍教育、研究的信息
(7) 妨碍他人业务或工作的信息
(8) 虚假信息
(9) 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上发布针对他人的诽谤、中伤或歧视性言论，或虚假内容。
在SNS等平台发布考试题目、答案等妨碍教学或工作的信息。
未核实真伪就传播SNS上的帖子或AI生成的文章。
发布或泄露个人信息、成绩信息、研究信息。

③禁止不当使用著作物。

擅自复制并分发音乐、视频、书籍、论文、软件等著作物的行为属于侵犯著作权，可能构成犯罪。此外，下载非法传播的音乐、视频、书籍、论文、软件程序等也是违法行为，不仅可能受到**刑事处罚**，还可能因对权利人造成损害而被要求赔偿。

④禁止大量下载。

本校订阅的电子期刊和数据库禁止一次性大量下载内容。本校与服务提供方之间已规定数据使用条件，如有人不遵守这些条件，可能导致本校整体服务被暂停。除此之外，还有其他注意事项，请务必阅读第10页的“电子资源使用时的注意事项”

⑤禁止盗用或出借账户（ID和密码）。

擅自使用他人的账户（ID和密码）属于犯罪行为。共享账户或在登录后让他人操作信息设备，均视为账户出借。所有使用者都有义务安全管理自己持有的账户、信息设备、软件等。请妥善管理本校提供的账户，并承担相应责任。

Ⅱ 东京大学信息安全规则基础知识

①请设置难以推测的密码，并启用多因素认证。

仅使用密码进行认证存在风险。若系统支持**多因素认证**，请务必启用。密码应避免使用名称、单词、出生日期、键盘排列等容易被猜测的内容，建议使用多个单词并通过符号或数字连接，形成足够长度的字符串。每个系统应使用不同的密码。若密码泄露，请立即更改密码。

管理多个密码的方法包括：将密码记录在纸上并妥善保管，或使用具备加密功能的密码管理应用程序，并做好备份。为了进一步提高安全性，可在记录时添加或删除几位字符，使即使记录泄露也难以被立即滥用（例如：在记录中添加不属于实际密码的字符，使用时再去掉）。

②请彻底做好病毒防护和软件漏洞防护。

所有具有管理权限的计算机应保持病毒定义文件为最新版本，并定期对所有文件进行病毒检查。**操作系统和应用程序**应及时应用最新补丁，避免使用旧版软件。停止支持的产品因无法修复漏洞，原则上禁止使用。请考虑使用本校提供的防病毒软件。

③请警惕通过邮件进行的网络攻击。

恶意邮件数量正在增加，包括附带计算机病毒或下载链接的邮件，以及进行钓鱼或定向攻击的邮件。请谨慎处理邮件中的附件和URL。钓鱼邮件或定向攻击邮件通常看似正常，因此请对所有邮件保持警惕。

④请避免使用不可信提供者的Wi-Fi。

若Wi-Fi提供者或其他用户存在恶意，通信内容（包括ID和密码）可能被窃取。请避免连接非可信运营者提供的Wi-Fi。传输机密信息时，请采取措施，如使用UTokyo VPN。

⑤请注意进行在线课程或远程办公的“场所”。

在家庭餐厅、咖啡馆等公共场所参加视频会议或在线课程，或查看文件，可能导致信息泄露。请在自己单独使用的房间等安全场所进行。

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请注意防止信息设备的盗窃或丢失。

本校已发生笔记本电脑、平板电脑、智能手机、便携式存储设备等含有重要信息的设备丢失或被盗，导致信息泄露。若丢失含有本校系统账户的设备，请立即联系所属部门负责人或办公室（参见第10页）。

发现或感觉到可疑情况时……

如果您发现或怀疑出现以下情况：自己的账户可能被他人使用、计算机可能感染病毒、收到可疑邮件，请立即联系所属部门的负责人或办公室。

如果收到提醒或指示……

当收到教职员工或网络管理员的提醒或指示时，请立即遵从。请勿在感染病毒的情况下继续使用计算机，也不要继续不当使用，因为这可能导致对他人的网络攻击或信息泄露风险。

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 도쿄대학교 정보윤리 규칙 기본지식

①본교 정보시스템의 이용은 '교육·연구 목적'에 한정됩니다.

본교에서 제공하는 정보시스템(네트워크 포함)의 이용은 **교육 및 연구와 관련된 목적**에만 제한됩니다. 이 목적에 부합하지 않는 부적절한 행위, 불법 행위, 윤리에 반하는 행위를 금지합니다.

②부적절한 정보 발신·공개는 금지됩니다.

본교의 정보시스템을 이용하여 다음과 같은 정보를 발신하거나 공개하는 것은 금지됩니다.

(1) 실명 이외의 익명·가명에 의한 정보
(2) 지적재산권·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) 비밀유지 의무 위반에 해당하는 정보
(10) 교육·연구 활동에서의 민감 정보

위반 사례 예시) SNS에 타인을 비방하거나 차별적인 글, 허위 글을 게시하는 행위
SNS 등에 시험 문제나 답안을 게시하여 업무를 방해하는 행위
SNS 글이나 AI가 생성한 문장을 진위 확인 없이 확산하는 행위
개인정보, 성적 정보, 연구 정보를 게시하거나 유출하는 행위

③저작물의 부정 이용은 금지됩니다.

음악, 영상, 서적, 논문, 소프트웨어 등의 저작물을 권리자 허락 없이 복제·배포하는 행위는 저작권 침해에 해당하며 범죄가 될 수 있습니다. 또한, 불법으로 배포되는 음악, 영상, 서적, 논문, 소프트웨어 프로그램 등을 다운로드하는 것은 불법이며, **형사 처벌** 대상이 될 뿐 아니라 권리자에게 손해를 끼친 경우 배상 청구를 받을 수 있습니다.

④대량 다운로드는 금지됩니다.

본교에서 계약한 전자저널이나 데이터베이스는 한 번에 대량의 콘텐츠를 다운로드하는 것이 금지됩니다. 본교와 서비스 제공자 간에 데이터 이용 조건이 정해져 있으며, 이를 준수하지 않을 경우 본교 전체에 대한 서비스가 중단될 가능성이 있습니다. 기타 주의사항도 있으니, 10페이지에 있는 '전자 리소스 이용 시 주의사항'을 반드시 읽어 주시기 바랍니다.

⑤계정(ID·비밀번호)의 도용·대여는 금지됩니다.

타인의 계정(ID·비밀번호)을 무단으로 사용하는 것은 범죄입니다. 계정을 공유하거나 로그인 후 정보기기를 다른 사람에게 조작하게 하는 것은 계정 대여에 해당합니다. 모든 이용자는 자신이 보유한 계정, 정보기기, 소프트웨어 등을 안전하게 관리할 의무가 있습니다. 본교에서 제공하는 계정은 책임감을 가지고 적절히 관리해 주시기 바랍니다.

Ⅱ 도쿄대학교 정보보안 규칙 기본지식

①추측하기 어려운 비밀번호를 설정하고, 다중 인증을 활용하세요.

비밀번호만으로 인증하는 것은 위험합니다. **다중 인증** 설정이 가능한 경우 반드시 활성화하세요.
비밀번호는 이름·단어·생년월일·키보드 배열 등 쉽게 추측 가능한 것을 피하고, 여러 단어를 기호나 숫자로 연결하는 등 충분히 긴 문자열을 사용하세요. 시스템마다 다른 비밀번호를 사용해야 합니다. 비밀번호가 유출된 경우 즉시 변경하세요.

여러 비밀번호를 관리하는 방법으로는 종이에 기록하여 철저히 보관하거나, 암호화 기능이 있는 비밀번호 관리 앱을 사용하는 방법이 있습니다. 백업을 만들어 안전하게 보관하세요. 기록 자체가 유출되더라도 바로 악용되지 않도록, 예를 들어 실제 비밀번호에 포함되지 않는 몇 글자를 앞뒤에 추가하고 사용할 때 제거하는 등의 방법을 쓰면 더욱 안전합니다.

②바이러스 대책과 소프트웨어 취약성 대책을 철저히 하세요.

관리 권한이 있는 모든 컴퓨터에서 바이러스 정의 파일을 최신 상태로 유지하고, 정기적으로 모든 파일을 검사하세요. **OS와 애플리케이션**은 최신 패치를 적용하고, 오래된 소프트웨어 사용은 피하세요. 지원이 종료된 제품은 수정이 이루어지지 않으므로 원칙적으로 사용 금지입니다. 본교에서 제공하는 바이러스 대책 소프트웨어를 이용하는 것을 검토하세요.

③이메일을 통한 사이버 공격에 경계하세요.

컴퓨터 바이러스나 다운로드 URL이 첨부된 이메일, 피싱이나 표적형 공격을 시도하는 악의적인 이메일이 증가하고 있습니다. 이메일에 첨부된 파일을 열거나 URL에 접속할 경우 충분히 주의하세요. 피싱이나 표적형 공격 이메일은 겉보기에는 의심스럽지 않은 경우가 많습니다. 모든 이메일에 경계하세요.

④신뢰할 수 없는 Wi-Fi 사용을 피하세요.

Wi-Fi 제공자나 다른 이용자가 악의를 가질 경우, ID·비밀번호를 포함한 통신 내용이 도청될 가능성이 있습니다. 신뢰할 수 있는 운영자가 제공하는 Wi-Fi 외에는 접속을 피하세요. 비밀 정보를 전송할 때는 UTokyo VPN을 이용하는 등의 대책을 취하세요.

⑤온라인 수업이나 재택근무를 하는 '장소'에 주의하세요.

패밀리 레스토랑이나 카페 등 공공장소에서 화상회의나 온라인 수업에 참여하거나 파일을 열면, 주변에 정보가 유출될 위험이 있습니다. 반드시 개인 공간 등 안전한 장소에서 진행하세요.

⑥이메일 '발송 방식'에 주의하세요.

'BCC'로 보내야 할 이메일을 'TO'나 'CC'로 보내면, 수신자(이메일 주소, 이름)가 유출됩니다. 동일 메일을 여러 명에게 보낼 때는 정보 유출이 발생하지 않도록 세심히 주의하세요.

⑦정보기기 도난 및 분실에 주의하세요.

노트북, 태블릿, 스마트폰, 휴대용 저장장치 등 중요한 정보가 담긴 기기의 분실·도난이 본교에서도 발생하며, 정보 유출로 이어지고 있습니다. 본교 시스템 계정이 들어 있는 기기를 잃어버린 경우를 포함해, 즉시 부서 담당 창구(10페이지 참조)에 연락하세요.

의심스러운 상황을 발견하거나 느낀 경우…

자신의 계정이 누군가에게 사용되고 있을 가능성, 컴퓨터 바이러스 감염 가능성, 의심스러운 이메일 수신 등 의심스러운 상황을 발견하거나 느낀 경우, 즉시 부서 담당 창구에 연락하세요.

주의를 받은 경우…

교직원이나 네트워크 관리자에게 주의나 지시를 받은 경우, 즉시 따르세요. 다른 사람을 사이버 공격하거나 정보 유출이 발생할 위험이 있으므로, 바이러스에 감염된 상태에서 컴퓨터를 계속 사용하거나 부적절한 이용을 지속해서는 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

- 部局窓口部署一覧(UTokyo Accountでの認証が必要)
- Departmental Contact List（Authentication with your
- UTokyo Account is required.）
- 部门和办公室列表（需要使用UTokyo Account进行认证）
- 부서 창구 부서 목록(UTokyo Account 인증 필요)
- https://univtokyo.sharepoint.com/sites/Security/SitePages/List_of_Departmental_Contacts.aspx

- 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