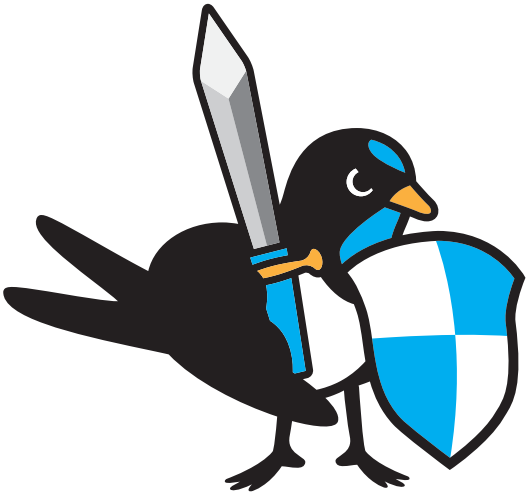
信息伦理及安全速览手册



東京工業大学

Tokyo Institute of Technology

信息伦理及安全速览手册

以下为简单的注意事项摘要。关于信息伦理及安全的详细内容请参照本册，简单易懂的 Q&A 部分总结在后。

【伦理及法规上的注意事项】

邮件及网页的浏览	要防范诈骗及侵扰 要确认信息的来源以及目标地址
SNS 及博客等的使用	要意识到 SNS 是向全世界公开的
个人信息、 隐私及人权的保护	要保护个人及他人的隐私
研究者的伦理	学生作为研究者的一员也要有高度的伦理意识
信息及知识产权的保护	特别要注意侵犯著作权的问题
软件的利用	须获得相关许可
法律的遵守	有可能被追究法律责任
教职员工	有履行就业规则的责任

【安全上的注意事项】

移动终端的使用	要注意防范信息的丢失和泄露
备份及安全更新	要定期地更新为最新版本
密码管理及对网络攻击的 对策	要始终使用安全的密码
共享设置及网络管理	要严格管理访问权限
发生故障、网络侵害、 信息泄露时的对策	要立即与系统管理员及相关部

信息伦理及安全速览手册

信息，因为在社会中传播而具有重大的意义。特别是在计算机以及连接它们的因特网上传播的信息，因其内容量之大、速度之快，在它传播的瞬间便有可能影响全世界。为了社会的稳定发展，在处理这些信息时我们需要各种各样的制约。

本手册以本校学生及教职员工为对象，简单总结了在社会中使用信息时要遵守的相关规则及注意事项。为了更好地利用信息及因特网，使它们更好地服务于生活，我们需要时时注意遵守这些注意事项，注意避免事故的发生或被卷入事故。

本手册分为上册 --- 伦理及法规篇，下册 --- 安全篇两大部分，并附有实例及问答部分。在目录部分，根据大家使用的计算机及网络环境的不同，各标有以下 5 种标志：

目录

信息伦理及安全速览手册

05 伦理及法规篇

12 安全篇

16 Q&A 篇

22 相关网页等

伦理及法规篇

我们在通过因特网自由地传播信息的同时，也被要求遵守伦理道德及相关法律。

邮件及网页的浏览

近年来，在因特网上收发信息时，无意识中发生犯罪或违法的行为并不少见。比如违法药物交易、赌博、传销或诈骗等伴随刑事处罚的违法行为。由于好奇心和巧妙的引诱手法，我们可能很轻易地就通过智能手机参与这些违法行为，所以要特别注意不要成为加害者。

通过邮件催偿借款或收取成人网站的使用费等诈骗事件不绝于耳。一旦遭遇了诈骗，多数情况下我们无法收回被骗的钱财，所以要注意不要成为诈骗的受害者。

要注意，公开自己的邮件地址就意味着增加了遭遇诈骗的风险。请注意不要在不相关处留下自己的邮件地址，这也将会导致我们耗费大量的时间处理垃圾邮件。

即使只是浏览网页，也有可能遭受侵害。如若不仔细确认网址，有可能被引入与原网页极为相似的假网站中去。这是一种以盗取浏览者 ID、密码等重要信息为目的的钓鱼网站。在我们登入网站时，要仔细确认网址，如果网址没有安全证书（开头不是 https 的网址）等，觉得可疑，就请不要输入信息。

不允许有性骚扰等让对方厌恶的行为。要知道即使是自己喜欢的事，也许正是对方所厌恶的事，因此在交换信息的时候要注意考虑到对方的感受。

邮件与普通的对话不同，感情往往容易被扩大化，需要我们有较强的自制心。不要在生气的时候发送邮件，在发邮件前有必要进行冷静地思考。

邪教或恐怖组织等的宣传、劝诱有时也是通过邮件进行的，请大家充分警惕。

SNS及博客等的使用

我们在利用微型博客（Twitter、LINE、Google+），SNS（GREE、Mobage、Facebook）* 等时也要特别注意。开设个人主页或微型博客等，对于个人的自我发现来说非常重要，它也作为表达的自由，受到保护。现在，学校对个人利用这些平台并没有特别的限制。

但是，在博客或者 SNS 上发布的信息中，大多含有与使用者的生活密切相关的信息。因此，会有个人信息被意外地公开的情况。此外，对有些发布的信息，浏览者的反应会与期待不符，严重的时候有可能出现恶意中伤的情况。

在利用这些便捷服务的时候，需要意识到以下几点。此外，在使用 SNS 时，多数情况下，初期设定会选择个人信息的公开，所以请务必事先确认设定。

- SNS 不是私人空间。
- SNS 不是指责他人的地方。
- SNS 不是忏悔自己行为的地方。
- SNS 上的发言是永久不可删除的。
- SNS 上的信息是早晚会流出的。
- SNS 上的匿名发言早晚会被识破。
- 不要忘记在使用 SNS 的人群中，也有伪善者。
- 在 SNS 上不经意的发言可能会遭到激烈的批判。

* 各公司网络服务等的注册商标

个人信息、隐私及人权的保护

因特网，通过个人主页、博客、邮件等服务，使每个人的个人信息向世界公开、传播成为可能。人们想要传递出各种各样信息是非常自然的。但是，我们需要充分了解危险的一面。

个人信息：公开个人信息是非常危险的。比如若被公开姓名、住址、电话号码、生日的话，有可能遭遇盗用等恶意操作。

当我们协助填写有报酬或礼物的问卷调查时，也面临着个人信息向第三方泄露的危险。

用智能手机拍摄的照片会包含位置等信息。个人住址等位置信息也是个人信息的一部分。当我们使用带有 GPS 定位功能的智能手机拍摄照片向博客等发布时，请注意不要加入位置信息。朋友在自己的个人住所拍摄时也要注意。位置信息也有可能给跟踪、盗窃等犯罪创造条件。

即使自己不亲自提供信息，在免费的 Wi-Fi 环境下进行的收发邮件等也会完全曝光于第三方。

他人的个人信息：我们要时刻谨记不侵犯他人的隐私及人权。
对待他人的信息，要比对待自己的信息还要慎重。要注意未经他人的许可不要公开他人的个人信息。

绝对不允许偷窥他人的邮件。例如，参与管理服务器的人员可能有机会接触到邮件的收发历史记录等，但是谁与谁收发过邮件本身，就可能是隐私问题。

在 SNS、YouTube、nikoniko 动画等动画投稿网站上投稿时，如果擅自上传拍摄有他人的影像有可能会引起肖像权或者侵犯人权等问题，所以要充分注意。

研究者的伦理

学生做为参与研究活动的一员，也必须要遵守做为研究者的伦理。

最近报告、论文等的“复制粘贴”已成为话题。剽窃或盗用的严重性可能大家也已经耳熟能详。在完成报告或论文时，将他人的文章或照片图表进行复制、粘贴等不恰当地引用即为剽窃或盗用。这不仅侵犯了他人的著作权，还违反了研究者的伦理。

在不标明出处而引用因特网上的信息内容时，即使不侵犯著作权，从研究者的伦理来说也不可为之。另外，即使是被认为值得广泛传播的内容或者像字典一样的内容也未必是真实的。一定要引用确认过出处及确凿内容的信息。

研究相关的资料数据是确认研究结果正当性的重要信息。故意更改数据的行为被称为篡改数据。篡改数据本身便是否定研究本身，违反了研究者的伦理，所以绝对不可为之。

而且，在研究内容涉及到他人隐私的时候，也要十分注意保护他人的个人信息。

除此之外，在大学中我们可能会接触到可以应用于武器或者危险品制造的技术信息。比如，把3D 打印机的相关数据或者制造过程等轻易地教给外部人士或在因特网上公开之类的事情也不要做。

信息及知识产权的保护

文字、照片、音乐等创作，从完成时起便作为著作受到相关法律的保护。不仅是纸质出版物、因特网及 CD 等电子化的信息也都做为著作受到法律的保护。他人的拥有著作权的信息原则上不经允许不能随意使用。要注意这些著作在使用时，大多会附加使用条件，特别是电子化的信息很容易被复制和发送，所以我们要特别注意不要侵犯他人的著作权。在使用 SNS、文件共享系统或免费视频网站等的时候，上述情况也同样适用。

在未经许可的情况下可以复制或使用的著作，仅限于以下几种情况：

- 为了个人使用的复制
- 在一定的条件下进行复制（在图书馆等的复制）
- 明确出处，以自己的论述为主的引用（也请参考伦理及法规篇：研究者的伦理）
- 在不影响销售的情况下以教育为目的的复制或作为考题的复制
- 为了备份而进行的程序复制（下载版中也有禁止复制的情况）
- 以非营利为目的的放映（在大学学园祭上的放映，需要另与提供录像内容的公司缔结业务使用契约，或进行音乐著作的版权处理）
- 为了报道时事事件等

而且，通过躲避复制保护等技术性保护手段进行复制的行为是被禁止的。

下面我们详细看一下关于著作的法律法规。

二次著作权：除了原著外，以原著为基础进行编辑的著作及作为数据库保存的著作拥有二次著作权。要注意即使是以电子化的方式公开的著作，也大多在利用规则中禁止随意使用自动下载功能大量下载。

著作邻接权：除了著作者本身，与其相关联的表演家，唱片制作商，播放企业也同时拥有著作邻接权，所以不要侵犯其相关权利。除了无线播放以外，有线播放的相关企业也属于播放企业。

送信可能化权：复制或重新发布因特网上的信息时也需要注意。将他人的著作在因特网上公开时，要取得本人的（通过自动公众通信送信可能化权的）许可。向免费视频网站投稿时也同样。

著作者人格权：除了复制权与放映权等与财产相关的权利以外，被称为著作者人格权的权利，即与著作的同一性，与著作相关的名字的表示及公开等也受到相关法律的保护。例如，随意更改著作的内容并将其作为原著作者的著作进行公开等是不被允许的。

动画 / 声音的商标：动画 / 声音的商标受法律保护。未经授权，随意在因特网上使用他人商标中所包含的声音或动画，是违反商标法的行为，是不被允许的。

文件的自动共享：P2P 等具有自动共享文件功能的软件可以随意共享他人的著作，所以很容易卷入侵犯他人的知识产权的事件当中。
此外，从安装有 P2P 软件的计算机中泄露重要个人信息及企业机密的事件常有报道，因此，在大学网络中禁止使用 P2P 软件。

软件许可证

U N P

软件一般通过许可证（使用许可契约）的形式进行交易。使用许可契约禁止随意在多台电脑上安装和使用软件。即使是指导教师或上司等提出这种要求，也要果断地拒绝。

如果确实需要在数台电脑上使用软件，也要根据使用台数增加使用许可契约。

在大学里，有些在研究或者业务中使用的软件已缔结了统筹使用许可契约。

其他相关法律的遵守

U N P S

遵守法律规定及其宗旨，要杜绝以下行为：

- 偷偷调查他人的账号密码，利用程序的安全漏洞访问被保护的信息。
- 通过通信终端或因特网侵入他人管理的计算机，获取被保护的信息或者对其进行删除、修改（禁止非法访问的相关法律）。
- 编写计算机病毒等（有关刑法中的非法指令电磁性记录的犯罪）。
- 发送令人不快的无意义的邮件（垃圾邮件），或将收到的垃圾邮件转发给他人。

- 对于因特网上提供的服务，通过发送大量请求，导致服务出现性能故障（刑法中的妨碍业务罪，在开展业务时，发送特殊邮件的正当化的相关法律）。
- 在主页上投稿或在博客上预告犯罪的行为（刑法中的妨碍业务罪、恐吓罪）。
- 以恶作剧为目的将研究室共用的计算机或信息加密不告诉他人密码。
- 不断重复发送骚扰邮件（骚扰等相关法律）。
- 关于性的视频（儿童色情相关法规处罚及儿童保护相关的法律，防止因提供私人视频而侵犯他人权利的相关法律）。
- 随意在主页上使用企业或商品商标（商标法）。
- 以不正当的形式获取企业的顾客信息或技术情报（防止不正当竞争法）。
- 将收集的个人信息利用于收集时承诺的目的之外（个人信息保护法、研究者伦理）。
- 未经共同研究者的同意将共同研究成果的保密部分在因特网上公开或告知第三人（著作者人格权、研究者伦理）。

  具体行为是否违法或者违反社会道德，有时可能最终需要司法的判断。例如，他人做出的违法行为，即使没有受到任何追究，自己也绝对不可以那样去做。不要自己把自己的行动正当化。此外，我们不要做容易引起他人怀疑的行为，要“瓜田李下”地严以律己。

关于就业规则---主要面向教职员工

关于国立大学法人东京工业大学教职员工的行为，要遵循就业规则的规定。教职员工同法人化前的国家公务员一样，需履行以下义务：

- 专注于工作的义务。
- 遵守法令、大学规则及遵从职务上命令的义务。
- 保守工作中的秘密。
- 禁止做出有损大学信誉或名誉的行为。
- 禁止扰乱大学规则及秩序。

例如，在办公时间利用计算机处理私人事务，将含有大学秘密的文件转送给他人，在因特网的公告板留下与业务无关的内容等都属于违反就业规则的行为。教职员工若违反了这些义务，有可能受到惩戒解雇、停职、减薪、警告等惩戒处分或训告、严重警告等。

给一同进行研究或者工作的人员发送过量的指示邮件，也会造成职权侵扰的问题。同样，给所指导的学生发送过量的指示邮件也会出现学术侵扰问题。

遇到问题时

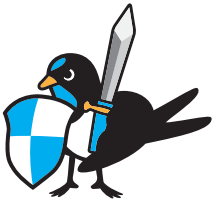
发生具体问题时，请通知信息伦理委员会

【信息伦理委员会联络地址】

邮箱：cce@jim.titech.ac.jp

安全篇

在遵守有关伦理和法律的同时，考虑到他人的攻击及计算机的故障，也为了保护自己及他人的数据，有必要在安全上采取万全的对策。以下列举安全方面最低限度的注意事项，请大家在利用计算机的时候充分注意。



移动终端的使用

U P S

利用智能手机、平板计算机、笔记本计算机等移动终端进行邮件往来或写作文书已经非常普遍。但是，一旦丢失了存有大量重要内容的邮件或数据的移动终端，其中的个人信息或机密信息就会有泄露或被恶意利用的危险。在自动转送大学的邮件到其他邮件地址时要充分注意。在注意不要在移动终端上传输机密信息的同时，为防止万一不慎丢失时被他人非法访问，需要设定好密码。

备份

U P S

用户的数据是贵重的个人财产。要时刻记住定期进行备份。如果做到定期备份，即使万一出现要重新安装操作系统的情况，也能保全各自的贵重数据。然而，备份设备有一定的寿命，其读取环境随着技术的急速发展也会有丢失的可能。意识到这一点，有必要分别采取最适当的方法进行短期备份和长期备份。如果不是机密数据，利用外部的可信赖的存档设备也是选择之一。

对病毒的对策

U P S

PC 和智能手机等移动设备都会遭受病毒的侵害。病毒有时会破坏数据，如果轻视了这一点会带来巨大的风险。更加严重的是，在不自觉中病毒的传染会通过因特网不断扩大，甚至会破坏友人的数据。针对病毒，要充分留意以下几点。

- 要在各自的 PC 里安装查毒软件。
- 养成进行定期升级和更新病毒库的习惯。

每天细密的留意和习惯，会在危险的时候保证自己不受侵害。

要注意即使安装了查毒软件也并不能保证万无一失。即使定期更新病毒库，新型的病毒刚刚出现后也有立即被感染的危险。另外，针对特定的机关或个人的目标型攻击也在持续增加。这些攻击会使 PC 在打开可疑邮件、附件文档或者可疑的网页后被感染。
为此，要注意

- 不打开发件人不明确的邮件。直接跟发件人确认。
- 即使发件人是熟人，也不要打开可疑邮件内的附件。

要彻底做到只要感到有一丝疑问就不轻易打开邮件。

有的病毒，只要浏览网页就会被感染。注意不要在好奇心的驱使下阅览可疑的网页。

不要对无法信赖的免费软件进行无必要的安装。有一种被称为间谍软件的程序，会在安装软件的同时被嵌入移动设备，在用户无法察觉的情况下，将 PC 内重要的个人信息或者 PC 的操作历史记录报告给外部。

安全更新

U P S

务必要对安装在 PC 的操作系统或者应用软件进行安全更新。如果因感到麻烦而拖延处理，到了紧急关头便会造成严重后果。要养成习惯在启动 PC 时就确认是否有必要进行安全更新。继续使用软件制造方终止提供服务的操作系统会无法进行安全更新，所以请尽早更换新的操作系统。

密码管理及对攻击的对策

U N P S W

密码如同利用信息系统时的钥匙，一旦泄露就会导致无使用权限的第三者窃用信息系统。这就如同家里的钥匙被盗招来窃贼一样。因此，关于密码管理一定要注意以下的事项。

- 即便对方是友人，也不要将密码告知他人。另外，将写有密码的便签粘贴在显示器上的行为等同于泄露密码。密码要做到只有自己知道。
- 设置足够长度的密码，避免设置他人能容易推测出的简单的密码。
- 不要设置连续的数字及重复使用同一文字的密码。
- 伪装成系统管理者，谎称需要测试系统更新后的效果，使用户在难辨真假的伪造网页上登

陆并窃取密码的钓鱼手段屡见不鲜。要知道任何系统管理员都不会做出如此要求，请勿被上述内容的邮件欺骗。

对计算机以外的复合打印机、网络相机等网络器材也需要谨慎。这些器材也可以设定密码。如果不设置密码或者保持购入时的初始密码，会使第三者从因特网上登陆这些器材，具有泄露信息的风险。请务必采取对策设置安全适当的密码。

SNS，免费邮件，云服务等的相互连结形成了便利的因特网环境。另一方面，在攻击者看来这也意味着我们将诸多重要的信息公布在网络上，存在着被攻击者入侵的危险性。在多个服务中使用相同的用户 ID 和者密码，会使他人通过分析每个信息推导出重要的邮箱密码等信息。为了避免上述的风险，要注意密码的设定以及避免重复使用相同的 ID 和密码。云服务也包含很多种类。不要将个人或者大学的重要信息上传到外部的，尤其是免费的云服务上。云服务会有突然无法使用的情况发生，所以要提前做好应对准备。

共享设置及网络管理

要尽量避免 PC 的共用。因为有泄露个人信息及机密信息的风险。即使是家人或朋友之间也切勿共用。

坚决不要共用 ID 或者密码。杜绝密码的循环使用（重复使用在其他服务上正在使用的或者曾经使用过的密码等）。

即便不共用 ID 或者密码，也存在着在诸如 Google 登陆等云服务上通过一次的登陆在邮件中接受保存文档等服务时，即使关闭了浏览器，也可能仍然保持着登陆服务的状态。在使用这些服务之后，务必留心进行登出（注销）。

高度重视共享文档的设置，留心不要共享非必要的文档。特别是在新建文档或者文件夹的时候，有必要确认其共享设置。防火墙可以在路由器或者个人计算机上设置。除去必要的情况，养成尽量关闭从外部可以访问的端口的习惯。

出现问题时的对策

故意对信息系统及信息资产进行破坏的行为自不必说，要注意由于操作失误，无意识或者无恶

意的兴趣使然的行为，在结果上也可能会导致信息系统的故障或者对他人信息资产带来损害。万一发生了这种情况，一定不要隐瞒，要立即联系系统管理员，努力防止被害扩大。

发生非法访问及信息泄露

如果发生非法访问以及信息泄露（安全事故）的情况，个人是很难对应的。要马上联系所属部门或者研究室的系统管理员，同时向负责全校安全的部门东工大 CERT 进行联系。

【东工大 CERT 的联系地址】

邮箱：contact@cert.titech.ac.jp

Q&A 篇

回答有关信息伦理及安全方面的问题。

Q. 连接个人计算机到大学网络

自己的计算机能否连接到大学的网络？如果允许的话，应该注意哪些点？

A. 请遵从研究室的网络管理员的指示。另外，校内食堂等公共区域设有无线 LAN，学生可以将自己的计算机连接至校园网络。在连接的时候，请务必细心留意自己的计算机有没有被病毒感染。本校发生过数起病毒感染事件，其中一例的感染源就是来自学生连接的计算机。同样，也请注意共享设置及防火墙的设置。

Q. 访问大学的校园门户网站为什么需要这么麻烦的步骤？

A. 访问校园门户网站的时候，需要通过 ID 密码以及矩阵认证。这是为了防止外来的非法访问采取的措施。虽然麻烦，但为了安全，请习惯于双重认证，证书认证等认证方式。

Q. 在个人计算机里安装大学的软件

可以将在研究室里购买的软件安装到自己的计算机里吗？

A. 这个问题需要从软件的许可证契约以及大学的财产使用目的的角度去考虑。只要遵从许可证契约，在许可范围内并无大碍。但这是研究室购买的物品，所以使用目的仅限于与研究室业务相关联的事物上，这点与其他物品相同。
因为有可能会被怀疑私自挪用公物，所以不要将软件安装到个人计算机上。

Q. 文献搜索

外校的熟人托我在本校可利用的数据库以及电子报刊上搜索文献，我可以帮忙吗？

A. 数据库以及电子报刊是本校缔结了许可契约后利用的，利用者范围仅限于本校所属的教员和学生。个人的学术研究・教育目的之外的使用，或者将检索结果提供给他人是违反契约的行为。如果确定有上述情况，供应方会中止本校全体的利用，所以绝对不要这样做。

Q. 下载数据库

在数据库或者学术杂志网站上下载数据或文献的时候，应该注意哪些点？

A. 曾经有数次由于本校的教员・学生大量下载文献，导致供应方中止了本校全体的使用。在教育・研究方面进行大量下载时，需要供应方的应允。如有需要大量下载的情况，请到附属图书馆进行咨询。

Q. 复制更新好的软件

因为曾发生过将感染病毒的计算机连接到大学的网络上而导致严重后果的事件，所以，我们考虑到设定规则来限制那些没有进行安全更新或者是没有更新对病毒定义的计算机连接到大学的网络。可是对于来访者而言，如果他的计算机无法连接到网络又会造成不便。而且，如果计算机不能连接到网络，它的安全更新或者病毒定义的更新也无法进行。对此，我们想制作能够在某种程度上可以安心使用计算机的 CD，可以吗？

A. 在无法确定是否更新了的情况下，访问者的计算机不能连接到大学的网络上，可以考虑把数据转移到大学管理下的计算机供访问者使用等方法。

Q. 论文的公开

在研究会等发表的论文可以在自己的主页上公开吗？

A. 在研究会等发表的论文或者在国际会议以及论文杂志上投稿的论文，通常是在投稿的时候发布在自己的主页上。然而，有的学会规定，即使论文的著作权属于作者本人也限制该论文在学会刊物之外的地方公开。特别是论文被采录后，要向学会咨询并服从学会的规定（也请参考东工大 T2R2 的运用方针）。

Q. 研究状况的公开

我可以将自己的研究课题的进度情况公开在因特网上吗？

A. 即使是个人的研究，在很多情况下这项研究本身是基于老师的指导或是受了同事的启发或者得助于未发表的研究成果。你在因特网上公开了自己研究进度，或许会违背了不希望公开的老师以及同事的意愿。另外，在不知不觉中他人看了你在因特网上公开的研究进度后，有可能会抢先于你发表相同内容的论文。结果是你将很难证明这是自己的研究成果。因此，需要谨慎对待在因特网上公开研究进度这件事。学生请和指导教员商量。

Q. 计算机及网络的使用（禁止其他目的的使用）

关于大学改革等的问题点正在网络上议论着。我通过因特网参与议论，指出了问题症结等等，我这样的行为属于处罚的对象吗？

A. 该行为并非直接的研究教育活动，而是作为一名大学人思考大学未来的重要行为。计算机和网络在广义上是寻常的信息基础平台的一部分，支撑着大学的业务运转。从这个角度看，这种行为或许并无大碍。关键是该行为在业务工作时间之内进行是否妥当，是否处罚要取决于这一层面的判断。

Q. 陈述事实也是一种中伤?

我不小心将友人不想被人知道的事实，通过群组邮件或者博客让大家知道了。我并无中伤友人的意思，只是单纯地陈述事实而已，可友人似乎无法原谅我。

A. 大家心里都清楚不能散布不实的谣言，但即使是陈述事实也会造成中伤。反而实际上造成中伤的，大多数是类似这样的事例。要充分注意，即便是陈述事实也有可能造成对他人的损害名誉或者侵犯人权。

Q. 如何界定个人之间的交流?

针对我的邮件，友人进行了相当强烈的反驳，并以 CC 给其他友人的形式发给了我。如果只是给我单独的回信，属于个人间的交换意见，并没有什么问题，可是像这种擅自在群组邮件里 CC 回复的做法恰当吗?

A. 在某种程度上，这有可能演变成在公共场合强烈批判个人的行为。会被认作损害他人名誉，所以在参考对方邮件或将对方邮件添加为附件的时候，一定要事先得到对方的许可。

Q. 复制保护

通过软件解除 CD 或者 DVD 的防止复制功能（复制保护）并进行复制的行为属于侵害著作权吗?

A. 著作权法第 30 条第一项提到，以在个人或者是家庭内等在规定的范围之内使用为目的的情况下，使用者对著作物的复制是被许可的（私用目的的复制）。然而，在明知道通过解除技术性保护手段使其变为可复制的事实的情况下仍然进行了复制的行为，就不属于私用目的的复制（同项目第 2 号）。

上述事例，就是通过软件在明知道防止复制机能被解除的情况下使用其软件并进行复制，所以不被认定为私用目的的使用，而是属于对著作权（复制权）的侵犯。

Q. 多人利用客户机 / 服务器系统的程序

想在校内客户机 / 服务器系统的服务器上保存一个程序，使客户机能暂时调用并使用的做法，在法律方面应该注意哪些点？

A. 不仅需要取得把一个程序复制到服务器上的复制权许可，而且要从程序的著作权拥有者那里得到发信可能化权的许可。有关这类的使用，多数情况下都需要获得有关许可的许可证契约。

Q. 多人使用服务器上的电子书籍

在校内的内部网系统里，在服务器上保存非程序的电子书籍等著作物，例如一册电子百科辞典，并供多数客户使用时，应该注意哪些点？

A. 即使是被许可复制到硬盘上的电子百科辞典，多数客户的利用也存在被限制的情况。另外，自己利用扫描仪将书籍电子化，就是所谓的开小灶也可能出现问题。

Q. 对计算机的入侵以及恶意破坏

对计算机的入侵以及破坏具体包括哪些？

A. 大家对“病毒”“蠕虫病毒”“特洛伊木马”等词语一定不会感到生疏。这些被称作恶意软件的程序，会通过计算机非法获取个人信息，或者对系统进行恶意的操作。另外，还存在着通过大量的集中访问点击，使网络服务器陷入瘫痪的攻击。

正因为各种各样新型的入侵方式会陆续出现，才非常有必要做好最新的安全对策。

Q. 防止恶意入侵

为了防止恶意入侵，应该注意哪些点？

A. 因为 Windows 等复杂且规模庞大的操作系统存在着安全漏洞（也可以视作软件的缺陷），入侵者便乘虚而入。对于已被检测出的安全漏洞，软件制造方会提供《补丁程序》，请自己留心进行安装。这种操作一般被称作“打补丁”。另外，将自己的计算机连接到设置有“防火墙”的网站的同时，在自己的计算机上安装防火墙也是非常重要的。除此之外，利用查毒软件不松懈对病毒的检测也是很重要的。

Q. 因特网上侵害自己名誉的留言

有人在博客里发布了损害自己名誉的留言，我该怎么做？

A. 可以请求博客的管理员（服务提供商）进行删除该留言。在多数情况下，仅靠本人是难以应对的。也可以向法务局或者警察等申诉人权侵害或者名誉损害，请求援助。当留言过多的时候，也可以使搜索引擎无法显示出来，但是其手续也非常复杂。也有必要依靠律师等专业人员的协助。如果不知道该找谁商量，可以向法援（日本司法支援中心）进行求助。

【法援（法テラス）的官方主页】

http://www.houterasu.or.jp/index.html

相关主页

【东京工业大学信息伦理委员会（信息伦理委员会与安全向导）】
http://www.titech.ac.jp/rinri/

【东京工业大学信息系统紧急应对小组】
http://cert.titech.ac.jp/

【东京工业大学信息伦理原则】
http://www.jyoho.jim.titech.ac.jp/kik_sui/security/policy_1.pdf

【东京工业大学信息伦理安全原则】
http://www.jyoho.jim.titech.ac.jp/kik_sui/security/policy_2.pdf

【关于信息安全事故发生时的报告】
http://www.jyoho.jim.titech.ac.jp/kik_sui/security/index.html#higai

当发生信息安全事故的时候，需向文部科学省国立大学法人支援课进行汇报，因此，请在填写确认事项表格之后，联系研究推进部情报基盘课企划组（kib.kik@jim.titech.ac.jp）。
关于确认事项表格，并不需要全部填写完再递交，请在了解到突发情况后第一时间迅速汇报。

信息伦理委员会 WG

委员长　金子宏直 准教授

副委员长　胁田 建 准教授

石川 谦 准教授

樱井 实 教授

伊东利哉 教授

山口雅浩 教授

渡边 治 教授

横田治夫 教授

友石正彦 教授

饭田胜吉 准教授

松浦知史 准教授

佐藤礼子 准教授

战 晓梅 准教授（监译）

秋友丰香 广报・社会连携课长

田中 升 教务课长

松原康夫 情报基盘课长

（顺序不同）

（专业用语中文翻译监修）金勇 特任助教

（事务）情报基盘课 小寺 孝志、森谷 宽

信息伦理及安全速览手册

発行年月（初版）　平成 17 年 4 月 1 日
（第 2 版）平成 28 年 4 月 1 日
企画編集　情報倫理専門委員会 WG
発　　行　東京工業大学

201703.300 / gram inc.