筑波大学
University of Tsukuba

为了安心·安全地使用信息系统

在使用筑波大学的信息系统（网络、电脑等）时，有必须遵守的规章守则。使用本校的信息系统前，请确认以下与规章守则相关的选项，在自己符合的条目上打上记号。 如有不符合的条目时，请阅读手册内的说明，在遵守规章守则的前提下，使用本校的信息系统。此外，本手册的详细说明可在 **https://oii.tsukuba.ac.jp/oii-security/details/** 上查阅。

☑Check！

- ☐ 没有非法拷贝或让第三者能够使用网络阅览有版权的作品
  （著作权法作了修改，从 2012 年 10 月起，违法下载将受刑事处罚。）
- ☐ 没有安装文件共享软件
  文件共享软件的代表性例子有 Xunlei, BitTorrent, μTorrent, LimeWire, Cabos, WinMX, Share, Winny, PerfectDark 等。
- ☐ 不要下载，安装来路不明的软件
- ☐ 定期实行 Windows Update 等，使用最新状态的软件
- ☐ 安装杀毒软件。并且经常更新病毒定义文件以防治最新的电脑病毒
- ☐ 没有将密码告诉他人
- ☐ 没有使用他人的用户名和密码
- ☐ 没有设定简单的密码
- ☐ 对个人信息等进行全面管理，采取了防止信息泄露措施
- ☐ 向社交网络等互联网发布信息时，请自觉以筑波大学的一员规范自己
- ☐ 使用网络时，有注意对滥用网络的诈骗行为（钓鱼式诈骗，单击诈骗等）进行提防
- ☐ 注意不打开可疑邮件

情 报 环 境 机 构

没有非法拷贝或让第三者能够通过网络阅览有版权的作品

所谓著作权法，是“以确定关于作品、表演、录制品、广播和电视节目的著作者的权利及与之相关的权利，注意这些文化产品的正当利用的同时，谋求保护著作者的权利，为文化的发展作出贡献为目的”的法律。在未经作者许可，以及法律允许范围之外，拷贝、让第三者能够通过网络阅览他人著作的，将受到处罚。此外，在明知上载的音乐、影像等已侵犯版权的情况下还对其下载的行为将受到处罚。

没有安装文件共享软件

由于文件共享软件同时会散发电脑病毒等恶意文件，使用时非常危险。并且下载的文件自动会上载给他人。在筑波大学，即使是私人所有的电脑也禁止在大学内部网络里使用文件共享软件。**学校采取自动屏蔽文件共享软件的网络通讯的方式，**使用者也有可能受到学校处分。

如希望在校内将文件共享软件用于正当目的的，请联系本手册末尾的咨询处。

不要下载，安装来路不明的软件

若见到来路不明的网站免费或低价提供本来很高价的软件，也绝不要下载。 很多时候这些软件的提供未经授权，不单侵犯版权，而且软件本身已被改造因而有感染计算机病毒的危险。 筑波大学监控着来历不明软件的下载行为，触犯者或受校内处罚。

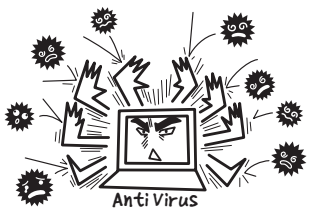
定期实行 Windows Update 等，使用最新状态的软件

电脑病毒针对 OS（Microsoft Windows、macOS 等）及其常用软件（Microsoft Office, Adobe Flash Player, Adobe Reader, Java 等）里存有的缺陷进行感染。因此，在 Microsoft Windows 上，请定期运行 Windows Update、Microsoft Update 等操作；在 macOS 上，则请定期进行软件更新，一直让其保持为最新状态。此外，厂家不再提供维护的旧版本 OS，必须升级到最新版本。其他软件也请不断更新为最新版本。

安装杀毒软件。
并且经常更新病毒定义文件以防治最新的电脑病毒

在感染上电脑病毒时，不仅仅破坏电脑的数据，还将利用被攻占的电脑向外发送垃圾邮件、攻击其他电脑等。电脑病毒不仅仅通过邮件传播，还可以通过浏览网页，使用 USB 内存盘时等发生感染，其感染途径正趋于多样化。因此不要因为粗心大意的操作而感染上电脑病毒，请安装杀毒软件，并定期更新病毒定义文件。筑波大学提供的防毒软件可以安装在不超过 3 台的私有 PC 等 (Windows, Mac, 移动端末) 上。如果你的机器上已装有的防毒软件不确定是否已付费，可以安装大学提供的防毒软件。

详细信息，请阅览 **https://oii.tsukuba.ac.jp/oii-security/details/**



没有将密码告诉他人

进入筑波大学的信息系统时，所用的用户名和密码，是使用电脑者本人特有的重要信息。将自己的用户名和密码告诉给他人，让他人使用筑波大学的信息系统，当他人发生问题时，告诉他人密码的你也要负相应的责任。反过来，也不能使用他人的用户名和密码。

没有使用他人的用户名和密码

通过某种方式得到他人用户名、密码，冒充他人登录，或者利用安全漏洞（程序问题）等，避开用户名、密码验证而登录等情况均违反了有关禁止不正当访问行为这条法律。

没有设定简单的密码

设定容易猜测的密码（与用户名、个人姓名、生日、电话号码等相同，重复同一文字，重复英文单词，键盘上的同一排列（qwerty 之类），以及以上各种情形的逆序）时，可能遭受不正当访问的侵害。因此请设定难以被猜测的密码（比如 8 文字以上，混合英文字母的大小写，符号、数字的密码），并定期更换。即使是难记的密码，写在备忘本等上时，请不要放在他人容易看到的地方。

另外，不要在不同的网络服务上使用同一口令。在别处泄漏的口令被用来非法登录校内电脑并发送垃圾邮件的事案已有发生。如果你使用多个系统，可以考虑利用口令管理软件来管理各个口令。

对个人信息等进行全面管理，采取了防止信息泄露措施

不用说教职员，即使是学生，也有可能通过课程、演习时的问卷调查之类得到个人信息或诊疗信息等。这些个人信息，不得将其公布在网上。并且原则上禁止将其带出校外，有不得不将其带出校外的情况时，也应当在管理该信息者或其委任人（如任课教员或研究室的指导教员）的许可下，实行加密等安全措施后再带出。此外，尽量不要将个人信息存放在自己个人管理的电脑上。不得已的情况，要施以加密保护。

向社交网络等互联网发布信息时，请自觉以筑波大学的一员规范自己

在互联网上的言行，有可能被多数的人看到。因此，轻率的投稿难免会引起麻烦或带来别人对你作为本校一员的理智的怀疑。请注意不要在互联网上发布不应公开的私密事项或者有伤风化的信息。

为了防止更进一步的感染，请切断被感染电脑的网络（拔掉网线、外接无线网卡，关闭内置无线网卡等），到本手册末尾的咨询处进行咨询。

使用网络时，注意对滥用网络的诈骗行为（钓鱼式诈骗，单击诈骗等）进行提防

使用网络得到方便的同时，也有可能被卷入意想不到的麻烦中。以下介绍学生生活支援室学生生活课发行的“安全的生活～为了过上舒适的学生生活～”小册子中关于使用网络时应当注意的诈骗行为。在面临问题，且自己不能判断时，不要轻易尝试随便的解决方法，而应跟朋友、教职员等商量，或者到消费生活中心等进行咨询。

钓鱼（Phishing）式诈骗

所谓钓鱼诈骗，是指冒充银行，乐天，亚马逊，苹果，微软等等实际存在的网站的管理员，引诱你去访问貌似的诈骗网站，骗取 ID 和暗号的行为。银行等不会通过电子邮件让输入或确认个人信息。因此有可疑通知时，请联系本来的公司，不要轻易输入个人信息，不要与发来的通知里的联系地址联系。

单击式诈骗（单击商法）

所谓单击诈骗，是指只点击了 1 次电子邮件或网页上的链接，就被单方达成了合同，被要求支付费用的诈骗。不要理会这样的诈骗要求，不与不相识的人联系，不将住址、姓名等告诉不相识的人，不汇现金到不记得使用过的付款要求里。

但是，有可能有滥用裁判手续的要求。对于这种情况，不要忽视来自法院的通知，请与从法院网站（http://www.courts.go.jp/）确认到的联系地址联系，不要与寄来的通知里要求的联系地址联系。

注意不打开可疑邮件

本校确认了不少各种伪装邮件。有的是装成电邮系统管理员来的，欺骗你访问伪造网页进而盗取账号信息的钓鱼欺诈邮件；有的是装成送货员的送货通知，欺骗你打开附件后感染病毒从而进行网络空间攻击的可疑邮件。如果觉得标题，送件人，内容等等与你无关或邮件可疑，请予以删除。不要轻易打开附件，也不要访问邮件中的链接网页。

（参考）全校计算机系统上收集的钓鱼欺诈邮件：https://www.u.tsukuba.ac.jp/phishing-collection

当发现问题时，请报告

如有发现筑波大学信息系统的安全脆弱性及其问题，侵犯版权，泄露机密信息、个人信息等行为，或筑波大学的机密信息、大学成员的个人信息等被公开在校外信息系统，以及大学拥有权利的内容被擅自使用时，请尽快与以下咨询处联系。

咨询处

信息环境机构（学术信息部信息基盘课）
e-mail ▶ oii-security@oii.tsukuba.ac.jp

更详细的说明请参照此网页：**https://oii.tsukuba.ac.jp/oii-security/details/**

本手册由筑波大学信息环境机构信息环境企划室制作。

2020 年 3 月发行