为了守护您的生活和研究，
度过安全而又充实的 JAIST 生活

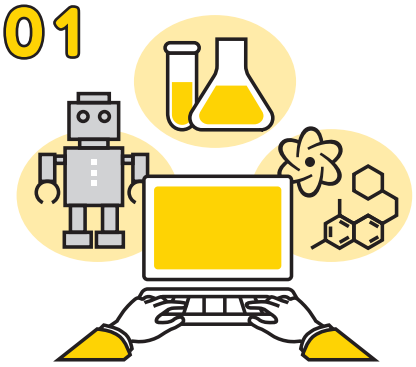
信息安全宣传册

对于研究活动和日常生活来说，电脑和网络已经成为不可缺少的重要工具。而其使用，会伴随各种危险，如果使用方法错误，很容易让您的研究或生活受到威胁，或人生由此被打乱。本校为了守护您的生活和研究，将信息安全方针及社交媒体指南等作为规则 / 规定进行规定。作为属于本校成员中的一员，请您务必遵守这些规定。在使用本校的信息环境系统之前，请确认本安全宣传册的确认表，进行确认。如果有不符合或不明白之处时，请阅读宣传册内的说明，按照规则使用信息环境。

在使用本校的信息环境系统之前，请确认本安全宣传册的确认表，进行确认。
如果有不符合或不明白之处时，请阅读宣传册内的说明，按照规则使用信息环境。

信息安全措施

01



JAIST 的 ICT 环境，要理解为是为了教育、研究后利用。

关于怎样的利用被认可为教育、研究目的，强烈依存于各自的研究内容，因此不能做一样的判断，但当疑似为目的之外的利用时，请自行考虑是否能解释为用于教育、研究目的。尤其是学生，指导教员是否认可其解释会变为判断材料。当难以进行判断时，请预先向指导教员咨询。

02

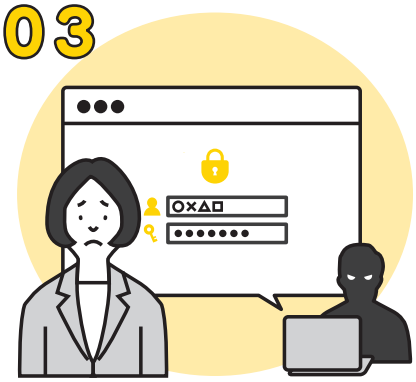
不设定简单的密码。密码不告诉他人。

密码请设定为他人难以推测的非常复杂的密码 (※)。另外，发生过重复使用与校外服务相同的密码，由于密码从该服务泄漏而被非法访问的事例。请有效利用密码管理软件等，避免重复使用。当然，您的用户名和密码也不可告诉他人。当让他人使用时，会被做什么等所有的责任将由您承担。

另外，本校职员绝对不会要求您公开您的密码。

※建议您使用 10 个字符以上，由多种文字类型（大小字母、符号、数字）组合，并容易记住的密码。用户名、自己的名字、生日或电话号码，键盘的同一排等容易被推测出来。详情请参照末尾记载的“补充信息・链接集”。

03



不使用他人的用户名 / 密码等进行非法访问。

除了利用安全漏洞等，非法访问未被允许的系统等这种确凿的行为外，使用某种方法取得他人的用户名 / 密码，变为他人使用服务，或固执地持续访问相同页面，在没有意识到的情况下给服务带来了不良影响时，也会被视作非法访问行为，可能被追究刑事或民事责任。

04

进行 OS 或应用程序的定期更新，在最新的状态下使用软件。

电脑病毒，恶意使用 OS (Windows 或 macOS 等) 或经常使用的软件 (Office，Java 等) 的缺陷进行感染。

请定期进行“Windows Update”或“ 软件升级 ”，总是保持最新的状态。其他的软件也总是更新为最新版。建议按照最新的安全补丁自动被应用的设定使用。

此外，PC 以外的智能手机或网络设备（无线 LAN 路由器等）、IoT 设备 (因特网家电等) 等，连接网络的设备也请总是更新为最新版本。

05

使用本校指定的杀毒软件。

总是使用最新的病毒定义文件。

如果 PC 感染恶意软件，除了发生 PC 的数据被破坏 / 泄漏这种直接的受害外，电脑本身还有可能被远程操作，被用于发送垃圾邮件或对别的地方进行攻击。恶意软件，除了被用邮件等发送过来外，还会从网页、USB 存储器等各种路径感染。为了不会因为不注意的操作而感染恶意软件，请使用与本校要件一致的杀毒软件 (※)，病毒的定义文件也请定期更新。

※作为杀毒软件，销售或发布的种类很多，但是其中，有一些性能存在疑问，或看不到充分的效果。因此，本校制定了应使用的杀毒软件的要件。详情请参照末尾记载的“ 补充信息・链接集 ”。

06

注意不要打开钓鱼邮件或可疑的 WEB 页面。

请注意诈骗银行或信用卡公司、手提电话公司、门户网站等盗取个人信息等的钓鱼邮件。如有可疑的邮件，请向原本的公司等咨询，而不是写在该邮件上的联络方式。

请不要访问用 SNS 或搜索引擎等找到的盗版软件、在版权上有问题的视频 / 音乐 / 漫画、违法的药物 / 武器 / 色情页面、销售个人信息等的 Web 网站。除了不法行为会被处罚外，还可能感染恶意软件。

信息安全措施

07

对有关个人信息和研究的数据进行彻底管理，采取对策防止信息泄漏。

在大学，会举办各种各样的教育研究活动，其中，有时会使用有关个人信息或研究的文件或数据。教职员不言而喻，即便是学生，有关自己本身的研究的研究数据或讲义等也许也会使用个人信息。有关研究的数据或法人文件等，请按照本校的信息分级指南适宜地使用。

尤其在研究数据中，武器或可转用于军事等的涉及安全保障之物，可能会被限制带出到国外。用电子邮件等操作时，也要注意弄错收件人或误操作。

08

不违法复制他人的著作，不让其在网络上处于第三方可阅览的状态。

除了书籍、论文、报告、音乐、影像，刊载在 Web 页面上的文章或图像、软件、应用程序也属于著作。未经拥有著作权者的许可，在法律的允许范围外复制著作，在网络上让其处于第三方可阅览的状态属于违法。

此外，侵害著作权上载的音乐或影像等，如果在知道该事实的情况下进行下载，也属于违法。

09

SNS 等向网络发送信息，作为本校的成员，要在遵守伦理道德的基础上进行。

因特网上的发言或动作，可能会让很多人看见，很容易由于个人的简单加注而引发问题，或发生本校或本校成员的良知受到质疑等事态。请注意不要发送本来应视作秘密的事项，或违反公序良俗的内容的加注等不适宜的信息。请理解本校的社交媒体指南，理解在 SNS 上发送信息时的基本须知。

10

本校外部的人员不可让其使用本校网络。

对大学外部的人提供与本校 LAN(无线 / 有线) 的连接性，会让其访问限定校内提供的信息或服务，置整个大学于危险之中。
为此，除了访客的使用已被允许外，不允许提供。

此外，如果以逃避审阅等为目的，在校内使用 VPN 或通信匿名化的应用程序，会向他人提供因特网连接性，让校内限定信息等被全世界的用户访问，非常危险。因此，不可在校内无准备地使用这些应用程序。

11

不使与法律相抵触、威胁安全的应用程序。

即便是初看方便的应用程序，当不是很了解其结构时也要注意。
例如，在文件交换应用程序 (尤其是称为 P2P 型之物) 中，就有转发他人共享的文件的自动公众发送功能，这样，可能会进行无意识的不法行为。

请仔细调查应用程序的结构或评价等，当有可能与法律相抵触，或可能威胁到安全时，请在使用前向指导教员或信息社会基础研究中心咨询。

※与法律相抵触，威胁安全的可能性高的应用程序举例
- 通信匿名化 /VPN/ 通信限制迂回应用程序
  VPNgate, Tor, Hotspot Shield, SpotFlux, HolaUnblocker, Mobility XE, Freenet,Hamachi 等
- 具有自动公众发送功能的文件共享应用程序
  Xunlei, LimeWire, Cabos, Winny, WinMX, Share，eMule, Perfect Dark, 等

12

掌握发现有关信息安全的问题时的咨询 / 报告窗口

攻击方的技术也在年年进步，无论怎样特别注意，还是有可能被钓鱼，感染恶意软件。这种时候，最重要的是迅速报告、咨询。

您自身感染恶意软件等问题发生时自不必说，当您发现本校的信息系统在安全上存在脆弱性或异常时，有版权的侵害行为或机密信息或个人信息等被泄漏时，或在校外的信息系统发现大学的机密信息或本校成员的个人信息等被公开时等，请马上向下述地址联络。

有关JAIST CSIRT的联系信息，请参见下一页

确认！

01 ☐ JAIST 的 ICT 环境，要理解为是为了教育、研究后使用。

02 ☐ 不设定简单的密码。密码不告诉他人。

03 ☐ 不使用他人的用户名 / 密码等进行非法访问。

04 ☐ 进行 OS 或应用程序的定期更新，在最新的状态下使用软件。

05 ☐ 使用本校指定的杀毒软件。

06 ☐ 注意不要打开钓鱼邮件或可疑的 WEB 页面。

07 ☐ 对有关个人信息和研究的数据进行彻底管理，采取对策防止信息泄漏。

08 ☐ 不违法复制他人的著作，不让其在网络上处于第三方可阅览的状态。

09 ☐ SNS 等向网络发送信息，作为本校的成员，要在遵守伦理道德的基础上进行。

10 ☐ 本校外部的人员不可让其使用本校网络。

11 ☐ 不使用与法律相抵触，威胁安全的应用程序。

12 ☐ 掌握发现有关信息安全的问题时的咨询 / 报告窗口。

但是，关于这些方面的部分内容，当具有研究目的等正当的理由时，有时也会被作为例外而许可。请事前按照本宣传册末尾的咨询方式咨询。

有关信息安全的问题的咨询 / 报告窗口

JAIST CSIRT

JAIST
JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY 1990

E-mail
sec-incident@ml.jaist.ac.jp

通报 URL
https://www.jaist.ac.jp/csirt/

本宣传册的补充信息・链接集
https://www.jaist.ac.jp/iscenter/security/

0761-51-1300
（信息社会基础研究中心/工作日白天）

0761-51-1000
（防灾中心/假日・夜间）

制作 JAIST 信息社会基础研究中心 (2021.09)