INFOSS 信息伦理 速习版

目录

教材的构成

将按照以下结构推进信息伦理的学习，请一边复习一边进行。完成全部内容后，请关闭教材并挑战“结业测试”。

序章 互联网基础

在网络（有线或者无线，信息设备之间连接的结构）社会中，与现实社会一样，许多人进行着沟通交流。网络社会中应当遵守的规则和礼仪，与现实社会的规则礼仪有许多共同点。

例如，即使是在使用您所在学校的内部网络时，也需要自觉意识到自己是学校组织的一员，并采取有责任感的行为。

本章将学习参与网络社会时最基本的思想准备和注意事项。

0-1 互联网素养

互联网是继报纸、广播、电视之后诞生的新型媒体。然而，通过这个媒体接收信息时，与报纸、广播、电视相比，更需要充分注意所获取信息的可靠性。

在互联网上，无论是公共机构，企业，甚至普通个人，都可以轻松地在 SNS（用于建立人际社交联系的线上服务。可以通过网页浏览器或者应用程序使用）上发帖，上传（将自己的电脑中的文件通过网络发送至其他计算机）视频。因此，互联网信息并不总是高度可信。通过互联网获取的信息是否正确，需要由我们自己来判断。

1．媒体素养

信息往往经过发布者的意图加工后才形成。例如，刻意强调某一部分或反复呈现某些内容，会改变信息给人的印象。因此，接收者可能会以与原意不同的方式理解信息。

为了不被片面信息或谣言（传闻，流言）所迷惑，需要理解媒体的特性并且具备判断能力。能够主动，批判性地分析和评价获得的信息，这种能力就称为媒体素养。

判断信息时特别应注意以下 4 点 ：

通过多个信息来源（如书籍，报纸，电视，博客等）进行确认。
谁会从这个信息中获利、谁会受损，培养判断信息是否因利害关系而被传播的习惯。
思考数据的获取方式，呈现方式，及数据展示的真正目的。
思考“说了什么”以及“没有说什么”。
考虑信息是由什么立场，带着什么意图的人所发布的。

2．信息伦理

互联网遍布全球，使人们能够不受时间与距离的限制进行交流和信息交换。但与此同时，也出现了例如不当信息被故意传播，以往不存在的新型犯罪增多等问题。

“信息伦理”（信息道德）指的是本来处理信息时“人应遵守的原则”，不仅在网络（有线或者无线，信息设备之间连接的结构）社会，在现实社会中也同样重要。随着互联网普及，人人都可以轻松发布和接收各种信息，信息伦理的重要性进一步提升。

与现实社会相同，在网络社会中为了不给他人造成困扰，不卷入犯罪，需要充分的心理准备与具体知识。

为了享受网络社会带来的便利，我们每个人作为网络社会的一员，都必须认真地把信息伦理的重要性当成自己的问题来思考。

0-2 网络犯罪

以互联网为代表的信息通信技术（ICT）普及，使日常活动变得更加便利。但与此同时，遭遇各类纠纷和风险的危险性也随之增加。

根据日本总务省发布的《2023 年通信利用动向调查》（2024 年 6 月公布），日本国内互联网使用率（个人）为 86.2%。在 13 岁至 59 岁的各年龄层中，互联网用户比例均超过九成。除了企业和团体，针对个人、手段巧妙的网络犯罪也在增加，伴随着智能手机的普及，近年各类受害事件频发。

1．网络犯罪趋势

2023 年（令和 5 年），网络犯罪的查处件数为 12,479 起，自 2021 年以来持续处于高位的被捕件数。

违反《禁止非法访问行为法》的被捕件数为 521 起，与上一年（522 起）几乎持平。以大学等学术机构为目标、在窃取信息的不正访问行为发生频繁。

与非法指令电磁记录以及计算机/电磁记录相关的犯罪达到 1,000 起，较上一年（948 起）有所增加。信用卡盗用和网银非法转账案件数量创历史新高。

恶意软件造成的损害，特别是使用勒索软件的手段显著增多。不仅限于数据加密模式，还出现了“不加密数据、直接以公开窃取的信息为威胁”的勒索模式也在增加。

网络犯罪查处数量变化推移

2019 年 2020 年 2021 年 2022 年 2023 年

违反《禁止非法访问行为法》

有关非法指令电磁记录的犯罪以及计算机/电磁记录相关犯罪

违反《儿童买春·儿童色情禁止法》

欺诈罪

违反《著作权法》

其他类型犯罪

资料：根据警察厅《关于 2023 年网络空间威胁形势等的报告》制作

0-3 学校使用规定与礼仪

1．参加远程授课

为防止新型冠状病毒感染的扩大，使用 Zoom、Microsoft Teams 等视频聊天系统的远程授课与视频会议得到了广泛普及。

在参加远程授课时，请注意以下事项：

软件或应用程序请从官方网站下载。

注意避免误发送信息或不必要的背景曝光。

不要将课程链接（URL）或会议号码泄露给非课程参与者。

姓名请使用真实姓名（若学校另有指示，请遵照执行）。

※ 若未使用真实姓名，可能会被认为是无关人员，被计为缺席或被拒绝进入远程课堂。

着装应整洁得体。

请不要迟到。
集中注意力，请不要一边做其他事情一边听课。
未经许可不得擅自拍摄、录像或录音（如果获准许可，也必须在适当范围内使用）。

0-4 手机的使用

1・设备本体的管理

使用智能手机或移动电话等移动终端的人，通常会在设备中存储家人、朋友或熟人的电话号码、电子邮件（指电子邮件的发送目的地（地址）。电子邮件地址由“@”分隔，前半部分是用户名（账户），后半部分是表示组织名或国名的区域名。）地址等个人信息。手机的丢失或随意放置可能导致个人信息泄露。为了保护亲友的个人信息，必须对自己的手机进行负责任的管理。
具体要点如下：

- 为防止丢失或被盗，应设置密码并开启锁屏功能。
- 更新操作系统（OS），保持设备在最新状态。
- 对于智能手机，请勿进行改装（比如更换电池或更换零部件）。
- 应用程序要从可信来源（官方应用商店）下载。
- 对于安卓设备，在安装应用前，请确认其权限申请项目。
- 安装应用后，也要定期查看该应用的评价与安全性。
- 根据评价，有些应用出于保护隐私的考虑，最好予以卸载（删除已安装的软件。软件若不按照指定步骤进行卸载，可能无法从系统中完全删除。）。
- 智能手机上需要安装安全软件。

2．使用注意事项

使用智能手机或移动电话等移动终端时，必须遵守以下礼仪。同时，在有他人在场时，注意顾及他人感受，例如避免大声通话等。

拍摄功能使用注意事项

使用移动终端的拍摄功能进行照片或视频交流的人日益增多。虽然拍摄便捷带来了方便，但随之也产生了「偷拍」和「数字扒窃」（指使用带摄像头的手机拍摄书店的杂志或书籍内容的行为。）等犯罪行为。
即使是随意拍摄的照片或视频，未经当事人许可就将其发布到网页（通过「Google Chrome」、「Microsoft Edge」、「Safari」等浏览器可以查看的、包含文本、图片、视频或音频的页面，

采用 HTML 格式编写。）或 SNS（用于建立人际社交联系的线上服务。可以通过网页浏览器或者应用程序使用）上，也可能构成对隐私权、肖像权或著作权（保护小说、电影、音乐、美术、程序等作品的权利。该权利归属于作者。在日本，著作权分为作者人格权与著作权两部分。）的侵犯，所以请务必杜绝此类行为。

人气偶像特集

边走路边使用手机非常危险

一边操作智能手机一边走路是极其危险的行为。不仅可能撞到行人，还可能引发与汽车、自行车相撞的事故。现实中已发生因在车站楼梯上看手机而摔倒，或从站台跌落的事故。此外，由于对周围环境疏于注意，也可能被可疑人员盯上。

这不仅仅是危害自身安全，还可能波及他人。请认识到"低头走路"是危险行为，绝对不要这样做。

驾驶时禁止使用

许多事故是由于驾驶汽车时使用移动终端所导致的。驾驶时请关闭电源或开启驾驶模式，如需使用手机，请将车停在安全地点后再进行。驾驶时使用手机是违反《道路交通法》的行为。此外，骑自行车时操作智能手机等分心驾驶行为，属于违反道路交通法第 70 条规定的安全驾驶义务。

这是因为无论是驾驶汽车还是自行车，在行驶过程中使用智能手机等设备，注意力会集中在屏幕上，从而延迟对周围状况的察觉，导致事故发生。同时，如果佩戴耳机等设备，也会无法通过声音感知周围环境，因此而引发事故。

请避免在驾驶时进行使用智能手机等违法行为。

第 1 章 用户认证与账户

在网络社会中，为了识别本人身份而进行设置的就是账户。账户由用户 ID 和只有本人知晓的密码组成。

账户扮演着网络上的使用许可证的角色，因此需要妥善保管。若因管理疏漏或疏忽导致账户信息被他人知晓，不仅可能卷入意想不到的重大犯罪，有时甚至可能危及其所属组织的整个网络安全。

本章将学习如何设置安全的密码以及使用和管理密码时的注意事项等内容。

1-1 密码的设置与管理

密码是重要的信息，请严格管理以防止被他人知晓。

此外，设置密码时，有必要想办法避免使用容易被他人推测的字符组合。

由于各个学校规定可能有所不同，请遵循学校的规定。

1．密码的管理责任

密码是证明电脑使用者即注册者本人的重要信息。若被恶意的第三方知晓，可能导致系统遭受非法访问，甚至可能危及整个系统和网络的安全。

切勿轻视区区一个密码的重要性。黑客只需一个密码侵入系统后，还可能进一步入侵网络上的其他系统，并将其用作犯罪的跳板。仅仅一个人的疏忽可能会给所有系统使用者带来麻烦。请务必注意密码的管理。

2．使用密码时的注意事项

使用密码时，请遵守以下注意事项：

不要将密码告诉家人或亲密的朋友。

不要将密码写在显眼的地方或贴在显示器上。

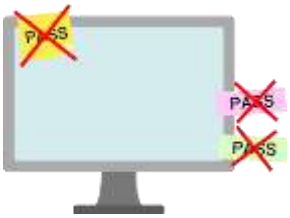
不要将密码保存在共用电脑上。（不使用自动完成功能。）

不要将密码念出声。

不要在邮件中写入密码。

输入密码时，需要注意防止他人窥视手指的动作。

若怀疑密码被盗或被他人看到，请尽快更改密码。



3．不良密码示例

以下为容易被他人猜测的不良密码示例，请尽量避免设置此类密码：

自己、家人、朋友或宠物的名字（Masako、Pochi、Tama 等）

使用自己的生日、电话号码等他人易于获取的个人信息组成的字符串（July04 等）

字典中收录的单词

地名、人名、球队名等专有名词（Kyoto 等）

全部相同的字母（AAAAAAAA 等）

曾经使用过的密码

键盘上相邻的字符串（asdf、qwer 等）

将上述密码拼写反转或者仅添加数字的形式（Otoyk77、masako3 等）

请避免使用键盘上相邻的字符。

4.设置好密码的技巧

以下为通常认为好密码的设置标准：

混合使用大写字母、小写字母、数字和特殊符号。

自己容易记住，但他人难以推测的字符串。

具有足够的长度，10 个字符以上。

5．设置更安全密码的窍门

采用以下方法可以创建更安全的密码：

使用句子中的首字母单词

将只有自己知道的事实转化为英文（或罗马字表示的日文）。

例文： Our family went to Nikko by train in April.

取单词首字母 → ofwtnbtia

混合大小写 → OfwtNbtiA

加入特殊符号 → OfwtNbtiA#

6．密码重复使用存在风险

几乎所有的互联网服务在注册时都需要设置密码。每注册一项新服务，就需要一个新密码，密码一多，记住它们就变得很困难。

但是，因为怕麻烦而全部使用相同密码是非常危险的行为。

假设某个互联网服务发生密码泄露了。如果在其他服务也设置了相同密码，就有可能被他人擅自登录。这被称为“账号盗用”。曾发生过因购物网站或 SNS 的密码泄露导致 LINE 账户被盗用的案例。

因此，请尽量避免在多个服务中重复使用同一密码。

列表型攻击（密码列表攻击、列表型账户黑客攻击）

使用非法获取用户 ID 和密码列表尝试进行非法访问的攻击。由于许多用户在网络购物等各种网站重复使用同一密码，此类攻击已造成实际损害。

市面上也有销售用于管理各服务所密码的密码管理工具。

此外，为不同服务设置不同密码时，也可采用在日常使用的密码后添加服务名称缩写的方法。但应注意，像「line」、「facebook」等，原始密码与服务名称的区分方式若容易被推测则并不合适。这种做法一旦某个服务密码泄露，其他服务的密码也可能被轻易推测出来，所以存在风险。若在密码中包含服务名称，应尝试混合符号等方式加以处理。同时，请勿直接使用此处示例中的密码。

IaulBET# + l!E（LINE） → IaulBET#l!E

IaulBET# + f!K（facebook） → IaulBET#f!K

1-2 非法获取用户 ID 与密码

破解（Cracking）是指恶意侵入他人的计算机或网络系统，进行破坏数据、篡改信息或偷窥等行为。而从事这类行为的人被称为黑客/破解者（Cracker）。

破解者会通过各种手段窃取他人的密码并侵入网络。以下是几种主要的攻击手段：

暴力破解攻击 (Brute-force Attack)

这是一种尝试所有可能的字符组合的“穷举法”。虽然人工操作非常困难，但如果交给计算机处理，且密码长度较短，则可以在（相对）较短的时间内轻松破解。

字典攻击 (Dictionary Attack)

破解者使用专门用于破译密码的“字典”（词汇表）。通过程序尝试字典中记录的所有单词来破解他人密码。大型字典可能包含多达 30 万个词汇，不仅有英文单词，还包括著名科学家、

政治家、运动员及偶像的名字。

社会工程学 (Social Engineering / Social Cracking)

这是一种利用心理陷阱的手段。破解者冒充管理员或相关人员，通过电话、邮件等方式骗取用户的密码。 此外，偷看键盘输入（肩窥）或翻找垃圾（搜寻有用信息）也属于社会工程学的范畴。

键盘记录器 (Keylogger)

键盘记录器是一种记录用户键盘输入记录的软件。最初是程序员为了调试代码而开发的工具。然而，现在常发生网吧电脑被植入键盘记录器导致密码被盗的事件。因此，明智的做法是避免在网吧等公共计算机上输入重要的个人信息（如账号、信用卡号等）。

网络钓鱼 (Phishing)

诱导用户访问要求输入用户 ID 和密码的假冒网站，从而窃取信息的手段被称为“网络钓鱼”。这是一种被视为非法访问的犯罪行为。

密码一旦落入破解者之手，对方就会通过身份冒用获取更多信息。甚至可能将该计算机作为“跳板”侵入其他网络，导致损害进一步扩大。因此，密码管理至关重要。

通信拦截 (Eavesdropping / Sniffing)

互联网上的通信存在被拦截的风险。但是，通过后文提到的通信加密技术，即使通信被拦截，内容被解密的概率也会降得非常低。因此，在输入 ID 和密码等重要信息时，请务必确认通信是否已加密。

特别是可以免费使用的公共 Wi-Fi，如果没有设置密码（即未加密），通信内容极易被拦截读取。此外，在使用酒店等不特定多数人使用的电脑时也需格外注意。

备忘录应用

智能手机等设备上的备忘录应用非常方便，因为数据会自动保存到云端。但如果云服务器存在

漏洞，则存在信息泄露的风险。因此，请勿在备忘录应用中保存密码等重要信息。

1-3 认证方式

用于认证用户的方式，除了前面章节学习的密码之外，还有以下几种。

一次性密码认证

为了防止因非法访问导致密码被盗，有一种方式叫做一次性密码认证。顾名思义，一次性密码是在每次登录时生成、仅使用一次随即作废的密码。即使被他人知晓，该密码在下次登录时也已失效。

生物特征认证

将用户本人的身体特征作为生物信息使用的认证方式称为生物特征认证。用于认证的特征包括指纹、面部、声纹、手掌或手指静脉、眼睛虹膜等，每种都需要专门的设备。　在这些方式中，最普及的是指纹认证。笔记本电脑、USB 存储器，以及最近出现的智能手机等小型且易被盗的设备，都开始配备指纹传感器进行销售。　由于生物特征认证使用的是身体特征，因此可以避免丢失或忘记的问题。但另一方面，成本较高，并且可能因随时间推移的变化、受伤或疾病等原因，即使本人也可能出现认证失败的情况。　最初，因为利用的是身体特征，难以复制，所以被认为比密码认证方式能提供更强大的安全性。然而，最近破解生物认证的技术也在进步，因此已不能断言其绝对安全。

3．多因素认证

有些银行采用将 IC 卡与手掌或手指静脉认证相结合的方式，这称为双因素认证。

此外，还有密码与指纹组合等方式。将多种要素组合在一起的认证方式统称为多因素认证。相比单一的认证方式，能够提供更强大的安全性。

4．双重验证

为了与多因素认证一样强化认证，双重验证技术也开始被广泛使用。双重验证是指在登录网络服务或应用程序时，完成登录 ID 和密码认证之后，额外再进行一次其他验证的安全措施。仅使用 ID 和密码进行认证时，一旦发生密码泄露等情况，就可能允许非法访问。而使用双重验证时，因为需要持有智能手机等设备，所以被认为具有更高的安全强度。

第 2 章 网络基本注意事项

电子邮件是日常生活中频繁使用的联络手段。此外，还有论坛、X（原推特）、LINE 等可以发布信息、收发消息的社交媒体。而且，网页不仅可以浏览，还可以自己创建并公开。

本章将学习在互联网上收发信息时应该了解的规则和礼仪。

2-1 社交媒体（SNS）的使用

1. 使用社交媒体时的注意事项

社交媒体作为互联网上的沟通工具，已爆炸式普及。虽然能够轻松发布信息，但也可能因欠缺考虑的随意发言而伤害他人或构成犯罪行为。在发帖前，请务必注意以下事项：

引用他人发言时要准确无误。

不发诽谤中伤、淫秽言论、侵犯隐私的言论。

不发歧视性言论。

注意发言信息的内容。

注意照片的发布。

不拍摄过激视频。

不发布“恶意扰乱店铺运营”（如针对店铺的恶搞骚扰行为）等构成妨碍业务罪的骚扰视频。

不发布个人隐私信息。

不发布爆炸、杀人等犯罪预告。

不使用不必要的标签。

在小组使用时，不发送私人消息。

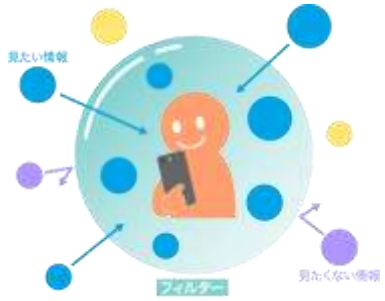
在论坛发言时，确认运营方针和规则，避免发表与论坛主旨无关的言论。

注意有关选举的帖子。

信息茧房（Filter Bubbles）

互联网上的各种服务，通过追踪浏览记录、根据偏好显示搜索结果（过滤），采用了向用户选择性推送其可能感兴趣信息的系统。其结果，由于网页搜索历史等原因，系统会预测并显示符合用户兴趣爱好的内容，导致信息被局限于符合自己喜好的范围内，这种现象称为"信息茧房"。

因此请记住，互联网上存在这样的机制：你喜欢的或倾向于浏览的内容会被优先显示。



回音室效应（Echo Chamber）

在 SNS 或互联网论坛上，如果只与价值观相近的用户深入交流，就会逐渐只接触到相似的意见。

这种现象因其类似于信息在封闭空间内不断回响，故被称为"回音室效应"。

在封闭的网络空间中，需要注意，被与自己相似的意见包围，会更容易导致自己的思维方式变得更加偏激和强化。

2．辨别信息的真伪

例如，仅仅因为看到网站上"A 公司股价会上涨"的帖子，就立即购买该股票，从媒介素养的角度来看，这并非恰当的行为。需要考虑网站这种媒介的匿名性等特征，确认其是否是虚假信息。

假信息、错误信息与谣言的扩散

不符合事实的虚假信息或错误信息称为假信息/错误信息（Fake News）。

有些帖子只是为了增加点击量、吸引关注，或是出于诽谤中伤的目的。其中也存在为了在政治或选举中获取优势而恶意使用的情况。为了不被这种虚假信息迷惑并妥善应对，具备辨别信息真伪的素养非常重要。

此外，在地震发生后等混乱时期，有时会出现如"动物园动物逃跑了"、"购物中心发生火灾"等趁乱传播的谣言。

这类信息有时会被广泛扩散，但我们需要核实事实、获取佐证，慎重应对。

例如在 2021 年，就曾有 YouTuber 因散布谣言，将一名与路怒症施暴者无关的普通女性称为"翻盖手机女"，并谎称其与事件有关而被起诉。谣言扩散导致受害女性接到了大量骚扰电话和诽谤中伤的帖子。受害女性以名誉受损为由，提起了赔偿请求。

这类谣言会伤害他人、将人逼入绝境，甚至夺走其正常生活。成为谣言的加害者，就必须承担法律责任。因此，请注意不要不负责任地传播无依据的信息。

深度伪造（Deep Fake）

指利用人工智能技术制作的伪造视频。由于使用了非常先进的图像识别和合成技术，因此难辨真伪。

例如，通过将某位政治人物的影像与他人的影像合成，可能会被用作虚假信息，仿佛是该政治人物在发言。

因其使用了人工智能研究成果之一——深度学习算法，故得此名。

网红（Influencer）

指在互联网上对用户的购买行为具有强大影响力的人。特别是在 SNS 上拥有大量粉丝的知名博主、YouTuber、Instagrammer、TikToker 等都属于网红。

暗中委托网红并支付酬劳，让其进行如介绍自家产品等公关活动的行为，称为隐形营销（Stealth Marketing）。普通用户有时会受到这种隐形营销的鼓动或欺骗而购买商品。

因此，不要全盘接受网红的信息，应自己多方收集信息并进行确认。

生成式 AI

指根据通过聊天或语音输入的问题，AI 自动生成文本、图像、视频等的服务。例如 ChatGPT、Copilot（原 Bing Chat）、Gemini（原 Google Bard）等服务。ChatGPT 中的 GPT 是 Generative Pre-trained Transformer 的缩写，是一种可以用日常语言与 AI 对话的机制。它支持多种语言，包括日语。因其能根据用户输入的提问或图像，输出宛如人类般自然的回复文本或图像，应用范围正在不断扩大。

然而，其输出内容未必总是正确的。此外，输出的内容也可能涉及侵犯版权，使用时请注意。

2-2 网络游戏

1．注意消费，合理使用

网络游戏可以让众多用户通过互联网同时参与。其中有许多内容非常吸引人，例如对战或协作击败敌人。

但是，为了在游戏中获取某些道具，有时需要进行充值消费。请注意不要沉迷其中，避免花费巨额金钱。

同时，请自己严格控制游玩时间。昼夜颠倒的玩法会导致生活不规律，对健康和学业产生不良影响。

2．网络游戏中的欺诈

存在利用网络游戏内的聊天功能，将用户诱骗至钓鱼网站以非法获取个人信息的网络钓鱼诈骗。此外，也有诱导安装恶意软件或非法应用程序的手段。

恶意用户会花言巧语地进行欺骗，例如："注册就能获得游戏内购物货币"、"赠送强化角色的道具"、"交易稀有武器吧"等等。因此，请警惕聊天中看似"好事"的提议。

3．游戏实况

指将自己玩游戏的过程录制并上传为实况视频的行为。然而，游戏是受著作权保护的，未经制作公司等许可擅自上传，原则上会构成侵犯著作权法。

关于实况视频，如果遵守一定的指导方针（例如不上传包含游戏结局的最终场景等），有时游戏公司会允许上传实况视频。

2023 年 9 月，就有人因擅自公开可以了解游戏全部剧情的实况视频并获利，而被判有罪。上传的视频包含了从游戏开始到结局的全部内容。

将游戏实况视频上传到视频网站时，请务必充分考虑著作权问题，并确认允许发布的范围。

2-3 IT 技术的滥用

3D 打印机

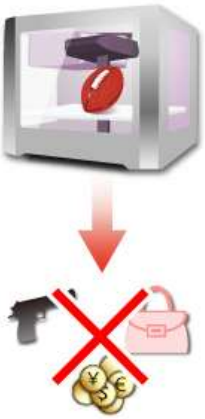
3D 打印机和激光切割机可以根据设计图制作出三维立体物品。但是，并非任何物品都能制作，制作下列物品可能构成违法。即使能获取设计图，也请不要考虑制作以下物品：

枪支刀具（具有杀伤能力的武器）

仿冒品（如名牌商品等）

伪造货币

淫秽物品



IoT 的问题

迄今为止，互联网主要连接的是计算机、服务器等 IT 设备。

近年来，电视、数码相机、空调、音箱、汽车等各种"物品"也开始连接到互联网。这种将以往未连接到互联网的物品进行连接的技术，被称为"物联网"。
它有很多优点，例如可以远程控制物品、通过物品收集信息、实现物品间的对话等。但另一方面，它也伴随着风险。例如，以下问题日益凸显：
一个产品存在缺陷，可能导致整个系统变得脆弱。
由于物联网技术本身也在不断发展，旧设备随着时间的推移，其安全性会下降。
不同领域的设备和服务相互连接，其相互间的可靠性存在隐患。
个别用户可能会采用制造商未预料的连接或使用方式。

在上述情况下，实际发生了以下事件：
监控摄像头的影像被窃听并公开。
实验设备被黑客攻击，陷入危险状态。
家用电器感染恶意软件，进行 DDoS 攻击（物联网恶意软件）。

因此，连接互联网时需要充分注意每台设备的脆弱性。每台设备都内置了软件（固件），如果发现安全漏洞，请立即安装安全补丁。
同时，请不要继续使用物联网设备不牢固的初始密码，在开始运行前应更改设置。
此外，物联网设备很多情况下通过无线方式进行初始化和更新，存在通信被拦截、设备被劫持的风险。因此，请确认无线局域网是否已加密。

第 3 章 互联网上的交流

互联网作为交流工具发挥着重要作用。然而，因与他人联系而产生的纠纷也层出不穷。
本章将列举当前成为问题的案例，学习互联网交流中应有的正确态度。

3-1 电子邮件引发的受害事件

电子邮件虽然便捷方便，但也可能遭受以下类型的损害：
1. 邮件引发的纠纷

冒名顶替

电子邮件可以冒充他人身份发送邮件。收到可疑内容的邮件时，不要直接回复，而应通过电话等方式直接向本人确认，必要时可咨询系统管理员。
曾发生过一起案件：一名大学生盗取了他人的 ID 和密码，冒充该学生向其已获得内定录取的公司负责人发送了拒绝录用的邮件，最终被捕。为避免此类情况发生，请务必妥善管理自己的 ID 和密码。

邮件诈骗

近年来，还出现了以"环境保护"或"儿童福利"等名义发送电子邮件骗取钱财的案例。若要进行捐赠，请务必通过正规机构进行。

垃圾邮件

未经收件人事先同意、无差别大量发送的邮件称为垃圾邮件（也称为骚扰邮件或 Spam）。垃圾邮件以宣传广告为主，但其中也不乏以诈骗为目的的邮件。垃圾邮件不仅会增加网络线路的负载，还会使收件人承担通信费用，因此作为违法行为已成为一大社会问题。未经收件人同意，以营利为目的发送直邮广告的行为是违法的。

垃圾邮件行为在社交网络中也十分猖獗，常向不特定多数用户发送广告信息。若发现重复进行恶劣垃圾邮件行为的账号，应向管理员举报并要求其停止使用。

3-2 交流中的注意事项

1．SNS 上的受害案例

近年来，由于对交友网站的监管日趋严格，在 SNS 上进行类似交友网站信息交换的案例有所增加。然而，根据发布内容的不同，可能构成处罚对象。

此外，由离家出走的儿童遭受侵害的"出走者留言板"也成为了问题。这些留言板上，持有少量资金的儿童为寻找住宿而联系他人，对儿童而言是充满危险的接触渠道，实际上已导致多起涉及儿童性交易、暴力伤害等犯罪的案例。

若发现此类留言板，应向警察等相关窗口举报，协助查处。

跟踪骚扰行为

单方面对抱有好感的对象、曾有恋爱关系的对象、前配偶等持续纠缠的行为，作为跟踪骚扰行为，已被《跟踪骚扰行为规制法》所禁止。

该法律不仅禁止实际进行埋伏、在对方住处附近徘徊等行为，还将被拒绝后仍持续发送邮件、在 X 等 SNS 上反复纠缠留言等行为列为"纠缠骚扰等"予以禁止。2021 年修订后，未经本人同意使用 GPS 获取位置信息、被拒后仍持续发送文书等行为也被新增为规制对象。

诱骗

指以性虐待为目的者接近儿童，通过巧言令色获取信任并拉近距离的行为。
近年来，利用 SNS 进行的诱骗已成为突出问题。加害者常伪装身份使对方放松警惕，通过询问对方兴趣爱好并提供其可能感兴趣的信息来建立亲密关系。最终可能发展为网络跟踪，或诱导线下见面进而实施性虐待。
为防止受害，首先应避免随意与 SNS 上认识的人见面。若需见面必须保持高度警惕，即使对方提出性要求也要明确拒绝。

人肉搜索
指根据 SNS 上发布的照片或视频，锁定当事人住址、姓名等个人信息的人（或团体）。作为提供个人信息的回报，人肉搜索者有时会从委托人处收取报酬。
此类搜索行为和委托可能被跟踪者滥用。因此，请勿随意上传可能泄露个人信息的图像或视频。
现实中已发生多起案例：上传人物照片后通过瞳孔倒影中的风景锁定地点、根据窗外景色推断位置，甚至因上传料理照片时面部反射在勺子上而被识别出容貌。

私人逮捕类 YouTuber
根据日本《刑事诉讼法》第 213 条，普通民众可逮捕现行犯，但该行为的适用条件规定极为严格，不应轻率实施。然而，目前出现一类"私人逮捕系"YouTuber，他们武断地将非犯人者认定为罪犯进行逮捕，并拍摄上传视频，这已成为社会问题。为博取流量而刻意拍摄犯罪或逮捕场面的行为本身就极具危险性。

2．匹配交友应用
匹配交友应用是近年来兴起的新型服务。其作为连接网络用户的应用程序，有时被用于与交友网站类似的目的。
该类应用在注册时需通过驾照或护照等进行年龄验证。部分平台还强制要求关联 Facebook 账户或通过手机号认证等方式确认本人身份。虽然设有交友网站不具备的用户认证限制，但与相识者线下见面仍可能引发纠纷。需注意的是，《交友网站规制法》将未满 18 岁者定义为"儿童"，要求相关企业、监护人、国家及地方政府必须努力防止儿童通过匹配交友应用使用网络异性介绍服务，并特别规定企业负有确认用户非儿童的义务，以及采取防止损害儿童健康成长行为的措施。

3．虚假 SNS 账户

目前出现多起冒用学校等机构官方 Instagram 账号的伪造账户问题。这些伪造账户冒充机构身份，向不慎受骗的关注者发送虚假信息。

随着越来越多学校将 SNS 用于宣传或联络工作，不仅限于 Instagram，对 X 等平台的伪造账户也需保持警惕，注意辨别是否为真正的官方账号。

3-3 有害信息

1．助长犯罪的网站

网络上存在一些承接杀人等犯罪活动的网站，警察厅正在对此类网站进行严厉打击。

这类网站中，有些是以承接业务为幌子、旨在骗取钱财的诈骗网站；有些则是真正承接犯罪业务并伤害他人的犯罪网站。此外，犯罪组织也会利用此类网站进行毒品密卖或非法账户的转售。

无论属于哪种情况，接触这类网站极易卷入犯罪活动，或导致自己被追究刑事责任，极具危险性。请务必绝不与此类网站取得联系。

暗黑兼职（闇バイト）

社交媒体（SNS）上常会出现招揽“高薪兼职”的广告。这些所谓的“暗黑兼职”通常以“短时间、轻松赚钱”为诱饵，诱导他人从事违法行为。例如，有的委托内容仅为“运送包包”，但包内其实是违禁药品，导致当事人在未察觉的情况下参与了违法活动。

最近，作为犯罪组织洗钱环节的“钱骡（Money Mule）”兼职问题日益突出。所谓“Mule”即骡子。犯罪组织利用与自己无直接关系的兼职人员代为转账，将其作为非法资金的“搬运工”。当事人虽然没有犯罪自觉，只是办理了转账手续，却在不知不觉中参与了洗钱（Money Laundering：掩盖资金来源），并可能因此受到处罚。

此外，还有一些案例是让人在电信诈骗（如冒充熟人诈骗）中充当负责接收现金的“取款手（受け子）”。

工作简单却报酬丰厚的情况是不符合常理的，因此请远离这些可疑的兼职。

这类招聘通常会要求发送学生证或驾照的复印件，从而获取你的个人信息。一旦你试图拒绝，对方可能会利用这些信息威胁并强迫你继续从事犯罪行为。请务必注意不要轻易提供个人信息。同时，滥用个人信息本身就是犯罪，如果遭到犯罪威胁，请立即向警方求助。

3-4 网络欺凌与恐吓行为

1．网络欺凌

网络欺凌是指在互联网上的博客、留言板等平台，针对个人或群体进行诽谤中伤的行为。网络欺凌的特点是施暴者人数极多且具有匿名性，还可能导致个人信息泄露或侵犯隐私。在网络发言时，请务必换位思考，发表充满关怀的言论。

近年来，在社交媒体（SNS）上孤立他人的欺凌现象也时有发生。

此外，还存在一些被称为“学校地下网站”的非官方留言板，专门讨论特定学校的话题，这使得欺凌和中伤问题更加严重。虽然这类网站难以发现，但一旦发现，请立即向学校老师等报告，将受害程度降至最低。

2．复仇式色情（Revenge Porn）

复仇式色情是指为了报复，将前配偶或前交往对象的私密性影像、照片散布到网上的行为。随着智能手机的普及，拍摄照片和视频变得轻而易举，这使得复仇式色情成为一种严重的骚扰手段。数据一旦在网上扩散，现实中极难彻底删除。甚至还出现过以“将淫秽照片传到网上”为由进行恐吓的案例。

为了避免此类受害，请务必注意：即使是交往对象，也不要轻率地让对方拍摄私密照片；即便对方要求“发张照片过来”，也绝不要发送。

另外，根据《复仇式色情防止法》（正式名称：《关于防止提供私密性图像记录等造成被害的法律》），将私下拍摄的性影像公开到网上，将被处以 3 年以下有期徒刑或 50 万日元以下罚金。

3．摄影罪（性姿态等摄影罪）

2023 年，日本制定了《性姿态拍摄等处罚法》。该法律旨在强化对偷拍及非法拍摄行为的监管，因为这些行为是导致儿童色情和复仇式色情的原因之一。在该法律中，明确规定了“摄影罪（性姿态等摄影罪）”。虽然此前已有取缔偷拍的法律，但新法扩大了对偷拍及非法拍摄行为的处罚范围。

触犯“性姿态等摄影罪”将被处以 3 年以下有期徒刑或 300 万日元以下罚金。

不仅拍摄行为本身，提供（分享）或保存此类拍摄数据的行为也将受到处罚。

第 4 章 网络交易

通过互联网进行的各类交易日益增多，但由于无法直接面对交易对象，诈骗行为容易泛滥，受害金额逐年攀升。此外，还存在卷入违法交易的风险。

本章将通过具体案例分析网络交易中的陷阱，学习如何防患于未然。

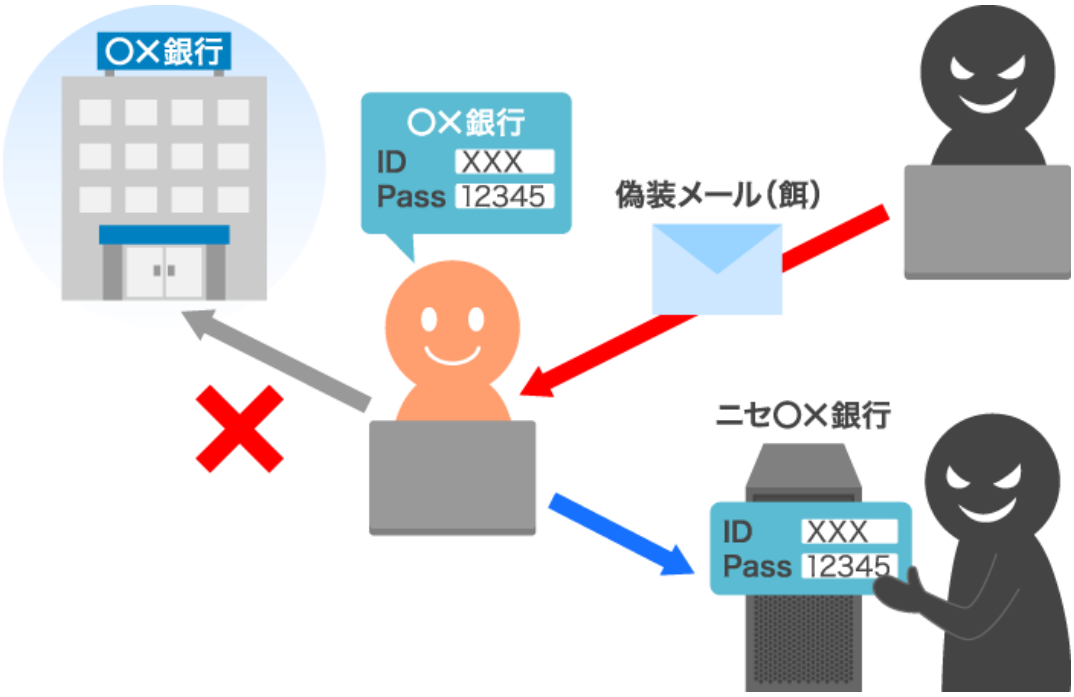
4-1 钓鱼欺诈

1. Phishing

网络钓鱼是指冒充正规邮件或网站，窃取密码及信用卡号码的诈骗行为。由于网页本身易于复制，导致大量用户误信伪造网站而遭受个人信息被盗的损失。

其主要手法是：冒用金融机构、信用卡公司、电商平台、票务公司等名义群发邮件，诱导收件人点击邮件正文中的 URL 链接，进入伪造的银行、运营商、电商等网站，进而骗取个人信息。

近年来，短信服务（SMS）也成为被滥用的渠道，这种欺诈被称为“短信钓鱼”（Smishing）或“短信欺诈”（SMS Phishing）。常见手法包括伪装成快递公司发送“包裹已送达但因您不在家而退回，请通过下方网址确认”等通知，诱导用户访问钓鱼网站。其中部分信息还会诱骗用户安装恶意应用程序。2020 年还出现了新型手法：智能手机日历会悄然添加日程安排，点击显示的 URL 链接即被引导至钓鱼网站。



切勿轻易相信邮件发件人姓名，务必核实网站 URL 的真实性。同时请确认是否采用 SSL 或 SET 等加密技术。

此外还存在更具欺骗性的“网络嫁接（Pharming）”手法。

语音钓鱼（Voice Phishing）

这种与网络钓鱼相似的诈骗手法，通过诱饵邮件引导受害者接听语音电话，进而窃取个人信息，简称 Vishing（Voice Phishing）。

传统网络钓鱼诱导用户点击伪造网址输入信息，而语音钓鱼则在邮件中标注电话号码，诱骗用户拨打后通过语音应答系统窃取个人信息。

防范此类诈骗的关键在于：切勿轻信邮件中的电话号码，务必通过官方网站等渠道核实。

近年来，利用 AI 技术的犯罪手段中出现了“声音深度伪造”。不法分子通过 AI 生成高保真声音，冒充他人实施诈骗电话，诱导受害者访问伪造网站。即使来电声音与熟人相似，也需警惕诈骗风险，切勿轻信可疑内容。尤其涉及金钱事务或自称金融机构来电时，请立即挂断电话并核实号码真实性。

4-2 点击诈骗

1. 一键点击诈骗

存在一种名为“单击诈骗”的骗取费用的手段。当用户在某网站点击按钮时，会突然弹出要求支付会费等费用的页面。

此外，点击电子邮件中的 URL 链接时，也可能遭遇同样的突然收费要求。

屏幕上会显示诸如“会员注册已完成”‘请将会费汇至以下账户’“若一周内未完成手续将采取法律措施”等信息。

其中还存在一种手法：在显示“已读取您的信息”的提示时，同时展示电脑 IP 地址及浏览器信息等内容，伪装成已获取个人隐私的状态。

2. 手机诈骗软件

在成人网站等平台尝试观看视频时，常会遭遇诱导下载专用播放应用的骗局。一旦安装，虚假收费界面便会反复弹出，最终骗取用户费用。此类诈骗不仅存在于可疑应用中，甚至伪装成看似实用的图片编辑软件，需格外警惕。

一旦安装诈骗应用，即使关闭收费界面，经过一定时间后仍会反复弹出收费画面。

此外，安装时诈骗应用可能窃取通讯录信息。安卓设备用户需特别留意安装时“访问权限”或“权限”栏显示的项目。若个人信息被犯罪分子窃取，可能收到通过短信发送的恐吓信息。

4-3 网购

1. 网购的主要纠纷

随着网络购物的普及，相关纠纷也呈上升趋势。

主要纠纷类型

围绕网络购物，已出现以下各类纠纷：

预付货款后未收到商品。

收到的商品与订购不符，或为假冒商品。

被要求支付未订购商品的款项（例如信用卡信息遭窃取）。

无法联系到销售方，其网页也已消失。

咨询时遭到敷衍搪塞。

此外，在网络拍卖的个人间交易中也存在类似问题。由于个人交易难以锁定对方身份，买家往往只能自认倒霉。

2. 隐形营销（Stealth Marketing）

指在不被普通用户（消费者）察觉的情况下进行宣传活动。有时简称为“隐形营销”。

伪装成普通信息提供者，以口碑传播的形式在社交媒体发布宣传或推广特定企业商品的帖子。即所谓的“托儿”手法。通过托儿进行的隐形营销可能构成违法行为。

此外，在 Instagram 等社交平台还存在通过为特定商品大量点击“点赞”获取报酬的“代点赞业务”，以及承接虚增粉丝数量的代运营机构。

需警惕此类托儿文章与虚假评价的误导。隐形营销往往导致“点赞”数量或粉丝数异常增长，务必审慎评估其可信度。

第 5 章 安全防护措施

互联网存在着计算机病毒、安全漏洞导致的非法入侵、窃听等风险。

本章将学习为保护个人信息和系统而必须掌握的安全措施，包括病毒防护和通信加密等内容。

5-1 电脑病毒

1・什么是计算机病毒

所谓“计算机病毒”，是指为在计算机系统中引发某种故障而制作的计算机程序。

从计算机的角度来看，它与 Word、Excel 等软件同属“程序”范畴。其运作方式如同流感病毒般，会在用户不知情的情况下潜入计算机内部引发故障，或通过电子邮件等途径侵入其他计算机（即感染），因此得名计算机病毒。

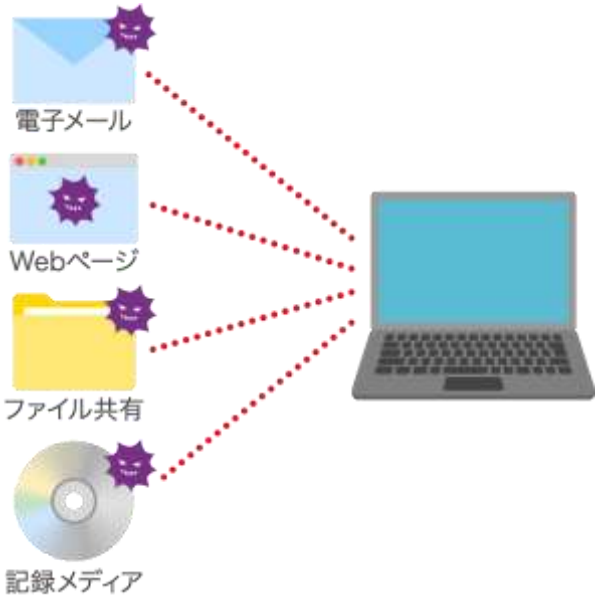
智能手机与电脑相同，虽然可以自由添加应用程序，但这些软件中可能混有计算机病毒。

此外，恶意程序的统称称为恶意软件（Malware）。

2・病毒的感染途径

病毒的感染途径主要有以下四种。除这些途径外，还存在通过 USB 设备感染病毒的案例。

电子邮件	通过打开附件感染
网页	执行下载文件，或浏览利用脚本/ActiveX 漏洞的网页感染
文件共享	文件共享软件的共享文件夹被植入感染文件导致感染
存储介质	通过感染病毒的 CD、DVD、U 盘等介质传播



病毒通过互联网可瞬间扩散，造成巨大损失。打开外部文件前务必进行病毒检测，同时注意浏览器警告信息，立即停止访问可疑网站。

技术支持诈骗

此类诈骗通过在用户电脑显示“已感染病毒”等虚假信息，伪装成正规技术支持人员诱骗用户拨打指定电话号码，从而骗取技术支持费用。

有时会反复在浏览器弹出虚假警告，导致浏览器无法操作，进而诱导用户访问虚构的技术支持网站。

即使出现“病毒感染”等提示也请保持冷静，直接忽略警告。

若遇到反复弹出陌生提示的情况，请安装正规渠道获取的杀毒软件进行检测。

3・疑似感染时

若怀疑计算机感染病毒，请采取以下措施：

立即断开网络连接。
停止使用该计算机。
向系统管理员报告。
尝试使用杀毒软件修复。
（需从未感染的计算机访问杀毒软件开发商官网下载杀毒程序，将其复制到 CD 等介质后在受感染计算机上运行修复。）

若杀毒软件无法修复，则需删除受感染系统并重新安装干净系统。

4・计算机病毒防护措施

执行病毒扫描
使用软件厂商提供的最新版本程序
避免使用来源不明的软件
即使来自熟人的邮件，也需对附件进行病毒检测
开启文件扩展名显示功能
设置禁用 Office 宏功能
智能手机病毒防护
与电脑相同，需安装杀毒软件并仅使用可信来源的应用程序

5-2 系统更新

1・针对安全漏洞的更新操作

操作系统、浏览器等应用程序中可能存在安全漏洞。所谓安全漏洞，是指软件开发者或用户未预料到的、允许网络入侵的脆弱性。若此缺陷被恶意利用，可能导致计算机或网络遭非法入侵，或信息被擅自窃取。

软件厂商发现漏洞后，会立即开发并发布“安全补丁”（修复问题的程序）。

个人电脑用户需自行管理设备。请时刻关注安全漏洞相关新闻，一旦发现漏洞，应立即下载安全补丁进行更新。

Windows 系统可设置自动接收安全补丁及更新程序，也可通过 Windows Update 获取最新信息并执行更新操作。

浏览器虽是网站访问的必需工具，但可能存在重大漏洞。在安全补丁发布前，应避免使用存在漏洞的浏览器。因此建议用户平时在电脑中预装多种浏览器。

2・关于终止支持的操作系统等

Windows 7 已于 2020 年 1 月、Windows 8.1 于 2023 年 1 月终止支持。这意味着软件供应商微软公司今后即使发现 Windows 7/8.1 存在漏洞，也不会开发修复程序。继续将此类操作系统连接至互联网使用存在风险。

请尽量避免使用已终止支持的系统。若存在仅支持旧版操作系统的应用程序，请将其与网络隔离使用。

除操作系统外，应用程序方面：Internet Explorer 已于 2022 年 6 月终止支持 浏览器视频播放常用的 Adobe Flash 亦于 2020 年底停止维护。

部分学校及机构已禁止安装过期操作系统的电脑接入网络。

Windows 系统支持终止日期

操作系统	支持终止日期
Windows XP	2014 年 4 月 8 日
Windows Vista	2017 年 4 月 11 日
Windows 7	2020 年 1 月 14 日
Windows 8.1	2023 年 1 月 10 日
Windows 10	2025 年 10 月 14 日

5-3 加密技术

1・通信加密

在互联网等通信过程中，为防止文档、图像等信息被第三方窃取或篡改，按照特定规则对数据进行转换的技术称为加密。

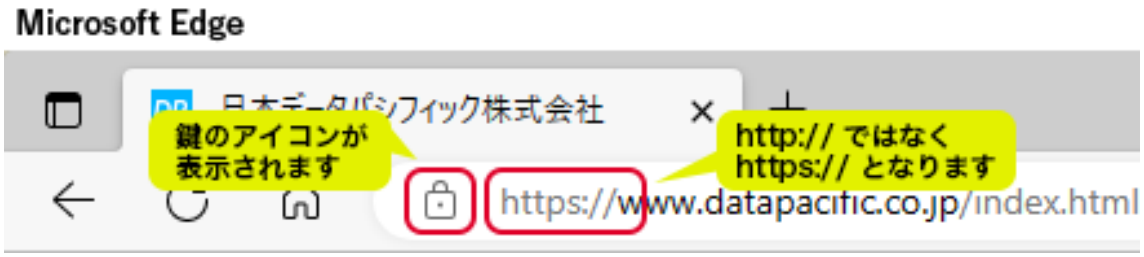
在 Web 环境中，采用名为 SSL（安全套接层）的机制对用户 ID 和密码进行加密传输。近年来，安全性更强的传输层安全协议（TLS）已成为标准配置。（因 SSL 名称已广泛普及，TLS 有时仍被称为 SSL，或标注为 SSL/TLS。）

加密通信的确认

在商业网站输入会员信息或商品购买的信用卡号时，请确认是否启用了 SSL/TLS 加密通信。

近年来，为防范窃听和篡改行为，非商业网站也普遍采用 SSL/TLS 加密通信。

SSL/TLS 加密通信时，浏览器地址栏将显示为“https://...”（而非常规的“http://...”），同时页面会显示锁形图标作为标识（不同浏览器显示位置及样式存在差异）。



2・无线局域网窃听防范

为在公司、学校等场所构建多人自由使用的网络环境，无需铺设有线电缆的无线局域网正广泛普及。但无线传输存在安全隐患：若未设置安全措施，外部人员可能窃取局域网内部数据，导致个人信息泄露事件频发。

在家中部署无线局域网时，请务必选用具备通信内容加密功能的路由器作为无线接入点，以

防未然阻止非法访问。通常无线路由器出厂时未预设加密及密码功能，请参阅说明书进行手动配置。

第 6 章 著作权与个人信息保护法

互联网上的网站包含无数内容。每张图片和视频都拥有版权，受到法律保护。稍有不慎就可能因侵犯版权而受到处罚。

本章将学习在使用互联网时尤为重要的版权等知识产权知识，同时了解近年来日益严格的个人信息保护相关法律。

各法律法规的原文可通过总务省“e-Gov 法令检索”进行查询。感兴趣者不妨查阅参考。

【e-Gov 法令检索】 https://laws.e-gov.go.jp/

6-1 著作权

与现实社会相同，在网络社会中，以著作权为首的知识产权也受到法律保护。随着互联网的普及，任何人都能轻松发布信息，因此对知识产权的关注度也日益提高。

1・著作权

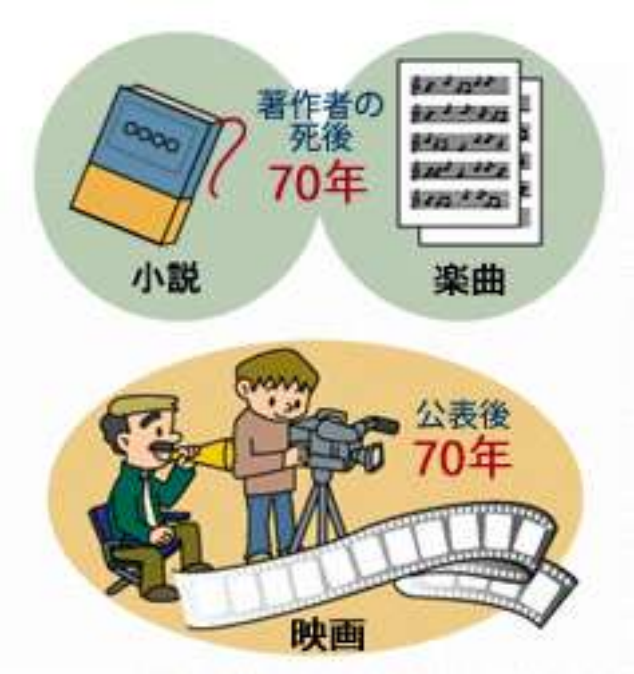
著作权人的权利在创作作品的瞬间即自动产生。著作权人的权利包括著作人格权与作为财产权的著作权。

著作权人的权利

著作人格权	著作权（财产权）
发表权	复制权
署名权	表演权·演奏权
作品完整权	放映权
	向公众传播权等
	口述权
	展览权
	发行权
	转让权
	出租权 翻译权·改编权等
	关于二次创作利用的原著作权人权利

著作人格权主要保护作者的精神利益，包含发表权、署名权、作品完整权三项权利。

著作权（财产权）是指授予著作物创作者的专有权利，在日本自著作物创作完成时起，至作者去世后 70 年止（2018 年著作权法修订后，著作物、表演及录音制品的保护期已从作者去世后 50 年延长至 70 年）。电影作品及以出版社、报社等团体名义发表的著作物（如杂志、报纸等），其保护期为自发表之日起 70 年。死亡后发表的著作物，其保护期自死亡次年 1 月 1 日起计算。此外，二次著作物（如著作物的翻译、改编作品）在特定范围内亦受著作权保护。



6-2 著作物的使用和著作邻接权

1・利用著作物时

根据《著作权法》规定，原则上利用他人著作物需获得著作权人许可。但满足下列条件时除外。

无需许可的情形

-保护期届满的著作物（第 51 条～第 58 条）（权利已消灭）
-仅陈述事实的新闻报道（第 10 条第 2 项）（不构成著作物）
-宪法及其他法令、法院判决（第 13 条第 1 项、第 3 项）（虽属著作物但不构成著作权保护对象）
-国家、地方自治团体机关等发布的告示、训令、通达及其他类似文件（第 13 条第 2 项）（虽-属著作物但不构成著作权保护对象）
-个人私用、引用、学校及图书馆等公共设施的非营利性使用等（第 30 条至第 50 条）（受著作权法认可）

著作物的合理使用

根据著作权法规定，在满足特定条件下，个人私用、引用、学校及图书馆等公共设施的非营利性使用等情形，无需获得著作权人许可即可复制或加工著作物。

但需注意：在互联网公开的网页等使用行为属于“向公众展示”，即使是个人网页也不视为私人使用，即便学校等公共用途网站也构成违法。企业等内部局域网内的使用同样违法（第 49

条第 1 项第 1 号）。

私人使用目的的复制

若用于个人或家庭内部使用，在满足以下条件时可无需获得著作权人许可进行复制（第 30 条）。

禁止解除复制保护进行翻录（Ripping：将数字数据导入电脑）的行为

（例）解除电影 DVD 的复制保护进行复制。

禁止下载非法复制内容

（例）明知流媒体网站上未标注使用许可的电视节目或电影属于非法内容仍进行下载。

著作物正当引用的条件

撰写报告或论文时，在满足下列条件下可无需获得著作权人许可进行引用（第 32 条、第 48 条）。

引用自已公开发表的著作物

存在引用的必然性及必要引用范围

确保引用部分与自身表述清晰区分

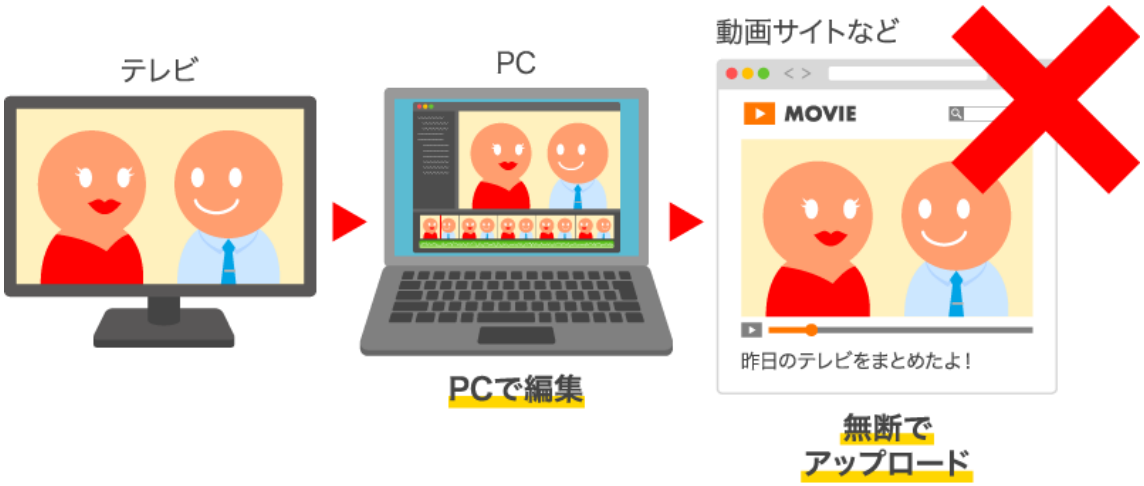
确保自身表述为主体，引用内容仅作为参考

明确标注出处

2・著作邻接权

表演者、唱片制作者、广播机构等作为“著作物传播者”，受著作邻接权保护。各著作邻接权包含广播权、传输权、转让权、出租权、复制权等要素。

具体构成著作邻接权侵害的案例包括：将音乐会录像上传至互联网的行为，以及将购买的 CD 曲目等内容在网络上传播的行为（此类行为同时构成对著作权本身的侵犯）。第三方使用时需获得著作权人与著作邻接权人的许可。



6-3 著作权侵害行为

为避免违反著作权法，原则上不得擅自使用他人创作的作品。若需复制、引用他人著作物或将其刊登于网页等处，除法律明确规定“无需许可”的情形外，必须事先获得许可。

1・软件许可协议

软件许可协议即软件使用许可合同，规定了可安装的电脑数量及使用期限等条款。请严格遵循许可协议内容使用软件。擅自复制、传播软件将受到法律制裁。

2・网络环境下的著作权侵权行为

在互联网领域，下列行为均构成著作权侵权并被明令禁止。此类行为属于犯罪行为，务必严加防范。

非法发布/上传（符合引用规范且仅涉及极小部分内容时可能例外）
未经授权将书籍、杂志内容通过扫描仪等设备采集后发布于网页等平台
在网络发布尚未发售的书籍（即“提前泄露”）
未经授权将电视节目或录像内容发布至网页等平台
未经授权在网页销售电视节目录像制品
未经授权在网页发布他人拍摄的照片
在网页发布对艺人（偶像）照片进行合成加工的作品（即“偶像合成图”）

（即使为本人拍摄，仍构成肖像权侵害及名誉损害）
擅自将他人网页的图片、照片、著作物副本等用于自身网页。
未经著作权人许可，使程序处于可通过互联网或校园局域网下载的状态。
使用文件共享软件擅自传播他人创作的程序或其修改版本。
未经授权将 CD、唱片或他人创作的音乐作品音源直接或转换为 MP3/MIDI 格式后发布至网络。
未经发件人许可公开电子邮件内容。
（可能构成隐私侵犯或名誉损害。）
明知系盗版软件、音乐或影像作品仍通过网络拍卖等渠道销售。
未经授权上传游戏实况视频。游戏运行画面（静态图/动态视频均属著作物）禁止擅自上传。
（部分游戏公司可能允许，但需事先确认。）
通过生成式 AI 创作的文本或图像，若与原始作品存在相似性及依赖性，即构成版权侵权，上传至互联网时需格外谨慎。

非法下载（属犯罪行为）
明知音乐或影像系非法上传，仍进行下载（录音或录像）的行为即属违法。此外，随着 2020 年《著作权法》修订，自 2021 年 1 月起，对于公开于互联网的漫画、书籍、论文、小说、程序等所有著作物，在知晓其系非法上传的情况下进行下载的行为均构成违法。

速看电影（Fast Movies）
速看电影是指将电影正片通过影像或静态画面剪辑，浓缩成约 10 分钟视频的作品。亦称速看影院或剧情摘要视频。
当速看被上传至视频分享网站时，观众无需观看正片即可了解剧情梗概，这种行为构成对电影发行公司的重大损失，已成为严重的版权侵权问题。
2022 年 11 月，东京地方法院作出判决（令和 4 年 11 月 17 日判决），以侵犯著作权为由，责令快剪电影上传者赔偿 5 亿日元损失。
虽然视频剪辑在电脑上操作简单，但严禁制作并上传快剪电影。

剧透网站
剧透网站指公开漫画剧情概要而非漫画图片的网站。由于直接复制漫画中的台词内容，此类行为不构成合理引用，属于侵犯著作权法。

3・画面附带内容
在博客等平台公开拍摄的照片或录制的视频时，若背景中偶然出现小型海报、绘画等非主拍摄对象，或街头播放的音乐被意外录入，通常不构成著作权侵权。

但需注意以下情形因不当损害著作权人利益，原则上需获得著作权人许可：

- 以海报或绘画为主要拍摄对象进行拍摄并发布于博客
- 以展示绘画或海报为主目的进行录像，并将影像通过互联网传播
- 为给主要拍摄对象增添附加价值而拍摄包含角色形象的照片，并在网络上公开

6-4 个人信息和肖像权

1・隐私权侵害

网络上时有发生个人隐私信息在本人不知情或不同意的情况下泄露、公开的事件。以下是网络中常见的隐私权侵害行为。隐私权作为人格权之一受法律保护，此类行为绝不可为。

未经本人同意擅自公开他人肖像照片。(详见下文“肖像权·公开权”部分说明)
未经本人许可公开私人电子邮件全文或部分内容。(邮件内容同样受著作权保护。)
擅自公开他人电子邮箱地址、住址、电话号码等个人信息。
公开他人犯罪记录、病史、职业经历、学历等隐私信息。
未经本人同意，在社交媒体或博客公开其与他人共同行动等内容。

隐私观念随时代演变。随着社会信息化进程，“所有人皆享有不受隐私侵犯的权利”这一理念日益普及。处理自身或他人信息时，请务必谨记此原则。

2・肖像权·公开权

肖像权指个人对其肖像（面容或身姿照片等）享有的权利。虽然日本目前尚无专门规定肖像权的法律，但该权利已被社会普遍认可。

肖像权包含以下两类：

人格权范畴的肖像权

人格权旨在保护个人人格利益，即禁止他人擅自使用本人照片等形象。未经许可公开他人肖像、侵犯隐私的行为均属违法。无论普通民众或名人，任何人都可主张此项权利。

作为财产权的肖像权

名人（艺人、职业运动员等）可通过肖像照等形象创造经济收益。基于财产权的肖像权旨在保护这种经济价值，防止第三方擅自使用。通常称为“公开权”。

为避免侵犯肖像权及公开权，请注意以下事项：

拍摄照片或视频时，须获得被摄主体本人许可。

对照片中意外入镜者进行模糊处理等操作。

不得擅自使用名人照片。

6-5 个人信息保护法

1・个人信息保护法是什么

这是在信息化社会中，为应对频发的个人信息泄露及非法使用问题，旨在保护个人权利与利益而制定的法律。即保护个人隐私信息的法律，规定处理个人信息的企业不得向外部泄露信息。

该法律明确了个人信息合理处理的基本理念、民间企业应遵守的事项及处罚条款等。

正式名称为《个人信息保护法》（以下简称《个人信息保护法》），于 2003 年 5 月公布（部分施行），2005 年 4 月全面实施。该法分别于 2015 年、2020 年、2021 年进行修订，其中 2020 年修订内容及 2021 年部分修订条款自 2022 年 4 月 1 日起施行。

2003 年	个人信息保护法成立（2005 年全面施行）
2015 年	大幅修订（2017 年全面施行，新增每三年进行一次审查的规定）
2020 年	修订（2022 年 4 月 1 日全面施行，根据每三年审查结果进行修订）
2021 年	修订（部分条款于 2022 年 4 月 1 日施行）

(1) “个人信息”定义

个人信息指能够识别特定在世个人的信息。2015 年修订明确了受保护个人信息范围，规定包含以下三类：

个人信息

生存个人的住址、姓名、出生日期、性别等可识别特定个人的信息

个人识别符号

特定个人身体特征的数字化信息（如指纹数据）

个人专属符号（护照号、驾照号、个人编号等）

需谨慎处理的个人信息

种族、信仰、病史、犯罪记录等敏感信息

(2) 完善个人信息有效利用机制

2015 年修订版新增匿名加工信息（经加工无法识别特定个人的个人信息）相关规定。

2020 年修订版新增假名加工信息（未经其他信息比对无法识别特定个人的个人信息）相关规定。

(3) 强化个人信息保护

获取个人信息时，须事先向本人明确告知使用目的。

向第三方提供所收集个人信息时，须事先获得本人同意。

(4) 设立个人信息保护委员会

2016 年 1 月新设个人信息保护委员会，将对个人信息处理事业者的监督权限统一归属该委员会。2021 年修订后，该委员会的监管范围进一步扩大，除个人信息处理机构外，国家行政机关、独立行政法人及地方政府机构的个人信息处理行为均纳入统一监督体系。

(5) 其他修订

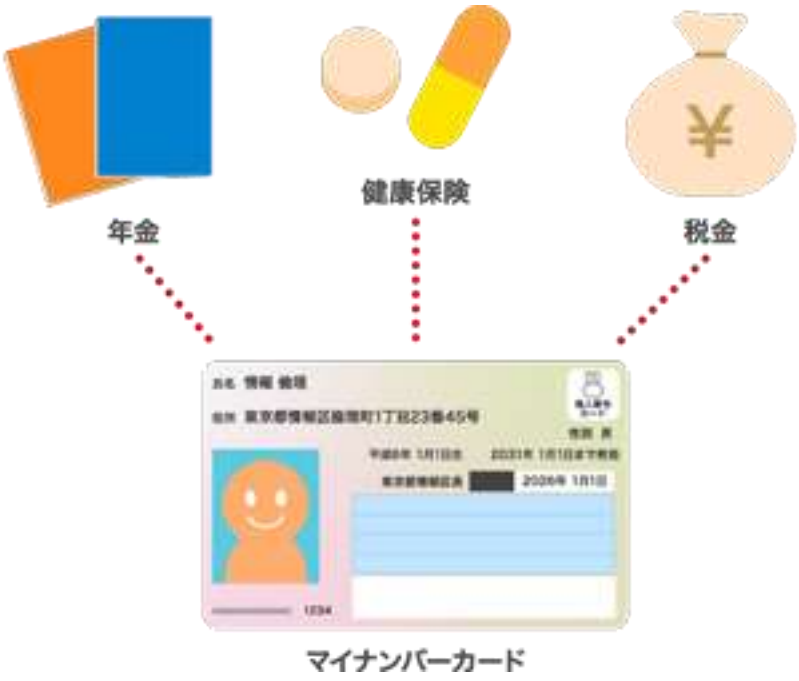
2015 年修订中新增或修改了以下内容：

将处理 5000 人以下个人信息的企业纳入法律适用范围（此前法律未涵盖该类主体）。关于“选择退出”（即在事先通知或确保本人知悉的前提下，若本人未表示反对则视为同意向第三方提供个人数据）的程序予以严格化，要求将通知事项等内容向个人信息保护委员会申报。新增了关于向日本境外提供个人信息的限制、个人信息保护法在国外的适用范围，以及个人信息保护委员会向外国执法机构提供信息的相关规定。

2・个人编号

1・个人编号制度概述

该制度通过向个人发放 12 位数字编号“个人编号（My Number）”，用于确认分散在多个机构中的个人信息属于同一人。个人编号制度于 2015 年 10 月正式实施。自 2016 年 1 月起，该号码开始应用于社会保障、税务及灾害对策等行政手续；2021 年起更可作为健康保险证使用。传统健康保险证自 2024 年 12 月 2 日起停止新发，所有功能将统一整合至已完成健康保险证使用登记的个人编号卡（个人编号保险证）中。



第 7 章 网络社会相关法律

随着互联网的普及，各种问题接踵而至，例如非法访问和计算机病毒等。利用互联网实施犯罪的行为年年出现新手法，相应的监管规则也相继制定。

本章将重点学习与互联网密切相关的法律法规。

各法令原文可通过总务省的“e-Gov 法令检索”进行查询。感兴趣者不妨查阅参考。

【e-Gov 法令搜索】 https://laws.e-gov.go.jp/

7-1 禁止非法访问法

1・《禁止非法访问法》概述

《禁止非法访问行为等相关法律》（以下简称《禁止非法访问法》）自 2000 年 2 月起正式实施。该法律旨在防范日益猖獗的高科技犯罪、维护网络秩序、促进高度信息通信社会的健康发展。

此后法律经过修订，现行版本除禁止非法访问行为本身外，还将网络钓鱼等非法访问准备行为纳入禁止范围，并加重了处罚力度。

2・《禁止非法访问法》概要

所谓“非法访问行为”包括以下情形：

使用他人 ID 和密码进行访问（冒名顶替）

利用系统或软件漏洞（安全漏洞）进行访问（破解）

“非法访问准备行为”包括以下行为：

为非法访问目的获取他人 ID/密码

未经本人许可向第三方提供其 ID/密码用于非法访问（恶意协助非法访问行为）

“协助非法访问行为”指未经本人许可向第三方提供他人密码等信息的行为。即使第三方无非法访问意图，仍构成犯罪。为避免卷入此类犯罪，切勿向他人透露自身 ID/密码。

为非法访问目的而保管他人非法获取的 ID/密码。
为获取他人 ID/密码而创建并公开钓鱼网站。
发送要求输入 ID/密码的钓鱼邮件以窃取他人账户信息。

7-2 社交媒体中的违法行为和法律

1・在留言板发布犯罪预告

诸如“＊月＊日将炸毁＃＃站”之类的犯罪预告被发布在留言板等平台后，常会引发重大骚乱。

此类发帖动机多源于“想看看会闹出什么动静”的猎奇心理。预告地点及周边区域往往因此停工停课，造成广泛影响。

在论坛发布犯罪预告属于严重扰乱社会秩序的行为，可能构成刑法规定的欺诈妨害业务罪或暴力妨害业务罪。

近年来为加强监管，已能追踪到发帖者身份。同时开发出自动检测网络犯罪预告的程序。

此外，散布谣言损害企业或个人信誉、妨碍业务的行为构成信用毁损罪或业务妨碍罪；发送大量垃圾邮件或暗示自杀等方式妨碍业务的行为，则属于欺诈性业务妨碍罪或暴力业务妨碍罪。

2・业务妨碍等骚扰性发帖

大学生在主题公园恶作剧并配图发布至 X 平台（原推特）的恶意行为引发广泛报道。

此外，兼职店员在社交媒体发布的恶作剧照片还包括：

便利店冰柜内拍照
汉堡店趴在面包胚上拍照
披萨店将披萨面团贴在脸上拍照
拉面店叼着未烹饪香肠拍照
此类事件接连发生。

对发布者而言或许只是恶作剧，却可能演变为妨碍业务等严重后果。甚至存在导致店铺被迫关闭的情况。对于在打工场所获取的仅限当事人知晓的内部信息，也需谨慎判断是否发布。

上述行为除可能构成信用毁损罪、妨碍业务罪外，还可能面临损害赔偿请求。

绝不能以“朋友间的恶作剧炫耀”为由轻视，切勿发布此类内容。

3・仇恨言论

《仇恨言论对策法》（正式名称：《关于推进消除针对外国籍人士不当歧视性言论的法律》）旨在消除针对民族、种族的歧视性言论，即所谓“仇恨言论”。该法以“禁止歧视性言论”为基本理念，于 2016 年 6 月施行，要求中央政府及地方政府采取消除仇恨言论的措施。

请注意，社交媒体上的歧视性言论将触犯此法。

4・隐私保护

即使事实属实，发布“A 君和 B 女士正在同行”等内容也构成隐私侵犯，严重时可能构成名誉损害。未经许可不得擅自发布他人信息。

同时禁止使用智能手机内置摄像头等设备在未获同意情况下拍摄他人照片，更不得随意在社交媒体公开此类照片。

5・侮辱罪

2020 年，一名女子职业摔跤选手因不堪网络诽谤中伤而自杀身亡。即便在她去世后，侮辱性言论仍在持续出现，其家属遂以侮辱罪提起诉讼。虽然最终被告被判有罪，但仅处以极轻微的罚金刑这一结果引发了社会广泛质疑。

为此，2022 年修订刑法通过并生效，其中包含严惩侮辱罪的条款。原先侮辱罪仅处以 30 日以下拘留或 1 万日元以下罚金，修订后则改为处以一年以下有期徒刑或禁锢，或 30 万日元以下罚金，或拘留或罚金。

7-3 电子商务法

1・电子消费者合同法

在使用网络购物等服务时，可能发生误点击或订购数量错误的情况。《电子消费者合同法》（正式名称：《关于电子消费者合同的民法特例法》）考虑到此类操作失误的可能性，规定网站运营方必须在订单确认前明确显示订单内容确认页面。若未设置此类确认页面，即使误点按钮，消费者仍可基于错误事由撤销合同。

此外，针对“单击诈骗”（误以为免费点击后，突然跳转至收费网站会员注册页面并要求付款）等虚假索款行为，无需适用电子消费者合同法，因其本质上不构成有效合同。因此无需支付任何费用，若收到不明账单请全部忽略。但若已向对方提供地址或姓名等信息，对方可能通过简易法院的小额诉讼程序等途径追讨款项。若收到法院正式文件，请勿忽视，应立即向警方咨询。

2・票务非法转售

音乐会、体育赛事等门票常以天价出现在网络拍卖平台。由于大量囤票的商家或个人，导致真正需要购票者无法获得门票，或无法以正规售价购票，已成为严重社会问题。

为此，《禁止不正当票务转售法》已于 2019 年 6 月 14 日正式实施。

该法律全称为《关于通过禁止特定演出门票不正当转售确保演出门票合理流通的法律》。

该法律明确禁止以超出定价的金额进行转售。违规者将面临一年以下有期徒刑或 100 万日元以下罚金，或两者并罚。

严禁为转售目的获取门票，或将禁止转售的门票发布于网络拍卖平台。同时请勿通过非法转售渠道获取门票。

7-4 电脑病毒相关法律

制作、持有或提供计算机病毒属于犯罪行为。刑法中称之为“非法指令电磁记录罪”，通称“计算机病毒罪”。即使计算机病毒未造成实际损害，在以下情形下仍将受到处罚：

计算机病毒的制作与提供（刑法第 168 条之 2）

未经授权为在他人计算机上执行病毒而制作或提供计算机病毒时构成犯罪。出于开发杀毒软件、研究等正当目的制作病毒的情况不适用此条款。

制作或提供病毒的行为将被判处三年以下有期徒刑或五十万日元以下罚金。

获取或保管计算机病毒（刑法第 168 条之 3）

未经授权为在他人计算机上执行病毒之目的而获取或保管计算机病毒时构成犯罪。

若因邮件等途径被主动发送病毒导致感染受害，则不适用本罪。

获取或保管病毒的行为将处以 2 年以下有期徒刑或 30 万日元以下罚金。

社交媒体病毒传播与病毒罪适用范围

2019 年，一名在论坛发布浏览器崩溃程序链接的中学生受到警方训导。所谓浏览器崩溃程序，是指在浏览器上反复弹出非预期窗口的程序。

该行为是否构成计算机病毒罪中的“制作提供计算机病毒”成为争议焦点。即便出于恶作剧等轻率心态，此类行为也可能引发严重后果，应予以严防。

至此，《INFOSS 信息伦理》的学习教材全部结束。

请合上教材，通过结业测试检验您的学习成果。