<面向一般使用者>

信息安全

手册

令和６年４月

室兰工业大学

情报基盘委员会

目录

1. 前言

信息安全和我们的生活

在现代生活中，使用电脑和手机已成为常态。为了将日益发展的信息技术活用于日常生活、工作和研究活动中，就必须注意信息处理。

本手册简明易懂地总结了信息安全的基本事项。本手册是一本明确记载了使用信息系统的具体方法的说明手册。

我们希望各位遵守本手册中记载的规则和礼仪，将本校的信息系统活用于教育和研究中，并能在日常生活中舒适地使用向公众提供的信息服务。

室兰工业大学的信息安全策略

在使用大学的信息系统时，制定了“信息安全策略”作为使用规则。无论教职人员还是学生，所有使用者都必须遵守信息安全策略。

信息安全策略的对象范围

信息安全策略适用于以下范围。

- 信息基盘及教育系统
  - 大学的官方邮件(网络邮件)
  - 大学的官方网站
  - 学习支持系统(Moodle)
  - 自习室内配备的电脑
  - 图书馆的电脑及国际交流室等校内配备的电脑
- 校内的网络系统(校园信息网络系统)
  - 从校内发起的互联网接入(通过 SINET 访问)
  - 使用校内设置的无线网络(airmit17)进行的通信
  - 使用研究室的有线网络和无线网络(WiFi)进行的通信
    (包含使用私人电脑或私人手机。)
- 图书馆信息系统、教务信息系统(CAMPUS SQUARE)和群件系统(Garoon)等一切校内信息系统

补充 1. 即使使用私人电脑或私人手机，当连接到大学的网络环境使用时，也须遵守信息安全策略。

补充 2. 在连接研究室或部局等设置的无线局域网访问接入点时，也须遵守信息安全策略。使用时请遵守本手册中的说明事项。

2. 目的以外行为的禁止及协助运用

●大学的电脑和网络不得用于教育和研究以外的目的

例：不得通过 WiFi 或研究室的网络下载非法内容、浏览游戏或成人网站。

●不得使用文件共享软件

禁止规定目的以外的使用

本校提供电脑和网络用于教育和研究的目的。请勿将其用于除教育和研究以外的目的。以下为教育和研究目的以外的使用示例。

(1) 从校内访问规定目的以外的站点

使用本校的网络（包括 WiFi）浏览以下站点。

・音乐和电影的非法下载站点　・商业程序的非法下载站点

・游戏或成人网站　　・破解工具的下载网站

因可能导致感染病毒等风险，请勿访问以上站点。

(2) 教育和研究目的以外的电脑使用

请勿用于兼职工作的传单制作、政治或宗教活动等。

(3) 禁止使用 Winny 等文件共享软件

由于文件共享软件存在很大的安全风险，因此建议在家里也不要使用。

协助运用

(1) 一旦将未执行防病毒措施的电脑、手机或怀疑感染病毒的电脑连接到网络，会将病毒感染到他人的电脑或手机，从而对他人造成不便。由于这会导致研究室等的网络中断，因此，请不要将怀疑已被病毒感染的电脑或手机连接到网络。

(2) 网络是校内共享的有限资源。为了有效地利用，请注意不要单独占用网络资源。例如，下载大容量文件等时，会长时间增加网络负担，因此请避免此类行为。

(3) 为了迅速解决问题，如果发现信息教育中心提供的电脑出现故障或服务出现问题等异常情况，请联系信息教育中心技术办公室。

问询・建议・报告窗口

信息教育中心　技术室(C301)

电 话 号 码)　0143-46-5895 或 0143-46-5896

官 方 网 站)　https://wp.mmm.muroran-it.ac.jp/

3. ID、密码的正确使用

- **使用强密码，并定期更改**
- **不得将校内的密码用于校外的服务**

  （禁止重复使用）
- **不将密码告知他人**

  （不要将密码写在便笺并粘贴到电脑上）

ID 和密码是用于验证本人的手段。一旦它们被盗取，第三方就可以随意使用系统并窃取信息。因此必须彻底管理 ID 和密码。

密码的设定

(1) 密码请设置为至少 8 位以上的字母、数字和符号的组合。
(2) 不要使用容易猜到的单词，以防使用字典攻击破解密码。
(3) 请定期更改密码。
(4) 请勿将大学服务的密码用于校外服务。如果校外服务的密码泄露时，会增加校内服务被入侵的风险。

ID、密码的管理

·请保护您的 ID 和密码，避免泄露给他人。

防止密码泄漏到外部的管理十分重要。请不要将密码告知他人，或将其写在便笺上并粘贴到电脑上。请勿张贴在可能有很多人看到的地方，例如校内的公告栏。

·请勿将中心发出的通知遗留在教室等地方。

请在更改好初始密码后撕毁。

·禁止借用 ID。

即使得到朋友的允许，也请不要使用朋友的 ID 和密码登录系统或使用服务。

·请注意关联 ID。

SNS 等服务提供有关联 ID 登录的机制。
（例如，使用 Facebook 帐户登录到 Instagram）
如果关联的情况下，一旦被关联的原 ID 和密码泄露，则关联的多个服务的 ID 和密码就会被盗用。因此更加需要谨慎管理 ID 和密码。

4. 电脑软件

●不得使用不受支持的 OS、应用程序

●务必执行 OS 和应用程序的更新

电脑软件是“原始的”。基础软件(OS)和应用程序软件由软件供应商提供的支持服务是有一定期限的。如果持续使用不受支持的软件，则存在利用漏洞攻击进而感染病毒的风险。

因此，请务必使用受支持的软件。

在室兰工业大学，禁止将不受支持的 OS 连接到校园网络。如果在研究室等地点使用旧的电脑时，请检查安装的 OS 是否受支持。

禁止使用不受支持的 OS

请使用当前支持的 OS，请勿使用旧版本的 OS。
以下 OS 不允许连接到校园网络。

- Windows 7 之前版本的 Windows 和 20H2 之前版本的 Windows10
- macOS 10.14 Catalina 之前版本的 MacOS

OS 的自动更新

请设置为自动更新 OS，并在发布更新版本时执行更新。

禁止使用不受支持的应用程序

请使用受支持的应用程序，请勿使用不受支持的应用程序。
以下应用程序在 2023 年 3 月时点已停止提供支持，不可使用。

- Adobe 产品
  - Acrobat 2017/ Acrobat Standard 2017/ Acrobat Reader 2017 之前版本的 Acrobat
  - Acrobat DC Pro / Acrobat DC Standard /Acrobat Reader DC
- 甲骨文公司
  - Oracle Java 10 (LTS)、Oracle Java 17 (LTS) 以外的产品
  - OpenJDK 11(LTS), OpenJDK 17(LTS) 以外的产品

应用程序的更新

请务必执行应用程序的更新。
如果可能，请设置为自动更新，始终保持为最新版。

5. 软件许可证

●软件须遵守许可证使用
（不得使用盗版软件）

电脑的软件是受版权保护的作品，许可证协议规定了其适用范围。请遵守使用条款并正确使用。**如违反许可证协议，您或大学可能会被版权持有方起诉及受到法律制裁。**

软件许可证的遵守

请根据许可证协议使用软件。不可安装没有许可证的软件。另外，请勿安装从互联网上下载的许可证不明确的软件。

自由软件的使用

在互联网上，免费的(不发生许可费用)所谓自由软件是公开的。使用时，请注意以下事项：

・许可证协议的确认

自由软件具有各种许可证。其中有如禁止商业使用这样的条件，因此须确认自己的使用目的是否符合许可证协议。

・获取源

请从软件发布方的站点或大型存储库等可信任的位置获取软件。网络上可能散布着被病毒感染、被恶意篡改的软件。

禁止使用被非法修改的软件

请不要从互联网上下载和使用被非法修改的无需激活的商业软件(盗版软件)。

即使被修改为无需激活，但在运行时它们也存在与软件供应商的激活认证服务器通信的情况。商用软件供应商可通过此通信检测到大学内存在非法使用该软件的情况。曾经发生过因违法许可证，用户和大学被起诉的事例。

大学购买的软件的使用

大学购买提供的软件许可证仅可在在校期间使用。

- Microsoft(OVS-ES)
- Apex One

毕业后将无法继续使用，因此请卸载软件。
如果毕业后仍需使用时，需自行购买软件。

6. 防病毒软件

必须务必安装大学提供的软件(Apex One)

仅凭 Windows Defender 是不完备的

也需安装 macOS 或 Linux

开启病毒防护(实时扫描)并执行病毒定义文件的自动更新

定期执行完全扫描

一旦将没有安装防病毒软件的电脑连接到互联网时，它必定会感染病毒。请务必执行防病毒措施。未执行防病毒措施的电脑禁止连接到本校的网络。

安装

购买电脑后，请务必安装大学提供的 Apex One。

如果电脑的 OS 是 Windows，其虽附带有 WindowsDefender，但该软件检测率低且很少更新，因此作为防病毒软件是不完备的。此外，也存在很多针对 macOS 和 Linux 的病毒，因此请安装 Apex One。

如果购买的电脑附带了商业防病毒软件时，可继续使用该软件。但是，一旦超过试用期或许可证过期时，就会无法继续使用，因此请在许可证过期前安装 Apex One。

病毒定义文件的更新

安装防病毒软件后，请开启实时扫描。该措施可在保存文件时检查该文件是否包含病毒(病毒检查)。

此外，请开启自动更新以定期更新病毒定义文件。

定期扫描的执行

开启实时检测扫描后，文件保存时会执行病毒检查，但病毒模式可能会在文件保存后更新，并存在被认证为新的病毒的情况。因此，请定期(补充 1)执行完全扫描(补充 2)，以确保现有文件未感染病毒。

补充 1. 最好每周执行一次以上。

补充 2. 如果没有“完全扫描”，请针对电脑的硬盘进行扫描。

感染病毒时的对策

如果电脑出现显示异常或运行速度非常迟钝等疑似感染病毒的症状时，请执行以下操作。

Step.1　脱机

拔下网线并关闭无线局域网（WiFi）功能。
（阻止病毒通过网络攻击其他电脑）

Step.2　在其他电脑上获取对策文件

使用另一台没有感染嫌疑的电脑下载最新的防病毒软件（Apex One）的安装程序。

Step.3　安装防病毒对策文件

使用 CD 或 USB 将防病毒软件（Apex One）保存在此电脑中，并运行安装程序。

Step.4　更新病毒定义文件

连接到网络后更新防病毒软件的病毒定义文件。

补充 1. 请仅执行更新操作。

补充 2. 正常情况下，不应在被病毒感染或怀疑被感染的情况下连接到网络。如果条件允许，应先在 Step2 中获取最新的病毒定义文件，同时 Step4 应在脱机状态下执行。但是，近来有一些防病毒软件须联机才能使用，因此存在如不联机就无法执行更新的情况。

Step.5　脱机状态下，执行完全扫描

再次断开网络连接（执行 Step1 的操作）。然后，使用防病毒软件执行完全扫描，以清除病毒。

Step.6　更新 OS

连接到网络后更新 OS。
（Windows 对应“WindowsUpdate”，macOS 对应“Software Update”。若是 Linux，根据 OS 不同，对应的名称也不同。）

如遇到无法清除病毒等问题时，

请联系咨询信息教育中心。

●如联系不上中心时

请保持电脑脱机状态并关闭电源。如果自行解决，请在安全的电脑上搜索信息，并请留意信息是否可靠。网络上公开的信息中存在虚假的解决方法和工具。

7. 手机的使用

使用受支持的移动端和 OS，不使用旧的移动端

从受信任的位置获取应用程序，且务必执行更新

使用密码或生物识别锁定，并采取防丢失措施

使用保护功能，以防万一丢失

手机在功能上与电脑相当，需要采取安全措施。由于存储了朋友的地址、联系方式等大量不能泄露的个人信息，因此需要保护这些信息免受恶意应用程序的侵害。由于每天都随身携带，一旦丢失后果十分严重，因此需要采取安全措施。

OS

较旧的 OS 存在漏洞，较容易受到攻击，使用时会感染病毒。请务必执行 OS 的更新。建议设置为自动更新。使用受支持的移动端和 OS，避免使用较旧的设备。室兰工业大学**禁止将不受支持的手机连接到校园网络**。

应用程序

请从受信任的位置(官方应用商店等)获取应用程序。非线上正式发布的应用程序存在泄露手机中的信息或包含恶意程序的情况。此外，在安装后存在发现漏洞的情况，因此如获取的应用程序一旦有更新，请更新至新版本。使用 SNS 应用程序时，请对个人信息进行设置，使其不会意外泄露。

保护

请使用密码或生物识别等锁定手机，以防被他人使用。此外，为防止手机丢失或忘记拿走手机等情况，请采取如挂吊饰等防范措施。即使万一丢失手机，为了防止信息泄露，请预先进行远程操作等设置。

8. 电子邮件的使用

检查收件人电子邮件地址后再按发送键

发送电子邮件时，务必输入主题

垃圾邮件不要点开直接删除，不打开链接 URL 或附件

使用免费电子邮箱服务时，请采取防信息泄露对策

新建电子邮件时的注意事项

- **防止错误发送电子邮件**

  由于一旦发送后就无法取消，因此请务必在发送之前检查收件人的电子邮件地址，以免出错。建议使用发送内容的预览功能和延迟发送功能(按下发送键一段时间后才会发送)。

- **输入主题**

  在电子邮件中，请编辑简洁明了表达主旨的主题。

- **发送附件时，请在正文中告知此信息。**

- **请不要发送超大容量的文件（超过几十 MB)。**

接收电子邮件时的注意事项

- **可疑邮件不要点开，直接删除**

  特别要注意来自陌生人的电子邮件。检查是否是垃圾邮件，确认不是虚假发件人。此外，也请根据主题判断。无主题的电子邮件有可能是垃圾邮件，请不要点开，直接删除。如果无论如何都需要确认邮件内容时，也请不要打开电子邮件中包含的链接(URL)或附件。

- **不得使用 HTML 邮件**

  请将电子邮件软件设置为以纯文本格式接收邮件，不以 HTML 格式显示电子邮件。一旦点开 HTML 电子邮件时，链接中的图片和文件将被自动下载，即会被对方知道邮件已被阅读。

使用本校以外的电子邮箱服务

使用 Gmail 或 Yahoo!等本校以外提供的电子邮箱服务时，邮件正文可能会被提供商确认（阅读）。

使用时请注意以下事项。

- **不得将本校以外的电子邮箱服务用于工作用途。**
- **如须使用本校以外的电子邮箱服务时，不得发送如成绩信息等机密内容。**
- **如须使用本校以外的电子邮箱服务发送成绩信息等机密内容时，将发送内容使用密码保护、加密后发送。**

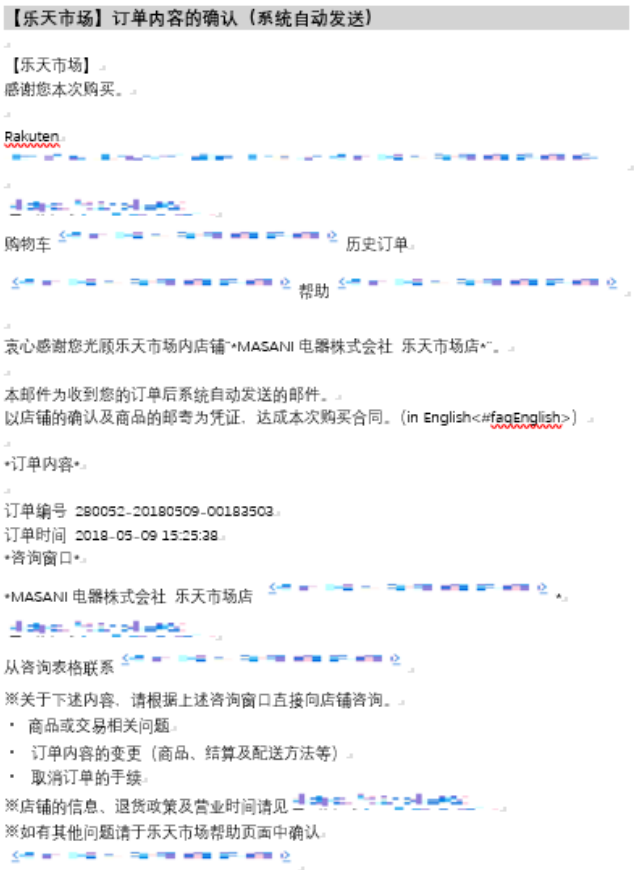
注意网络钓鱼电子邮件

网络钓鱼电子邮件是冒充公司或组织，将收件人诱导至恶意网站并诈取信息的电子邮件。对于没有印象的邮件，不要点击链接或打开附件，请直接删除。

网络钓鱼电子邮件的例子

如今，越来越多被精心伪装的可疑电子邮件，发生了冒充公共机构和大型企业的事例，以及伪装成快递公司、购买程序的自动通知等事例。

【实例】冒充乐天市场的电子邮件



【乐天市场】订单内容的确认（系统自动发送）

【乐天市场】
感谢您本次购买。

Rakuten

购物车 历史订单

帮助

衷心感谢您光顾乐天市场内店铺"*MASANI 电器株式会社 乐天市场店*"。

本邮件为收到您的订单后系统自动发送的邮件。
以店铺的确认及商品的邮寄为凭证，达成本次购买合同。（in English<#faqEnglish>）

订单内容

订单编号 280052-20180509-00183503
订单时间 2018-05-09 15:25:38
咨询窗口

*MASANI 电器株式会社 乐天市场店 *。

从咨询表格联系

※关于下述内容，请根据上述咨询窗口直接向店铺咨询。
・ 商品或交易相关问题
・ 订单内容的变更（商品、结算及配送方法等）
・ 取消订单的手续
※店铺的信息、退货政策及营业时间请见
※如有其他问题请于乐天市场帮助页面中确认。

9. LINE 的使用

使用 LINE 时需了解其中的风险
进行防止通讯簿等信息泄露的设置
不收取及接听来自陌生人的消息或电话

LINE 作为一种便捷的信息传输手段获得广泛使用。在大学生之间也很受欢迎，几乎所有本校的学生都在使用。
请遵守以下注意事项，并安全地使用。

防止通讯簿泄露

为防止通讯簿泄露，须严格管理隐私。

例：请在“添加好友设定”中进行以下设置。

- **关闭“自动添加好友”功能**
- **关闭“允许对方添加我到好友”功能**
- **关闭“隐私管理”中的“允许通过 ID 添加好友”**

如果不进行上述设置，存在和无意添加的人成为“好友”，不知不觉中作为好友取得联系的情况。

为了不被卷入犯罪

为了避免因陌生人发来的联络而卷入犯罪的风险，请记住以下对策：

- 阻止来自陌生人的消息或电话。
- 不和陌生人通过网络交换 ID。
- 帐户被盗取后可能会被用于犯罪，因此须彻底管理 ID 和密码。

信息泄露风险

就算是仅在朋友之间发送的消息，服务提供商也可以看到消息内容。重要的信息需要考虑通过其他方式联系。

10. 社交网络服务(SNS)的使用

SNS 是公开平台，发表言论需谨慎

不交换个人信息或敏感信息

不发表中伤他人的言论

SNS 的使用

如 X（Twitter）、Facebook、Instagram 和 LINE 等社交网络服务作为非正式信息交流的媒体十分受欢迎，并且作为朋友之间交换信息的手段也十分便捷。

尽管十分便捷，但是仍然存在风险，因此在发表信息时须注意。

使用上的注意事项

- **须注意发表的内容**

在 SNS 中不存在匿名性，请在理解这一点后再发表言论。即使当时认为没有人在看，但是之后在网上搜索一下的话，就能知道之前发表过言论。例如，如果有违法行为的发言，或是发表了不道德言论时，发布者可能会被搜索出来并遭到强烈谴责（在网络上引起热议）。

- **信息一旦泄露就无法撤回**

信息一旦被发布到网络上，即使发布者撤回了该发言，该发言也会在网络上被复制，无法再次撤回。

- **不发表个人信息或敏感信息**

请勿在 SNS 上交换以下信息。

个人信息： 姓名、地址、出生日期、性别、电话号码、邮箱地址等能够特定到个人的信息

敏感信息： 银行账号及余额信息、信用卡号或是否有借款、健康保险卡号等相关信息，病史、患病、血型等医疗信息，家庭、亲属关系、出生地等信息，个人兴趣和爱好等相关信息

- **不发表诽谤、中伤等言论**

诽谤中伤他人的言论最终会传到本人那里，可能会破坏和那个人的关系。

- **须注意图像的附加信息**

图像文件中同时记录了拍摄时间和拍摄地点等信息（EXIF）。上传到图像共享网站时，请进行设定，确保这些信息不会泄露。

11. 云服务

请在了解 SNS、存储服务、电子邮箱服务等免费云服务的风险后再有效地利用。

不存储重要数据

加密

使用其他方式备份

在本书中将在互联网上提供的免费应用程序称为云服务。云服务包括以下服务。

- X(Twitter)或 LINE、Facebook 等 SNS
- Dropbox 或 Google Drive、iCloudDrive 等存储服务
- Gmail 或 Yahoo!邮箱等邮箱服务

虽然云服务可以免费使用且十分方便，但也存在以下风险。

使用上的风险

(1) 服务提供商对于用户数据的使用

由于免费服务的提供商利用累积的用户数据来开展业务，因此可以认为数据内容正在被利用(被读取)。例如，用户数据被用于市场营销或广告投放等，但不仅限于此。

(2) 服务提供商的管理失误等导致的用户数据泄露

存在由于服务提供商的操作失误等原因，而导致用户数据泄露到互联网上的风险。

(3) 用户数据丢失及服务连续性

存在由于服务提供商的操作失误等原因，而导致用户数据丢失的风险。此外，存在由于服务提供商的原因而导致突然终止服务，且无法恢复存入的用户数据的风险。

使用上的注意事项

(1) 防止泄露(不存入)

请勿用于交换或存储重要数据和工作数据等重要数据。

(2) 防止泄露(加密)

如果必须处理重要数据或业务数据时，请在存储前先在电脑上对数据进行加密。

(3) 重要数据的备份

为了防范由于服务提供商的操作失误或服务突然终止而导致数据丢失等情况，请通过云服务以外的其他方式对数据进行备份。

12. 信息发布相关注意事项

进行信息发布时请注意以下事项。

不得将敏感信息存储在用于信息发布的服务器上

对定期发布的信息进行评估

不得侵害他人的权利

为了通过互联网安全地发布传播信息，请注意以下事项。

确保信息发布系统的安全性

(1) 确保安全性

OS 和各种软件须及时更新补丁等，始终保持与最新的信息同步。将网页制作外包给外部公司时也须如此。

(2) 禁止使用 CGI/SSI，禁止开设网络论坛(BBS)等

由于可能会被擅自使用，因此禁止在本校的公共服务器上使用。

(3) 隐藏目录相关注意事项

关于外部非公开的敏感信息，即使是隐藏目录中也不允许存储。

对定期发布的信息进行审查

(1) 显示有效期限

在网页上发布的信息必须清楚地标示有效期限。
当有效期限到期时，须将该信息从服务器中删除。

(2) 实施定期盘点

每年至少进行一次信息的盘点，并评估信息发布的需求。
针对在盘点的时间点时已过期的信息，须删除或者更新其有效期限。

(3) 组织变更时的应对方法

如果组织发生变更时，须与接管的组织进行业务交接。
（如果没有接管的组织时，须停止信息发布。）

版权等知识产权的遵守

请注意以下几点

- 不得侵害他人的知识产权
- 不得侵害肖像权、宣传权
- 不得发布诽谤中伤他人或侵犯隐私的信息
- 使用公司商标等商标时，须事先与对方进行协商
- 充分考虑在照片等中出现人脸时的风险

13. 信息泄露对策

不需要的信息不要带出去。尽可能减少带出去的信息

带出去时,务必防止电脑被盗

不要把重要数据保存在 USB 存储器中随身携带

废弃信息设备时，须删除或破坏硬盘

为了防止信息泄露，至关重要的是不带出不需要的信息。如果无论如何都需要把信息带出时，必须采取措施防止信息泄露。此外，废弃信息设备时，请注意不要让信息从废弃设备中泄漏。

信息带出

请记住不需要的信息不要带出去。如果无论如何都需要带出时，请尽量只带出最小需要限度的信息。在电脑上事先设置好开机密码。为了防止从被盗的电脑中取出硬盘进行解析，请事先对硬盘进行加密。

信息设备的防盗窃措施

驾车出行时，请勿将电脑放在无人的车内，以防被盗窃。

地铁出行时，请勿将装了电脑的提包放在车内行李架上，请随身携带保管。此外，在出差地参加商务聚餐时，请勿将电脑带到会场。

USB 存储器的使用

由于 USB 存储器容易丢失，因此请不要把重要信息保存在其中随身携带。不得已需要使用时，请采取使用带有密码功能的 USB 存储器等其他方法。为了避免不小心将不必要的信息带出的情况，在将使用完毕的 USB 存储器收起来之前先将其中信息删除。

信息设备的废弃

废弃电脑时，使用专用软件删除硬盘内的信息。如果可能的话，请对硬盘进行物理性地破坏等处理。此外，向外部的专业公司等委托废弃的情况下，请委托可靠的公司并取得销毁证明。

【参考】 关于工作用途的电脑，由于现为技术部代行废弃处理，如有需要请联系。

14. 发生信息安全事故时的处理

发生(发现)信息安全事故时，不要惊慌，联系 CSIRT
尽可能早得联系

信息安全事故

将类似于以下的事件视为信息安全事故。

- 含有机密信息的电脑或 USB 存储器的丢失或失窃
- 机密信息(文件)的丢失或失窃
- 电脑感染病毒
- 含有机密信息邮件的错误发送(发错收件人)
- 发送大量垃圾邮件
- 从 WEB 服务器或电脑上的信息泄露(无意公开)
- 从废弃的信息设备中的信息泄露

信息安全事件应对小组

发生信息安全事故时，为了使受害程度降到最小，需要尽早应对。为此，组成了针对事故的紧急应对小组(信息安全事件应对小组，CSIRT)。

信息安全事故发生时的联系窗口

电子邮箱： m-csirt@mmm.muroran-it.ac.jp (CSIRT)
电话：0143-46-5896 (信息教育中心　技术室)

联系时，请告知详细的具体情况。

2024 年 4 月　　第 9 版
2023 年 3 月　　第 8 版
2020 年 4 月　　第 7 版
2019 年 11 月　　第 6 版(电子版)
2018 年 3 月　　第 5 版
2014 年 3 月　　第 4 版
2012 年 3 月　　第 3 版
2010 年 3 月　　第 2 版
2009 年 3 月　　初版

主编･制作

室兰工业大学　信息教育中心
https://www.icte.muroran-it.ac.jp