爱媛大学信息安全对策指南

1 最新状态

电脑,智能设备的操作系统和软件需要随时进行安全系统的更新,所以请将电脑等保持为最新状态

2 病毒对策

必须安装防毒软件,并执行更新病毒定义文件

3 电子邮件

注意不明目标的攻击,不打开陌生奇怪的附件和链接

4 密码保持

密码设置要数字英文和符号混合使用,不告诉他人或者通用

5 文件交换

文件交换软件可能泄露电脑内个人信息,不使用p2p软件

爱媛大学的吉祥物人物"Emica"

6 备份

定期备份防止文件因故障或者误操作受损

7 信息管理

重要信息不放在桌上,个人信息相关的记录仪器usb等不许携带外出

8 信息废弃

如果要废弃含有重要信息的电脑或者存储设备时,或找专业人士并使用专业删除软件

① 切断您的电脑与校园网络的链接

② 联系综合情报媒体中心（分机8803）

【联系方式】 爱媛大学综合情报媒体中心
URL：http://www.cite.ehime-u.ac.jp/
MAIL：center@dpc.ehime-u.ac.jp
TEL : +81 89-927-8803

爱媛大学
EHIME UNIVERSITY

爱媛大学信息安全对策指南的确认纸

1．保持最新状态

- ☐ 电脑,智能设备的操作系统和软件需要随时进行安全系统的更新，所以请将电脑等保持为最新状态。
- ☐ 未更新到最新版本的机器容易被恶意软件攻击，请不要使用。

2． 病毒对策

- ☐ 为了防止不受攻击，必须安装防毒软件并保持更新。
- ☐ 确认病毒定义文件为更新状态。否则，防病毒软件将无法正常运行。

3．电子邮件

- ☐ 发送邮件前，为了防止误传，请反复确认收件人地址。
- ☐ 未经许可，不要泄漏他人邮件地址。给互相不认识的很多人同时发信邮件时，请使用bcc功能屏蔽收件人邮件地址。
- ☐ 不得已需要通过电子邮件发送重要文件时，请不要将内容发送与正文中，使用附件并设置打开密码，打开密码不要在同一份电子邮件中记载，请使用其他通讯方式告知对方。
- ☐ 通过电子邮件进行攻击的例子很多，不光要确认发件人的地址/内容是否可疑，还要警惕看似正规的伪装电子邮件。如有可疑邮件时，不要打开附件也不要点击链接，删除该邮件。

4．密码保持

- ☐ 请不要使用自己的姓名，生日等信息作为密码使用，设置他人无法推测出的以字母数字符号等组合后的密码。不要重复使用同一个密码。
- ☐ 不要把密码信息贴在别人可以看到的地方，不要告知他人。
- ☐ 路由器等网络系统的初期密码，请变更密码后再使用。如果一直使用出厂密码，有被非法入侵的可能。

5．文件交换

- ☐ 如果使用以Winny，Share等为代表的文件交换软件，可能会导致感染病毒，以致电脑内的情报泄漏。请勿使用与业务操作无关的任何交换软件。

6．备份

- ☐ 保存在PC或服务器中的数据可能会由于故障或错误操作而消失。另外还有一种叫“RANSAMWARE”的病毒，它在未经许可的情况下对数据进行加密，并以赎金为目的对其进行解密，因此要定期备存数据以防备以上情况的发生。

7．信息管理

- ☐ 毫无防备的将付有信息的资料放置于工作桌面，会有被别人随意拿走或盗用的可能。 重要资料不要随意放置，归放于指定场所，并将其保存于密码库中归放于指定场所另外，办公室的门锁也要谨慎防范。
- ☐ 笔记本电脑，平板电脑，USB存储器等便于携带，但遭遇盗窃的风险也很高。请不要把含有重要信息的电子仪器带出校外。

8．信息的废弃方法

- ☐ 如果将含有重要信息的文件直接丢弃在垃圾桶内，会造成严重的泄漏事故，请切碎后丢弃。
- ☐ 废弃个人电脑/存储设备时，即使删除操作完成，还有被恢复的可能性。为了避免删除信息的还原，处理时请使用专门的删除软件或请专业承办商家删除。

主编: 爱媛大学CSIRT（计算机安全事件响应小组）