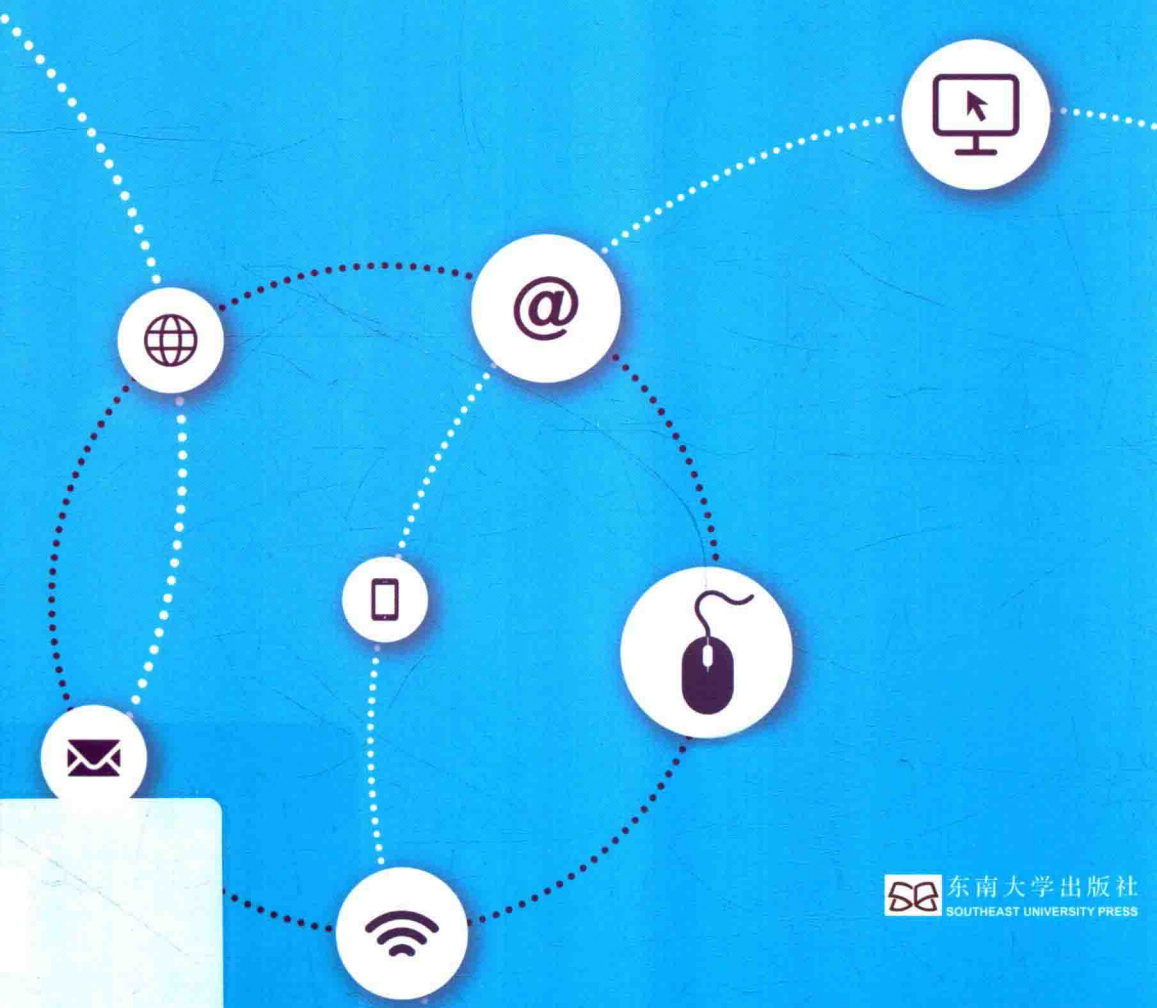
ICDL Asia

国际电脑使用执照（ICDL）考试官方指定教材

ICDL 资讯安全

ICDL 基金会 著
ICDL 亚　洲 译



东南大学出版社
SOUTHEAST UNIVERSITY PRESS

ICDL 资讯安全

课程大纲 2.0

ICDL 基金会 著
ICDL 亚 洲 译

东南大学出版社
SOUTHEAST UNIVERSITY PRESS
·南京·

图书在版编目(CIP)数据

ICDL 资讯安全/爱尔兰 ICDL 基金会著；ICDL 亚洲译. —南京：东南大学出版社，2019.4
书名原文：IT Security
ISBN 978-7-5641-8352-3

Ⅰ.①I… Ⅱ.①爱…②I… Ⅲ.①信息安全—安全管理—教材 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字(2019)第 061138 号

江苏省版权局著作权合同登记
图字：10-2019-055 号

ICDL 资讯安全(ICDL Zixun Anquan)

出版发行：东南大学出版社
社　　址：南京市四牌楼 2 号　　邮　　编：210096
网　　址：http://www.seupress.com
出 版 人：江建中

印　　刷：南京京新印刷有限公司
排　　版：南京月叶图文制作有限公司
开　　本：700 mm×1000 mm　1/16
印　　张：6.5
字　　数：125 千
版　　次：2019 年 4 月第 1 版
印　　次：2019 年 4 月第 1 次印刷
书　　号：ISBN 978-7-5641-8352-3
定　　价：45.00 元

经　　销：全国各地新华书店
发行热线：025-83790519　83791830

说　明

ICDL 基金会认证科目的出版物可用于帮助考生准备 ICDL 基金会认证的考试。ICDL 基金会不保证使用本出版物能确保考生通过 ICDL 基金会认证科目的考试。

本学习资料中包含的任何测试项目和(或)基于实际操作的练习仅与本出版物有关，不构成任何考试，也没有任何通过官方 ICDL 基金会认证测试以及其他方式能够获得认证。

使用本出版物的考生在参加 ICDL 基金会认证科目的考试之前必须通过各国授权考试中心进行注册。如果没有进行有效注册的考生，则不可以参加考试，并且也不会向其提供证书或任何其他形式的认可。

本出版物已获 Microsoft 许可使用屏幕截图。

前　言

ICDL 资讯安全

资讯安全的日常维护是确保专业、个人和财务安全的重要在线技能。了解有关数据管理的最佳做法以及个人信息保护和在线安全浏览的方法将有助于用户在网络世界的信息安全。本书将帮助考生了解日常生活中安全使用资讯的主要概念，并利用相关技术和应用程序来维护网络连接，安全地使用Internet，并适当地管理数据和信息。

完成本书学习后，考生将具备以下能力：

- 了解有关安全信息和数据、物理安全以及隐私与身份窃取重要性的关键概念。
- 保护计算机、设备或网络免受恶意软件和未经授权的访问。
- 了解网络类型、连接类型和网络特定问题，包括防火墙。
- 浏览互联网并进行安全通信。
- 了解与通信有关的安全问题，包括电子邮件和即时消息。
- 妥善安全地备份和恢复数据。
- 安全处理数据和设备。

学习本书的意义

在完成本书的学习后，考生将能够展示这些领域的能力，并以安全的方式进行在线活动。一旦考生掌握了本书提供的技能和知识，有可能通过 ICDL 资讯安全的国际标准认证。

有关本书每个部分所涵盖的 ICDL 资讯安全课程大纲的具体领域的详细信息，请参阅本书结尾的 ICDL 课程大纲。

目　录

第 1 课

安全概念

在本节中，用户将了解到：

- 数据威胁
- 信息的价值
- 个人安全
- 文件安全性

1.1 数据威胁

维护数据安全无论对于个人、小型企业还是大型企业都至关重要。确保数据安全是避免个人和企业在工作上发生意外损失的关键。但不幸的是，由于恶意或无意的行为，这可能是一项艰巨的任务。

以下是与数据威胁相关的一些常见术语：

● 数据

数据是与物体相关的事实、数字和统计数据的集合，可以处理数据以创建有用的信息。数据是原始和无组织的事实和数字。

● 信息

信息是组织和处理的数据，给数据赋予了更多意义和上下文。如果说数据像一片片拼图，那么信息就像一个完整的拼图，向用户显示最终的图片。

● 网络犯罪

网络犯罪是涉及使用互联网或计算机进行非法活动的罪行，往往是为了经济或个人利益。包括身份盗用和社会工程等。

● 黑客入侵

黑客入侵是涉及使用计算机专业知识来获取未经授权访问计算机系统的途径。黑客可能希望篡改计算机上的程序和数据，使用计算机资源，或者只是证明他们可以访问计算机。

数据安全的主要威胁：

- 系统崩溃和硬盘崩溃——系统崩溃或硬盘崩溃可能会对存储介质造成物理损坏。
- 可能会删除或损坏文件的计算机病毒。
- 造成磁盘和磁盘驱动器故障——例如坏扇区。
- 意外删除或覆盖文件，造成数据丢失。

- 由未经授权的用户或黑客造成信息的删除。
- 遭受自然灾害，如洪水、火灾或地震等破坏。
- 恐怖主义行为或战争。
- 员工意外或恶意删除。

云计算

云计算是一种基于互联网的按需计算服务，可让用户随时随地与其他设备共享资源和数据。在云计算环境中，服务、应用程序、存储和服务器通常由第三方数据中心管理，这样可以以最少的管理成本轻松访问服务和应用程序。

云计算漏洞

云计算有其优缺点。在决定使用云端时，您需要考虑一些可能的云计算漏洞：

- **会话劫持**。当攻击者拦截或窃取用户的账户以便使用应用程序时，被盗的账户允许攻击者模拟用户，并使用用户的身份验证凭据登录。
- **服务可靠性**。与内部服务和私有云一样，云计算也会造成偶尔停机和服务不可用。云服务提供商有不间断的电源，但有时可能会出现意外，所以，百分之百的正常运行时间不太可能实现。
- **依靠互联网**。云服务的可用性高度依赖于互联网连接。如果 Internet 连接失败或暂时不可用，用户将无法使用所需的云服务。这也将大大影响需要运行的服务，例如，如果在医院中发生这种情况，生命就可能受到威胁。

云计算威胁

云计算威胁包括以下几个方面：

- **数据控制**。数据控制是企业迁移到云的一个大问题。将公司的敏感和机密数据放在云服务提供商的服务器上，这是一些公司不愿意承担的风险。还有关于公司数据的安全性以及是否会被不合适的人掌握的担忧。

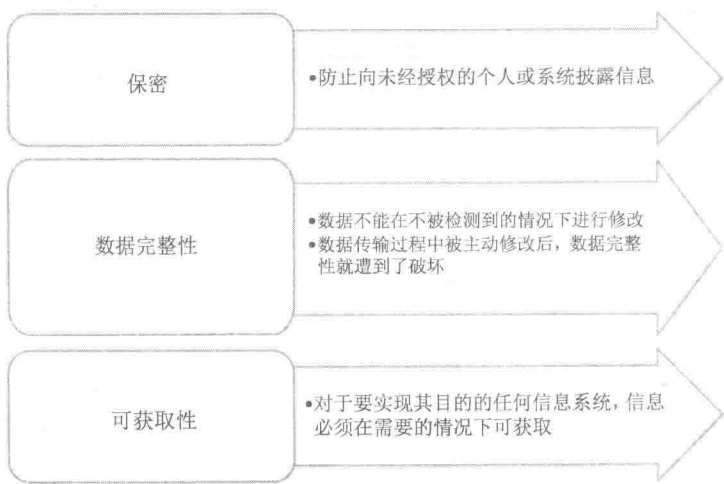
- **拒绝服务**。由于对某些云服务进行了相当简单或匿名的注册过程，云服务可能会被用于恶意目的，例如垃圾邮件、僵尸网络、分布式拒绝服务（DDoS）或恶意软件分发等。
- **潜在的隐私丢失**。由于云服务可以从互联网上的任何地方访问，所以可能会存在数据的隐私泄露问题。当数据从客户端传输到云端时，攻击者可能会拦截通信。
- **恶意内部人员**。在云服务工作的员工有可能访问用户的数据并窃取机密信息。
- **数据丢失**。如果云服务提供商的硬盘驱动器未实现正确的数据备份，则可能会发生这种情况，CSP 也可能会意外删除用户的数据。

1.2 信息的价值

信息安全的基本特征

信息安全意味着保护信息和信息系统免受未经授权的访问、使用、披露、中断、修改、阅读、检查、记录或销毁。

信息安全的目标是保护信息的机密性、完整性和可用性。



保护个人信息的原因

如今，越来越多的人正在使用互联网和移动设备进行在线购物、银行、商业、通讯等活动。一些公司依靠各种云服务和其他基于网络的服务来运营他们的日常业务。

信息更容易通过互联网访问使企业面临严峻的安全问题。黑客能够利用在线数据传输中的漏洞，获得系统和网络未经授权的访问。过去几年来，有很多有关数据泄露和身份盗用的报道。网络犯罪分子经常窃取个人信息，如银行记录、信用卡详细信息、用户名和密码，以获得经济利益。

个人信息通常被公司用来识别和授权用户在网站上业务交易。例如，购物网站可能会有用户姓名、地址、信用卡详细信息等记录。黑客可能窃取这些信息，以冒充使用者，然后进行欺诈和未经授权的交易以及其他欺诈活动。没有足够的安全和对个人信息的保护，用户将面临身份盗用、欺诈以及隐私权的丧失等。不保护用户个人信息的公司可能会失去客户的信任和业务。

保护商业敏感信息的原因

商业敏感信息可能是公司拥有的任何信息，如果以任何方式丢失、误用、被盗或更改都可能会造成损失。

可能被归类为商业敏感信息的示例如下：

- 财务报表，如资产负债表、现金流量表、损益表或资产陈述。
- 信息，例如当前和过去客户的列表。
- 商业秘密，如设计、配方、生产流程等。
- 有关新产品、营销策略的信息或专利信息。

必须保护商业敏感信息，以防止：

- 窃取个人和公司的机密信息。公司信息可能被企业间谍或黑客窃取。这些数

据可能会转交给公司的竞争对手，不利于信息所有者。

- 意外丢失数据。用户可能会错误地删除或更改敏感数据，包含敏感信息的存储介质或移动设备。
- 欺骗性地使用公司数据。如客户信息和信用信息。
- 企业破坏。一些竞争对手可能会使用信息来破坏公司的业务。

数据隐私或保护控制

随着各种业务和个人交易在互联网上的广泛使用，需要采取措施确保个人或公司正在使用的数据的隐私和安全性。因此相关法律和准则被制定，以确保数据和信息不被滥用及用于任何非法行为。

数据保护的相关法律通常规定保护个人信息，不得非法使用某人的个人资料和泄露其隐私。然而，数据保护的相关法律可能会因国家而异。

一般来说，拥有个人资料的人员必须确保：

- 个人资料以公平合法的方式处理。
- 总是采用良好的做法处理个人资料。
- 个人资料的收集只能用于合法和明确的目的。
- 如果与收集信息的目的不兼容，则不得处理个人资料。这被称为比例原则。
- 处理的个人资料是充分的和相关的。
- 不会对个人资料进行不必要的处理。
- 处理的个人数据是准确和最新的。
- 个人资料的保存时间不得超过必要时间。

数据主体和数据控制器

一个数据主体是个人信息的主体，而数据控制器是控制和使用个人数据的个人（或人的集合）。在这种关系中，为了安全和公平，有必须遵循的准则和法规。数据控制器将负责公平地获取和处理数据，保证安全，确保数据的充分性和相关性，并将根据要求提供数据主体的副本。

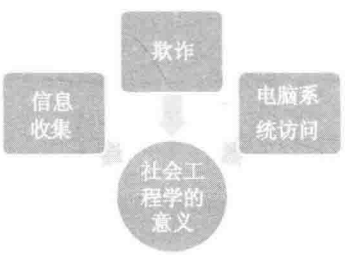
ICT 规则

ICT(Information and Communication Technology,信息和通信技术)规则通常在工作场所实施,以确保安全和适当地使用互联网服务和连接。公司可以签发由员工签字的文件,以符合公司规定。不在公司工作的人,也可能使用这种服务,例如具有共享 Wi-Fi 网络的大学、餐馆和公共交通工具等也可能有 ICT 规则,要求使用者在连接到网络之前确认遵守规则。

1.3 个人安全

社会工程学

社会工程学是一种操纵或影响人们的方式,目的是非法获取敏感数据(例如密码或信用卡信息)。社会工程师研究并了解其目标的个人环境并伪造其身份,从受害者处获得机密信息。在大多数情况下,它们渗透到第三方计算机系统中以侦测敏感数据。



社会工程学方法

- 电话

通过电话进行欺诈是最常见的方法之一。攻击者可以模仿权威人士、权威人士

代表或服务提供者，从一个不知情的用户身上提取信息。例如，一个声称是该公司首席执行官的人，就会利用打电话给不知情的用户，以各种借口要求其提供相关的密码。

- **网络钓鱼**

网络钓鱼是另一种欺诈方式，其中欺诈者发送似乎来自合法来源（例如银行）的电子邮件，电子邮件中通常要求对信息进行验证，并有时在邮件中警告收件人，如果不遵守邮件中的要求，会有可怕的后果。网络钓鱼电子邮件通常包含指向欺诈性网页的链接，这些网页与合法网页（包括标识和内容）非常相似。

- **肩窥**

肩窥是指使用直接的观察技术，站在别人身后、越过肩膀观察别人操作进而获取信息的做法。它通常用于获取密码。

身份盗用及其影响

身份盗用是指有人蓄意冒充和使用另一人的身份。通常是使用他人的身份以获得经济利益、信用或其他利益。例如，当某人使用另一个人的身份获得驾驶执照。这种欺诈行为可能会对身份被认定的人造成严重的影响。

身份盗用的初始含义是重新建立用户的身份和信用记录。

身份盗用的影响

个人 这种身份盗用的后果是致命的，会引起情感抑郁、焦虑甚至抑郁	财务 财务历史和信用记录可能遭受身份盗用，导致一个或多个现有账户的丢失或滥用
企业 尤其是在信贷和金融领域，会造成经济损失。当受害者是员工时，企业还会遭到时间损失和产能损失	法律措施 重新建立合法身份，包括个人资料、护照和税务记录

身份盗用的方法

- 信息挖掘

信息挖掘也称为垃圾搜寻，它是通过挖掘丢弃文件或物品的垃圾箱或垃圾桶获取个人或个人信息的方法，如搜索垃圾桶里的费用单或信用卡对账单等。

- 侧录

身份盗用者通过使用小型电子设备捕获受害者的个人数据的方法称为侧录。侧录器通常是连接到 ATM 机卡槽的设备。受害者可能不知不觉间将卡片滑入侧录器，然后被读取并存储卡片磁条上的所有信息。

- 假托

假托涉及创造和使用捏造的场景（借口）来吸引目标受害者。这个借口增加了受害者在一般情况下不太可能获得信息或采取行动的机会，例如冒充来自提供服务公司的人，劝说用户与他们分享银行账户详细信息。

1.4 文件安全性

通常，一些最重要的信息会存储在电子文档和电子表格等文件中。用户应该知道，对于这些文件应该有一系列的安全考虑。

启用/禁用宏安全设置

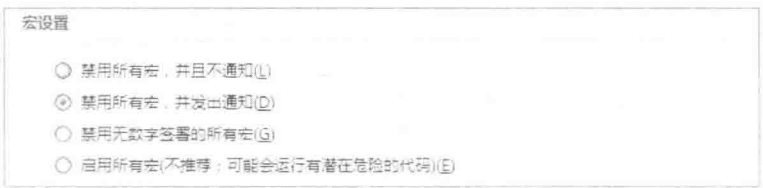
宏用于在 Microsoft Office 应用程序中自动执行重复或经常使用的任务。可以通过使用宏录制功能或由软件开发人员使用 VBA（Visual Basic for Applications）编写宏。有恶意的人可能会创建破坏性的宏，从而传播病毒。因此，宏是潜在的安全威胁。

用户可以自动禁用宏，只有在信任该文件的来源时才启用它们。宏安全设置可以在信任中心中找到。在某些组织中，默认情况下禁用这些设置，并且在没有系

统管理员授权的情况下不能更改。

示例：在 **Microsoft Excel 2016** 中进行宏安全设置

1. 单击**文件**选项卡。
2. 单击**选项**。
3. 单击**信任中心**，单击**信任中心设置**，然后单击**宏设置**。



4. 单击下面的选项之一：
   a. **禁用所有宏，并且不通知** 如果不想允许宏运行，请选择此设置，除非它们位于受信任的位置。当用户打开启用宏的文件时，用户将不会收到任何通知。
   b. **禁用所有宏，并发出通知** 打开启用宏的文件时，会显示安全警告，让用户选择是否启用宏。此设置是默认设置。
   c. **禁用无数字签署的所有宏** 使用此设置，只有受信任发布者进行数字签名的宏才能运行。如果该宏由用户不信任的发布商签名，则会出现通知，让用户信任发布商，从而启用宏。
   d. **启用所有宏(不推荐；可能会运行有潜在危险的代码)** 允许所有宏运行，没有通知或安全警告。此设置使计算机容易受到宏病毒的攻击，不推荐使用。
5. 单击**确定**按钮。

设置文件密码

在 Microsoft Office 系统中，可以使用密码来防止其他人打开和修改用户的文档、工作簿和演示文稿。

要设置 **Microsoft Word 2016** 文档的文件密码：