项目 1　信息安全概述

案例分析

2020 年，新冠肺炎（COVID-19）疫情暴发，人与人之间被口罩、安全距离等隔离措施所阻隔。网络，无可替代地成为保障生产生活有序进行的重要角色，甚至是保障抗疫成功和经济发展的必要条件。

新冠肺炎疫情贯穿了 2020 年，线上办公和在线教育的兴起，也带来了安全攻防重心的转移。英国 2020 年网络安全年报就指出，英国政府国家网络安全中心在 2020 年先后处理超过 200 次与新冠病毒相关的网络事件，几乎占上报事件总数的 1/3。

勒索软件感染医院网络，危害病人生命安全；黑客入侵网络视频会议，打断会议或窃取会议资料；疫情期间出现过个人信息泄露等安全事件。类似情况都暴露出网络安全行业亟待解决的问题。5G、量子计算机、量子网络等新技术的兴起，也使安全行业面临新挑战。国家也有针对性地发布了相关规范和发展政策，以引导行业的健康成长。

Zoom 作为一家远程会议软件服务提供商，在疫情暴发之初，其用户数量激增，但随后也暴露出大量的安全问题。在业务大量增长的同时，还需要修补历史遗留的安全漏洞，兼顾安全性，无异于一艘正在搏击暴风雨的航船还需要修补漏水的甲板。网络安全的保障工作不是一蹴而就的，没有未雨绸缪地防范，就可能出现各种网络安全问题。

项目介绍

米好安全学院针对我国信息安全的现状，秉持“注重实操，夯实基础，创新驱动”的理念，以实际工作能力需求建立人才培养方案，以工作内容制订教学内容，力争构建真实的企业网络安全环境和安全人才培养生态圈。本项目聚焦信息安全中的基本概念，让学生对信息安全有初步的认识。

（1）了解信息安全的基本概念。

（2）了解信息安全的威胁与隐患。

（3）了解信息安全的发展历程。

（4）了解信息安全事件。

（5）学习网络安全法的基本内容。

任务 1.1　了解信息安全

1.1.1　信息安全分析

任务描述

信息安全的概念在 20 世纪经历了一个漫长的发展阶段，自 90 年代以来得到了深化。进入 21 世纪，随着信息技术的不断发展，信息安全问题也日益突出，如何确保信息系统的安全已成为全社会关注的问题。米好安全学院决定以当下的信息安全时代背景为题材，对信息安全的概念进行介绍。

任务目标

- 了解信息安全包含的五大特征。
- 了解信息安全发展的 4 个时期。
- 了解目前信息安全的主要隐患。

1.1.2　信息安全概论

1. 信息安全的五大特征

信息安全具有五大特征，即信息的保密性、完整性、可用性、可控性、不可抵赖性。信息安全的范围很广，其中包括如何防范商业机密的泄露、青少年对不良信息的浏览以及个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名、消息认证、数据加密等），以及安全系统（如 UniNAC、DLP 等），只要存在安全漏洞，便可能威胁全局安全。

保密性（confidentiality）：保证信息不被非授权访问，即使非授权用户得到信息也无法知晓信息内容，因而不能使用。

完整性（integrity）：维护信息的一致性，即在信息生成、传输、存储和使用过程中不应该发生人为或者非人为的非授权篡改。

可用性（availability）：授权用户在需要时能不受其他因素的影响，方便地使用所有信息。这一目标是对信息系统的总体可靠性要求。

可控性（controllability）：信息在整个生命周期内都可由合法拥有者加以安全控制。

不可抵赖性（non-repudiation）：保障用户无法在事后否认曾经对信息进行的生成、签发、接收等行为。

图 1-1-1 为信息安全的五大特征。

信息安全学科可分为狭义安全与广义安全两个层次：狭义安全是建立在以密码论为基础的计算机安全领域，早期中国信息安全专业通常以此为基准，辅以计算机技术、通信

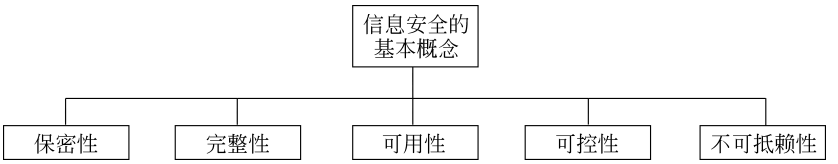

图 1-1-1　信息安全的五大特征

网络技术等方面的内容；广义的信息安全是一门综合性学科，从传统的计算机安全到信息安全，不仅是名称的变更，也是对安全发展的延伸，安全不再是单纯的技术问题，而是管理、技术、法律等问题相结合的产物。

1）狭义解释

网络安全在不同的应用环境下有不同的解释。针对网络中的一个运行系统而言，网络安全就是指信息处理和传输的安全，它包括硬件系统的安全、可靠运行，操作系统和应用软件的安全，数据库系统的安全，电磁信息泄露的防护等。狭义的网络安全侧重于网络传输的安全。

2）广义解释

网络传输的安全与传输的信息内容有密切的关系。信息内容的安全即信息安全，包括信息的保密性、真实性和完整性等。

广义的网络安全是指网络系统的硬件、软件及其系统中的信息受到保护，它包括系统连续、可靠、正常地运行，网络服务不中断，系统中的信息不因偶然的或恶意的行为而遭到破坏、更改或泄露。

其中的信息安全需求，是指通信网络给人们提供信息查询、网络服务时，保证服务对象的信息不受监听、窃取和篡改等威胁，以满足人们最基本的安全需要（如隐秘性、可用性等）的特性。网络安全侧重于网络传输的安全，信息安全侧重于信息自身的安全。由此可见，两者的侧重点与其所保护的对象有关。

由于网络是信息传递的载体，因此信息安全与网络安全具有内在的联系，凡是网上的信息必然与网络安全息息相关。信息安全的含义不仅包括网上信息的安全，而且包括网下信息的安全。现在谈论的网络安全，主要是指面向网络的信息安全，或者是网上信息的安全。

2. 发展过程与现状

中投顾问在《2016—2020 年中国信息安全产业投资分析及前景预测报告》中指出，信息安全是随着信息技术的发展而发展的，总体来说大致经历了 4 个时期。

第一个时期是通信安全时期，其主要标志是 1949 年香农发表的《保密通信的信息理论》。这个时期通信技术还不发达，计算机只是零散地位于不同的地点，信息系统的安全仅限于保证计算机的物理安全以及通过密码解决通信安全的保密问题，密码技术获得发展，欧美有了信息安全产业的萌芽。

第二个时期为计算机安全时期，以 20 世纪七八十年代《可信计算机系统评估准则》（TCSEC）为标志。半导体和集成电路技术的飞速发展推动了计算机软、硬件的发展，计

算机和网络技术的应用进入了实用化和规模化阶段。人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标，中国信息安全开始起步，并开始关注物理安全、计算机病毒防护等。

第三个时期是在20世纪90年代兴起的网络时期。由于互联网技术的飞速发展，无论是企业内部还是外部的信息都得到了极大的开放，而信息安全的焦点已经从传统的保密性、完整性和可用性三个原则衍生为诸如可控性、抗抵赖性、真实性等其他的原则和目标。中国安全企业研发的防火墙、入侵检测、安全评估、安全审计、身份认证与管理等产品与服务百花齐放，百家争鸣。

第四个时期是进入21世纪的信息安全保障时期，其主要标志是《信息保障技术框架》(IATF)。面向业务的安全防护已经从被动走向主动，安全保障理念从风险承受模式走向安全保障模式。不断出现的安全体系与标准、安全产品与技术带动信息安全行业形成规模，入侵防御、下一代防火墙、APT攻击检测、MSS/SaaS服务等新技术、新产品、新模式走上舞台。

图1-1-2为信息安全发展的四个时期。

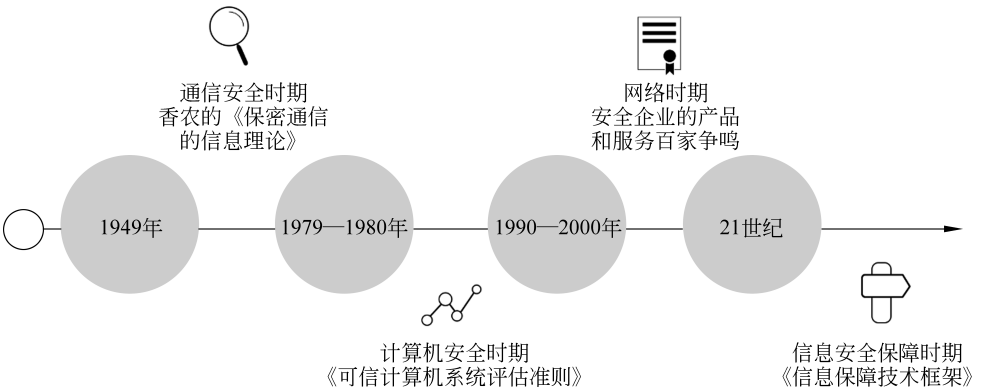

图1-1-2　信息安全发展的四个时期

总体来说，从安全体系与标准，到安全产品与技术，中国信息安全市场与成熟的欧美市场相比还有一定差距。我国在信息安全管理方面存在的问题如图1-1-3所示。当前国家重视、资本追逐为中国安全企业提供了一个很好的追赶国际领先企业的机会。

3. 安全隐患

网络环境中信息安全威胁如下。

(1) 黑客攻击：由原来的单一无目的攻击转变成为有组织、目的性很强的团体攻击犯罪，在攻击中主要以经济利益为目的，采取针对性的集团化攻击方式。

(2) DDoS攻击：目前非常有效的网络互联网攻击形式，常见的有SYN攻击、DNS放大攻击、DNS泛洪攻击和应用层DDoS攻击。

(3) 互联网金融业务支撑系统的安全漏洞：给病毒、DDoS、僵尸网络、蠕虫、间谍软件等侵入留下可乘之机，对其信息安全造成很大威胁。

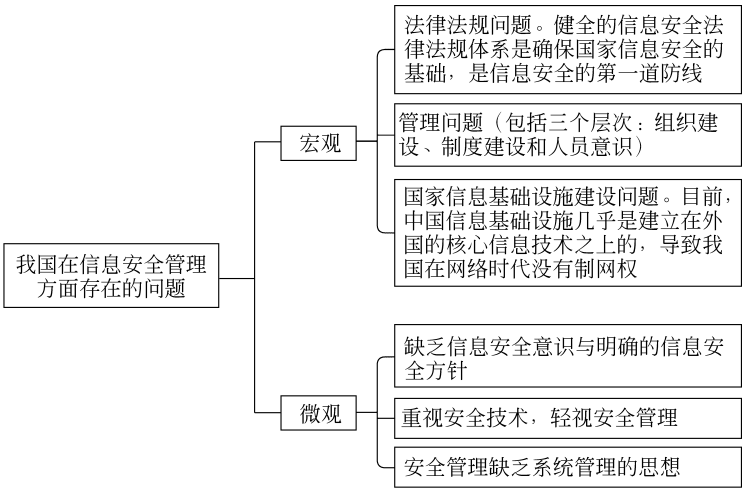

图 1-1-3　我国在信息安全管理方面存在的问题

（4）病毒木马：很多木马程序和密码嗅探程序等多种病毒不断更新换代，对网上银行实施攻击，窃取用户信息，可以直接威胁网上银行安全。其用户上网终端如果没有安装木马查杀工具，就很容易被感染。

（5）信息泄露：互联网金融交易信息是通过网络传输的，有些业务交易平台在信息传输、使用、存储、销毁等环节未建立保护信息的有效机制，致使信息很容易出现泄露。

（6）网络钓鱼：和其他信息安全攻击方式不同，网络钓鱼主要诱骗互联网金融用户误认为钓鱼网站属于安全网站，很容易将用户信息泄露，虽然政府、金融机构对此非常重视，但很多钓鱼网站建在境外，很难监管。

（7）移动金融安全隐患：目前移动金融 App 非常便捷，但由于用户安全防范意识比较薄弱及很多软件的信息安全存在安全隐患，可能会给用户造成损失，不利于移动金融的发展。

（8）互联网金融安全风险：互联网金融与金钱相关，信息就意味着金钱，所以互联网金融也成为 APT 的重灾区。

（9）互联网金融的外包服务数据泄露：有可能给服务机构带来数据泄露的风险。

（10）内控风险：互联网金融业务服务中信息系统与内部控制可能存在缺陷，不适当的操作也可引发信息安全风险。

1.1.3　信息安全事件

1. 网络安全法与互联网行为与防范

【事件一】　揭露地下黑市——央视曝光网上贩卖个人信息新闻

2017 年 2 月 16 日，央视新闻频道报道了记者亲身体验购买个人信息服务，揭秘个人信息泄露黑市状况的新闻。记者暗访得知，在这一地下黑市交易时，只提供一个手机号

码，就能买到一个人的身份信息、通话记录、位置信息等多项隐私，连打车的时间记录都可以精确到秒。泄露的是个人信息，留下的是各种隐患。贩卖个人信息的黑色产业如果不加以整治，势必影响整个社会治安，威胁公民人身安全。图 1-1-4 为信息泄露的概念图。

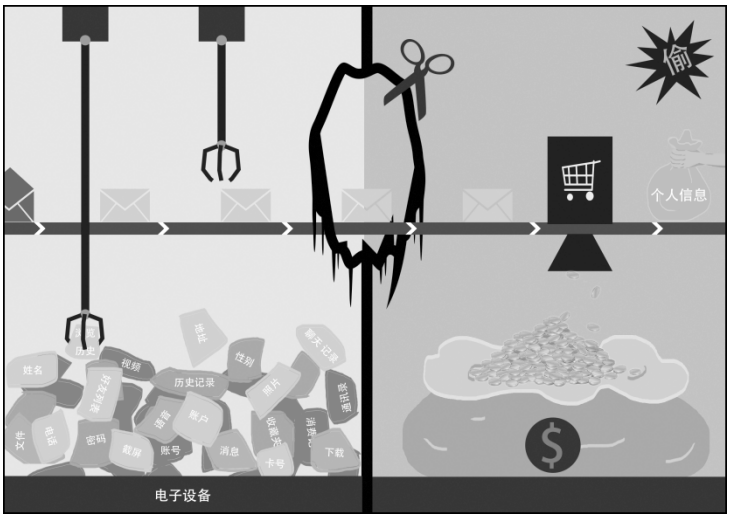

图 1-1-4　信息泄露的概念图

【事件二】 12306 官方网站再现安全漏洞

2017 年 4 月 21 日，记者朋友们在 12306 官方网站订票时发现，当退出个人账号时，网站页面竟自动转登他人账号，且与账号相关联的身份证号、联系方式等个人信息均可见，随后记者在该页面单击常用联系人选项时，页面再次刷新并显示他人账号及账号涵盖的所有信息。而记者尝试在网站账户页面的个人信息栏等其他选项进行操作，单击进入后，均得到不同的个人身份信息。图 1-1-5 是 12306 安全漏洞爆发时发布的公告。

关于提醒广大旅客使用12306官方网站购票的公告

[2014-12-25]

针对互联网上出现"12306网站用户信息在互联网上疯传"的报道，经我网站认真核查，此泄露信息全部含有用户的明文密码。我网站数据库所有用户密码均为多次加密的非明文转换码，网上泄露的用户信息系经其他网站或渠道流出。目前，公安机关已经介入调查。

我网站郑重提醒广大旅客，为保障广大用户的信息安全，请您通过12306官方网站购票，不要使用第三方抢票软件购票，或委托第三方网站购票，以防止您的个人身份信息外泄。同时，我网站提醒广大旅客，部分第三方网站开发的抢票神器中，有捆绑式销售保险功能，请广大旅客注意。

中国铁路客户服务中心

2014年12月25日

图 1-1-5　12306 安全漏洞爆发时发布的公告

【事件三】 勒索病毒模仿王者荣耀辅助工具袭击手机

游戏不光“吸粉”能力超强，同时吸引病毒的能力也非同一般。2017 年 6 月，360 手机

卫士发现了一款冒充时下热门手游“王者荣耀”辅助工具的手机勒索病毒，该勒索病毒被安装进手机后，会对手机中照片、下载、云盘等目录下的个人文件进行加密，并索要赎金。这种病毒一旦爆发，会威胁几乎所有安卓平台的手机，用户一旦中招，可能丢失所有个人信息。图 1-1-6 是勒索病毒挟持手机信息的截图。

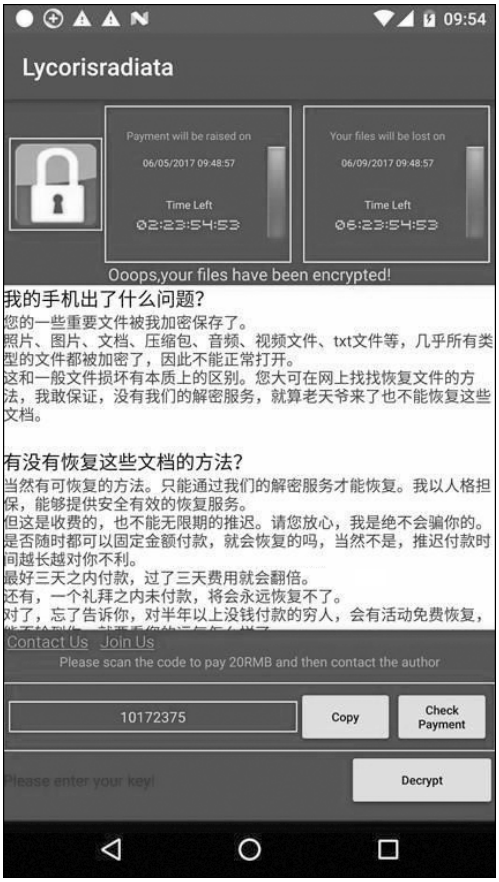

图 1-1-6　勒索病毒挟持手机信息的截图

【事件四】　央视调查发现大量家庭摄像头被入侵

2017 年 6 月，央视《每周质量报告》调查发现网上有众多家庭摄像隐私在售，黑客利用弱口令密码大范围扫描家用摄像头进行破解，可获得 IP 地址和登录密码，远程操作别人家的摄像头。随后在质检总局的抽检中，采样品牌涵盖市场关注度前 5 位产品，40 批次产品中有 32 批次存在安全漏洞，占比高达 80%。图 1-1-7 为安全隐私概念图。

针对以上事件，应找到信息安全问题的源头，并提出可行的防护改进措施。

2. 收集国内外网络信息安全事件

查找近两年国内外典型网络信息安全事件，完成表 1-1-1 的填写。

图 1-1-7　安全与隐私

表 1-1-1　典型网络安全事件列表

序号	网络安全事件

3. 熟悉网络安全职能部门

查找近年来国内外重要的网络安全保护组织与机构，了解各组织结构的主要职能，完成表 1-1-2 的填写。

表 1-1-2　国内外网络安全组织与机构

组织与机构(公司)名称	主要职能(业务)

4. 加强网络安全防范行为

正确认识网络安全问题的风险，根据表 1-1-1 和表 1-1-2，就如何提高个人信息安全问题，对可采取的实际行动进行归纳总结，完成表 1-1-3 的填写。

表 1-1-3　网络信息安全行动计划

安全活动范围	潜在信息安全风险	拟采取的行动计划
家庭		
校园		
公共场所		

任务总结

通过本任务学习与实践，使学生了解信息社会的网络安全知识，养成良好的个人信息安全与国家安全的保护意识。

任务 1.2　网络安全法

1.2.1　网络安全法分析

任务描述

网络安全法是维护网络安全及预防网络犯罪的刑事法律规范的总称。在我们学习网络安全技术之前，要熟知网络安全法的内容、定义和一些警示人们的事件。米好安全学院制订这个任务来让学员们知法懂法，坚守住网络空间安全的道德底线。

任务目标

- 了解网络安全法的定义、性质和作用。

- 掌握网络安全法的基本内容。

1.2.2 知识收集

1. 网络安全法的性质

1）网络安全法属于刑法

从法律性质上来说，网络安全法是刑事法律，属于传统刑法的范畴。由于计算机信息系统应用（尤其是在国家要害部门）的普遍性和计算机处理的信息的重要性，使破坏网络安全的行为具有严重的社会危害性。国际计算机专家认为，网络的普及程度、社会资产网络化的程度以及信息网络系统的社会作用的大小，决定了破坏网络安全行为的社会危害性的大小。网络的作用越大，普及程度越高，应用面越广，发生犯罪案件的概率就越高，潜在的社会危害性也就越大。破坏计算机系统功能的犯罪所造成的损失更是无法估量、无法弥补的，特别是被窃取的军事机密对整个社会所造成的损害和威胁，更是难以用金钱加以计算。例如，意大利机动车辆部的计算机被毁后，政府在两年时间里根本不知道谁拥有车辆和谁持有驾驶执照。

根据刑法学的一般原理，犯罪是一种严重危害社会且应受刑法惩罚的行为。而入侵计算机、制作和传播计算机病毒等威胁信息安全的行为，与传统犯罪相比，所涉及的财产数额更大，因而其社会危害性更加明显。一次计算机犯罪往往给社会造成几十万、上百万乃至上亿元的巨额损失。网络安全法是预防信息犯罪的法律，属于刑法范畴。

2）保护网络安全的其他法律

一国的法律错综复杂，只有有机地结合为一个整体，才能共同发挥治理社会的作用。在保障信息安全方面也是如此，有大量的民事法律法规和行政法律法规也起着保护信息安全的基础性作用。也就是说，有诸多法律都直接或者间接地起到保护信息安全的作用，但它们不是严格意义上的安全法。

网络安全法以外，能起到保护信息安全作用的法律，最为典型的是电子签名法和个人信息保护法。《中华人民共和国电子签名法》于 2004 年 8 月 28 日公布，并于 2005 年 4 月 1 日正式实施，是一部规范我国电子商务的基础性法律。

2. 网络安全法的特征

网络安全立法的目的是维护网络空间的正常秩序，保障信息网络的安全，维护当事人的合法权益。网络的全球性、技术性、虚拟性等特征以及网络安全立法的目的决定了我国立法的基本特征如下。

1）技术性

网络安全法的技术性是指该法是立足网络信息技术而构建的法律规范。从网络安全法的产生过程来讲，它是适应网络特点、遵循网络规律而制定的一个全新的部门法。我国在进行网络安全立法时，应适应网络的特点，在研究外国及国际立法的基础上，借鉴其先进、科学的法律制度，力求达到与国际标准统一，避免因法律制度的差异而阻碍网络的应