基础篇

第 1 章　电子商务安全概述

【学习目标】

1. 了解电子商务安全现状、电子商务安全问题的类型、电子商务安全问题产生的原因。

2. 熟悉电子商务安全的特点、电子商务安全的地位。

3. 掌握电子商务安全的概念、电子商务安全的构成、电子商务安全要素、不同主体对电子商务安全要素的需求。

【能力目标】

1. 了解电子商务安全问题，能知道目前电子商务面临的主要安全威胁、安全问题及成因。

2. 熟悉电子商务安全的重要性，能根据电子商务安全的重要性解释电子商务安全对于消费者、企业和国家的影响。

3. 掌握安全的内涵，能分析电子商务安全的本质，运用电子商务安全要素分析不同主体的安全需求。

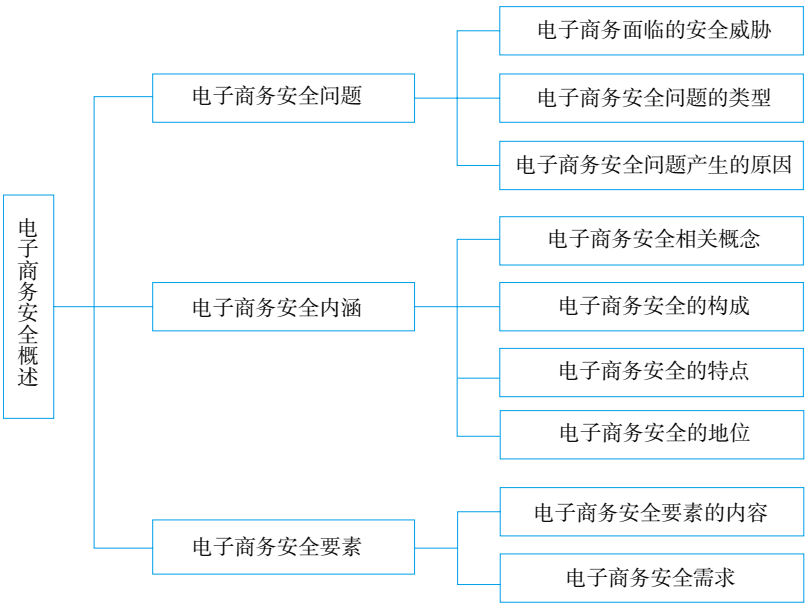
【思政目标】

1. 了解中国古今与安全有关的名言警句和重要论述，领会中国安全文化的博大精深。

2. 熟悉电子商务安全的特点，加强个人防范，增强安全意识。

3. 掌握电子商务安全要素的内容，能认识电子商务安全需求与电子商务发展的关系，树立安全与发展的辩证观。能从系统的角度分析安全问题，站在为人民谋福祉和维护国家安全的高度解决安全问题。

【思维导图】



【导入案例】

用户滥用电商平台会员权利事件

吴某于 2016 年 6 月 29 日注册为某平台公司运营的电商平台会员，在平台购物期间，针对数百起订单以七天无理由退货、拍错 / 多拍、不喜欢 / 不想要等理由大量发起退货申请，并存在重复使用同一订单号填写退货申请等情形，2017 年 11 月 17 日至 11 月 29 日 73 次虚填圆通速递单号 600490957046 申请退款，2017 年 10 月 31 日至 12 月 28 日 41 次虚填圆通速递单号 600466137147 申请退款，2017 年 11 月 17 日至 12 月 11 日 247 次虚填退货快递单号申请退款，导致其因退货信息虚假（错误单号、重复单号）、快递单号无相应物流信息等原因多次被平台卖家投诉。某平台公司以吴某滥用会员权利为由，对吴某账户进行了冻结。

资料来源：浙江新闻。

【讨论题】

1. 若吴某要求解冻账户，可以通过什么途径？

2. 吴某的行为是否触犯《中华人民共和国电子商务法》？

3. 在此案例中，该平台及卖家受到了来自吴某怎样的不良影响？

4. 在电子商务活动中，消费者、平台及商家应承担什么样的责任？

电子商务作为数字经济中规模最大、表现最活跃、发展势头最好的新业态、新动能，是新发展格局蓝图中非常重要的一环。同时电子商务的各个环节存在多种风险和安全问题。相对于传统商务，电子商务对管理水平、信息传输技术等提出了更高的要求。

1.1 电子商务安全问题

安全问题始终是电子商务的核心问题之一，基于电子商务发展与电子商务安全的刚性需求，电子商务安全自然成为当下人们关注的焦点。

1.1.1 电子商务面临的安全威胁

电子商务是基于计算机和网络实现的商务活动，电子商务安全与计算机安全和网络安全关系十分紧密，电子商务安全的风险有很大一部分来源于计算机和网络安全的威胁，这方面的威胁形势日益严峻。

1. 漏洞的威胁程度有增无减

移动互联网行业安全漏洞数量持续增长。近年来，智能终端蓝牙通信协议、智能终端操作系统、App 客户端应用程序、物联网（Internet of Things，IoT）设备等均被曝光存在安全漏洞，事件型漏洞增长幅度较大，这类漏洞涉及的信息系统大部分是在线联网系统。

2. 针对互联网的攻击威胁尤为严重

从攻击实现方式来看，更多高级持续性威胁（APT）攻击采用工程化实现，即依托商业攻击平台和互联网黑色产业链数据等成熟资源实现 APT 攻击。这类攻击不仅降低了发起 APT 攻击的技术和资源门槛，而且加大了受害方溯源分析的难度。目前境外 APT 组织主要利用当下热点时事或与攻击目标工作相关的内容作为邮件

主题，瞄准我国重要攻击目标，持续反复进行渗透和横向扩展攻击，并在我国重大活动和敏感时期异常活跃。

3. 网站数据和个人信息泄露屡见不鲜，“衍生灾害”严重

由于互联网传统边界的消失，各种数据遍布终端、网络、手机和云上，加上互联网黑色产业链的利益驱动，数据安全问题和个人信息泄露现象屡见不鲜。近几年针对数据库的密码暴力破解攻击次数日均超过百亿次，数据泄露、非法售卖等事件层出不穷，数据安全与个人隐私面临严重挑战。科技公司、电商平台等信息技术服务行业，银行、保险等金融行业以及医疗卫生、交通运输、教育培训等重要行业涉及公民个人信息的数据库数据安全事件频发。此外，部分不法分子已将数据非法交易转移至暗网，暗网已成为数据非法交易的重要渠道，涉及银行、证券、网贷等，金融行业数据非法售卖事件明显增加。

4. 移动互联网恶意程序趋利性显著，移动互联网黑色产业链已经成熟

网络黑产活动的专业化、自动化程度不断加深。以移动互联网仿冒 App 为代表的“灰色”应用程序大量出现，主要针对金融、交通等重要行业的用户。不断出现大量的仿冒 App，这些仿冒 App 主要集中在仿冒公检法、银行、社交软件、支付软件、抢票软件等热门应用上，以仿冒名称、图标、页面等内容为主。其中尤其以银行信用卡优惠、办卡等银行类 App 的仿冒数量最多，还有仿冒“微信”“支付宝”“银联”等社交软件或支付软件。另外，“12306”“智行火车票”的 App 和“个人所得税”App 均有大量仿冒应用程序出现。

5. 敲诈勒索软件肆虐，严重威胁本地数据和智能设备安全

近几年，勒索病毒活跃程度持续居高不下。随着加密货币价格持续走高，挖矿木马更加活跃。“永恒之蓝”下载器木马、WannaMiner 等挖矿团伙频繁推出挖矿木马变种，并利用各类安全漏洞、僵尸网络、网盘等进行快速扩散传播。2017 年 5 月 12 日暴发的 WannaCry 勒索病毒，通过将系统中数据信息加密，使数据变得不可用，借机勒索钱财。该病毒席卷近 150 个国家和地区，教育、交通、医疗、能源网络成为此轮攻击的重灾区。

1.1.2　电子商务安全问题的类型

1. 信息网络安全问题

从信息论角度来看，系统是载体，信息是内涵。哪里有信息，哪里就存在信

息安全问题。信息网络安全问题主要指电子商务系统及关联系统的安全问题，此类安全问题一般影响范围较大、发生频率较高。

1）物理安全问题

电子商务系统的物理安全问题也称实体安全问题，主要包括系统软硬件自身故障、外围保障设施故障、物理攻击、物理环境影响等。系统软硬件自身故障是指对业务实施或系统运行产生影响的设备硬件故障、通信链路中断、系统本身或软件缺陷等问题。外围保障设施故障是指外围保障设施基本服务的丧失，具体有空调或供水系统故障、失去电力供应故障、电信设备故障等。物理攻击指通过物理的接触造成对软件、硬件、数据的破坏，具体有物理接触、物理破坏、盗窃等。物理环境影响是指对信息系统正常运行造成影响的物理环境问题和自然灾害。有关物理威胁的案例有很多，知名网站网络经常遭遇这类威胁。

2）信息安全问题

信息安全问题主要包括越权或滥用、信息假冒、信息泄露、信息篡改、抵赖风险、信息窃取、恶意代码（malicious code）等。

（1）越权或滥用。越权或滥用是指通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用权限，做出破坏信息系统的行为，具体有未授权的设备使用、软件的伪造复制、非授权访问系统资源和网络资源、滥用权限非正常修改系统配置或数据、滥用权限泄露秘密信息等。

（2）信息假冒。信息假冒是冒充或盗用合法账户，获取非授权访问以及进行欺诈性认证，以达到制造欺诈信息、篡改合法信息的目的。

（3）信息泄露。信息泄露是指信息泄露给不应了解的人,具体有内部信息泄露、外部信息泄露等风险。此类风险通常由人为故意行为或意外的人为行为造成。如通过对阻止干扰信号的拦截、远程侦探、窃听、介质或文件偷窃、设备偷窃、回收或废弃介质的检索等手段损害信息。在泄露的信息中，用户账号、密码、邮箱等信息的泄露非常常见。

（4）信息篡改。信息篡改是指非法修改信息、破坏信息的完整性，使系统的安全性降低或信息不可用，具体有篡改网络配置信息、篡改系统配置信息、篡改安全配置信息、篡改用户身份信息或业务数据等。随着传统产业、应用、服务线上迁移进程的加速，网站信息篡改的威胁明显上升。

（5）抵赖风险。抵赖风险是指信息交互的参与者不承认发送或收到的信息和

进行的操作与交易，可能是消息原发者否认已创建消息内容并且已发送消息的服务，这种抵赖称为原发抵赖；也可能是消息接收者否认已接收消息的服务，这种抵赖称为接收抵赖。抵赖风险可能发生在电子商务交易的前、中、后各个环节，因此抗抵赖性是电子商务相当重要的一个要求。抗（不可）抵赖性就是防止以上抵赖风险的发生，如抗原发抵赖保证了恶意发送方无法在事后抵赖其创建并发送特定消息的事实。假设甲企业创建并发送了一个购买订单给乙企业，当乙企业处理了订单并开出汇票以后，甲企业应该无法抵赖发送购买订单这一事实。为了满足抗抵赖性的要求，会同时需要消息验证和发送方身份验证。抗抵赖性主要通过数字签名和身份认证技术实现。

（6）信息窃取。信息窃取是利用网络系统的漏洞、后门或隐蔽通道入侵（intrusion）他人系统，窃取数据或机密信息等。

（7）恶意代码。恶意代码是指故意在计算机系统上执行恶意任务的程序代码，具体有病毒、逻辑炸弹、特洛伊木马（以下简称“木马”）、蠕虫、陷门、间谍软件等。

3）网络安全问题

（1）网络通信安全问题。从网络通信的角度分析，网络通信安全面临的威胁可来自被动攻击和主动攻击。被动攻击是指在不影响网络正常工作情况下，进行截获、窃听、破译以获得重要机密信息的攻击行为。攻击的目的是截获在网上传输的重要敏感信息或机密信息。信息内容的泄露和流量分析是被动攻击的两种形式。主动攻击是指对数据甚至网络本身进行恶意的破坏，包括对数据进行篡改或伪造数据流，主要有阻断、伪造、重放、消息篡改和拒绝服务等形式。其中，重放是指被动地捕获数据单元，然后按原来的顺序重新传送，从而产生未经授权的效果。拒绝服务是指阻止或禁止通信设施的正常运行和使用。

（2）移动网络安全问题。移动网络安全问题来自多个方面：①网络协议方面，在无线装置组成的 Ad Hoc 网络中，主要通过移动节点的相互协作进行网络互联，不依赖任何固定网络设施，因此攻击者可以基于这种假设的信任关系入侵协作的节点。②无线链路方面，移动通信中的数据包大都以明文或安全性较弱的加密方式传输，因此极易被窃听和破解，加之无线信号的发散性和移动通信的移动性，发现攻击者行为的难度较大。免费 Wi-Fi（无线保真）热点服务危险重重，攻击者进入免费 Wi-Fi 后可以对网络中其他用户进行嗅探，通过专业软件截获用户传输

的信息。不仅如此,攻击者还可以恶意篡改 Wi-Fi 路由器的 DNS（域名系统）地址，当用户访问正常网站时，浏览器则被指向非法恶意网址，极易遭受钓鱼网站和病毒的威胁。③移动终端设备方面，由于移动设备使用方便、小巧、价值高，因此很容易丢失或被窃。另外病毒对设备的危害也很大，最严重的是手机病毒。

总体来说，网络安全问题主要来自网络攻击。网络攻击是指利用网络存在的漏洞和安全缺陷，利用工具和技术通过网络对信息系统进行攻击与入侵。攻击者可能从企业子网以外的地方向企业子网或者企业子网内的系统发起攻击。攻击者也可能来自企业内部，通过所在的局域网，向本企业的其他系统发起攻击，在本机上进行非法越权访问。企业内部人员还可能发起伪远程攻击，即为了掩盖攻击者的身份，从本地获取目标的一些必要信息后，从外部远程发起攻击，造成外部入侵的假象。网络攻击按照攻击方式可分为读取攻击、操作攻击、欺骗攻击、泛红攻击、重定向攻击以及 Rootkits 技术混合型攻击等。

2. 数据安全问题

数字经济下，数据作为关键驱动要素在电子商务企业的战略决策、市场预测、产品服务和创新、全渠道营销、供应链管理等各个方面发挥着重要作用。数据安全问题涵盖传统数据（小数据）和大数据，这里主要突出大数据安全问题。大数据的应用模式通常会使数据的所有权和使用权分离，因此产生数据所有者、提供者、使用者三种角色，数据作为重要的资产成为各方关注的焦点。由于大数据的大体量、多样性、时效性、价值性的特点使传统数据的安全和隐私保护技术受到局限或失效，数据的所有者很难像传统数据时代那样掌控和保护自己的数据，因而产生与传统数据不同的问题。

网络空间作为大数据产生、流通、应用的重要场所，在为不同行业和企业产生巨大价值的同时，往往成为网络攻击的重要对象。在新的数据防护措施不完善的情况下，对数据非法获取、使用的情况更为严重。

（1）大数据被利用成为攻击的载体。大数据挖掘和分析技术也被“黑客”用来发起攻击。

（2）存在大数据存储的安全问题、大数据传输的安全问题、大数据审计工具缺失问题、大数据内容可信性问题、大数据的隐私问题等。

（3）大数据跨境流动也存在诸多风险。电子商务和外包服务异军突起，产生大量贸易数据，这些数据在全球电子商务网络的推动下在各国（地区）之间

广泛流通。但是各国（地区）个人数据保护法律的异同可能形成新的壁垒，加之不同国家（地区）在跨境数据流动上都有自己的标准和制度，使跨境数据流动面临很多问题和风险。例如，美国基于本国互联网企业的强大采取了最为宽松的监管制度和最低限度的隐私保护制度，欧洲联盟（简称欧盟）基于传统文化强调更高标准的数据流动监管和隐私保护，俄罗斯出于保守主义采取了闭关策略。

3. 商务交易安全问题

电子商务交易不仅有传统交易安全问题，也有新型交易安全问题，这些问题也是影响电子商务安全的重要风险来源。

（1）传统交易安全问题。在传统商务中，交易安全主要是站在商务主体的角度，从商务活动参与者的自身安全、利益保护及外部影响等方面进行考量的，主要包括产品质量与产品安全问题、知识产权类的技术信息和商誉品牌问题、生产流程及人员安全问题、契约履约和投融资资金安全问题、组织管理及资金平衡等自身生存安全问题等，这些问题无论哪一个都是会对企业生存发展形成致命影响的，但又是经营活动中司空见惯的，容易遭到忽视，因此应当重视。

（2）新型交易安全问题。新型交易，本书中主要指电子商务，电子商务的发展使企业商务形态发生了巨大的变化，很多商业环节和事务是以前所没有的，如网络营销、网络直播、网络数据测评等。商务模式的变革导致一些新型交易问题，如刷单、炒信、个人信息过度收集、隐私信息泄露等。也有一些活动在传统商务活动中已经开展，或者影响不够大，或者反应比较缓慢，带来的不安全影响也就不太突出，但在网络时代，商务安全的要求已经与以往有了巨大不同。

4. 信用问题

电子商务的参与者可以是个人或机构，并且可以是匿名的。电子商务交易用户的虚拟性和非面对面的交易形式，导致交易过程存在严重的信息不对称。这种不对称产生的信用问题主要来自三个方面：①买方失信。个人消费者可能使用伪造的信用卡骗取卖方商品，而机构消费者则可能存在拖延货款的可能，卖方需要为此承担相应的风险。②卖方失信。卖方不能按照承诺的质量、数量和时间给消费者寄送其购买的商品，或者不能完全履行与机构消费者签订的合同，给买方带来相应的风险。③买卖双方都失信。买卖双方都可能抵赖曾经发生过的交易。

1.1.3 电子商务安全问题产生的原因

1. 数字化转型引起的契合度问题

电子商务是大跨度经济社会整体变迁的缩影，新兴细分业态的快速发展会产生衍生风险问题。新技术的诞生和应用要求既有产业尤其是制造业和商业同步发展，相关技术领域进步的协调性要求非常之高，既要有匹配度，又要有及时性，这样迅捷、全面的系统化变迁蕴含的风险因素是空前的。传统商务活动也有安全问题，但发酵周期短、影响范围小，商务和公众事件耦合可能小，所以没有得到有效重视，网络背景下电子商务安全与以往有非常大的区别，前述几个传统商务安全问题的特征在电子商务安全中完全逆转，可能演化成更为严重的安全事件。另外，在经济形态从工业经济向信息经济转换的过程中，商务形态也从以传统的工商业活动为主向以电子商务活动为主转换，安全问题比相对稳定的商业形态下要更多。

2. 安全基础设施和安全技术缺乏

电子商务安全基础设施包括网络基础设施、系统安全基础设施、交易安全基础设施、信用安全基础设施等。它们为电子商务安全提供支撑环境，为实施电子商务系统提供服务和决策支持。这些基础设施的缺少给电子商务安全带来较大安全隐患。

中国乃至全球的电子商务成长速度都远超业界的预期，这种成长速度对配套的相关管理和基础设施都提出了难以企及的要求，因而可以说电子商务安全问题的严重性、紧迫性与基础设施和相关技术的缺乏紧密相关。

3. 电子商务治理思维与模式不匹配

（1）重安全技术、轻安全管理。目前，电子商务治理思维偏重技术安全，包括设备安全、数据安全、软硬件的安全属性、网络通联状态等，也重视以系统运行稳定性为核心的各类硬件、软件和系统运行管理的安全，但总体上重安全技术、轻安全管理，尤其忽视与电子商务核心领域相关的商务安全的管理。

（2）传统治理体制与电子商务安全需要不匹配。互联网的兴起促进电子商务的勃兴，互联网早期是科研领域的信息传输方式，因此政府更多地将之作为基础设施进行建设，乃至后来逐步拓展到通信、商务、社会服务等领域，互联网的治理思维才从单一行政管理向多元治理逐步转变。但同时，电子商务安全要求有最终裁决者，分散、制衡的治理体制与电子商务的安全需要方向存在较大的夹角，因此需紧随网络经济、信息经济变迁的步伐，改革传统治理体制。

4. 电子商务安全基础环境不健全

电子商务安全基础环境的不健全表现在电子商务安全标准体系的建设滞后。电子商务的发展日新月异，新业务、新商务模式、新技术层出不穷，但电子商务相关的安全标准和协议还不完善。另外，目前我国没有一个完整的、具有指导意义的规范性法律法规来限定电子商务中的不安全行为，2019 年颁布实施的《中华人民共和国电子商务法》(以下简称《电子商务法》) 在某种程度上缓解了这一窘境，但与电子商务安全管理的制度需要尚有距离。需要注意的是，电子商务安全管理制度还有待继续完善，如电子商务市场的准入和退出制度、电子商务产品质量监督管理体系、电子商务信用体系等。

1.2　电子商务安全内涵

电子商务安全是一个系统而广泛的概念，电子商务的各个方面、各个环节都存在安全问题。为了准确把握“电子商务安全”，首先对电子商务安全相关的概念进行探讨。

1.2.1　电子商务安全相关概念

电子商务安全是由“电子商务”和“安全”两个概念组成的复合概念，下面在对“电子商务”和“安全”的概念进行分析的基础上，对电子商务安全的概念进行界定。

1.“电子商务”的概念

电子商务从萌芽到兴起，从勃兴到占据商务活动主渠道，演进迭更。伴随着电子商务的发展，曾经有多个国际组织、政府、企业和专家学者从不同角度对电子商务进行了解释，目前尚未形成一个公认的统一的定义。《电子商务法》第 2 条定义的电子商务，“是指通过互联网等信息网络销售商品或者提供服务的经营活动。”第 2 条第 2 款将“金融类产品和服务，利用信息网络提供新闻信息、音视频节目、出版以及文化产品等内容方面的服务”排除在《电子商务法》所称的电子商务之外。本书认为，以信息网络为基础媒介的商品化的物质产品、非物质服务和涉及产权的交易活动，全部是电子商务，因而所有通过、依靠、基于或借助信息网络实现的商务活动均可纳入电子商务范畴进行考察。

2.“安全”的概念

（1）汉语中的“安全”。古代汉语中没有“安全”一词，但“安”字却在许多场合下表达着现代汉语中“安全”的概念，表达了人们通常理解的“安全”这一概念。例如，“是故君子安而不忘危，存而不忘亡，治而不忘乱，是以身安而国家可保也”(《周易·系辞下》)。这里的“安”是与“危”相对的，并且如同“危”表达了现代汉语的“危险”一样，“安”所表达的就是“安全”的概念。

“安全”作为一个现代汉语的基本词语，在各种现代汉语辞书中的解释基本相同。例如《现代汉语词典》(第7版)对“安全”的解释是：“没有危险；平安”。《辞海》对“安”字的第一个释义就是“安全”,并在与国家安全相关的含义上举了《国策·齐策六》的一句话作为例证：“今国已定，而社稷已安矣。”除此之外，在标准中也有对“安全”的界定。

（2）英文中的“安全”。汉语中的“安全”翻译成英文时，可以与其对应的主要有 safety 和 security 两个单词，虽然这两个单词的含义及用法有所不同，但都可在不同意义上与中文的“安全”相对应。在谈到国家安全时经常使用 security，且认为安全具有两方面的含义：一方面是指安全的状态，即免于危险，没有恐惧；另一方面是指对安全的维护，即安全措施（security measure）和安全机构。

在这里，计算机信息系统安全、计算机系统安全、信息安全、网络空间安全等词汇中的安全在英文中通常使用 security，而不是 safety。电子商务安全与信息安全、网络安全密切相连。从课程起源看，“电子商务安全”起源于“密码学与网络安全”，没有密码学理论和网络安全技术，当今的电子商务就失去了技术基础。因此一直以来，电子商务安全的基础内容是以密码学与网络安全为主，基于这一点，本书使用 security。

综上所述，无论是中文的“安全”还是英文的 security，都表示一种存在的状态，即表示免于危险或没有危险的状态。

安全与危险是相对立的概念，安全的特有属性就是没有危险。而且这种没有危险的状态是不以人的主观意志为转移的，因而是客观的。没有危险的客观状态是一种属性，因此它必然依附一定的实体。当安全依附于人，便是人的安全；当安全依附于电子商务，便是电子商务安全；当安全依附于数字经济，便是数字经济安全；当安全依附于国家，便是国家安全。这样一些承载安全的实体，就是安全的主体。因此可以进一步说，安全是主体没有危险的客观状态。其中，没有危

险包括了没有外在威胁和没有内在危险两个方面。有人认为，安全既是一种客观状态，也是一种主观状态。本书认为，安全作为一种状态是客观的，是不以人的主观愿望为转移的客观存在。而安全感则与安全不同，安全感是安全主体对自身安全状态的一种自我意识、自我评价。这种自我意识和自我评价与客观的安全状态有时一致，有时可能相去甚远。例如，有人虽然在安全的状态下，但是感觉很不安全；也有人身处危险境地，却对危险视而不见，认为自己很安全。

3. 电子商务安全的概念

安全是有主体的，当安全的主体是电子商务时，便构成了电子商务安全。可以说电子商务安全就是使电子商务处于没有风险的客观状态。这里的风险泛指危险，安全管理的对象是风险，安全的特有属性就是没有风险。

电子商务要达到没有风险的客观状态并非易事。数字经济下万物互联互通，电子商务安全不是一个企业的安全，因为针对企业的攻击很容易通过互相连接的紧密网络迅速蔓延到其他个体，独立个体的威胁很容易转变为对整个电子商务生态系统的巨大威胁，形成难以应对的系统化风险。因此电子商务安全的主体是电子商务整体，是电子商务全链条、全流程和全环节，是整个电子商务生态系统，而不是电子商务局部或部分。首先，数字经济下电子商务的威胁方已发生变化，由原来独立的“黑客”和病毒制作者转变为有组织的黑灰产组织。这些组织具有专业化和国际化的特点，同时内部组织严密、运作效率高，高频且规模化的攻击越来越常见，给企业和政府造成巨大的外部威胁。其次，电子商务还面临来自内部的隐患，隐患可能是内部安全技术的短板，也可能是安全管理能力的不足。网络复杂程度的增加，对安全防空技术和体系提出了更高的要求，传统针对独立个体和企业的局部网络难以应对当前复杂且成规模的黑灰产的威胁，需要从一般局部防御向一体化攻防体系转变。而在安全能力方面，不能只是简单地进行安全修补，而应实现风险检测、预警和修复的自动化，构建全面的防护体系、制定完善的安全策略。

因此，本书认为，电子商务安全就是通过持续对电子商务危险识别和风险管理（risk management）的过程，将参与电子商务全流程的人员伤害或财产损失的风险降低并保持在可接受的水平或其以下的一种状态。这里所指的风险覆盖电子商务的整个流程，涉及电子商务的全部参与者、各类软硬件设施、内外部运行环境，包括但不限于信息与网络风险、交易风险、信用风险、人员风险等，这是电子商务普遍存在的，最为基础、最为关键的几类风险。

1.2.2 电子商务安全的构成

电子商务由多环节、多系统的众多内容构成，其蕴含的风险与这些内容相伴相随，安全问题的内容也相应地来自这些细分领域或环节。

1. 物理安全

电子商务体系必须与各类客观资源联通才能形成有效的产品或服务供给，网络产品供应商的设施、设备、厂房等，也是电子商务安全的关注对象。

2. 信息与网络安全

电子商务的顺利开展必须依托网络信息系统，在传统的商务安全内容之外，网络涉及服务器、通道、客户端，信息则包括（大）数据、资料、客户的身份信息和隐私，这也是电子商务安全必然的内容。

3. 交易安全

电子商务安全的内容首先是交易，即买卖，电子商务是商务活动的一种形态，但是电子商务过程具有繁复和非现场的特性，交易的整个过程都会产生安全问题，因此交易安全必然是电子商务安全的核心内容。

4. 信用与法律

市场交易离不开信用，市场离不开规则，如关于产品质量、数量及技术瑕疵等方面规则；同时，网络信息系统也是在一系列的规则和协议规范之下运行的，因此信用与法律也是电子商务安全需要重视的问题。

5. 人员安全

电子商务是依托网络信息系统的，其运行离不开人员，参与人员会面临人身安全问题，比如说健康问题、服务过程伤害等，因此，人员安全也是电子商务安全必然的内容。

总体上，在所有安全问题中，电子商务安全特别要关注信息与网络安全以及交易安全，这是电子商务安全与网下商务安全的主要差别点，也是电子商务安全问题的高发领域。

1.2.3 电子商务安全的特点

1. 系统化

电子商务体系一经确立，就会形成比较稳定的结构关系，但它是一个开放的系统，其存在和发展有赖于与外界不断进行的物质、能量和信息的交换。电子商

务与线下的商务活动相同，最基本的活动过程是由许许多多的主体共同落实完成的，各主体主要通过交易、协作、竞争等方式来参与，并承担相应的任务和职能。与线下商务活动存在显著差别的是，电子商务的结果更趋于总体共同努力形成，任何子系统的变化均会影响其他系统的变化，部分群体的逆向选择或道德风险会严重影响总体的绩效和安全。因此，电子商务安全应当是以整个系统的安全为核心目标，在系统安全的整体目标下，对应实现各参与主体的生命财产与运行安全。

2. 动态化

电子商务安全总是与技术的迭代更新、内外环境和条件的变动相联系，在与现代信息技术和管理的博弈中维持着一种相对稳定的安全状态。例如大数据技术将电子商务活动以数字形式进行记录及呈现，为风险防范提供了新的技术和方法，同时信息权、数据权的界定不清又为数据滥用、信息泄露和各种侵权行为提供了可乘之机。而相关立法的滞后性和被动性，导致新型威胁与安全防护难以同步。这不仅要求转换管理思想，提升安全意识，更需要与安全相关的技术、组织机构、管理流程达到匹配。

3. 相对化

电子商务安全是相对的安全，因为没有绝对的安全。首先，电子商务系统，无论是硬件系统还是软件系统都是人设计出来的，也是由人操作、使用和管理的，没有任何安全问题的电子商务系统是不存在的。其次，没有必要追求一个绝对永远攻不破的系统，因为任何电子商务的安全措施都有成本和代价，电子商务安全需要考虑代价问题。速度、便捷性和安全是矛盾的统一体，不能只注重速度和便捷性而忽略安全，也不能只注重安全而不考虑便捷性。无论是安全技术提供者还是管理者都应综合考虑这些因素，寻找其最佳平衡点。

1.2.4　电子商务安全的地位

1. 电子商务安全是国家经济安全的重要组成部分

一个国家的安全很大程度上依赖于这个国家的经济实力，而电子商务安全是影响国家经济安全的重要因素之一。

（1）电子商务是国家经济安全的重要保障。电子商务作为我国经济发展的新动力、新引擎，大大加快了我国信息网络基础设施的建设和发展，增进了互联网与各个行业的深度融合，进一步促进了传统行业的转型升级和行业间的跨界发展，

为我国经济高质量发展赋能。特别是在新型冠状病毒感染疫情期间，电子商务为国家抗疫和防疫、企业复工复产、社会公民恢复正常生活提供了有力帮助，成为防止经济发展下滑风险的重要保障力量。

（2）电子商务安全直接影响国家经济安全。电子商务网络成为“黑客”、恐怖主义的攻击目标，给国家安全带来了新的威胁。近几年破坏电子商务计算机信息系统、伪造或盗用账户、电子商务诈骗、侵犯电子商务秘密、电子商务中侵犯公民个人信息、电子商务中侵犯知识产权等犯罪呈高发态势。另外，大型电子商务平台在资本的助推下产生的垄断问题日益严重。这种垄断行为和不正当竞争行为破坏了公平竞争的市场秩序，不仅严重损害消费者的切身利益，而且不利于电子商务和国家经济的健康发展。可以看出，由于电子商务与国家经济深度融合、密切相关，电子商务安全与否对于国家经济是否平稳运行、能否抵抗危机非常重要。

2. 电子商务安全是企业安全的重要组成部分

电子商务安全是整个电子商务链条上所有企业安全的重要组成部分。电子商务安全对于电子商务平台运营企业和电子商务供应商具有特殊意义。电子商务平台运营企业是基于网络信息系统和互联网运行的企业，属于典型的“互联网 +”企业，其安全问题主要与网络信息系统安全关联，还有大量的合规合法问题。电子商务供应商充分运用或服务于互联网，此类企业更多属于“+ 互联网”。首先，其安全风险和网下普通企业类似，主要表现在产品质量和自身生产运营的安全。其次，因为其在网络上开展市场营销活动，其安全问题也更多地与网络有关。另外，在数据驱动、产业互联的推动下，整个产业链中各企业唇齿相依、脉脉相通。企业安全事件一旦发生，不仅直接威胁企业的生存和发展，也可能影响社会公众的隐私及利益，更有甚者可能危及国家安全。

3. 电子商务安全是消费者安全的重要保障

在电子商务飞速发展的今天，通过电子商务完成基本消费支出，实现生活服务的购买，是非常普遍的现象，各类机构组织也通过网络消费过程实现机构运行的基本资料的获取。

（1）电子商务安全保障个体消费者的安全。电子商务环境下，普通个体消费者通过网络实现生活消费的重要内容，安全主要体现在其自身生命安全、个人及财务信息安全、产品质量导致的健康安全问题，当然由此导致的沟通、纠纷处置等安全问题也需要考虑。

（2）电子商务安全保障机构消费者的安全。机构消费者通过网络进行各种必需资源的采购，包括工具、耗材、短期服务等，他们在消费过程中与普通个体消费者并无显著差异，但其安全问题一旦爆发带来的后果放大系数可能更大。

因此，电子商务安全对个人隐私和财产的安全、组织机构的正常运作和持续发展、国家经济安全等方面都具有重要影响，是国家整体安全至关重要的组成部分。

1.3　电子商务安全要素

电子商务安全要素是决定电子商务安全最为关键的因素。

1.3.1　电子商务安全要素的内容

1. 保密性

保密性通常是指只有发送方和接收方才能访问信息的内容，非授权人员不能访问。在电子商务交易中，涉及的商业机密、个人信息等均有保密的要求。电子商务经营主体应当建立健全内部控制制度和技术管理措施，防止信息泄露、丢失、毁损，确保电子商务数据信息安全。

2. 完整性

完整性是防止未授权信息的生成，防止信息在存储和传输过程中丢失、重复及非法用户对信息的恶意篡改。

3. 认证性

认证性也可称为真实性，即通过可靠的认证机制来确保对方身份和信息来源是真实的。电子商务中由于交易双方无法见面，假冒者或攻击者会伪造身份或信息，因此安全交易的前提是交易双方的身份或信息是真实的，这可以由可靠的认证机制来保障，通常需要第三方的介入。认证包括对信息本身的认证和对实体的认证。对信息本身的认证用于确认信息是否来源于声称的某个实体，而不是伪造的。对实体的认证可确定交易双方身份的真实性。

4. 可控性

可控性又称为访问权限的控制，这是一种按照事先设定的规则确定主体对客体的访问模式是否合法的安全机制，以此来保证系统、数据和服务是由合法人员访问，保证数据的合法使用。

5. 不可否认性

不可否认性又称不可抵赖性，是防止通信或交易双方对收发过的信息或业务进行否认。电子商务系统应保证交易一旦达成，发送方不能否认发送的信息，接收方不能篡改他收到的信息，保证交易双方对已发生的交易无法抵赖，防止商业欺诈行为的发生。

6. 可用性

可用性是指保证信息和信息系统在访问者需要时可随时为授权者提供服务，避免服务的中断，哪怕是短暂性的。例如像淘宝、天猫、京东等大型的电子商务平台发生故障或受到攻击，哪怕是几分钟的服务中断都将导致上千万次的交易无法进行，从而给平台或商家造成较大损失。

7. 匿名性

匿名性是确保合法用户的隐私不被侵犯。电子商务系统应防止交易过程被跟踪，防止用户个人信息的泄露，确保交易的匿名性。

8. 可信性

可信性是指交易双方在交易身份真实可靠的基础上，保障其交易行为是可信的。例如交易的产品或服务质量、配套服务及售后等是否与承诺的一致。可信性需要完善的信用评价体系，以降低电子商务交易的不确定性、高度动态性、交易用户虚拟性及电子商务技术与管理局限性等给交易双方带来的风险。

9. 合规合法性

合规合法性是指电子商务的各参与方的活动符合国家相关的标准、法律、法规。

1.3.2 电子商务安全需求

1. 运行角度安全需求

电子商务是多种技术和服务的集合体，从逻辑上可将电子商务体系分为网络层、支付层、交易层，不同的逻辑层次产生了不同的安全需求。

（1）网络层安全需求。认证性、可控性、保密性、完整性、可用性、不可否认性、合规合法性。

（2）支付层安全需求。保密性、匿名性、认证性、不可否认性、合规合法性。

（3）交易层安全需求。可信性、保密性、完整性、可用性、不可否认性、合

规合法性。

在以上逻辑层次中，网络层是基础层，必须为电子商务实现提供更加稳定的网络环境，对网络的可用性需求高。支付层涉及隐私信息，如用户名、账号、密码等，对保密性和匿名性需求高。交易层由于电子商务具有的虚拟性和身份不确定性，对可信性需求高。

2. 参与主体安全需求

电子商务安全要素体现了电子商务安全最核心的几个组成部分，在不同的电子商务模式下，交易的流程和参与方有所不同，如 C2C（消费者对消费者）、B2C（企业对消费者）、B2B（企业对企业）等。下面主要以 B2C 电子商务模式为例，介绍消费者、商家和政府对电子商务安全要素的需求，具体需求分析见表 1–1、表 1–2、表 1–3。

表 1–1　消费者安全需求

安全需求	消费者角度
保密性	我的信息没有被我指定的接收方之外的其他非授权者读取
完整性	我发出或接收的信息没有被篡改或重放
认证性	确保和我交易的人或商家就是他所声称的那个
可控性	我怎样获得访问该网站的权利，我具有哪些权利，我需控制个人信息的使用
不可否认性	和我交易的对方不能否认曾经进行过的交易
可用性	在我需要使用电子商务网站或平台时，随时都可以使用
匿名性	我的信息不被泄露，我的交易不能被跟踪
可信性	无不良消费记录，没有恶意评价
合规合法性	消费行为符合相关的法律法规

表 1–2　商家安全需求

安全需求	商家角度
保密性	信息或机密数据不能被非授权者读取
完整性	信息系统或网站上的数据没有被未授权者生成、修改或删除，信息被安全地存储和传输
认证性	确保消费者的真实身份
可控性	保证信息系统或网站正常运营，保证授权用户对系统资源和服务的使用，对用户个人信息和数据的收集与使用应控制在合理范围内
不可否认性	消费者不能否认曾经订购过产品，交易对方不能否认发生的交易
可用性	保证随时可以为用户提供所需的信息或服务

续表

安全需求	商家角度
匿名性	确保交易的匿名性、不可跟踪性，确保合法用户的隐私权
可信性	信誉度好，商品无质量问题，提供的服务与承诺的一致，无刷单、炒信行为
合规合法性	依照国家的相关法律法规生产和经营，采取有效措施保护平台或信息的安全

表 1–3 政府安全需求

安全需求	公共管理角度
保密性	信息或机密数据的合法上传、读取和传输
完整性	信息被安全地存储和传输，传输系统未受到严重篡改
认证性	确保参与各主体的真实合法身份
可控性	保证信息系统正常运营，对用户个人信息和数据的收集与使用合法
不可否认性	交易双方不能否认发生的交易
可用性	保证系统安全，可以适时为用户提供所需的信息或服务
匿名性	确保交易的不可跟踪性，确保合法隐私权
可信性	参与各方均应尊重爱护自身信誉，无失信行为
合规合法性	遵照国家法律法规，无不良政治企图，无违反社会公序良俗的行为

【本章小结】

电子商务面临前所未有的安全威胁，本章从电子商务安全现状出发，总结电子商务几类典型的安全问题，并分析这些问题产生的客观和主观的原因。然后在阐释电子商务和安全概念的基础上，分析电子商务安全的内涵并予以界定。分析电子商务安全的构成、自身的特点以及电子商务安全对于国家经济安全、企业安全、消费者安全的重要性。要想实现电子商务安全，首先要保证电子商务安全要素的安全，本章总结了九类安全要素，并从运行角度及参与主体两个角度分析对这些安全要素的具体需求。

【思考题】

1. 结合案例谈谈电子商务面临的主要安全威胁。
2. 分析电子商务安全与传统商务安全的异同点。
3. 简述电子商务安全对国家经济安全的重要性。
4. 分析电子商务安全与发展的关系。
5. 结合例子简要分析电子商务安全要素。
6. 结合实例分析商家和消费者的安全需求。

【即测即练】