# §1.2 信息安全的研究内容

信息安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的边缘性综合学科。

信息安全研究的内容包括：

一、信息安全基础理论研究

二、信息安全应用技术研究

三、信息安全管理研究

# §1.2 信息安全的研究内容

一、信息安全基础理论研究

1、密码理论

加密：将信息从易于理解的明文加密为不易理解的密文

消息认证：检测消息是否被篡改

数字签名：通过对信息进行私钥加密来实现

密钥管理：研究密钥的产生、发放、存储、更换、销毁等

2、安全理论

身份认证：验证用户身份是否与其所声称的身份一致

授权与访问控制：将用户的访问行为控制在授权范围内

审计跟踪：记录、分析和审查用户行为，追查用户行踪

安全协议：构建安全平台时使用的与安全防护有关的协议

# §1.2 信息安全的研究内容

二、信息安全应用技术研究

1、安全实现技术

防火墙技术：控制两个安全策略不同的域之间的互访行为

漏洞扫描技术：对安全隐患的扫描检查、修补加固

入侵监测技术：提取和分析网络信息流，发现非正常访问

病毒防护技术：

2、平台安全

# §1.2 信息安全的研究内容

二、信息安全应用技术研究

1、安全实现技术

防火墙技术、漏洞扫描技术、入侵监测技术、病毒防护技术

2、平台安全

物理安全：防止物理通路的损坏、窃听、干扰等

网络安全：保证网络只给授权的客户使用授权的服务，
保证网络路由正确，避免被拦截或监听

系统安全:操作系统自身的安全问题

数据安全:安全数据库系统、数据存取安全等

用户安全:账户的管理、用户权限和角色管理

边界安全:不同安全策略的区域边界连接的安全

# §1.2 信息安全的研究内容

三、信息安全管理研究

信息安全保障体系、信息安全应急反应技术、安全性能测试和评估、安全标准、法律、管理法规制定、安全人员培训提高等

1. 美国TCSEC(桔皮书)可信计算机系统评估准则。1985年由美国国防部制定。分为4个方面:安全政策、可说明性、安全保障和文档。该标准将以上4个方面分为7个安全级别,从低到高依次为D、C1、C2、B1、B2、B3和A级。

D类：最低保护。整个系统不可信。对于硬件来说，无任何保护；对于操作系统来说，容易受到损害；对于用户及其访问权限来说，没有身份认证。

# §1.2 信息安全的研究内容

C1类：自决的安全保护。对硬件进行了某种程度的管理，用户登录需要用户名和口令，对数据设置了访问权限。不能阻止系统管理员执行的操作，不能控制进入系统的用户的访问级别。

C2类：访问级别控制。除了C1级的特性外，还包含创建受控访问环境的安全特性。受控访问环境可以进一步限制用户执行某些命令或访问某些数据的能力。除许可权限外，还需要身份验证级别。

# §1.2 信息安全的研究内容

**B1类：有标签的安全保护**。系统中的每个对象都有一个敏感性标签而每个用户都有一个许可级别。许可级别定义了用户可处理的敏感性标签。系统中的每个文件都按内容分类并标有敏感性标签，任何对用户许可级别和成员分类的更改都受到严格控制，即使文件所有者也不能随意改变文件许可权限。

**B2类：结构化保护**。系统的设计和实现要经过彻底的测试和审查。系统应结构化为明确而独立的模块，遵循最小特权原则。必须对所有目标和实体实施访问控制。政策要有专职人员负责实施，要进行隐蔽信道分析。系统必须维护一个保护域，保护系统的完整性，防止外部干扰。

# §1.2 信息安全的研究内容

B3类：安全域。系统的安全功能足够小，以利广泛测试。必须满足参考监视器需求以传递所有的主体到客体的访问。要有安全管理员，安全硬件装置，审计机制扩展到用信号通知安全相关事件，还要有恢复规程，系统高度抗侵扰。

A1类：核实保护。最高级别，包含较低级别的所有特性。包含一个严格的设计、控制和验证过程。设计必须经过数学上的理论验证，而且必须对加密通道和可信任分布进行分析。

近年来,人们一直在努力发展安全标准,并将安全功能与安全保障分离,制定了复杂而详细的条款。但真正实用、在实践中相对易于掌握的还是TCSEC及其改进版本。在现实中,安全技术人员也一直将TCSEC的7级安全划分当做默认标准。

# §1.2 信息安全的研究内容

2、我国将计算机信息系统安全保护分为5级：

用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级、访问验证保护级。

用户自主保护级：相当于C1级

系统审计保护级：相当于C2级

安全标记保护级：相当于B1级　　属于强制保护

结构化保护级:相当于B2级

访问验证保护级：相当于B3～A1级

# §1.2 信息安全的研究内容

3、实际应用中主要考核的安全指标有身份认证、访问控制、数据完整性、安全审计、隐蔽信道分析等。

1) 身份认证：通过标识鉴别用户的身份，防止攻击者假冒合法用户获取访问权限。重点考虑用户、主机和节点的身份认证。

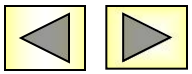
2) 访问控制：访问控制根据主体和客体之间的访问授权关系，对访问过程做出限制，可分为自主访问控制和强制访问控制。自主访问控制主要基于主体及其身份来控制主体的活动，能够实施用户权限管理、访问属性(读、写及执行)管理等。强制访问控制则强调对每一主、客体进行密级划分，并采用敏感标识来标识主、客体的密级。

3) 数据完整性：信息在存储、传输和使用中不被篡改

# §1.2 信息安全的研究内容

4) 安全审计：通过对网络上发生的各种访问情况记录日志，并统计分析，对资源使用情况进行事后分析，这是发现和追踪事件的常用措施。审计的主要对象为用户、主机和节点，内容为访问的主体、客体、时间和成败情况等。

5) 隐蔽信道分析：隐蔽信道是指以危害网络安全策略的方式传输信息的通信信道。这是网络遭受攻击的原因之一。采用安全监控，定期对网络进行安全漏洞扫描和检测，加强对隐蔽信道的防范。



# §1.2 信息安全的研究内容

4、相关的信息安全法律法规：

1）计算机病毒防治管理办法；

2）中华人民共和国计算机软件保护条例；

3）中华人民共和国计算机信息系统安全保护条例；

4）中华人民共和国计算机信息网络国际联网管理暂行规定；

5）计算机信息网络国际联网安全保护管理办法

6）互联网信息服务管理办法

7）商用密码管理条例

8）中华人民共和国保守国家秘密法

9）中华人民共和国网络安全法

10）中华人民共和国密码法

11）中华人民共和国数据安全法

# §1.2 信息安全的研究内容

**中华人民共和国计算机信息系统安全保护条例**

（1994年2月18日中华人民共和国国务院令147号发布）



中华人民共和国
网络安全法



中华人民共和国
数据安全法



中华人民共和国
个人信息保护法

# §1.2 信息安全的研究内容



中华人民共和国
网络安全法

我国颁布的第一部关于网络安全和数据保护的法律，2017年6月1日起施行。

限制了互联网企业某些行为，规定其不能泄露或者篡改收集的用户个人信息，与第三方进行数据交易时，也应当确保遵守法律上的数据保护义务。

# §1.2 信息安全的研究内容



中华人民共和国
网络安全法

第十二条　国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

# §1.2 信息安全的研究内容



中华人民共和国
网络安全法

第二十四条　网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

# §1.2 信息安全的研究内容



中华人民共和国
网络安全法

第二十七条　任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

# §1.2 信息安全的研究内容



中华人民共和国
网络安全法

第四十一条　网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

# §1.2 信息安全的研究内容



中华人民共和国
网络安全法

第四十四条　任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十六条　任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

# §1.2 信息安全的研究内容



中华人民共和国
网络安全法

第四十八条　任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

# §1.2 信息安全的研究内容



中华人民共和国
数据安全法

2021年9月1日起施行。

为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益。

数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

# §1.2 信息安全的研究内容



中华人民共和国
个人信息保护法

2021年11月1日起施行。

为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用。

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

第五条　处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

# §1.2 信息安全的研究内容



中华人民共和国
个人信息保护法

**第六条** 处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。

收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

**第八条** 处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

**第十条** 任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

# §1.2 信息安全的研究内容

中华人民共和国国务院令

第790号

《网络数据安全管理条例》已经2024年8月30日国务院第40次常务会议通过，现予公布，自2025年1月1日起施行。

总理　　李强

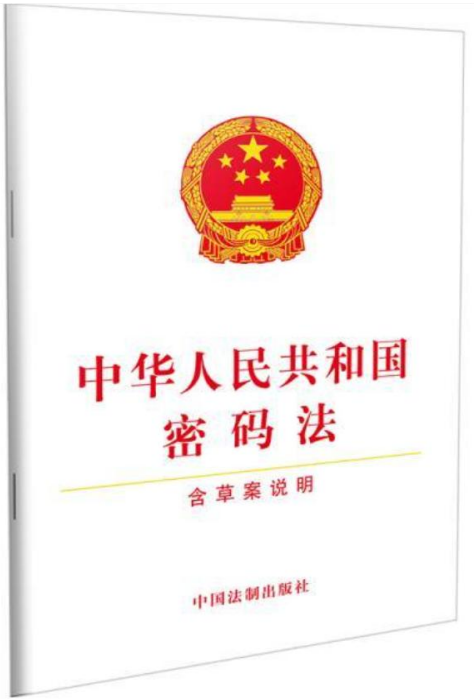
2024年9月24日

为了规范网络数据处理活动，保障网络数据安全，促进网络数据依法合理有效利用，保护个人、组织的合法权益，维护国家安全和公共利益。

第八条　任何个人、组织不得利用网络数据从事非法活动，不得从事窃取或者以其他非法方式获取网络数据、非法出售或者非法向他人提供网络数据等非法网络数据处理活动。

第十九条　提供生成式人工智能服务的网络数据处理者应当加强对训练数据和训练数据处理活动的安全管理，采取有效措施防范和处置网络数据安全风险。

# §1.2 信息安全的研究内容




中国密码领域第一部综合性、基础性法律，2020年1月1日起施行。

为了规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益。

密码法将密码分为核心密码、普通密码和商用密码，并对密码进行分类管理。核心密码、普通密码属于国家秘密，核心密码保护信息的最高密级为绝密级，普通密码保护信息的最高密级为机密级。商用密码用于保护不属于国家秘密的信息。