

# 网络安全防护体系

**2019年**

2019年5月我国《信息安全技术 网络安全等级保护基本要求》等核心标准正式发布，2019年12月1日正式实施

**2017年**

6月1日《网络安全法》正式生效

**2014年**

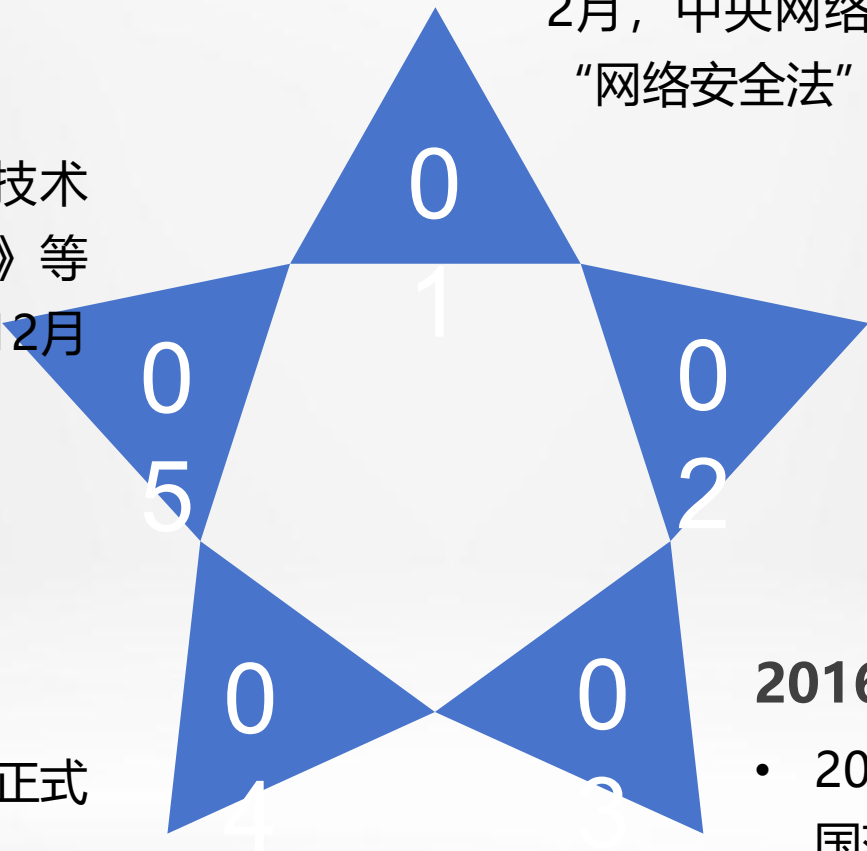
2月，中央网络安全与信息化领导小组成立  
“网络安全法”首次被写入政府工作报告

**2015年**

- 6月，十二届全国人大常委会审议了《网络安全法（草案）》
- 7月《网络安全法（草案二次审议稿）》

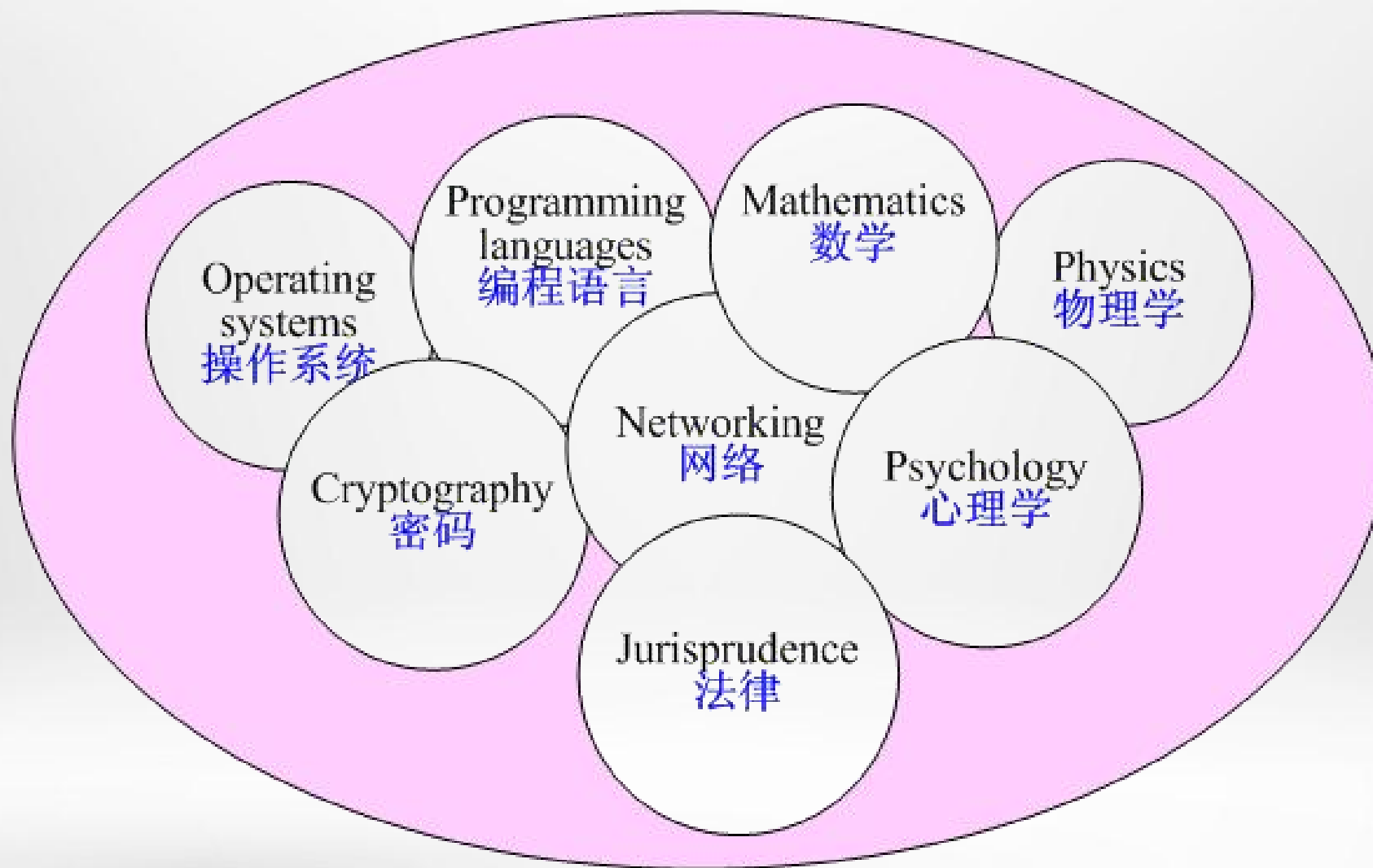
**2016年**

- 2016年7月启动关键信息基础设施全国范围内的检查工作
- 2016年12月27日发布并实施《国家网络安全战略》



## 1.3

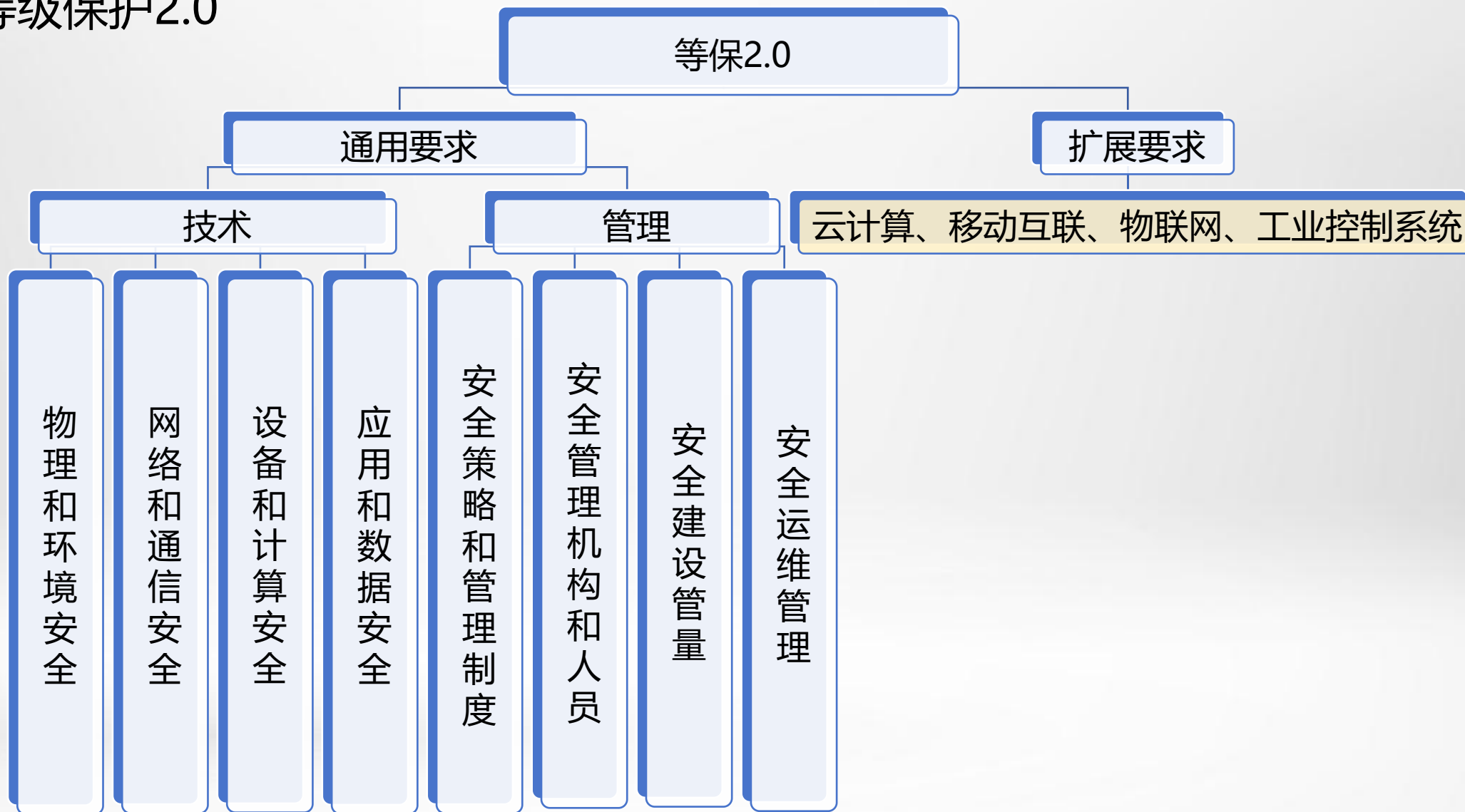
# 网络安全涉及的内容



## 1.3 网络安全涉及的内容



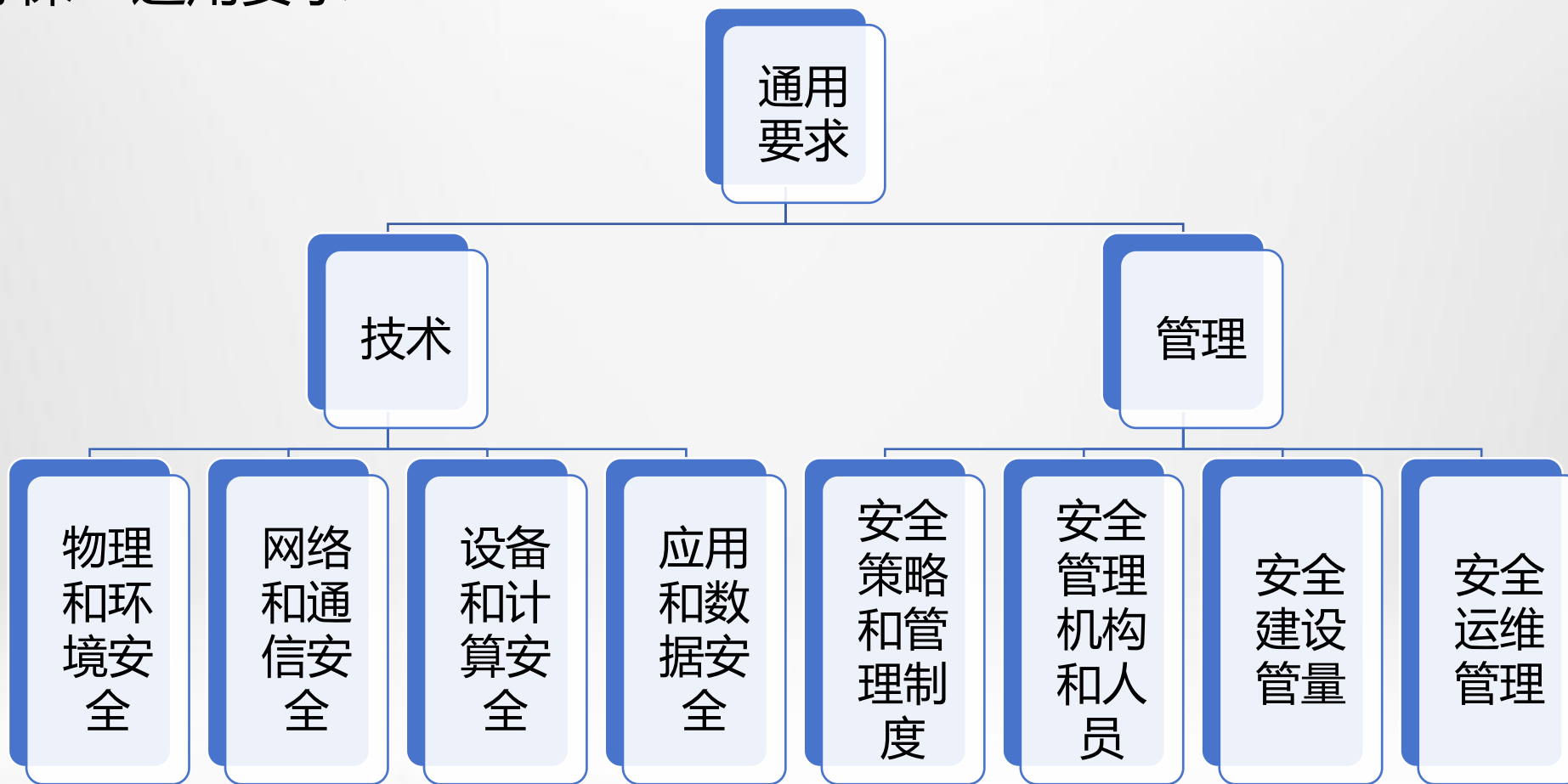
### 等级保护2.0



## 1.3 网络安全涉及的内容



### 等保—通用要求



## 01

OPTION

## 物理安全控制



## 设备安全

主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等。

---



## 物理访问控制安全

建立访问控制机制，控制并限制所有对信息系计算、存储和通讯系统设施的物理访问。

---

## 02

OPTION

## 环境安全



为了确保计算机处理设施能正确、连续地运行，要考虑及防范以下威胁：火灾、电力供应中断、爆炸物、化学品等，还要考虑环境的温度和湿度是否适宜。

---

表1-3 网络和通信安全的组成

|             |        |                                     |
|-------------|--------|-------------------------------------|
| 网络和通信<br>安全 | 子项     | 举例                                  |
|             | 网络架构   | 设计安全的拓扑、链路备份、IP划分等                  |
|             | 通信传输   | 防火墙等安全设备、数据加密（VPN等）                 |
|             | 边界防护   | 对内部用户非授权联到外部网络的行为进行限制或检查；限制无线网络的使用等 |
|             | 访问控制   | 访问控制功能的设备包括网闸、方后墙、路由器和三层路由交换机等      |
|             | 入侵防范   | 入侵检测系统等                             |
|             | 恶意代码   | 关键网络节点处对恶意代码进行检测和防护                 |
|             | 垃圾邮件防范 | 关键网络节点处对垃圾邮件进行检测和防护                 |
|             | 安全审计   | 各系统配置日志，提供审计机制                      |
|             | 集中管控   | 集中监测、集中审计和集中管理                      |

- 瑞典1973 年就颁布了《数据法》， 这是世界上首部直接涉及计算机安全问题的法规。
- 1983年美国公布了可信计算机系统评价准则 (TCSEC) 简称橙皮书。

---

橙皮书为计算机的安全级别进行了分类，分为D、C、B、A级，由低到高。D级暂时不分子级。C级分为C1和C2两个子级，C2比C1提供更多的保护。B级分为B1、B2和B3三个子级，由低到高。A级暂时不分子级。

