# 华为等级保护解决方案

（等保二、三级）

# 目录

# 网络安全形势严峻

监测数据显示，互联网安全形势十分严峻，敲诈勒索病毒盛行，分布式拒绝服务攻击峰值持续新高、工业控制系统安全风险加剧！

## 大量主机被木马远程控制

1101万余台主机被境外控制服务器控制，来自美国的控制服务器数量居首位，其次是俄罗斯和日本。移动互联网恶意程序达到253万个，同比增长23.4%。

## 安全漏洞数量持续走高

国家信息安全漏洞共享平台（CNVD）所收录的安全漏洞数量达到15955个，同比增长47.4%。

## 互联网金融安全

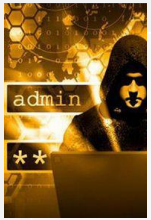
205万余个移动互联网恶意程序，较上一年增长39.0%，近7年来持续保持高速增长趋势


## 拒绝服务攻击变成常用手段

2017年我国遭受DDoS攻击依然严重，攻击峰值流量持续攀升。大流量攻击事件的主要攻击方式为TCP SYN Flood、NTP反射放大攻击和SSDP反射放大攻击。

## 工业互联网安全

国家信息安全漏洞共享平台（CNVD）共收录通用软硬件漏洞10822个，高危漏洞收录数量高达4146个，占38.3%，”零日”漏洞3203个，较2015年增长82.5%




## 网站安全形势十分严峻

2017年，CNCERT监测发现我国境内约2万个网站被篡改，较2016年的约1.7万个增长20.0%，其中被篡改的政府网站有618个，较2016年的467个增长32.3%

# 国家出台法律强化网络安全，合规需求上升为法律强制

国家实行网络安全等级保护制度，安全保护义务包括：

| | |
|---|---|
| 1 | 制定内部安全管理制度和操作规程，确定网络安全责任人，落实网络安全保护责任 |
| 2 | 采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施 |
| 3 | 采取检测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月 |
| 4 | 采取数据分类、重要数据备份和加密等措施 |
| 5 | 法律、行政法规规定的其他义务 |

**对不履行第二十一条规定的，将对运营者及直接负责的主管人员处以责令整改、警告、罚款等行政处罚，情节严重的还将追究刑事责任**

# 目录

# 等级保护定义

网络安全等级保护：对信息和信息载体**按照重要性等级分级别进行保护**的一种工作。

## 政策要求

主要内容：

- 实行网络安全等级保护政策
- 重视网络安全风险评估工作
- 建设和完善网络安全监控体系
- 保证网络安全资产
- 健全网络安全管理责任制

## 由公安监督检查

- 公安机关负责信息安全等级保护工作的监督、检查、指导
- 国家保密工作部门负责等级保护工作中有关保密工作的监督、检查、指导
- 国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导

## 各机关和行业执行

**（一）**电信、广电行业的公用通信网、广播电视传输网等基础信息网络、经营性公众互联网信息服务单位、互联网接入服务单位、数据中心等单位的重要信息系统

**（二）**铁路、银行、海关、税务、银行、电力、证券、保险、外交、科技、发展改革、国防科技、公安、人事劳动和社会保障、财政、审计、商务、水利、国土资源能源、交通、文化、教育、统计、工商行政管理、邮政行业部门的生产、调度、管理、办公等重要信息系统

# 等级保护价值

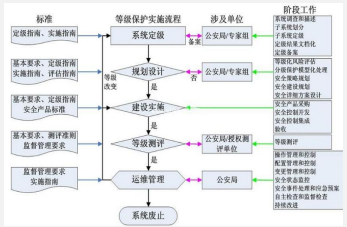
## 满足监管要求


满足政策、法律与行业要求，安全状况获得公安机关认可

## 明确安全责任


谁主管，谁负责
谁使用，谁负责
谁运营，谁负责

## 体系化建设




整体规划，分区域,分层,分类,分级别,分阶段进行建设，安全建设更加体系化

## 集约化运营

利于企业集约化运营，相同等级的信息资产共享相同的保护措施

## 优化安全收益


根据信息资产价值实施保护，平衡安全投入与产出