

## 等保2.0标准及变化



- 中国首批DevOps Master讲师
- CISP注册认证讲师 (CISI)
- 中国首批ITIL Expert讲师
- C-CSA专家团成员
- 国际最佳实践联盟专家团成员
- 参与出版《SAFe精粹》
- 参与出版《IT管理那些事儿》
- 参与编写CSA《大数据安全标准》
- 参与编写《ITSS-云服务管理标准》



信息安全课程

## 培训照片及网站博客



### • 豆瓣、简书-搜-北京老李

安全运营一体化：安全软件开发是网络安全法及等保2.0落地的基石

北京老李 (北京)  
中国信息安全管理师, CISP, PMP, Prince2专家, EXIN信息安全, ISO20000 I.A, ISO27001 I.A 等多领域认证。先后在天津、上海、广州等地主导软件开发、系统集成、运维服务等工作。主要研究方向云安全管理、DevOps落地实践。

2017-11-26 15:15:59

作者：北京老李，DevOps布道师，IT管理咨询师，拥有EXIN Agile, EXIN Lean IT, 提出EXIN DevOps Master模型，国际ITIL Expert级别，PMP, Prince2专家级，EXIN信息安全，ISO20000 I.A, ISO27001 I.A 等多领域认证。先后在天津、上海、广州等地主导软件开发、系统集成、运维服务等工作。主要研究方向云安全管理、DevOps落地实践。

1安全软件开发需求

敏捷从中文理解来看，原意一般是描述动作或行为的反应迅速快捷。在应用软件开发时，是指相对于传统瀑布模型提出过时的需求开发管理方法，网络点在于应对VUCA环境瞬息万变，并客户需求不断地进行变化地软件交付的方法。

敏捷形态下的网络安全法与等保2.0





北京老李 编辑

信息安全课程

## 议程



### 网安法概述及执法案例



### 等保2.0标准及变化



### 国内IT如何落实网安法



### 讨论与交流

北京老李 编辑

□ 《网络安全法》从草案发布到正式出台，共经历了三次审议，两次公开征求意见和修改。

#### 《网络安全法》出台背景

##### 落实国家总体安全观的重要举措

十八大以来，习总书记对加强国家网络安全工作做出了重要部署，对加强网络安全法制建设提出了明确要求

##### 维护网络安全的客观需要

我国迫切需要建立和完善网络安全的法律制度，提高全社会的网络安全意识和网络安全保护水平

##### 维护人民群众切身利益的迫切需要

网络侵权行为严重损害了公民、法人和其他组织的合法权益，广大人民群众迫切地呼吁加强网络空间法制建设、净化网络环境



北京志学·编辑

5

- 2013年下半年提上日程
- 2014年形成草案
- 2015年初形成征求意见稿，15年6月一审
- 2016年6月二审、10月31日三审、11月7日人大通过
- 2017年6月1日起施行
- 154票赞成、0票反对、1票弃权

- 1、不得出售个人信息。
- 2、严厉打击网络诈骗。
- 3、以法律形式明确“网络实名制”
- 4、重点保护关键信息基础设施
- 5、惩治攻击破坏我国关键信息基础设施的境外组织和个人。
- 6、重大突发事件可采取“网络通信管制”。

北京志学·编辑

- 网络、网络安全
- 网络空间安全
- 关键基础设施
- 网络运营者
- 个人信息
- 网络数据
- .....

网络空间 已成为领土、领海、领空、太空之外的“第五空间”或人类“第二类生存空间”  
成为国家主权延伸的新疆域



北京志学 编辑

7

### China Cyber Security Law

Cyber security站在国家、企业、提供者角度去思考，像是十字军东片保卫国王的骑士，同时他们也要兼顾这个城堡如何连接到外部的通道。

主要工作内容：

- 网络保护-监测并保护外部试图非法进入我们内部网络的不良分子
- 更新信息-跟踪黑客最新的攻击手段以及攻击方法
- 情报-识别外部攻击源并拒绝他们
- 应用程序-监控应用程序的指控并避免来自内部的意外违规
- 安全管理体系建设与实施

### Network Security

Network Security站在网络管理角度去思考，主要用于管理公司内的网络行为，监控公司内部的重要信息，员工的上网行为等等。

主要工作内容：

- 用户ID和密码--保证他们定期更换以及定时更新
- 防火墙-设置安全策略并监控流量
- internet访问-监控公司内员工访问网站
- 加密-加密重要员工的电脑以及公司重要文件，防止人为传播
- 备份-制定并遵循公司备份策略
- 扫描-定期扫描服务器弱点并监控客户端病毒
- 服务器连接监控-定期监控服务器日志以及不正常连接网络安全培训-定期给员工做安全培训

北京志学 编辑

8





信息安全课程

国家安全与网络空间安全

ITIL 先锋论坛

年代	利益诉求	威胁来源	应对手段
1987	国家生存 经济成长 价值拓展 世界和平 联盟关系	苏联	外交 防务
2000	生存, 包括基础设施安全 地区安全与稳定 推广价值	不确定 跨国威胁	军事 经济 外交
2006	安全 发展 民主	恐怖主义	军事 经济 全球合作
2010	安全 繁荣 价值	国家竞争者 跨国恐怖主义	反恐合作 反扩散合作 新的全面接触
2015	安全 繁荣 价值	多样化的威胁	能力建设

北京志学 编辑

信息安全课程

《国家网络空间安全战略》中的挑战

ITIL 先锋论坛

- 网络渗透危害政治安全。政治稳定是国家发展、人民幸福的基本前提。利用网络干涉他国内政、攻击他国政治制度、煽动社会动乱、颠覆他国政权, 以及大规模网络监控、网络窃密等活动严重危害国家政治安全和用户信息安全。
- 网络攻击威胁经济安全。网络和信息系統已经成为关键基础设施乃至整个经济社会的神经中枢, 遭受攻击破坏、发生重大安全事件, 将导致能源、交通、通信、金融等基础设施瘫痪, 造成灾难性后果, 严重危害国家经济安全和公共利益。
- 网络有害信息侵蚀文化安全。网络上各种思想文化相互激荡、交锋, 优秀传统文化和主流价值观面临冲击。网络谣言、颓废文化和淫秽、暴力、迷信等违背社会主义核心价值观的有害信息侵蚀青少年身心健康, 败坏社会风气, 误导价值取向, 危害文化安全。网上道德失范、诚信缺失现象频发, 网络文明程度亟待提高。
- 网络恐怖和违法犯罪破坏社会安全。恐怖主义、分裂主义、极端主义等势力利用网络煽动、策划、组织和实施暴力恐怖活动, 直接威胁人民生命财产安全、社会秩序。计算机病毒、木马等在网络空间传播蔓延, 网络诈骗、黑客攻击、侵犯知识产权、滥用个人信息等不法行为大量存在, 一些组织肆意窃取用户信息、交易数据、位置信息以及企业商业秘密, 严重损害国家、企业和个人利益, 影响社会和谐稳定。
- 网络空间的国际竞争方兴未艾。国际上争夺和控制网络空间战略资源、抢占规则制定权和战略制高点, 谋求战略主动权的竞争日趋激烈。个别国家强化网络威慑战略, 加剧网络空间军备竞赛, 世界和平受到新的挑战。
- 网络空间机遇和挑战并存。必须坚持积极利用、科学发展、依法管理、确保安全, 坚决维护网络安全, 最大限度利用网络空间发展潜力, 更好惠及13亿多中国人民, 造福全人类, 坚定维护世界和平。

北京志学 编辑

10

### • 完善网络治理体系

- 坚持依法、公开、透明管网治网，切实做到有法可依、有法必依、执法必严、违法必究。健全网络安全法律法规体系，制定出台网络安全法、未成年人网络保护条例等法律法规，明确社会各方面的责任和义务，明确网络安全管理要求。加快对现行法律的修订和解释，使之适用于网络空间。完善网络安全相关制度，建立网络信任体系，提高网络安全管理的科学化规范化水平。

### • 护关键信息基础设施

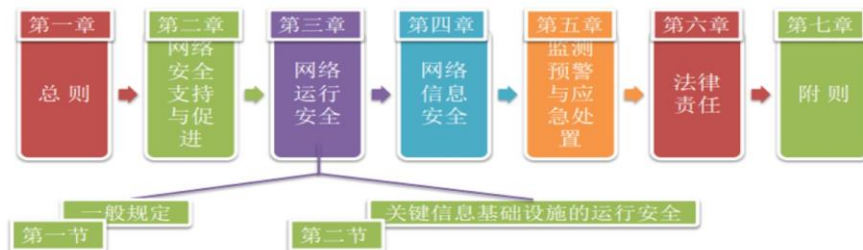
- 国家关键信息基础设施是指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等。采取一切必要措施保护关键信息基础设施及其重要数据不受攻击破坏。坚持技术和管理并重、保护和震慑并举，着眼识别、防护、检测、预警、响应、处置等环节，建立实施关键信息基础设施保护制度，从管理、技术、人才、资金等方面加大投入，依法综合施策，切实加强关键信息基础设施安全防护。

**• 夯实网络安全基础**

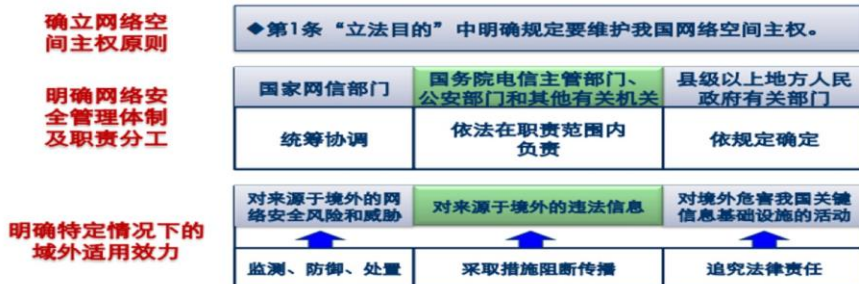
- 建立完善国家网络安全技术支撑体系。加强网络安全基础理论和重大问题研究。加强网络安全标准化和认证认可工作，更多地利用标准规范网络空间行为。做好等级保护、风险评估、漏洞发现等基础性工作，完善网络安全监测预警和网络安全重大事件应急处置机制。
- 实施网络安全人才工程，加强网络安全学科专业建设，打造一流网络安全学院和创新园区，形成有利于人才培养和创新创业的生态环境。办好网络安全宣传周活动，大力开展全民网络安全宣传教育。推动网络安全教育进教材、进学校、进课堂，提高网络媒介素养，增强全社会网络安全意识和防护技能，提高广大网民对网络违法有害信息、网络欺诈等违法犯罪活动的辨识和抵御能力。

**• 提升网络空间防护能力**

- 网络空间是国家主权的新疆域。建设与我国国际地位相称、与网络强国相适应的网络空间防护力量，大力发展网络安全防御手段，及时发现和抵御网络入侵，铸造维护国家网络安全的坚强后盾。



- 明确网络空间主权原则
- 作为我国网络安全治理的基本法，《网络安全法》在总则部分确立了网络主权原则，明确了网络安全管理体制和分工，及域外的适用效力。



北京志学 编辑

13



北京志学 编辑

16



- 建立和完善网络安全标准体系建设
- 统筹规划，扶持网络安全产业（产品、服务等）
- 推动社会化网络安全服务体系建设
- 鼓励开发数据安全保护和利用技术、创新网络安全管理方式
- 开展经常性网络安全宣传教育
- 支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流

- 第二十一条 国家实行**网络安全等级保护制度**。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：
  - （一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；
  - （二）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；
  - （三）采取监测、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；
  - （四）采取数据分类、重要数据备份和加密等措施；
  - （五）法律、行政法规规定的其他义务。

**解读：**网络安全等级保护制度即等保2.0的更新，是网安法的下位文件《网络安全等级保护制度》

## • 明确网络运营者的安全义务

- **内部安全管理**：制定内部安全管理制度和操作规程，确定网络安全负责人
- **安全技术措施**：采取防范网络安全行为的技术措施；采取监测、记录网络运行状态、网络安全事件的技术措施，留存相关的网络日志不少于六个月
- **数据安全**：采取数据分类、重要数据备份和加密等措施，防止网络数据泄露或者被窃取、篡改
- **网络身份管理**：办理网络接入、域名注册服务，或固定电话、移动电话等入网手续，或为用户提供信息发布、即时通讯等服务，应要求用户提供真实身份信息。
- **应急预案机制**：制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并向有关主管部门报告。
- **安全协助义务**：为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助

## • 明确网络产品、服务提供者的安全义务

- **强制标准义务**：网络产品、服务应当符合相关国家标准的强制性要求，不得设置恶意程序；网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供
- **告知补救义务**：网络产品、服务提供者发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，及时告知用户，向有关主管部门报告。
- **安全维护义务**：网络产品、服务提供者应为产品、服务持续提供安全维护，在规定或者当事人约定的期限内不得终止；
- **个人信息保护**：网络产品、服务具有收集用户信息功能的，网络产品、服务提供者应向用户明示并取得同意；涉及用户个人信息的，还应遵守相关法律、行政法规中有关个人信息保护的规定。

## • 明确一般性安全保护义务

- **安全信息发布**：开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。
- **禁止危害行为**：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。
- **信息使用规则**：网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

## • 关键信息基础设施保护

## 1、关键信息基础设施内涵

- 公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务重要行业和领域的关键信息基础设施
- 其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施

## 2、关键信息基础设施外延

- 关键信息基础设施的具体范围由**国务院**制定
- 鼓励关键信息基础设施以外的网络运营者**自愿**参与关键信息基础设施保护体系

## 3、关键信息基础设施管理机制

- 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门具体负责实施**本行业、本领域**的关键信息基础设施保护工作
- **国家网信部门**统筹协调有关部门对关键信息基础设施采取安全保护措施

## 4、关键信息基础设施建设要求

- 确保具有支持**业务稳定、持续运行**的性能
- 安全技术措施同步规划、同步建设、同步使用



## • 关键信息基础设施保护

## 5、关键信息基础设施运营者安全保护义务

- **人员安全管理**：设置专门安全管理机构和安全管理负责人；对负责人和关键岗位的人员进行安全背景审查；定期对从业人员进行网络安全教育、培训和考核。
- **数据境内留存**：在我国境内运营中收集和产生的个人信息和重要数据应当在境内存储。确需向境外提供的，需经国家安全评估；对重要系统和数据库进行容灾备份。
- **应急预案机制**：制定网络安全事件应急预案，并定期进行演练。
- **安全采购措施**：采购网络产品和服务可能影响国家安全的，应当通过国家安全审查。应与网络产品和服务提供者签订安全保密协议。
- **风险评估机制**：自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关部门。

北京志学·编辑

23

- 关键基础设施运营中产生的数据必须**境内存储**。2017年04月10日国家互联网信息办公室发布关于《**个人信息和重要数据出境安全评估办法（征求意见稿）**》公开征求意见的通知。明确了
  - 个人信息和重要数据出境的范围
    - 有50万人以上的个人信息
    - 数据量超过1000GB
    - 7大重要领域数据等
  - 数据出境评估原则
  - 评估7个方面主要内容

**解读：**下列数据在其它法律里有本地化要求：国家秘密和国家安全数据、征信数据、个人金融信息、地图数据、网络出版服务所需的必要的技术设备、网约车相关数据和信息。

北京志学·编辑

24



- 明确我国实行网络安全审查制度

## 第三十五条

关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

- 2017年05月02日中央网信办正式发布《网络产品和服务安全审查办法（试行）》。其中就审查的目的、需要审查的网络产品和服务的范围、网络安全审查的管理部门（网络安全审查委员会）、审查的机构（国家统一认定网络安全审查第三方机构）和对党政机关和重点行业的审查工作提出要求。并于2017年6月1日同《网络安全法》一同实施。

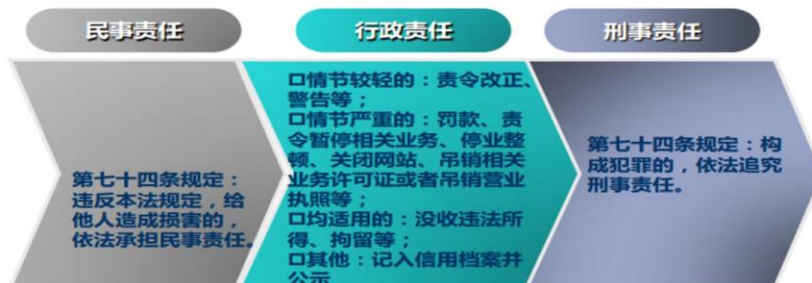
- 规范信息管理



- 确定信息管理中相关职责



- 对违反《网络安全法》的行为，第六章规定了民事责任、行政责任、刑事责任



## 信息安全课程

## 安徽网警依法查处一起违反案例



- 8月12日，蚌埠怀远县教师进修学校网站因网络安全防等级保护制度落实不到位，遭黑客攻击入侵。蚌埠市公安局网安支队调查案件时发现，该网站自上线运行以来，始终未进行网络安全等级保护的定级备案、等级测评等工作，未落实网络安全等级保护制度，未履行网络安全保护义务。根据《网络安全法》第五十六条之规定，省公安厅网络安全保卫总队约谈怀远县教师进修学校法定代表人、怀远县人民政府分管副县长。蚌埠市局网安支队依法对网络运营单位怀远县教师进修学校处以一万五千元罚款，对负有直接责任的副校长处以五千元罚款。
  - 执法机构：安徽省公安厅网络安全保卫总队；蚌埠市局网安支队
  - 处罚行为：网站因网络安全防等级保护制度落实不到位，遭黑客攻击入侵。
  - 处罚措施：约谈怀远县教师进修学校法定代表人、怀远县人民政府分管副县长；对网络运营单位怀远县教师进修学校处以一万五千元罚款，对负有直接责任的副校长处以五千元罚款。
  - 法律依据：《网络安全法》第21条、56条、第59条第1款。

北京志学·编制

## 信息安全课程

## 网络安全法执法



- 12月12日，长沙市公安局网技支队接到公安部、省公安厅网络与信息安全情况通报，浏阳市烟花爆竹总会网站系统被留有后门，**存在严重的安全隐患漏洞**。接通报后，网技支队立即组织力量赶赴浏阳市，会同浏阳市公安局网安大队将情况通报至相关责任单位。



北京志学·编制

- 经公安机关对存在安全隐患的网站系统进行核查，证实该网站被留有后门，可获取网站后台权限，控制网站服务器。该网站自上线运行以来，**一直未进行网络安全等级保护的定级备案、等级测评等工作**，未落实网络安全等级保护制度，未履行网络安全保护义务。



北京志学·编辑

- 1. **普遍性**：《网安法》是中国针对网络空间安全制定的全国性的法律，与《刑法》一样
- 2. **抽检性**：网信部门将和工商税务、消防部门一样，拥有随时抽查企业的权利。
- 3. **真实性**：几乎所有网站都需要你提供身份信息，法律要求《网络运营者为办理网络接入、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
- 4. **管理性**：所有企业都需要一个安全头衔：法律要求《国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：
  - (一) 制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；
  - (二) 采取监测、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...
- 5. **审核性**：所有企业都需要更多的审核人员，法律要求《网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。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。电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告...

北京志学·编辑



- 十六、在刑法第二百四十六条中增加一款作为第三款：“通过信息网络实施第一款规定的行为，被害人向人民法院告诉，但提供证据确有困难的，人民法院可以要求公安机关提供协助。”
- 二十八、在刑法第二百八十六条后增加一条，作为第二百八十六条之一：  
**“网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：**
  - “（一）致使违法信息大量传播的；
  - “（二）致使用户信息泄露，造成严重后果的；
  - “（三）致使刑事案件证据灭失，情节严重的；
  - “（四）有其他严重情节的。
- **“单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照前款的规定处罚。”**
- “有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。”

- 二十九、在刑法第二百八十七条后增加二条，作为第二百八十七条之一、第二百八十七条之二：
- “第二百八十七条之一 利用信息网络实施下列行为之一，情节严重的，**处三年以下有期徒刑或者拘役，并处或者单处罚金：**
  - “（一）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、通讯群组的；
  - （二）发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪信息的；
  - （三）为实施诈骗等违法犯罪活动发布信息的。
- **“单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。”**
- **“有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。”**

- “第二百八十七条之二 明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的，**处三年以下有期徒刑或者拘役，并处或者单处罚金。**”
- “**单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。**”
- “有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。”
- 三十、将刑法第二百八十八条第一款修改为：“违反国家规定，擅自设置、使用无线电台（站），或者擅自使用无线电频率，干扰无线电通讯秩序，情节严重的，**处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。**”
- 三十二、在刑法第二百九十一条之一中增加一款作为第二款：“**编造虚假的险情、疫情、灾情、警情，在信息网络或者其他媒体上传播，或者明知是上述虚假信息，故意在信息网络或者其他媒体上传播，严重扰乱社会秩序的，处三年以下有期徒刑、拘役或者管制；造成严重后果的，处三年以上七年以下有期徒刑。**”

### ➤ 网络运营者法律合规要求

- 需要网络运营者建立企业的管理制度和操作规程，以满足法律合规性的要求，避免法律风险，主要包括如下：
- 1) 与**实施网络安全等级保护制度**相关的义务和制度建设，包括制定内部安全管理制度和操作规程，确定网络安全负责人等（第二十一条）；
- 2) **健全用户信息保护制度**（第二十二条和第四十条）；
- 3) **落实网络实名制**（第二十四条）；
- 4) **网络安全事件应急预案**（第二十五条）；
- 5) **关键信息基础设施的安全保护义务**，包括：设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；定期对从业人员进行网络安全教育、技术培训和技能考核；对重要系统和数据库进行容灾备份；制定网络安全事件应急预案，并定期进行演练；法律、行政法规规定的其他义务（第三十四条）；

## • 网络运营者法律合规要求

- 6) 采购**关键信息基础设施产品和服务**的保密制度（第三十六条）；
- 7) **关键信息基础设施安全性**的年度评估（第三十六条）；
- 8) **个人信息的收集和利用**规则及制度（第四十一条和第四十二条）；
- 9) **个人信息泄露事件**的报告制度（第四十二条）；
- 10) **违法使用**个人信息删除和**错误个人信息更正**制度（第四十三条）；
- 11) 网络运营者对用户**非法信息传播**的监管（第四十七条）；
- 12) 网络信息安全**投诉、举报**制度（第四十九条）。

## ➤ 产品研发

- ◆ 符合相关国家标准的强制性要求。不得设置恶意程序；发现存在安全缺陷、漏洞等风险时，应当立即采取补救措施，及时告知用户并向有关主管部门报告。
- ◆ 持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。
- ◆ 网络关键设备和网络安全专用产品安全认证合格或者安全检测符合要求后，方可销售

## ➤ 个人

- ◆ 规范上网行为：
  - ◆ 诈骗、传授诈骗方法、制售违禁物品
  - ◆ 不得危害网络安全（入侵、窃取等）、国家安全；
  - ◆ 不得发布不良信息
  - ◆ 不得侵犯他人权益
- ◆ 不为上述违法行为提供便利





- 一. 网信事业发展，让互联网更好造福人民
- 二. 网络良好生态，发挥网络引导舆论、反应民意的作用
- 三. 尽快在核心技术上取得突破
- 四. 正确处理安全与发展的关系
- 五. 互联网企业使命感、责任感，共同促进互联网持续健康发展
- 六. 聚天下英才而用之，为网信事业发展提供有力人才支撑

### 树立正确的网络安全观

- 是整体的，而不是割裂的
- 是动态的，而不是静态的
- 是开放的，而不是封闭的
- 是相对的，而不是绝对的
- 是共同的，而不是鼓励的

北京志学·编制



网安法概述及执法案例



等保2.0标准及变化



国内IT如何落实网安法



讨论与交流

北京志学·编制

40



为贯彻落实中央关于完善等级保护制度的有关要求，配合《网络安全法》的出台和实施，满足新应用环境下的等级保护工作的需求，自2014年4月起，公安部网络安全保卫局组织各标准起草单位对云计算、大数据、物联网、移动互联、工业控制系统等新技术、新应用安全问题进行了深入、广泛的调研，对《基本要求》、《设计技术要求》、《测评要求》原有标准修订为安全通用要求，并在此基础上增加了云计算平台、大数据、物联网、移动互联、工业控制系统环境下的安全扩展要求，形成等级保护系列国家标准。

北京志学·编制

- 《网络安全法》第二十一条明确要求：**国家实行网络安全等级保护制度。**
- 中央关于加强社会治安防控体系建设的意见、公安改革若干重大问题的框架意见要求 **“健全完善信息安全等级保护制度”**。
- 习近平总书记等中央领导批示要求：**健全完善以保护国家关键信息基础设施安全为重点的网络安全等级保护制度。**

北京志学·编制

信息安全课程

## 国家等级保护制度进入2.0时代

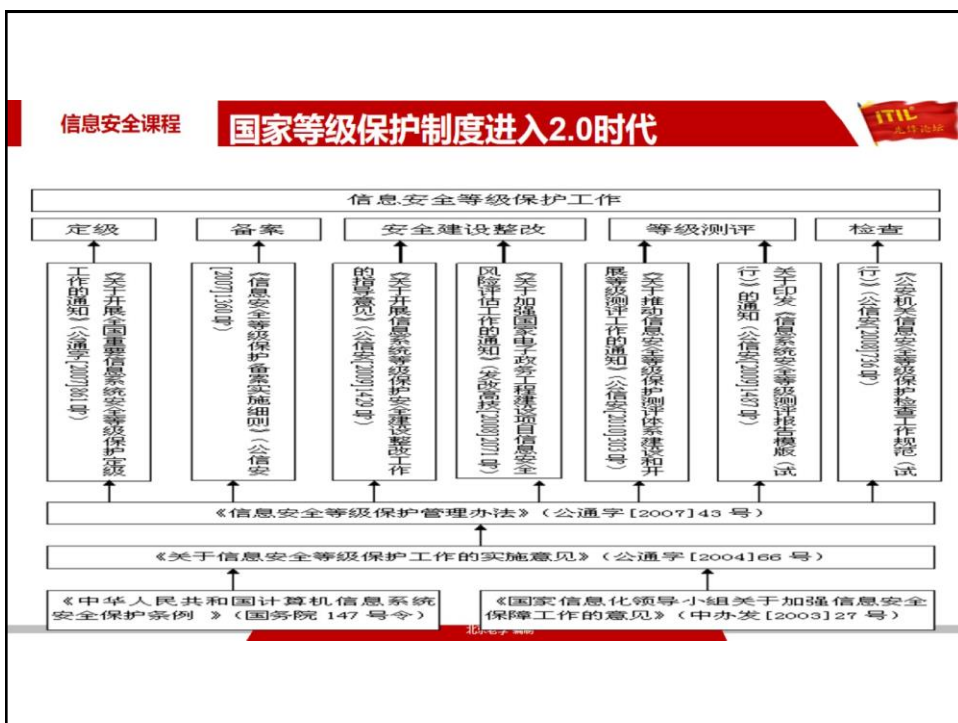
等级保护制度  
推行10年取得  
成效的同时符  
合程度达到稳  
态，需要提升  
台阶。

新技术新应用  
的发展催生了  
应用的新模式  
，需要等级保  
护制度覆盖这  
些新技术。

网络安全法  
第31条要求  
网络安全等  
级保护制度  
能够覆盖关  
键信息基础  
设施保护。

- 构建新的法律、政策体系
- 构建新的标准体系
- 构建新的技术支撑体系
- 构建新的人才队伍体系
- 构建新的教育培训体系
- 构建新的保障体系

北京志学 编辑



## 信息安全课程

## 国家等级保护制度进入2.0时代



序号	文 号	发文单位	名称
1	国务院令【1994】147号	国务院	中华人民共和国计算机信息系统安全保护条例 规定“计算机信息系统实行安全等级保护”
2	中办发[2003]27号	中央办公厅	国家信息化领导小组关于加强信息安全保障工作的意见
3	公通字[2004]66号	公安部4部委	关于信息安全等级保护工作的实施意见
4	中办[2006]18号	中央办公厅	转发《国家信息化领导小组关于推进国家电子政务网络建设的意见》的通知
5	公通字[2007]43号	公安部4部委	信息安全等级保护管理办法
6	公信安[2007]1360号	公安部	《信息安全等级保护备案实施细则》
7	公信安[2007]861号	公安部4部委	关于开展全国重要信息系统安全等级保护定级工作的通知
8	公信安[2008]736号	公安部	《公安机关信息安全等级保护检查工作规范（试行）》
9	发改高技[2008]2071号	发改委	《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》
10	公信安[2009]1429号	公安部	关于印送《关于开展信息安全等级保护安全建设整改工作的指导意见》的函

北京志学·编辑

## 信息安全课程

## 管理办法（43号文）规定的等级保护工作

**一是：定级。****二是：备案。****三是：系统建设、整改。****四是：开展等级测评。****五是：信息安全监管部门定期开展监督检查**

- ☐ 等级保护条例（修订）（总要求/上位文件）
- ☐ 等保2.0系列（GB/T 22239.x）
- ☐ 划分准则（GB 17859-1999）（上位标准）
- ☐ 实施指南（GB/T25058）（修订）
- ☐ 定级指南（GB/T22240）（修订）
- ☐ 基本要求（GB/T22239）（修订）
- ☐ 设计要求（GB/T25070）（修订）
- ☐ 测评要求（GB/T28448）（修订）
- ☐ 测评过程指南（GB/T28449）（修订）

北京志学·编辑

- 原来
- 《信息系统安全等级保护基本要求》
- 改为
- 《信息安全等级保护基本要求》
- 再改为
- 《网络安全等级保护基本要求》

北京志学·编辑

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

北京志学·编辑



## 新标准的变化-2、构成的变化

- 原来：一个标准GB/T 22239-2008
- 改为：系列标准
  - ——GB/T 22239.1-XXXX 信息安全技术 网络安全等级保护基本要求 第1部分：安全通用要求
  - ——GB/T 22239.2-XXXX 信息安全技术 网络安全等级保护基本要求 第2部分：云计算安全扩展要求
  - ——GB/T 22239.3-XXXX 信息安全技术 网络安全等级保护基本要求 第3部分：移动互联安全扩展要求
  - ——GB/T 22239.4-XXXX 信息安全技术 网络安全等级保护基本要求 第4部分：物联网安全扩展要求
  - ——GB/T 22239.5-XXXX 信息安全技术 网络安全等级保护基本要求 第5部分：工业控制系统安全扩展要求
  - ——GB/T 22239.6-XXXX 信息安全技术 网络安全等级保护基本要求 第6部分：大数据安全扩展要求

北京志学·编辑

## 新标准的变化-3、体系变化

- 原来：信息系统
- 改为：等级保护对象
- 安全等级保护的對象包括网络基础设施、信息系统、大数据、云计算平台、物联网、工控系统等。
- 重点对象是国家关键信息基础设施，主要包括涉及国家安全、国计民生的网络基础设施、重要信息系统、大数据，以及重要的云计算平台、物联网、工控系统等。



北京志学·编辑

### 新标准的变化-4、调整了控制措施的分类结构

□ 22239标准：其结构和分类调整为：

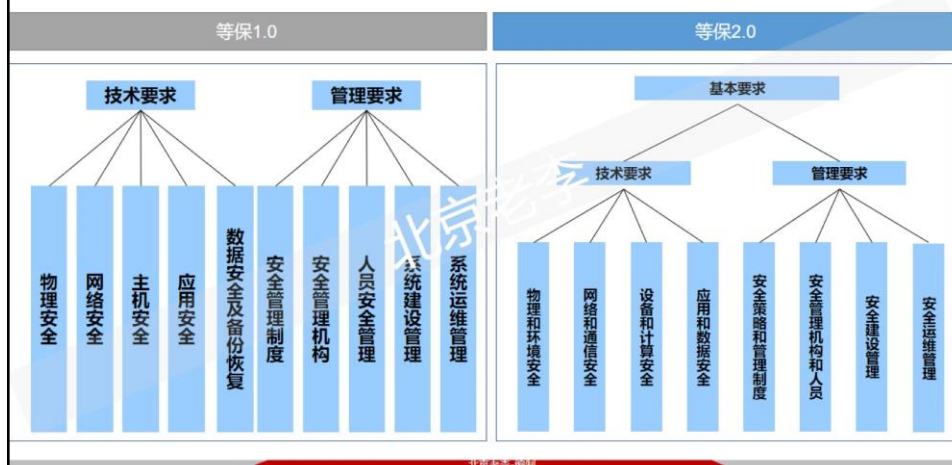
#### □ 技术部分

□ 物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全

#### □ 管理部分

□ 安全策略和管理制度、安全管理机构和人员、安全建设管理、安全运维管理

北京志学 编制



北京志学 编制



信息安全课程 等保1.0到2.0管理内容变化-控制点变化

旧标准	控制类	二级	三级	四级	等保2.0	控制类	二级	三级	四级
技术要求	物理安全	10	10	10	技术要求	物理和环境安全	10	10	10
	网络安全	6	7	7		网络和通信安全	6	8	8
	主机安全	6	7	9		设备和计算安全	6	6	6
	应用安全	7	9	11		应用和数据安全	9	10	10
	数据安全及备份恢复	3	3	3					
管理要求	安全管理制度	3	3	4	管理要求	安全策略和管理制度	4	4	4
	安全管理机构	5	5	5		安全管理机构和人员	9	9	9
	人员安全管理	5	5	5					
	系统建设管理	9	11	11		安全建设管理	10	10	10
	系统运维管理	12	13	13		安全运维管理	14	14	14
合计	/	66	73	77	合计	/	68	71	71
级差	/	/	7	4	级差	/	/	3	/

北京志李-编制



信息安全课程

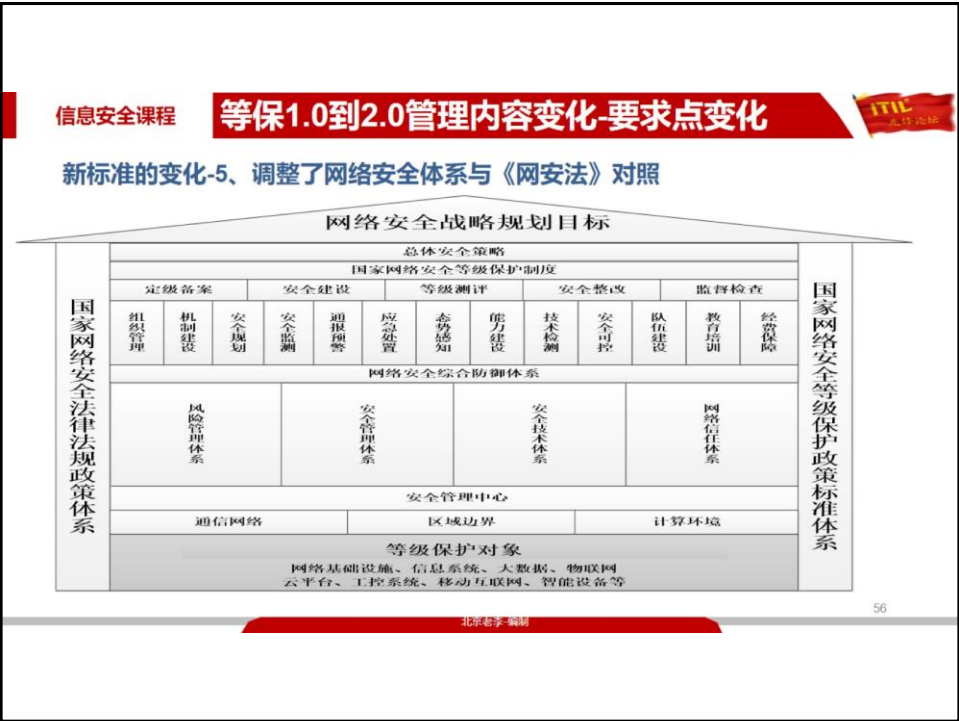
等保1.0到2.0管理内容变化-要求点变化

ITIL 先锋论坛

方面	控制类	二级	三级	四级	方面	控制类	二级	三级	四级
技术要求	物理安全	19	32	33	技术要求	物理和环境安全	15	22	24
	网络安全	18	33	32		网络和通信安全	16	33	35
	主机安全	19	32	36		设备和计算安全	17	26	27
	应用安全	19	31	36		应用和数据安全	22	34	38
	数据安全及备份恢复	4	8	11		安全策略和管理制度	6	7	7
管理要求	安全管理制度	7	11	14	管理要求	安全管理机构和人员	16	26	29
	安全管理机构	9	20	20		安全建设管理	25	34	35
	人员安全管理	11	16	18		安全运维管理	31	49	51
	系统建设管理	28	45	48	合计	/	148	231	246
	系统运维管理	42	62	70	级差	/	/	83	15
合计	/	175	290	318					
级差	/	/	115	28					

北京志学 编制

30





### 新标准的变化-6、取消了安全控制点的标注

- 为适应定级方法的变化，取消对控制点的“S”、“A”、“G”标注的使用，调整原标准附录B，增加安全控制措施选择时，控制点的标注及使用说明。
- 保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改的信息安全类要求（简记为S）；保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致系统不可用的服务保证类要求（简记为A）；其他通用性安全保护类要求（简记为G），所有管理安全要求均为通用性安全保护类要求

- 已备案的第二级（含）以上信息系统纳入安全建设整改的范围。
- 尚未开展定级备案的信息系统，要先定级备案，定级不准的要先纠正，再开展安全建设整改。
- 新建系统要同步开展安全建设工作。
- 管理制度建设和技术措施建设并重。
- 安全建设整改总体规划、实施。加固改造，缺什么补什么。

- 以《信息系统安全等级保护基本要求》为目标，从管理和技术两方面进行安全建设整改。
- 等级保护安全管理建设整改
  - 一是落实信息安全责任制。
  - 二是落实人员安全管理制度。
  - 三是落实系统建设管理制度。
  - 四是落实系统运维管理制度。

- ——GB/T 22239.1-网络安全等级保护基本要求
- 第1部分：安全通用要求；
- ——GB/T 22239.2-网络安全等级保护基本要求
- 第2部分：云计算安全扩展要求；
- ——GB/T 22239.3-网络安全等级保护基本要求
- 第3部分：移动互联安全扩展要求；
- ——GB/T 22239.4-网络安全等级保护基本要求
- 第4部分：物联网安全扩展要求；
- ——GB/T 22239.5-网络安全等级保护基本要求
- 第5部分：工业控制系统安全扩展要求；
- ——GB/T 22239.6-网络安全等级保护基本要求
- 第6部分：大数据安全扩展要求（待立项）。

- 云计算安全扩展要求章节针对**云计算**的特点提出**特殊保护要求**。由第2分册（之前的云计算安全扩展要求分册）合并为基本要求的X.2章节，合并后精炼保留针对云计算特点的特殊保护要求，增加包括“**基础设施的位置**”、“**虚拟化安全保护**”、“**镜像和快照保护**”、“**云服务商选择**”和“**云计算环境管理**”等方面。

- 移动互联安全扩展要求章节针对**移动互联**的特点提出**特殊保护要求**。由第3分册（之前的移动互联网安全扩展要求分册）合并为基本要求的X.3章节，合并后精炼保留针对移动互联网特点的特殊保护要求，增加包括“**无线接入点的物理位置**”、“**移动终端管控**”、“**移动应用管控**”、“**移动应用软件采购**”和“**移动应用软件开发**”等方面。

- 物联网安全扩展要求章节针对**物联网**的特点提出**特殊保护要求**。由第4分册（之前的物联网安全扩展要求分册）合并为基本要求的X.4章节，合并后精炼保留针对**物联网的感知网部分**特殊保护要求，增加包括“**感知节点的物理防护**”、“**感知节点设备安全**”、“**网关节点设备安全**”、“**感知节点的管理**”和“**数据融合处理**”等方面。

- 工业控制系统安全扩展要求章节针对**工业控制系统**的特点提出**特殊保护要求**。对工业控制系统主要增加的内容包括“**室外控制设备防护**”、“**工业控制系统网络架构安全**”、“**拨号使用控制**”、“**无线使用控制**”和“**控制设备安全**”等方面，针对工业控制系统实时性要求高的特点调整了“**漏洞和风险管理**”和“**恶意代码防范管理**”方面的要求。



## 信息安全课程

## 工控安全举例

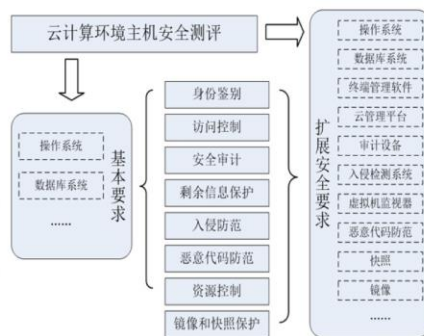


### 不同服务模式下的安全管理责任主体

云服务的服务模式包括基础设施即服务 (IaaS)、平台即服务 (PaaS)、软件即服务 (SaaS)，具体如下：

- a) **基础设施即服务 Infrastructure As A Service(IaaS)**。云服务方向云租户提供可动态申请或释放的计算资源、存储资源、网络资源等基础设施的服务模式；
- b) **平台即服务 Platform As A Service(PaaS)**。云服务方向云租户提供应用软件所需的支撑平台，包括用户应用程序的运行环境和开发环境，供云租户在此基础上开发和提供相关应用的服务模式；
- c) **软件即服务 Software As A Service(SaaS)**。云服务方向云租户提供运行在云基础设施之上的应用软件的服务模式。

不同服务模式下的云服务方和云租户的安全管理责任主体有所不同。



65

北京志学·编

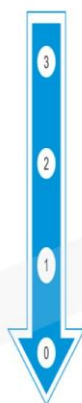
## 信息安全课程

## 工控安全举例



### 工控系统分层结构

- 层级4: 企业资源层
- 层级3: 生产管理
- 层级2: 过程控制层
- 层级1: 现场控制层
- 层级0: 现场设备层






- 一、安全软件选择与管理
- 二、配置和补丁管理
- 三、边界安全防护
- 四、物理和环境安全防护
- 五、身份认证
- 六、远程访问安全
- 七、安全监测和应急预案演练
- 八、资产安全
- 九、数据安全
- 十、供应链管理
- 十一、落实责任

66

北京志学·编

信息安全课程		等保标准要求举例	
分类	安全控制点	等保三级要求内容	应对思路
网络和通信安全	入侵防范	c) 应采取技术措施对网络行为进行分析, 实现对网络攻击特别是未知的新型网络攻击的检测和分析;	部署安全防护设备能够对新型网络攻击进行检测和分析, 对未知威胁检测需具备云端未知威胁分析引擎, 并实现本地防护设备能与云引擎进行联动的功能。具备与云引擎联动分析的下一代防火墙或安全感知平台可满足此要求。
	集中管控	f) 应能对网络中发生的各类安全事件进行识别、报警和分析。	部署能够对网络中发生的各类安全事件进行识别、报警和分析的安全防护设备可以满足此要求, 如安全感知平台。
	边界防护	c) 应能够对内部用户非授权联到外部网络的行为进行限制或检查; d) 应限制无线网络的使用, 确保无线网络通过受控的边界防护设备接入内部网络。	新提出从内到外网络的行为进行限制或检查, 传统防火墙无法满足此类要求, 必须采用具有双向检测能力的下一代防火墙或上网行为管理检测无法无线共享来满足。 必须在无线网络边界增加安全防护设备。
	安全审计	e) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。	新增对远程访问用户及互联网访问用户行为单独进行审计分析, 数据中心的服务器如果可以访问互联网或需要进行远程管理或访问, 需要在互联网出口单独部署上网行为管理或VPN
设备和计算安全	入侵防范	e) 应能够检测到对重要节点进行入侵的行为, 并在发生严重入侵事件时提供报警。	应在重要节点部署检测探针, 能够检测到对重要节点进行入侵的行为, 将日志汇总安全感知平台进行分析, 并在发生严重入侵事件时提供报警。

信息安全课程		议程	
		网安法概述及执法案例	
		等保2.0标准及变化	
		国内IT如何落实网安法	
		讨论与交流	

- 1、建立信息安全管理体系统（基于网络安全等级保护体系）
- 2、做好等级保护2.0相关定级、备案等工作
- 3、做好等级保护工作，落实网络安全等级保护制度；
- 4.做好网络安全防护工作包括，但不限于：
  - 3.2履行个人信息保护制度，不得泄露、篡改、毁损其收集的个人信息，并确保安全。
  - 3.3做好监测预警、应急处置工作，主动向主管部门报告，接受政府和社会的监督，承担社会责任。
  - 3.4建立安全责任制度，明确责任人；
  - 3.5多组织一些安全培训、安全教育、技能考核等
  - 3.6采购网络产品时关注网络产品、服务提供商资质，检查产品是否符合法规；
- 4、重点工作重点防护：重点基础设施企业包括 金融企业、大型互联网企业、电子政务等涉及关键基础设施的企业还需实现采购网络产品和服务通过国家安全审查、签订安全保密协议、重要数据境内存储、业务系统容灾备份、每年做好安全评估等工作

- 1、及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险，保障网络安全、稳定运行、维护网络数据的完整性、保密性、可用性
- 2、通过安全感知、安全探针等来有效监控网络的运行情况，并做好应急预案工作。监控到有网络风险时，马上启动应急预案；
- 3、可以通过防火墙、IPS、IDS、WAF等网络安全防护设备保障网络安全、稳定运行；
- 4、通过加密产品，进行数据加密，重视个人信息的保护；
- 5、建议使用具备可视化能力产品，能够及时向主管部门报告系统漏洞、信息泄露等风险事件；

信息安全课程

议程





网安法概述及执法案例



等保2.0标准及变化



国内IT如何落实网安法



讨论与交流

北京志学 编辑

71