教育信息化安全的“防”与“范”

网御星云售前工程师：庞婕

内容概要

- 一、背景介绍
- 二、教育信息安全现状分析
- 三、教育信息化安全的“防”与“范”
- 四、安全防护方向及新产品解读

教育信息化安全“防”与“范”

背景介绍

互联网技术的高速发展

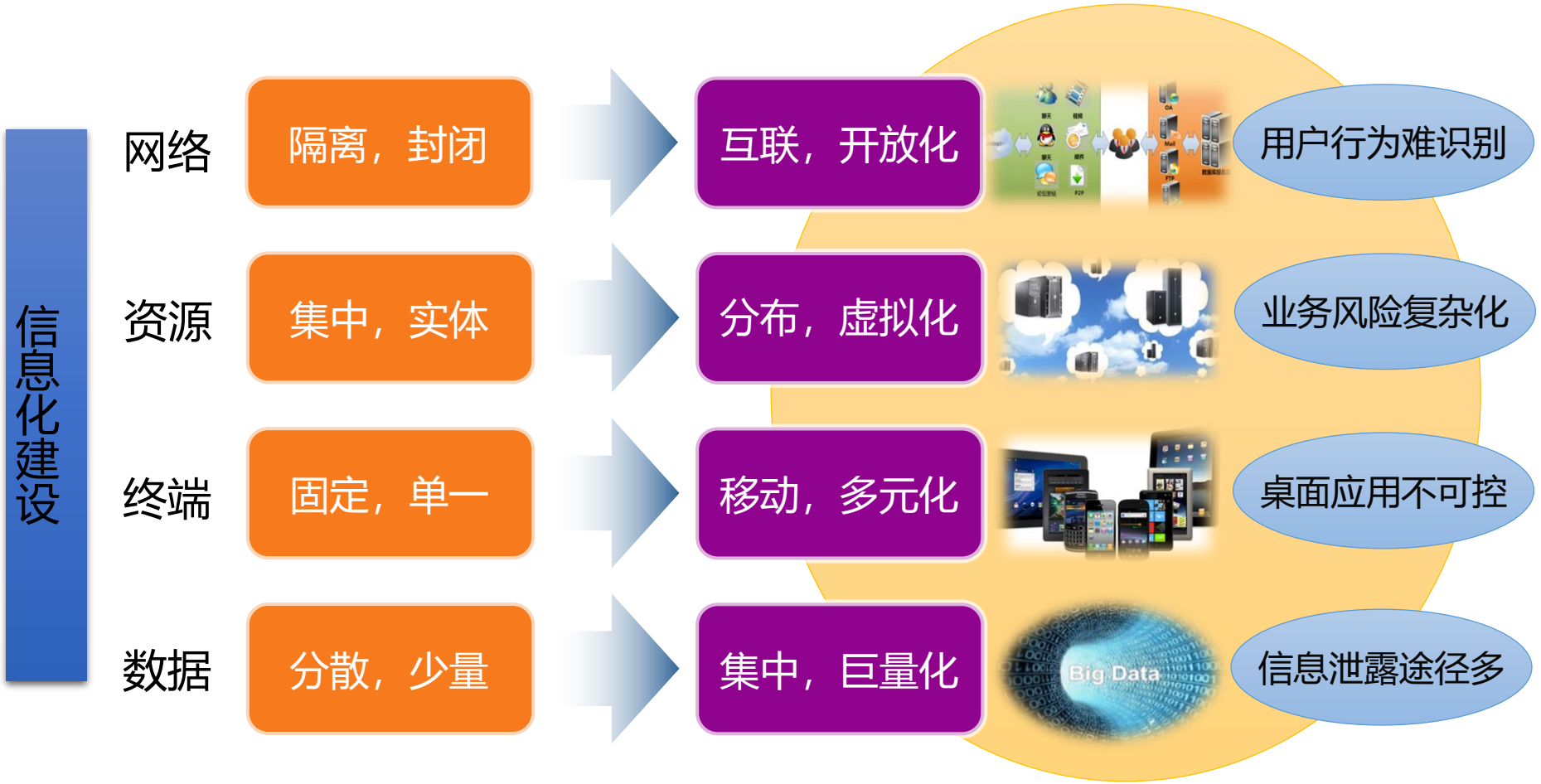
云计算

大数据

社交网络

移动互联网

互联网技术的高速发展


信息化建设
网络
隔离，封闭
互联，开放化
用户行为难识别
资源
集中，实体
分布，虚拟化
业务风险复杂化
终端
固定，单一
移动，多元化
桌面应用不可控
数据
分散，少量
集中，巨量化
Big Data
信息泄露途径多

教育信息化安全“防”与“范”

教育行业信息安全现状分析

黑客攻击不断

篡改网站信息

窃取学生信息

信息系统瘫痪

病毒传播不断

一种名为WannaCry（永恒之蓝）的电脑勒索病毒在全球蔓延，已波及99个国家。“永恒之蓝”通过自动扫描445文件共享端口的Windows机器，无需用户任何操作，就可以将所有磁盘文件加密、锁死，黑客可远程控制向用户勒索“赎金”。

各大高校通常接入的网络是为教育、科研和国际学术交流服务的教育科研网，此骨干网出于学术目的，大多没有对445端口做防范处理，这是导致这次高校成为重灾区的原因之一。

此外，如果用户电脑开启防火墙，也会阻止电脑接收445端口的数据。但中国高校内，一些同学为了打局域网游戏，有时需要关闭防火墙，也是此次事件在中国高校内大肆传播的另一原因。

黑色的经济链

新浪首页 新闻 体育 财经 娱乐 科技 博客 图片 专栏 更多

sina 新闻中心 国内新闻 新闻

北京200万名学生家长信息泄露 含姓名学校住址

2015年02月26日14:32 法制晚报 65

200万学生家长信息泄露 含姓名、学校、住址及联系方式均为本市中小学被告人在58同城、赶集网交易案发后仍有人发帖

2015年1月下旬，6名教育培训行业的从业人员，被海淀检察院以非法获取公民个人信息罪公诉至法院。

据检方调查，这起案件涉及200余万条个人信息，每条信息包含所在学校(北京市的中学或小学)、学生年级、学生及家长的姓名、学生及家长的联系方式，部分信息还含有家庭住址。

这些个人信息被家教、培训行业的人用来做精准的定向营销，向特定人群发送招生或培训信息，并取得明显效果。一名在案的培训机构负责人称，通过这种方式，他每年的招生量能增加25%。

专栏推荐

晏扬

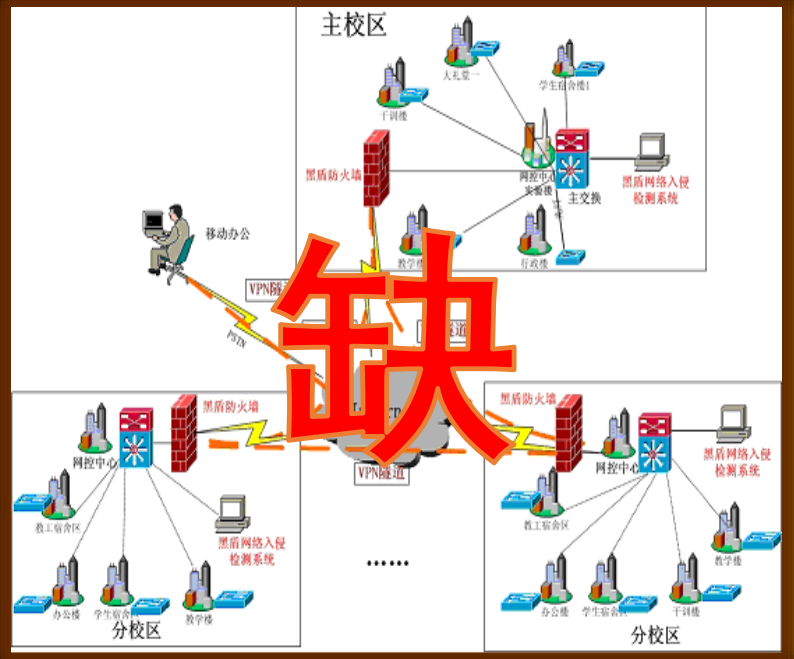
信息来源在教育机构私自拷贝

买卖目的做培训需要精准数据

获利诱人每年增加25%招生量

在58同城、赶集网交易

教育行业信息安全普遍存在的问题

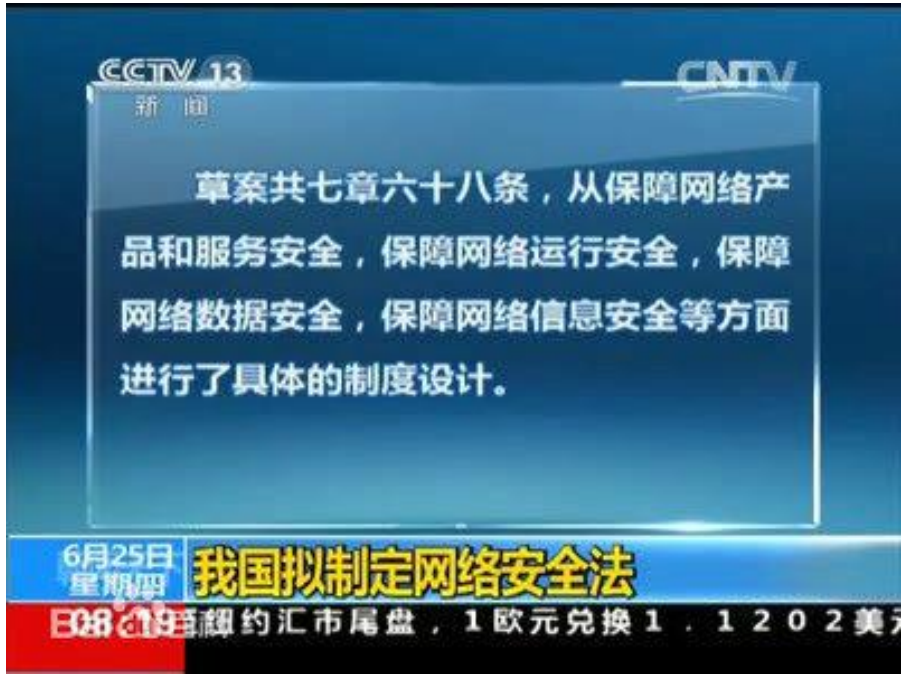


安全技术体系　　安全管理体系　　安全运维体系

教育信息化安全"防"与"范"

教育信息化安全的"防"与"范"

网络安全法正式实行



已于2017年6月1日正式实行

关键信息基础设施安全保护条例征求意见稿


中华人民共和国国家互联网信息办公室
Cyberspace Administration of China
WWW.CAC.GOV.CN
首页 权威发布 办公室工 网络安全 信息化 网络传播 国际交流 地方网信 执法督查 政策法规 互动中心 教育培训 业界动态 工作专题
当前位置：首页 > 正文
国家互联网信息办公室关于《关键信息基础设施安全保护条例（征求意见稿）》公开征求意见的通知
2017年07月11日 09:00:02 来源：中国网信网 【打印】【纠错】
国家互联网信息办公室关于《关键信息基础设施安全保护条例（征求意见稿）》公开征求意见的通知
为保障关键信息基础设施安全，根据《中华人民共和国网络安全法》，我办会同相关部门起草了《关键信息基础设施安全保护条例（征求意见稿）》，现向社会公开征求意见。有关单位和各界人士可以在2017年8月10日前，通过以下方式提出意见：
一、通过信函方式将意见寄至：北京市西城区车公庄大街11号国家互联网信息办公室网络安全协调局，邮编100044，并在信封上注明“征求意见”。
二、通过电子邮件方式发送至：security@cac.gov.cn。
附件：关键信息基础设施安全保护条例（征求意见稿）

国家互联网信息办公室今日上午刚刚发布了关于《关键信息基础设施安全保护条例（征求意见稿）》（以下简称《意见稿》）公开征求意见的通知。

该《意见稿》规定，任何个人和组织发现危害关键信息基础设施安全的行为，有权向网信、电信、公安等部门以及行业主管或监管部门举报。有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

此外，境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门、国家安全机关和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

网络安全法保护对象

- ✓ 1、关键信息基础设施
- ✓ 2、个人信息

关键信息基础设施保护范围

- 政府机关和能源、金融、交通、水利、卫生医疗、**教育**、社保、环境保护、公用事业等行业领域的单位；
- 电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位；
- 国防科工、大型装备、化工、食品药品等行业领域科研生产单位；
- 广播电台、电视台、通讯社等新闻单位；
- 其他重点单位

教育信息系统属于关键信息基础设施。

个人信息

- 个人信息是指以电子或其他方式记录的能够单独或与其他信息结合识别自然人身份的各种信息，包括与确定自然人相关的生物特征、位置、行为等信息，如姓名、出生日期、身份证号、个人账号信息、住址、电话号码、指纹、虹膜等。

教育信息系统中所存放的学生基础信息、学籍信息、教职工基础信息、社保信息等均属于个人信息范畴。

保护方法

- 1) 实施等级保护
- 2) 网络运行安全和关键信息基础设施保护
- 3) 个人信息保护
- 4) 网络安全检测与预警
- 5) 网络安全应急管理
- 6) 网络安全技术人才培养和安全意识宣传
- 7) 职责落实与违规处罚

教育关键信息基础设施运营者所承担的责任、义务

- **一是第二十一条关于网络安全等级保护5方面的要求。**即：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；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；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；采取数据分类、重要数据备份和加密等措施；法律、行政法规规定的其他义务。

- **二是第二十二条关为于网络运营者提供产品、服务时的要求。**即，如果对网络运营者提供产品和服务，则应当符合相关国家标准的强制性要求。具体是：不得设置恶意程序；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，按照规定及时告知用户并向有关主管部门报告。网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

教育关键信息基础设施运营者所承担的责任、义务

- **三是第三十三条关于“三同步”的要求。**即，建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

- **四是第三十四条提出的设置专门安全管理机构、培训等5方面要求。**即，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。

教育关键信息基础设施运营者所承担的责任、义务

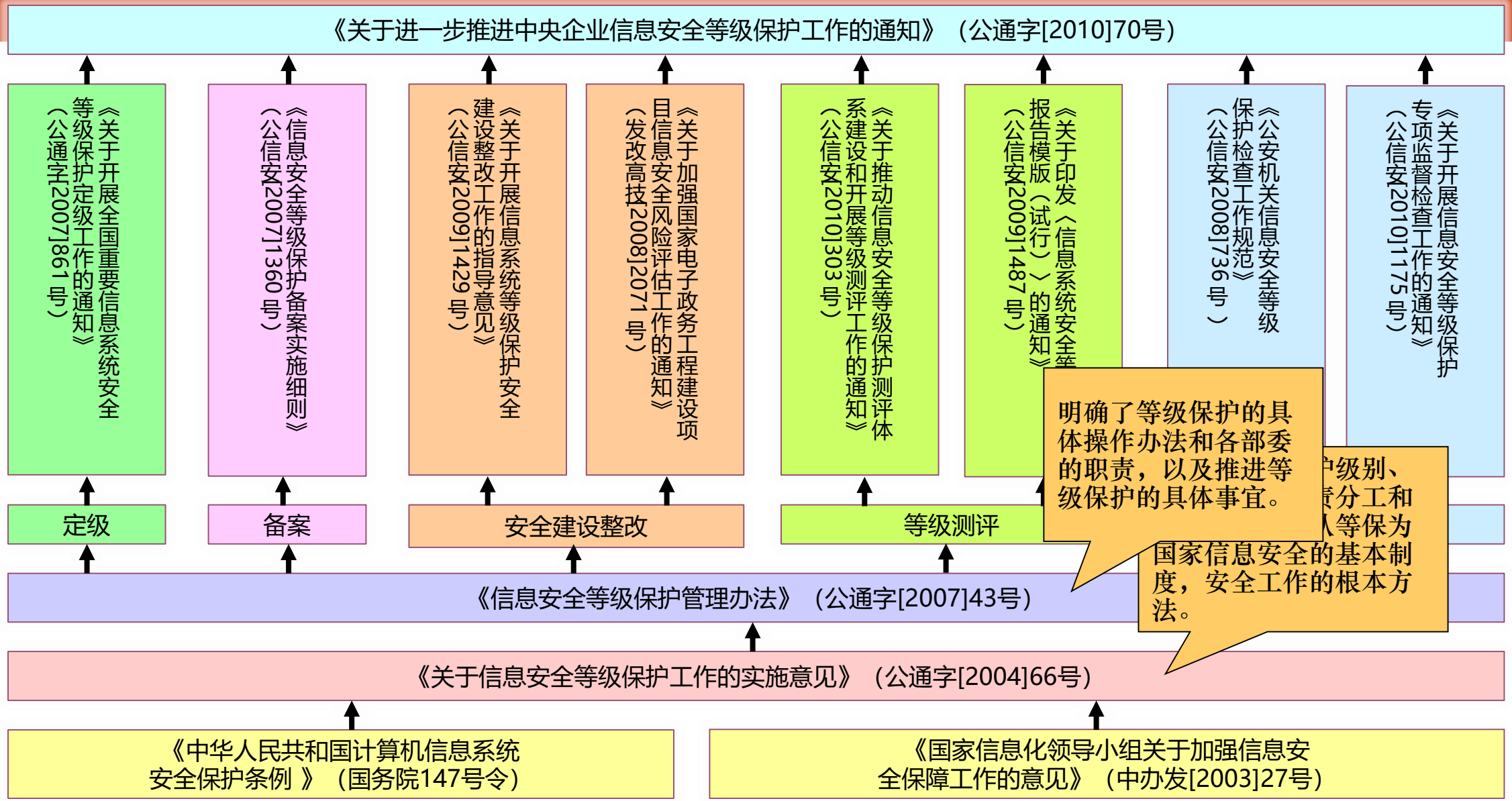
- **五是第三十六条关于签订安全保密协议要求。**即关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

- **六是第三十八条关于每年开展安全检测评估的要求。**即，关键信息基础设施的运营者应当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负责关键信息基础设施安全保护工作的部门。

违法处罚措施

1. 由有关主管部门责令改正，给予警告；
2. 拒不改正或者导致危害网络安全等后果的，处一万元以上一百万元以下罚款，对直接负责的主管人员处五千元以上十万元以下罚款。
3. 可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可
4. 尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；
5. 情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。
6. 受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；
7. 受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

信息安全等级保护国家政策



教育行业等级保护相关政策

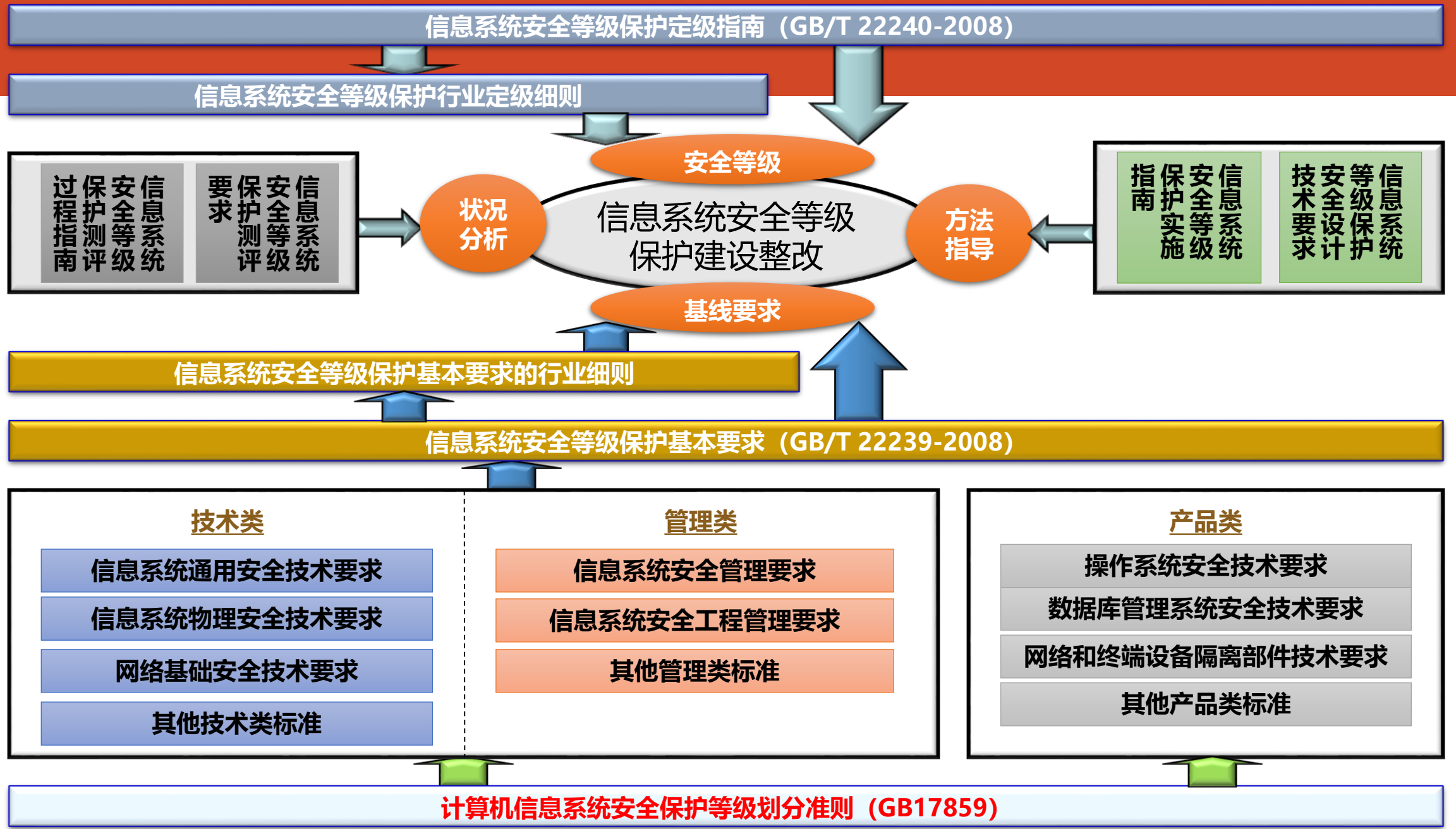
教育部办公厅关于开展教育系统信息安全等级保护工作专项检查的通知
教办厅函[2010]80号

教育部办公厅关于进一步加强网络信息系统安全保障工作的通知
(教办厅函[2011]83号)

教育部关于加强教育行业网络与信息安全工作的指导意见
(教技[2014]4号）

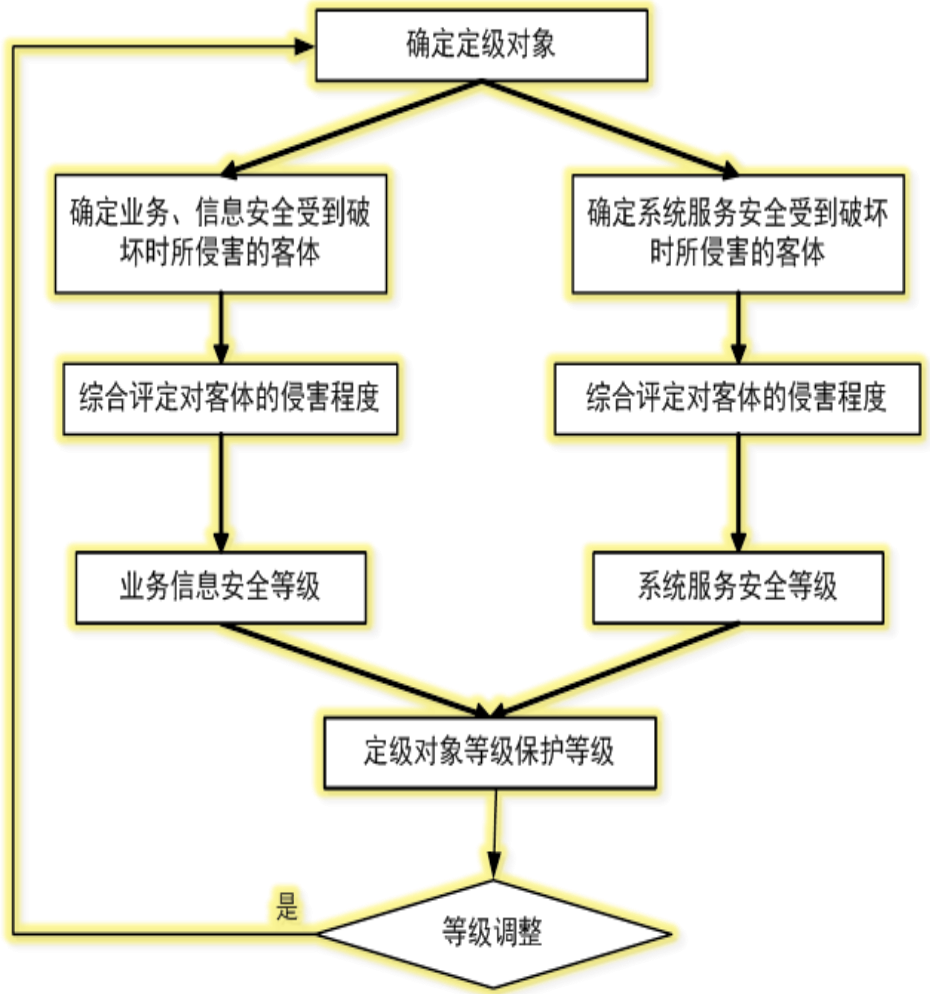
教育行业信息系统安全等级保护定级工作指南（试行）
教技厅函{2014}74号

等级保护国家标准体系


信息系统安全等级保护定级指南（GB/T 22240-2008）
信息系统安全等级保护行业定级细则
安全等级
信息系统安全等级保护测评要求
信息系统安全等级保护测评过程指南
状况分析
信息系统安全等级保护建设整改
方法指导
信息系统安全等级保护实施指南
信息系统等级保护安全设计技术要求
基线要求
信息系统安全等级保护基本要求的行业细则
信息系统安全等级保护基本要求（GB/T 22239-2008）
技术类
信息系统通用安全技术要求
信息系统物理安全技术要求
网络基础安全技术要求
其他技术类标准
管理类
信息系统安全管理要求
信息系统安全工程管理要求
其他管理类标准
产品类
操作系统安全技术要求
数据库管理系统安全技术要求
网络和终端设备隔离部件技术要求
其他产品类标准
计算机信息系统安全保护等级划分准则（GB17859）

- **信息系统定级原则**：“自主定级、专家评审、主管部门审批、公安机关审核”。

- **定级工作流程**：摸底调查、确定定级对象、对信息系统进行重要性分析、确定信息系统安全保护等级、组织专家评审、主管部门审批、公安机关审核。



定级备案 → 差距分析 → 整改规划 → 整改实施 → 等级测评

分类	信息系统	建议安全保护等级		
		I类院校	II类院校	III类院校
（01）校务管理类	（01）办公与事务管理	第二级	第二级	第二级
	（02）公文与信息交换	第二级	第二级	第二级
	（03）人事管理	第二级	第二级	第二级
	（04）财务管理	第二级	第二级	第二级
	（05）资产管理	第二级	第二级	第二级
	（06）后勤管理	第二级	第二级	第二级
	（07）学生教育工作管理	第二级	第二级	第二级
	（08）学生体质健康数据管理	第二级	第二级	第二级
	（09）档案管理	第二级	第二级	第二级
	（10）党务管理	第二级	第二级	第二级
（02）教学管理类	（01）教学改革管理	第二级	第二级	第二级
	（02）学科、专业管理	第二级	第二级	第二级
	（03）教务教学管理	第二级	第二级	第二级
	（04）教学资源管理	第二级	第二级	第二级
	（05）教学质量评估与保障	第二级	第二级	第二级
（03）科研管理类	（01）科研管理	第三级	第二级	第二级
	（02）科研协同与支撑	第三级	第二级	第二级

备案阶段需要提交材料

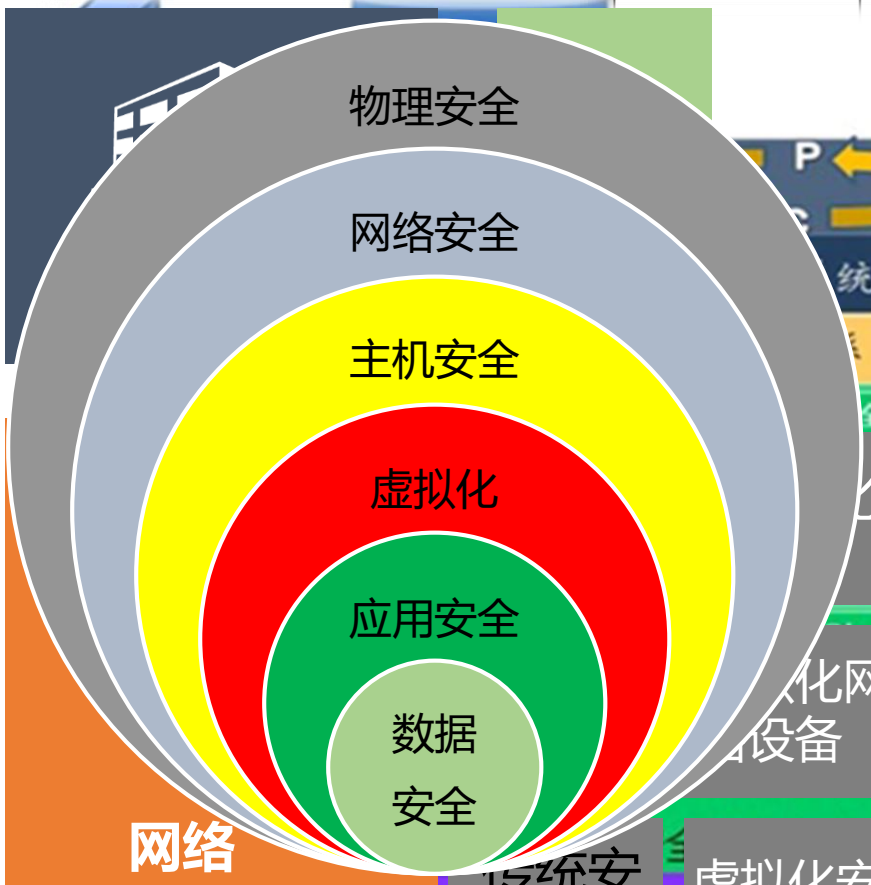
1	信息系统安全等级保护备案表
2	信息系统安全等级保护定级报告
3	系统拓扑结构及说明
4	系统安全组织机构和管理制度
5	系统安全保护设施设计实施方案或者改建实施方案
6	系统使用的信息安全产品清单及其认证、销售许可证明
7	信息系统安全等级保护测评报告
8	专家评审意见
9	主管部门审核批准信息系统安全保护等级的意见

二级以上

三级以上

安全分类	安全子类	一级		二级		三级		四级	
		控制点	具体要求	控制点	具体要求	控制点	具体要求	控制点	具体要求
技术要求	**物理安全**	7	9	10	19	10	32	10	33
	网络安全	3	9	6	18	7	33	7	32
	主机安全	4	6	6	19	7	32	9	36
	应用安全	4	7	7	19	9	31	11	36
	数据安全及备份恢复	2	2	3	4	3	8	3	11
管理要求	**安全管理制度**	2	3	3	7	3	11	3	14
	安全管理机构	4	4	5	9	5	20	5	20
	人员安全管理	4	7	5	11	5	16	5	18
	系统建设管理	9	20	9	28	11	45	11	48
	系统运维管理	9	18	12	41	13	62	13	70
合计	/	48	85	66	175	73	290	77	318
控制点级差	/	/	/	18	/	7	/	4	/
具体要求级差	/	/	/	/	90	/	115	/	28

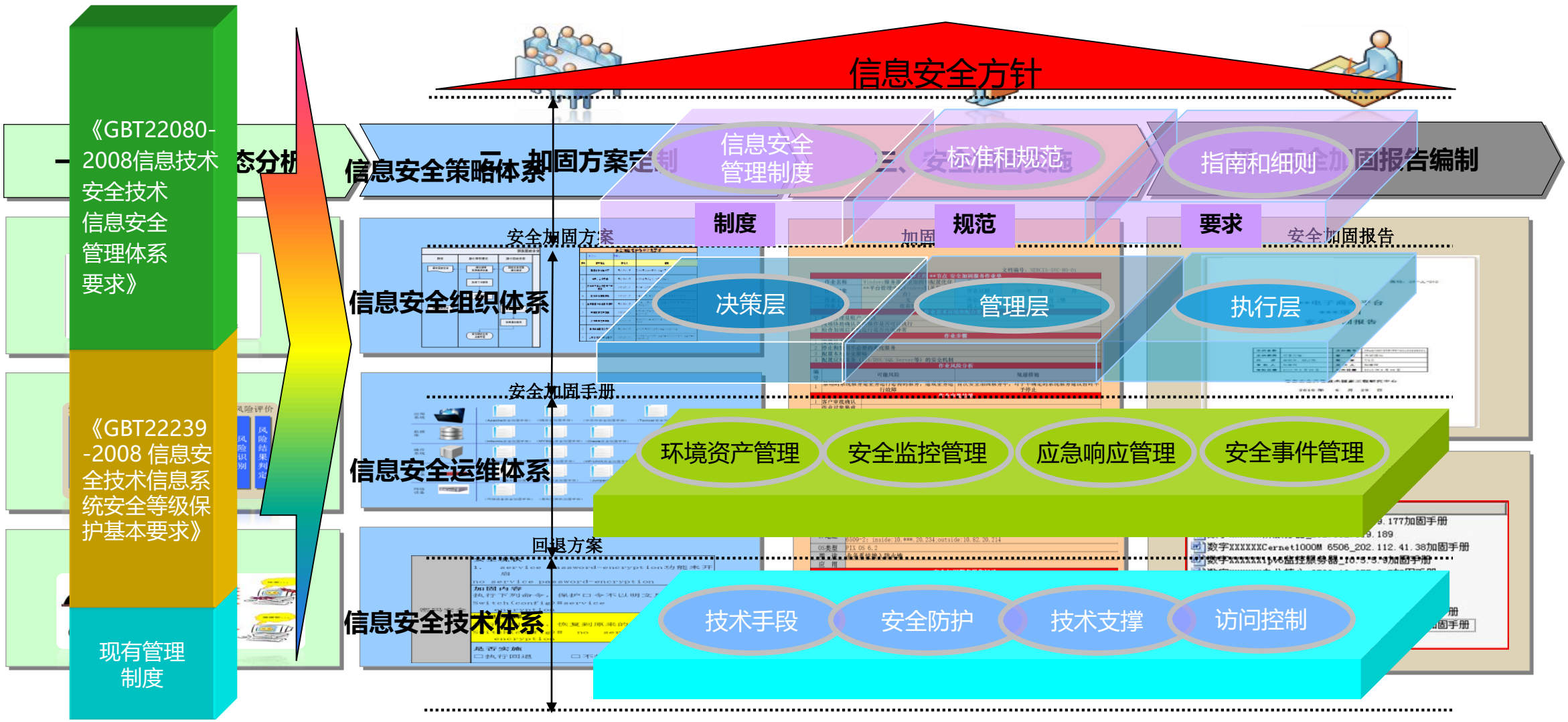
定级备案 → 差距分析 → **整改规划** → 整改实施 → 等级测评

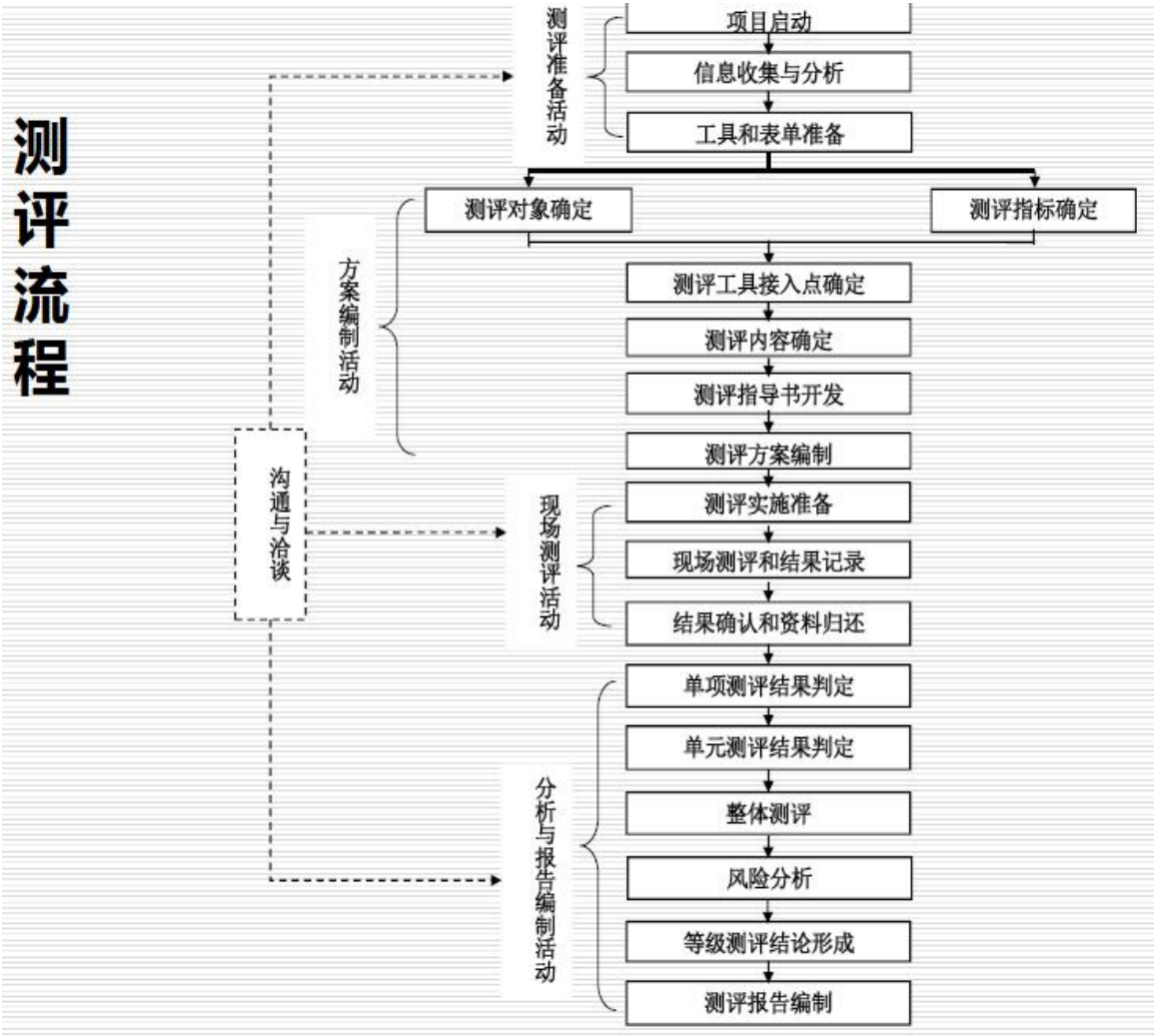


1. 门禁、机房监控系统、云监控
2. 防火墙、IDS/IPS、DDoS、安全隔离、传输加密
3. 终端安全、宿主机安全、系统完整性保护、OS加固、安全补丁、病毒防护
4. 虚拟化平台加固、虚拟机加固与隔离、虚拟网络监控、恶意VM预防、虚拟安全网关Vfw/vIPS
5. 多因素接入认证、WAF、安全审计、用户身份安全
6. 数据访问控制、DB-FW、镜像加密、数据脱敏、剩余信息保护、存储位置要求

安全合规、层层布控、互为补充、重点防护、协同保障

定级备案 → 差距分析 → 整改规划 → **整改实施** → 等级测评





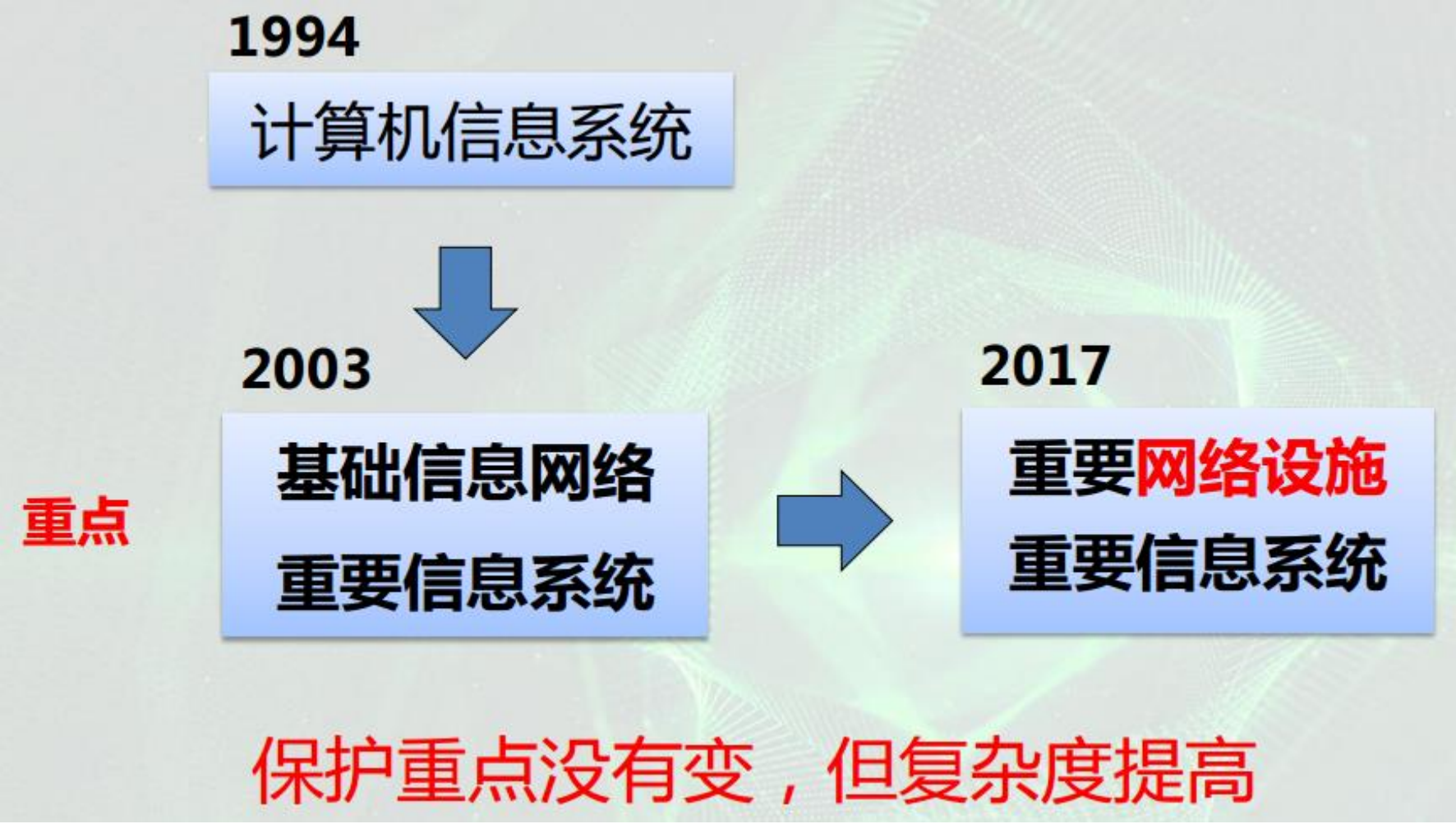
系统资料提供

测评对象核实

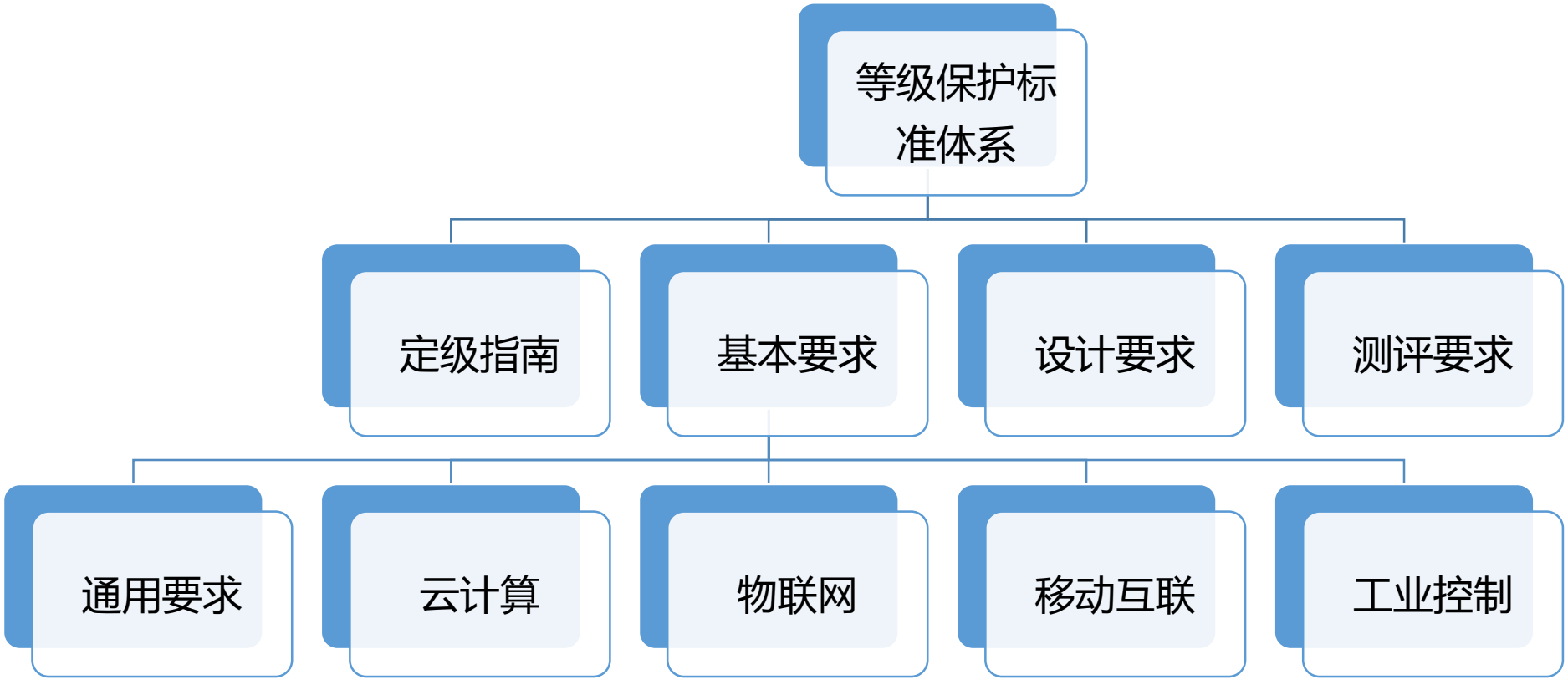
测评资料提供
测评问题答疑
测评操作协助

测评结果核对

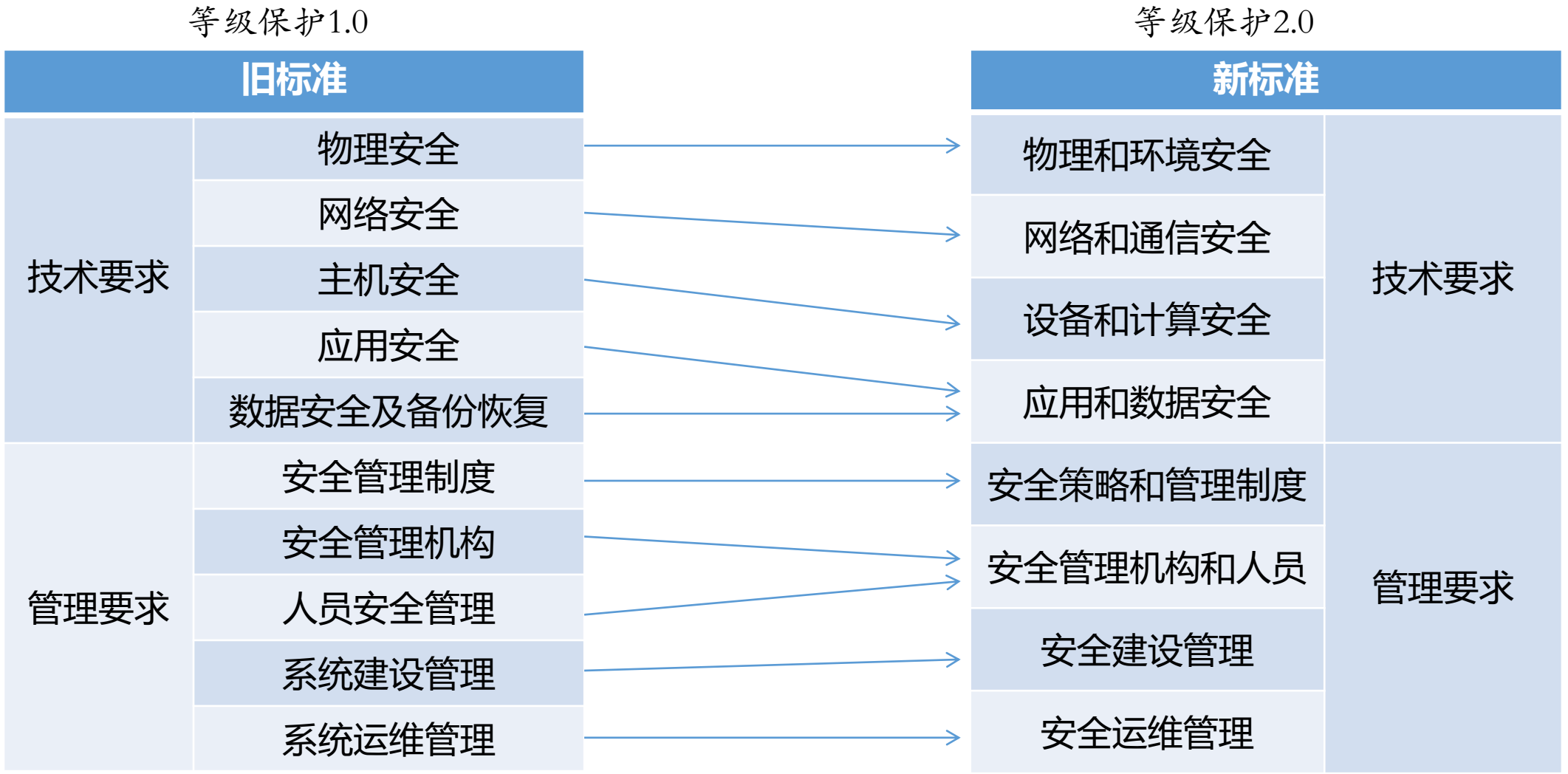
等级保护的对象演变


1994
计算机信息系统
2003
基础信息网络
重要信息系统
2017
重要网络设施
重要信息系统
重点
保护重点没有变，但复杂度提高

标准内容的变化



控制结构的变化


等级保护1.0
旧标准
技术要求
物理安全
网络安全
主机安全
应用安全
数据安全及备份恢复
管理要求
安全管理制度
安全管理机构
人员安全管理
系统建设管理
系统运维管理
等级保护2.0
新标准
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
技术要求
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
管理要求

要求项的变化

基本要求大类1.0	基本要求子类	信息系统安全等级保护级别	
		等保二级	等保三级
技术要求	物理安全	10	10
	网络安全	6	7
	主机安全	6	7
	应用安全	7	9
	数据安全	3	3
管理要求	安全管理制度	3	3
	安全管理机构	5	5
	人员安全管理	5	5
	系统建设管理	9	11
	系统运维管理	12	13
合计	/	66	73

基本要求大类2.0	基本要求子类	信息系统安全等级保护级别	
		等保二级	等保三级
技术要求	物理和环境安全	10	10
	网络和通信安全	7	8
	设备和计算安全	6	6
	应用和数据安全	9	10
管理要求	安全策略和管理制度	4	4
	安全管理机构和人员	9	9
	安全建设管理	10	10
	安全运维管理	14	14
合计	/	69	71

控制点的变化

基本要求大类1.0	基本要求子类	信息系统安全等级保护级别	
		等保二级	等保三级
技术要求	物理安全	19	32
	网络安全	18	33
	主机安全	19	32
	应用安全	19	31
	数据安全	4	8
管理要求	安全管理制度	7	11
	安全管理机构	9	20
	人员安全管理	11	16
	系统建设管理	28	45
	系统运维管理	41	62
合计	/	175	290

基本要求大类2.0	基本要求子类	信息系统安全等级保护级别	
		等保二级	等保三级
技术要求	物理和环境安全	15	22
	网络和通信安全	16	33
	设备和计算安全	17	26
	应用和数据安全	22	34
管理要求	安全策略和管理制度	6	7
	安全管理机构和人员	16	26
	安全建设管理	25	34
	安全运维管理	30	48
合计	/	147	230

	原控制点	要求项数		新控制点	要求项数
物理安全	1 物理位置的选择	2	物理和环境安全	1 物理位置的选择	2
	2 物理访问控制	4		2 物理访问控制	1
	3 防盗窃和防破坏	6		3 防盗窃和防破坏	3
	4 防雷击	3		4 防雷击	2
	5 防火	3		5 防火	3
	6 防水和防潮	4		6 防水和防潮	3
	7 防静电	2		7 防静电	2
	8 温湿度控制	1		8 温湿度控制	1
	9 电力供应	4		9 电力供应	3
	10 电磁防护	3		10 电磁防护	2

原控制项		新控制项	
物理位置的选择	b) 机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。	物理位置的选择	b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施
防静电	无	防静电	b) 应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。(新增)

	原控制点	要求项数		新控制点	要求项数
网络安全	1结构安全	7	网络和通信安全	1 网络架构	5
	2访问控制	8		2通信传输	2
	3安全审计	4		3边界防护	4
	4边界完整性检查	2		4 访问控制	5
	5入侵防范	2		5 入侵防范	4
	6 恶意代码防范	2		6 恶意代码防范	2
	7 网络设备防护	8		7 安全审计	5
				8 集中管控	6

原控制项		新控制项	
无		通信传输	a) 应采用校验码技术或密码技术保证通信过程中数据的完整性； b) 应采用密码技术保证通信过程中敏感信息字段或整个报文的保密性。
边界完整性检查	a) 应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断； b) 应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。	边界防护	a) 应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信； b) 应能够对非授权设备私自联到内部网络的行为进行限制或检查； 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。
入侵防范	无 无	入侵防范	b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；（新增） 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新型网络攻击行为的分析；（新增）

原控制项		新控制项	
恶意代码防范	无	恶意代码防范	b) 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。 (新增)
安全审计	无	安全审计	d) 应确保审计记录的留存时间符合法律法规要求；(新增)
			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)
无		集中管控	a) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控； (新增)
			b) 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理； (新增)
			c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测； (新增)
			d) 应对分散在各个设备上的审计数据进行收集汇总和集中分析；(新增)
			e) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
			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。 (新增)

解读

1. 根据服务器角色和重要性，对网络进行安全域划分；

2. 在内外网的安全域边界设置访问控制策略，并要求配置到具体的端口；

3. 在网络边界处应当部署入侵防范手段，防御并记录入侵行为（强调未知威胁检测）；

4. 对网络中的用户行为日志和安全事件信息进行记录和审计；

5.对安全设备、网络设备和服务器等进行集中管理。

	原控制点	要求项数		新控制点	要求项数
主机安全	1 身份鉴别	6	设备和计算安全	1 身份鉴别	4
	2 访问控制	7		2 访问控制	7
	3 安全审计	6		3 安全审计	5
	4 剩余信息保护	2		4 入侵防范	5
	5 入侵防范	3		5 恶意代码防范	1
	6 恶意代码防范	3		6 资源控制	4
	7 资源控制	5			

原控制项		新控制项	
安全审计	无	安全审计	d) 应确保审计记录的留存时间符合法律法规要求；（新增）
入侵防范	无	入侵防范	b) 应关闭不需要的系统服务、默认共享和高危端口；
			c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
			d) 应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；

解读

1. 避免账号共享、记录和审计运维操作行为是最基本的安全要求；

2. 必要的安全手段保证系统层安全，防范服务器入侵行为；

	原控制点	要求项数		新控制点	要求项数
应用安全	1 身份鉴别	5	应用和数据安全	1 身份鉴别	5
	2 访问控制	6		2 访问控制	7
	3 安全审计	4		3 安全审计	5
	4 剩余信息保护	2		4 软件容错	3
	5 通信完整性	1		5 资源控制	2
	6 通信保密性	2		6 数据完整性	2
	7 抗抵赖	2		7 数据保密性	2
	8 软件容错	2		8 数据备份和恢复	3
	9 资源控制	7		9 剩余信息保护	2
数据安全及备份恢复	9 数据完整性	2		10 个人信息保护	2
	10 数据保密性	2			
	11 备份和恢复	4			

原控制项		新控制项	
安全审计	无	安全审计	d) 应确保审计记录的留存时间符合法律法规要求；（新增）
软件容错	无	软件容错	c) 在故障发生时，应自动保存易失性数据和所有状态，保证系统能够进行恢复。（新增）
身份鉴别	无	身份鉴别	c) 应强制用户首次登录时修改初始口令；（新增）
			d) 用户身份鉴别信息丢失或失效时，应采用技术措施确保鉴别信息重置过程的安全；（新增）
个人信息保护	无	个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；（新增）
			b) 应禁止未授权访问和非法使用用户个人信息。（新增）

解读

1. 应用是具体业务的直接实现，不具有网络和系统相对标准化的特点。大部分应用本身的身份鉴别、访问控制和操作审计等功能，都难以用第三方产品来替代实现；

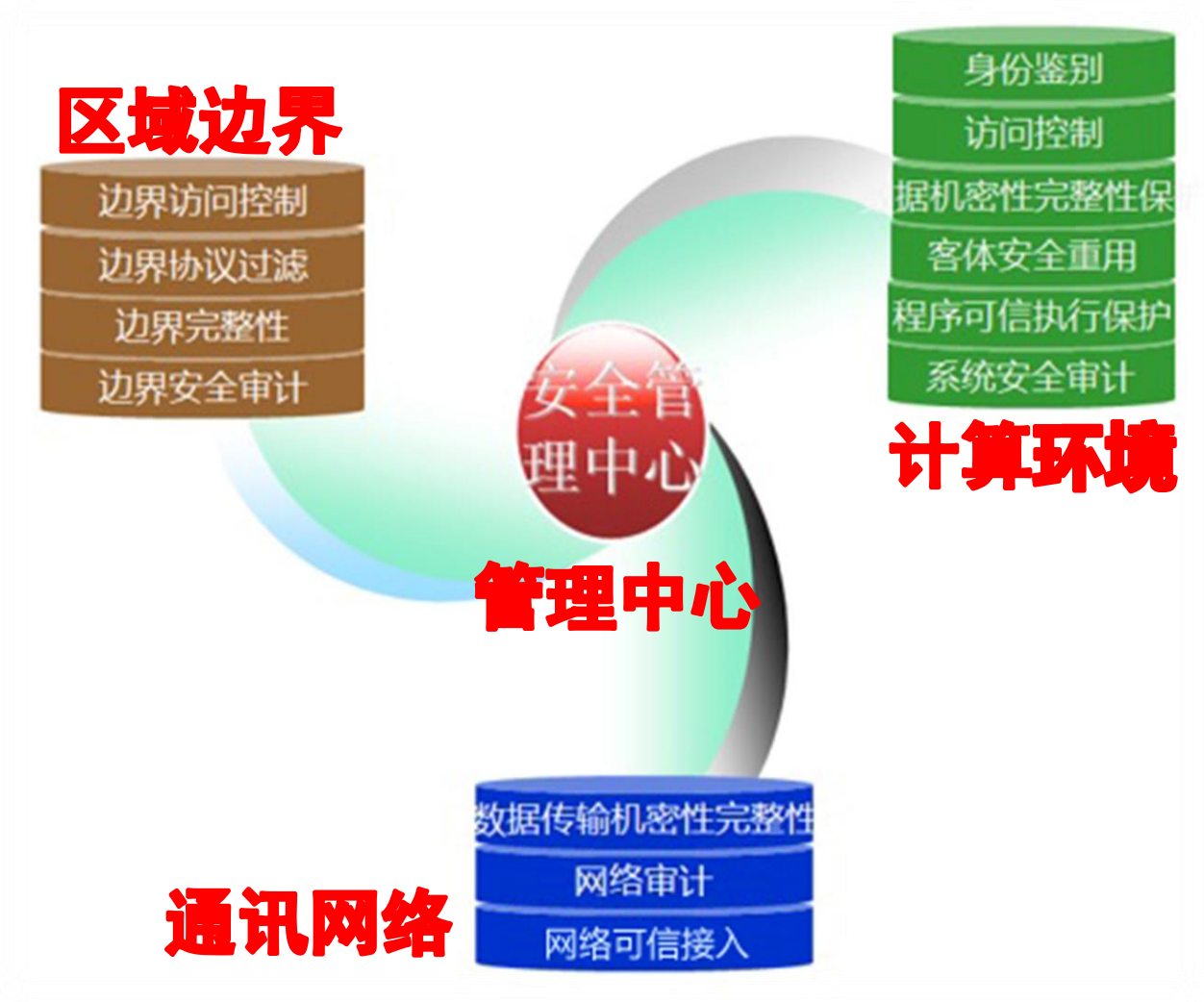
2. 数据的完整性和保密性，除了在其他层面进行安全防护以外，加密是最为有效的方法；

3. 数据的异地备份是等保三级区别于二级最重要的要求之一，是实现业务连续最基础的技术保障措施。

教育信息化安全“防”与“范”

安全防护方向及新产品

安全技术体系规划


区域边界
边界访问控制
边界协议过滤
边界完整性
边界安全审计
身份鉴别
访问控制
据机密性完整性保
客体安全重用
程序可信执行保护
系统安全审计
计算环境
安全管
理中心
管理中心
数据传输机密性完整性
网络审计
网络可信接入
通讯网络

网御非法接入检查系统

- 全网资产的快速识别和分类统计；
- 检测网络中私自扩展的网中网；
- 检测网络中私自接入的无线AP与随身Wifi设备；
- 检测双网卡之间的网络共享行为；
- 检测网络中以NAT方式私自接入的路由设备；

- 检测网络中私自接入的BYOD类设备（智能手机、平板等设备）；
- 提供网络中私自接入的BYOD类设备的快速筛选查询；
- 对私接设备可快速完成IP-MAC-Switch Port网络定位，直接定位到私接设备所连接的交换机端口，提供精准阻断控制；
- 对设备的私接行为进行全面跟踪审计，确保即使IP地址变更或接入位置变化也能回溯界定责任者；

网御安全流量分析系统

从业务角度	从行为角度	从来源角度	从隔离角度
梳理清IP资产	监控访问行为关系	监控数据包	设置合理访问控制关系
资产管理系统	访问行为关系采集技术DFI	数据包解析技术DPI	访问控制策略梳理技术
资产入网监控技术	行为异常检测技术	数据包攻击检测、审计技术	访问控制策略审核优化技术

网御高级可持续性威胁检测APT

已知威胁检测

IDS

攻击事件库\病毒库

模式匹配

特征匹配

协议解析+数据包检测

+文件还原

未知威胁检测

APT

各种学习模型

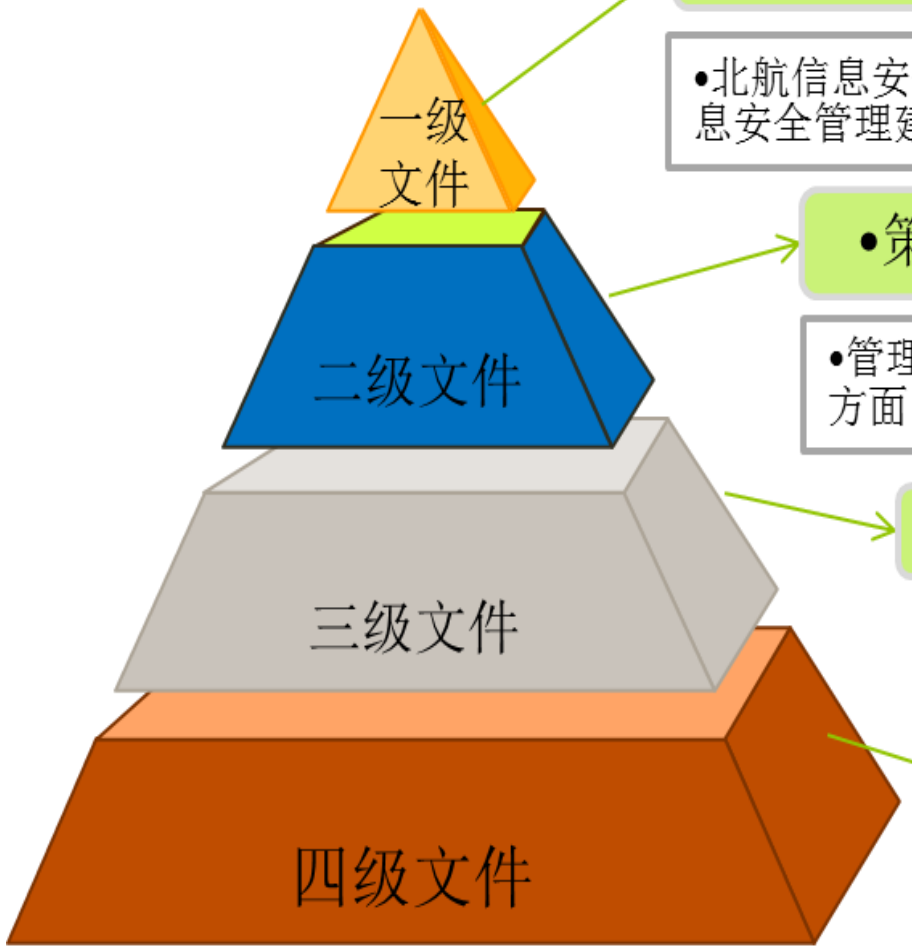
虚拟执行

行为模拟

文件检测+行为检测

+漏洞利用分析

安全管理体系建设



•方针 目标

•北航信息安全管理体系总体方针、目标，是北航信息安全管理建设的总体方向。

•策略 制度 流程

•管理体系文件的核心，根据等级保护的要求，从5个方面明确信息安全管理体系的具体要求。

•程序 指南 规范

•结合实际工作，针对具体系统，形成可指导的程序、指南、技术规范，保证日常工作的可操作性和规范性。

•相关记录 表单

•信息安全管理工作实际执行的结果记录。

安全管理体系建设输出

一级文件：框架性安全管理制度

二级文件：具体安全管理制度

三级文件：操作规程手册

四级文件：记录表格

信息安全管理制度
输出

安全运维体系实现

周期性安全评估

周期性安全加固

定期安全巡检

系统上线检测

应急响应

定期安全通告

安全培训教育

系统开发安全管控

网御应急处理工具箱

简介

依据国际应急处置标准，面向网络安全事件

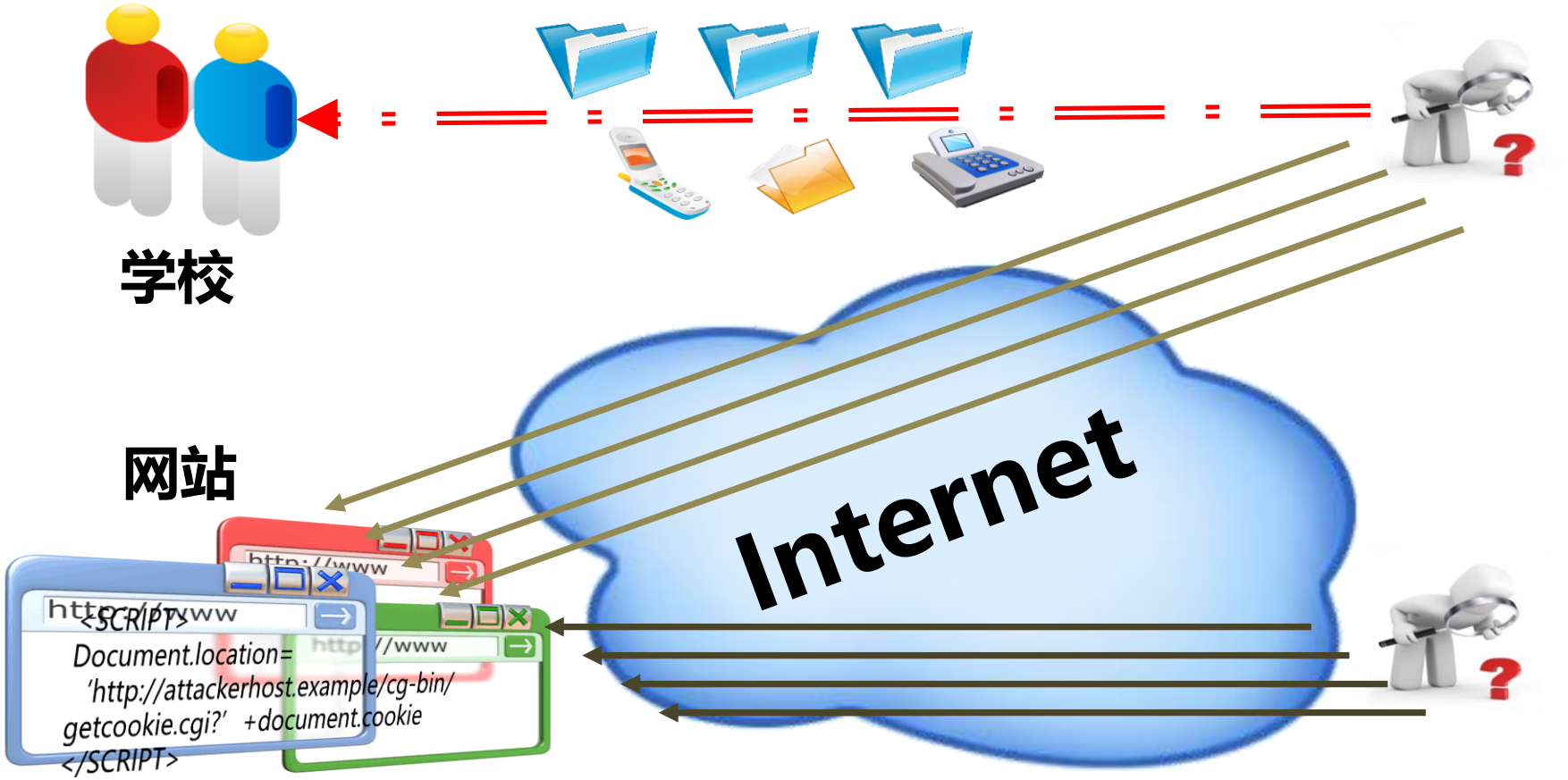
丰富的安全知识库，应急预案和工具及详细使用方法

安全防护人员应急响应安全事件的“瑞士军刀”

定位

为安全事件的应急处置提供简便、可靠、高效、专业的综合手段

网站安全监测系统



全面监测

专家分析

漏洞扫描

挂马检测

可用性监测

敏感内容

网页篡改

钓鱼网站

域名解析

安全通告

安全舆情

实时预警

及时响应

谢谢大家！