ISC 2017

2017 中国互联网安全大会 China Internet Security Conference

等级保护2.0下的云计算安全保护

任卫红

公安部第三研究所

公安部信息安全等级保护评估中心技术部 主任

目录

- 等级保护2.0带来的变化
- 云计算安全的等级保护要求
- 在等级保护基础上保护关键云计算平台

等级保护2.0带来的变化

- 等级保护制度上升为法律
- 等级保护对象的扩展
- 等级保护体系的升级
- 等级保护内涵的丰富

网安法相关条款

- 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： 。。。 。。。

- 第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、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，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

等级保护对象的演变

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

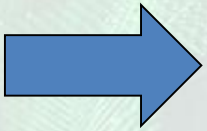
重点

保护重点没有变，但复杂度提高

等级保护2.0保护对象展现形态

系统对象

重要
信息系统



信息系统

计算机信息系统

工业控制系统

移动互联系统

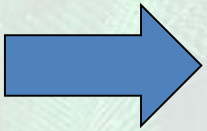
物联网系统

信息物理系统

等级保护2.0保护对象展现形态

网络对象

基础
信息网络



网络设施

电信网

广播电视网

互联网

云计算服务

大数据服务

等级保护内涵的丰富

运营使用单位/安全服务商　　测评机构　　监管部门

定级备案　建设整改　等级测评　监督检查

定级备案

建设整改
安全监测
通报预警
应急处置
安全可控
。。。

等级测评
渗透测试
攻防对抗
特勤安保
有效性评价
。。。

监督检查
专项检查
机构管理
案事件调查
。。。

等级测评技术的提升


等级测评
符合性
✓ 功能、机制符合
✓ 策略、配置符合
✓ 文档、记录符合
有效性
✓ 保护目标达成
✓ 措施取得成效
✓ 效果能够持续
自动化
✓ 自动配置检查和判断
✓ 状态信息自动收集
✓ 数据分析和评估

等级保护2.0-体系升级

- **政策体系**
  - **网络安全等级保护条例起草**
- **标准体系**
  - **主要标准修订**
- **测评体系**
- **技术体系**
- **教育培训体系**
- **。。。**

目录

- 等级保护2.0带来的变化
- 云计算安全的等级保护要求
- 在等级保护基础上保护关键云计算平台

《定级指南》修订-云计算系统定级

定级对象

- 在云计算环境中，将云计算平台作为基础设施，云客户业务系统作为信息系统分别作为定级对象定级。
- 对于大型云计算平台，当运管平台共用时，可将云计算基础设施与运管平台系统 分开定级。

责任分离，分别定级，各自备案。

《定级指南》修订-云计算系统定级

等级确定

- 云计算基础设施的安全保护等级不低于其所支撑的业务系统的等级。

《基本要求》修订

网络安全等级保护基本要求（GB/T 22239）

安全通用要求

云计算安全扩展要求

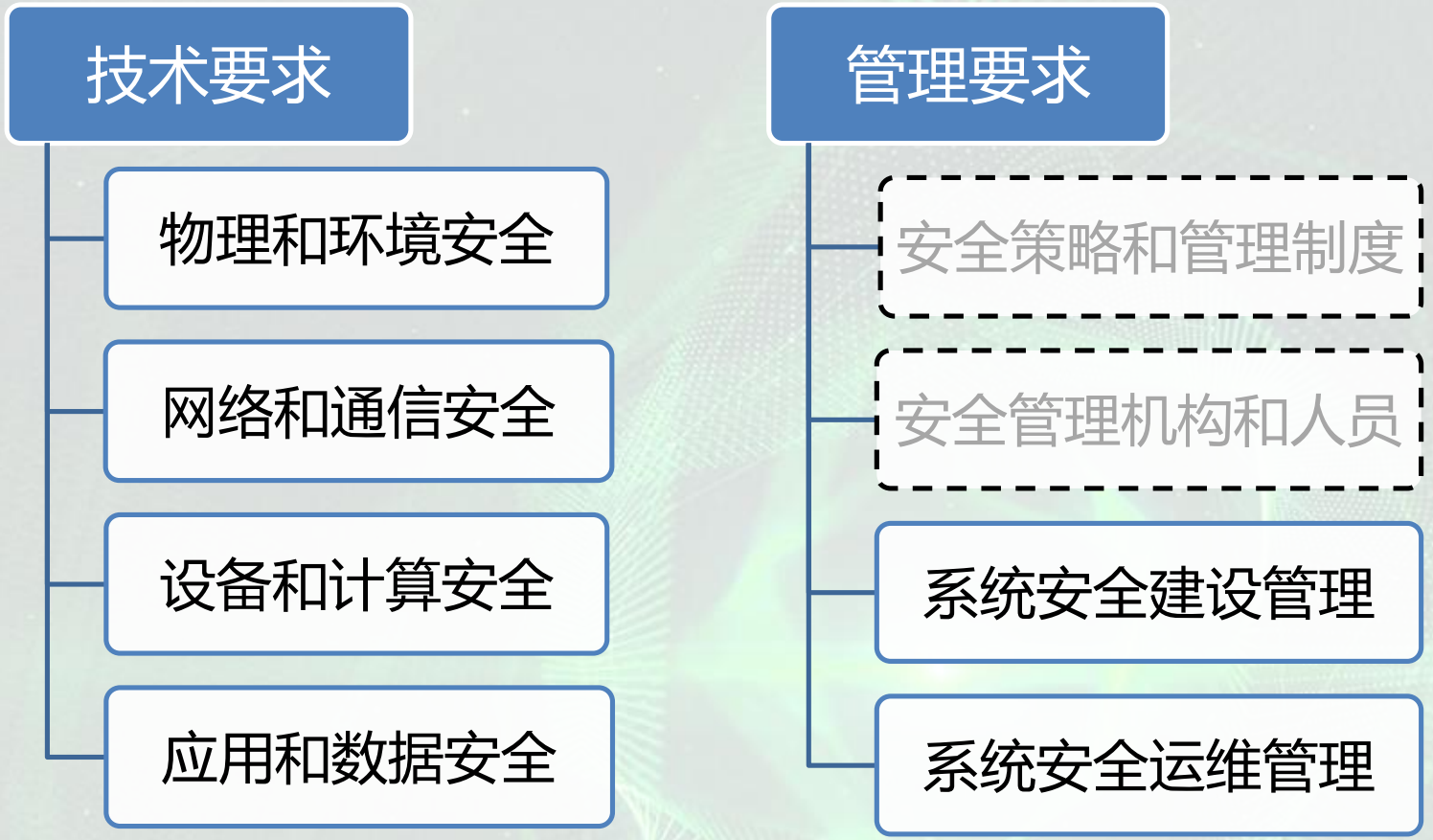
移动互联安全扩展要求

物联网安全扩展要求

工业控制系统安全扩展要求

大数据系统安全扩展要求

云计算安全扩展要求-结构



既包含云计算平台自身安全也包括提供的安全能力

云计算安全扩展要求-平台安全

- 登录Hypervisor、云管理平台等的管理用户进行相应等级身份鉴别；
- 进行远程管理时，管理终端和云平台边界设备之间应建立双向身份验证机制；
- 具备对异常流量的识别、监控和处理能力；
- 对发布到互联网的有害信息进行实时监测和告警
- 网络策略控制器和网络设备（或设备代理）之间双向认证、数据加密传输。

云计算安全扩展要求-资源隔离

- 应实现不同云服务客户虚拟网络之间的隔离；
- 应确保云服务客户的虚拟机使用独占的内存空间；
- 应保证云计算平台管理流量与云客户业务流量分离；
- 应保证不同云服务客户的审计数据隔离存放；
- 应保证虚拟机所使用的内存和存储空间回收时得到完全清除。

云计算安全扩展要求-访问控制

- 应具有根据云服务客户业务需求自主设置安全策略集的能力，包括定义访问路径、选择安全组件、配置安全策略；
- 实现云平台管理用户权限分离机制，为网络管理员、系统管理员建立不同账户并分配相应的权限；
- 确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限；
- 云计算平台应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云平台选择第三方安全服务。

云计算安全扩展要求-数据安全

- 应提供查询云服务客户数据及备份存储位置的方式；
- 保证虚拟机迁移过程中重要数据的完整性和保密性；
- 提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
- 对虚拟机快照中的敏感信息进行加密保护；
- 支持云服务客户部署密钥管理解决方案，确保云服务客户自行实现数据的加解密过程

云计算安全扩展要求-审计与监控

- 能识别、监控虚拟机之间、虚拟机与物理机之间、虚拟机与宿主机之间的流量；
- 保证云服务商对云服务客户系统和数据的操作可被云服务客户审计；
- 根据云服务方和云客户的职责划分，实现各自控制部分的集中审计；
- 应为安全审计数据的汇集提供接口，可供第三方审计。

目录

- 等级保护2.0带来的变化
- 云计算安全的等级保护要求
- 在等级保护基础上保护关键云计算平台

成为关键信息基础设施的云计算平台

第十八条 下列单位运行、管理的网络设施和信息系统，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，应当纳入关键信息基础设施保护范围：

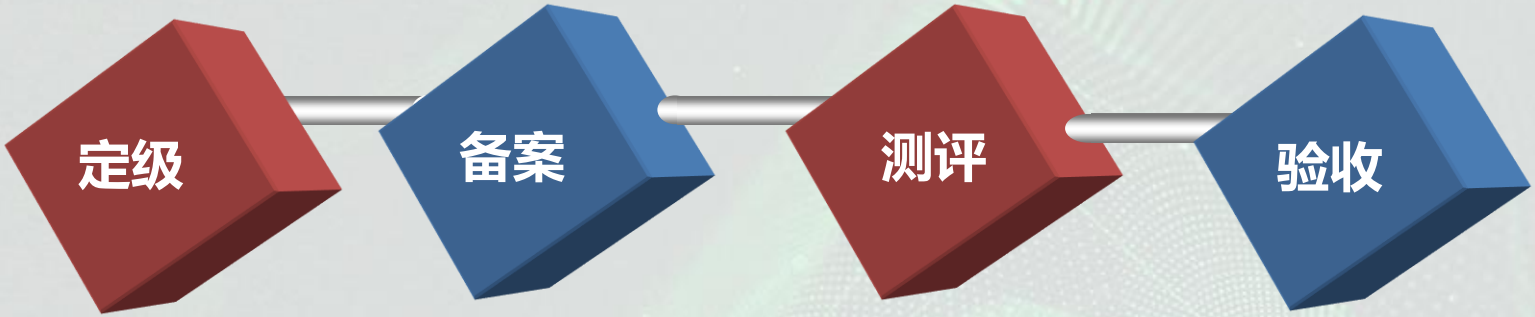
（二）电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位。

CII保护与等级保护的关系

- 等级保护是关键信息基础设施保护的基础
- 关键信息基础设施保护是等级保护的核心

关键信息基础设施的安全保护等级不低于第三级。

新建关键信息基础设施的等级保护流程



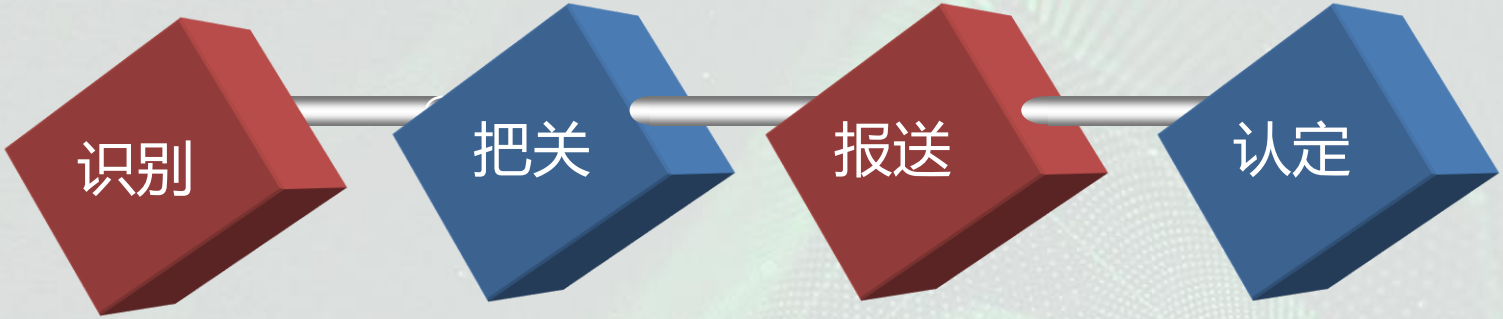
网络运营者在项目立项阶段或项目建设初期进行定级。

定级后10个工作日内到当地公安机关办理备案手续。

项目验收前选择具备资质的测评机构，开展等级测评。

等级测评合格后，方可验收并上线运行。

信息系统定级和CII识别认定



行业主管或监管部门按照识别指南组织本行业本领域识别工作。

识别认定过程中，应当充分发挥有关专家作用。

报送关键信息基础设施管理部门。报公安机关备案。

认定形成关键信息基础设施目录并持续维护。告知运营者

关键信息基础设施保护措施构成

网络运营者的保护措施

关键信息基础设施自身要求

行业/领域要求

对关键信息基础设施的增强要求

基线要求

通用要求

扩展要求

国家保障制度

网络安全等级保护制度

关键信息基础设施保护制度

产品和服务的安全审查制度

个人信息保护制度

安全监测预警和信息通报制度

关保条例中的对网络运营者要求

- ✓ 作为本单位安全保护工作第一责任人

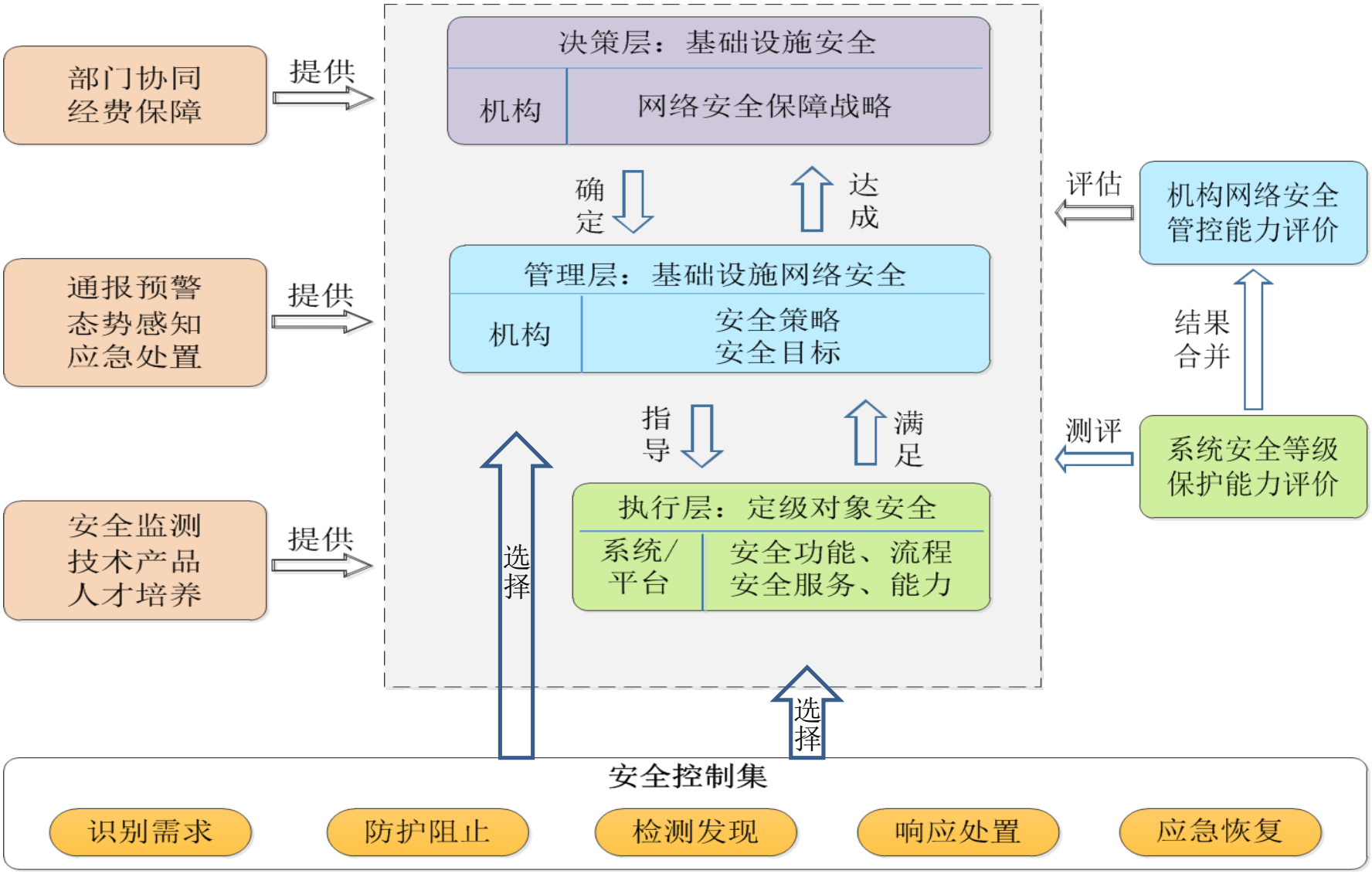
- ✓ 每年培训不少于1个工作日
- ✓ 安全背景审查
- ✓ 负责管理体系建设、人员考核、检查、事件处置和报告
- ✓ 安全背景审查
- ✓ 执证上岗
- ✓ 每年培训不少于3个工作日

关保条例中的对网络运营者要求

- ✓ 安全技术措施同步规划、同步建设、同步使用
- ✓ 个人信息和重要数据的境内存储
- ✓ 确需出境，安全评估

- ✓ 上线运行前安全检测评估
- ✓ 网络日志留存不少于6个月
- ✓ 每年至少一次检测评估
- ✓ 网络信息安全投诉举报制度

关键信息基础设施的等级保护技术框架



谢　谢

- 13718118048
- 010-88140977　www.djbh.net