2019 CTIC
网络安全分析与情报大会
CYBER THREAT INTELLIGENCE CONFERENCE

等级保护基本要求V2.0解读

朱建平
公安部第三研究所研究员

一、网络安全等级保护2.0-主要标准

- 网络安全等级保护条例（总要求/上位文件）
- 计算机信息系统安全保护等级划分准则（GB 17859-1999）（上位标准）
- 网络安全等级保护实施指南（GB/T25058）（正在修订）
- 网络安全等级保护定级指南（GB/T22240）（正在修订）
- 网络安全等级保护基本要求（GB/T22239-2019）
- 网络安全等级保护设计技术要求（GB/T25070-2019）
- 网络安全等级保护测评要求（GB/T28448-2019）
- 网络安全等级保护测评过程指南（GB/T28449-2018）

二、特点

➢新标准将云计算、移动互联、物联网、工业控制系统等列入标准范围，构成了“安全通用要求+新型应用安全扩展要求”的要求内容

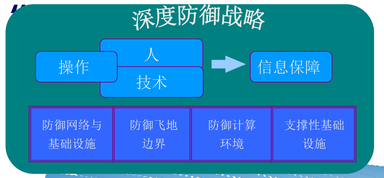
章节示例：

- 8 第三级安全要求
- 8.1 安全通用要求
- 8.2 云计算安全扩展要求
- 8.3 移动互联安全扩展要求
- 8.4 物联网安全扩展要求
- 8.5 工业控制系统安全扩展要求

二、特点

➢新标准“基本要求、设计要求和测评要求” 分类框架统一，形成了“安全通信网络”、“安全区域边界”、“安全计算环境”和“安全管理中心” 支持下的三重防护体系架构

信息安全保障技术框架



网络安全等级保护基本要求

二、特点

➢新标准强化了可信计算技术使用的要求，把可信验证列入各个级别并逐级提出各个环节的主要可信验证要求

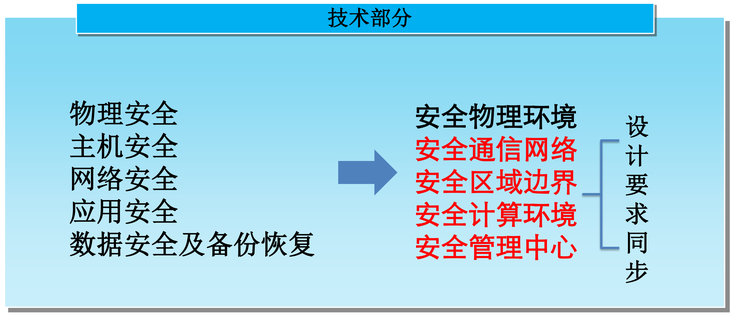
第一级：可基于可信根对设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警

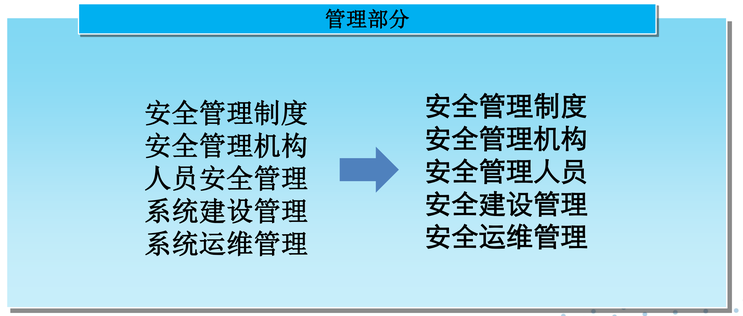
第二级：可基于可信根对设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

第三级：可基于可信根对设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

第四级：可基于可信根对设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

三、控制措施分类结构调整





要求项比较

等级保护1.0	安全通用要求	云计算扩展要求	移动互联扩展要求	物联网扩展要求	工控系统扩展要求
2级175	2级137	2级29	2级14	2级7	2级15
3级290	3级211	3级46	3级19	3级20	3级21
4级318	4级228	4级49	4级21	4级22	4级22

四、调整了部分要求项与控制项

电力供应：

d)应建立备用供电系统。

访问控制：

d)应在会话处于非活跃一定时间或会话结束后终止网络连接

e)应限制网络最大流量数及网络连接数

f)重要网段应采取技术手段防止地址欺骗

f)应对重要信息资源设置敏感标记（主机安全）

入侵防范：

b)应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施

四、调整了部分要求项与控制项

剩余信息保护：

取消了主机安全部分的要求，保留了应用安全的要求。

资源控制：

取消。

抗抵赖：

有条件放到第四级。

五、增强或增加了部分要求项

通讯传输：

应采用校验技术或密码技术保证通信过程中数据的完整性；

应采用密码技术保证通信过程中数据的保密性。

边界防护：

应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。

入侵防范：

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。（抗APT攻击系统、威胁情报、态势感知系统）

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；（计算环境）

五、增强或增加了部分要求项

恶意代码防范：

应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。（三级→二级）

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。

应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。（计算环境）

安全审计：

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。

身份鉴别：

应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

五、增强或增加了部分要求项

数据保密性：

应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

个人信息保护：

应仅采集和保存业务必需的用户个人信息；

应禁止未授权访问和非法使用用户个人信息。

五、增强或增加了部分要求项

安全管理中心:

从二级以上在技术上开始增加了“安全管理中心”要求。二级需要有“系统管理”和“审计管理”；三级以上需要有完整的“系统管理”、“审计管理”和“安全管理”，并且实现“集中管控”。

集中管控:

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；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；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；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，并保证审计记录的留存时间符合法律法规要求；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；应能对网络中发生的各类安全事件进行识别、报警和分析。

六、增加了扩展要求

云计算安全扩展要求

对云计算环境主要增加的内容包括“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

对移动互联环境主要增加的内容包括“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

对物联网环境主要增加的内容包括“感知节点的物理防护”、“感知节点设备安全”、“感知网关节点设备安全”、“感知节点的管理”和“数据融合处理”等方面。

六、增加了扩展要求

工业控制系统安全扩展要求

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。

大数据系统安全扩展要求

附录H描述大数据应用场景（安全扩展要求）。

THANK YOU

CTIC