CIS 2019
网络安全创新大会
Cyber Security Innovation Summit

网络安全等级保护2.0标准解读

宋好好 公安部第三研究所 博士/研究员/高级测评师

CIS 2019
网络安全创新大会
Cyber Security Innovation Summit

网络安全等级保护制度

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；（日志留存）

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：

（四）采取数据分类、重要数据备份和加密等措施；（数据安全）

（五）法律、行政法规规定的其他义务。

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。（CII必须落实国家等级保护制度，突出保护重点）

国家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。

网络安全创新大会
Cyber Security Innovation Summit

网络安全等级保护2.0标准解读

相关的等级保护标准

GB/T 22239-2019
信息安全技术 网络安全等级保护基本要求

GB/T 22240-XXXX
信息安全技术 网络安全等级保护定级指南

GB/T 25058-2019
信息安全技术 网络安全等级保护实施指南

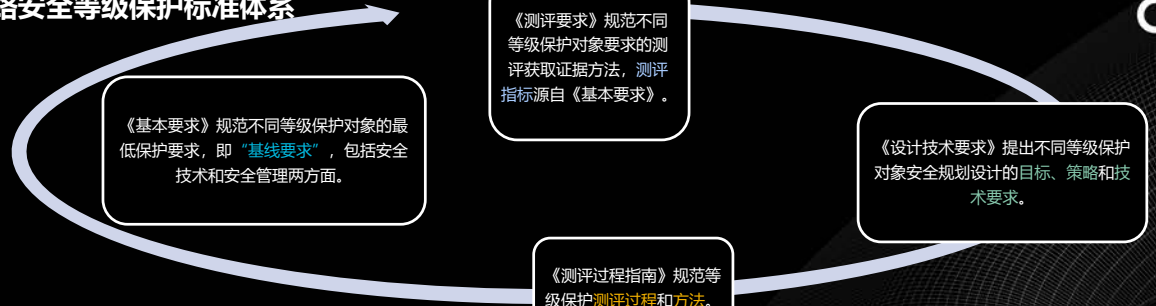
GB/T 25070-2019
信息安全技术 网络安全等级保护设计技术要求

GB/T 28448-2019
信息安全技术 网络安全等级保护测评要求

GB/T 28449-2018
信息安全技术 网络安全等级保护测评过程指南

GB/T 36627-2018
信息安全技术 网络安全等级保护测试评估技术指南

网络安全等级保护标准体系



相关的等级保护标准

GB/T 22239-2019
信息安全技术 网络安全等级保护基本要求

GB/T 22240-XXXX
信息安全技术 网络安全等级保护定级指南

GB/T 25058-2019
信息安全技术 网络安全等级保护实施指南

GB/T 25070-2019
信息安全技术 网络安全等级保护设计技术要求

GB/T 28448-2019
信息安全技术 网络安全等级保护测评要求

GB/T 28449-2018
信息安全技术 网络安全等级保护测评过程指南

GB/T 36627-2018
信息安全技术 网络安全等级保护测试评估技术指南

《信息安全技术 网络安全等级保护基本要求》

安全通用要求安全层面的差异

等保1.0 安全层面	等保2.0 安全层面
物理安全	安全物理环境
网络安全	安全通信网络
主机安全	安全区域边界
应用安全	安全计算环境
数据安全及备份恢复	安全管理中心
安全管理制度	安全管理制度
安全管理机构	安全管理机构
人员安全管理	安全管理人员
系统建设管理	安全建设管理
系统运维管理	安全运维管理

安全通用要求安全层面的差异

基本要求

GB/T 22239-2008
《信息安全技术 信息系统安全等级保护基本要求》

等保1.0 等保2.0

GB/T 22239-2019
《信息安全技术 网络安全等级保护基本要求》

1）安全通用要求

2）云计算安全扩展要求

3）移动互联安全扩展要求

4）物联网安全扩展要求

5）工业控制系统安全扩展要求

安全通用要求和安全扩展要求的使用场合

安全通用要求针对共性化保护需求提出，等级保护对象无论以何种形式出现，必须根据安全保护等级实现相应级别的安全通用要求—通用要求必须选

+

安全扩展要求针对个性化保护需求提出，需要根据安全保护等级和使用的特定技术或特定的应用场景实现安全扩展要求—

扩展要求根据需要选

=

等级保护对象的保护：

安全通用要求+安全扩展要求

技术方面，强化措施保护

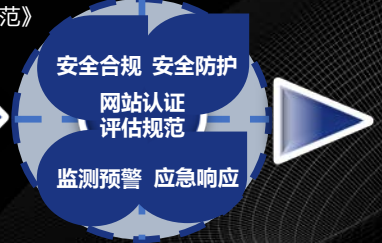
- 强化安全保护技术措施的落实，变被动防护为主动防护，变静态防护为动态防护，变单点防护为整体防控，变粗放防护为精准防护；
- 强化网络日志留存，按照规定留存六个月以上相关网络日志；
- 强化重要数据和个人信息安全保护要求；采取保护措施，保障数据和信息在收集、存储、传输、使用、提供、销毁过程中的安全。

动态防护-网站安全认证

网站安全认证是国家网络与信息系统安全产品质量监督检验中心（公安部第三研究所）针对互联网网站推出认证服务，是针对获取ICP备案的网站从**安全合规、安全防护、应急响应、监测预警**四个维度对网站安全防护能力进行认证评估，评估的结果会随网站的四个维度的落实情况**动态变化**，分为一星认证、二星认证和三星认证三个

- 建立网站安全认证体系
- 制定《网站安全认证评估规范》
- 推出网站认证服务业务

- 执行《网站安全认证评估规范》
- 向客户提供网站认证服务



三星认证证书

二星认证证书

一星认证证书

主动防御

为了提升网站的安全防护能力，获取高级别的星级认证，网站安全防御服务采用“主动防御”的创新模式，直接通过**云部署、硬件部署或软件部署**的方式，**结合用户行为信息搜集**和**代码加密**的手段进行高效的网站安全防御，能有效的分析和识别机器自动化请求并对异常请求阻断，在针对数据安全、交易安全、账户安全等方面的保护上实现**纵深防御**。

典型应用场景

- 防数据自动盗取
- 防批量自动注册
- 防“薅羊毛党”
- 防Web漏洞自动扫描和利用
- 防暴力破解
- 防自动发帖、恶意灌水
- 防非法内容提交
- 防.....

GB/T 28448-2019

《信息安全技术 网络安全等级保护测评要求》

增加测评对象的描述

测评指标:应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换

测评对象:终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等

测评实施包括以下内容:

- 应核查用户在登录时是否采用了身份鉴别措施
- 应核查用户列表确认用户身份标识是否具有唯一性
- 应核查用户配置信息或测试验证是否不存在空口令用户
- 应核查用户鉴别信息是否具有复杂度要求并定期更换

单元判定:如果1)-4)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求

该测评单元包括以下要求

等级保护制度进入2.0时代

《网络安全法》规定“国家实行网络安全等级保护制度”。标志了等级保护制度的法律地位

公安部会同中央网信办、国家保密局和国家密码管理局，联合起草并上报了《网络安全等级保护条例》（征求意见稿）

国家新标准出台并实施

网络安全创新大会
Cyber Security Innovation Summit

THANKS

13916228291
songhh@mctc.org.cn