【深度报告】等级保护 2.0 问题详解

- 2019-05-20 15:05:07
-

转载自：http://www.360.cn/n/10664.html

5 月 13 日，网络安全等级保护技术 2.0 版本（简称等保 2.0）正式公开发布，等保 2.0 覆盖工业控制系统、云计算、大数据、物联网等新技术新应用，为落实信息系统安全工作提供了方向和依据。

关于等级保护 2.0 相关问题，我们来详细了解下。

一、等级保护是什么

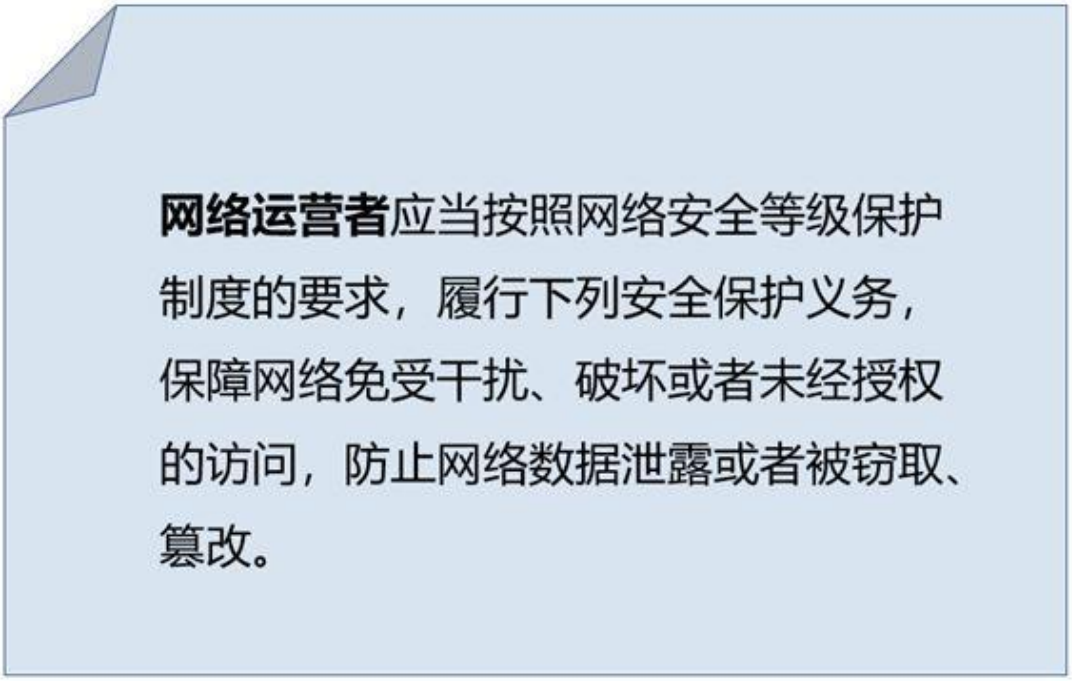
网络安全等级保护是国家信息安全保障的基本制度、基本策略、基本方法。网络安全等级保护工作是对信息和信息载体按照重要性等级分级别进行保护的一种工作。信息系统运营、使用单位应当选择符合国家要求的测评机构，依据《信息安全技术网络安全等级保护基本要求》等技术标准，定期对信息系统开展测评工作。

二、为什么要做等级保护

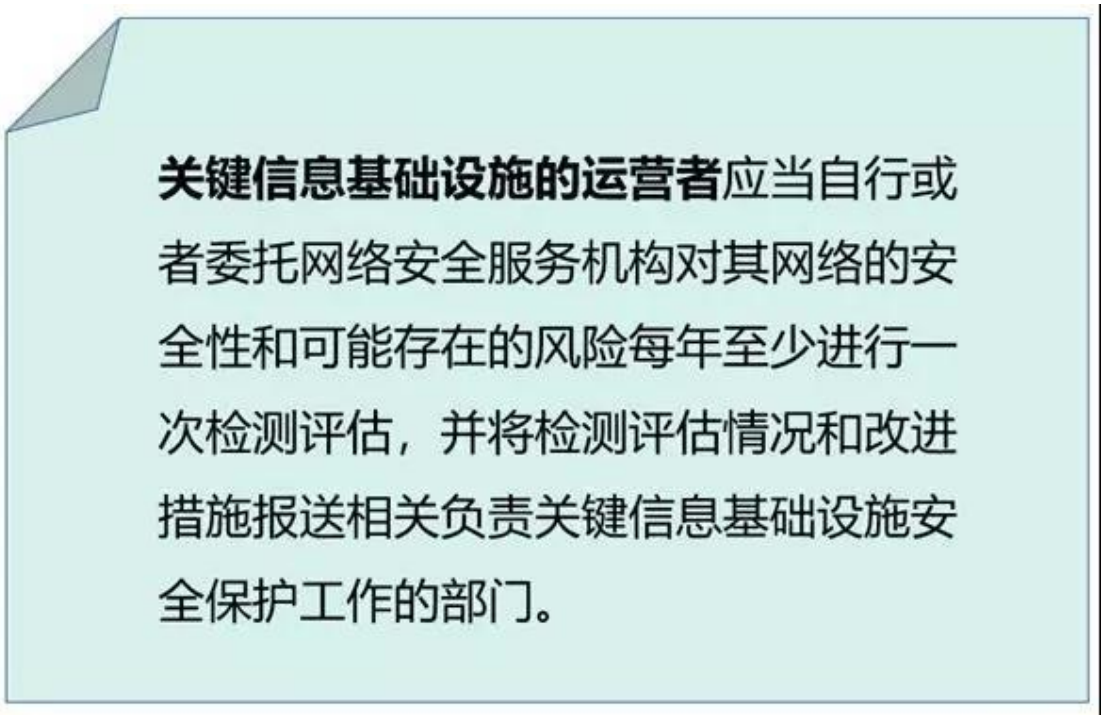
（一）法律规章要求

《网络安全法》明确规定信息系统运营、使用单位应当按照网络安全等级保护制度要求，履行安全保护义务，如果拒不履行，将会受到相应处罚。

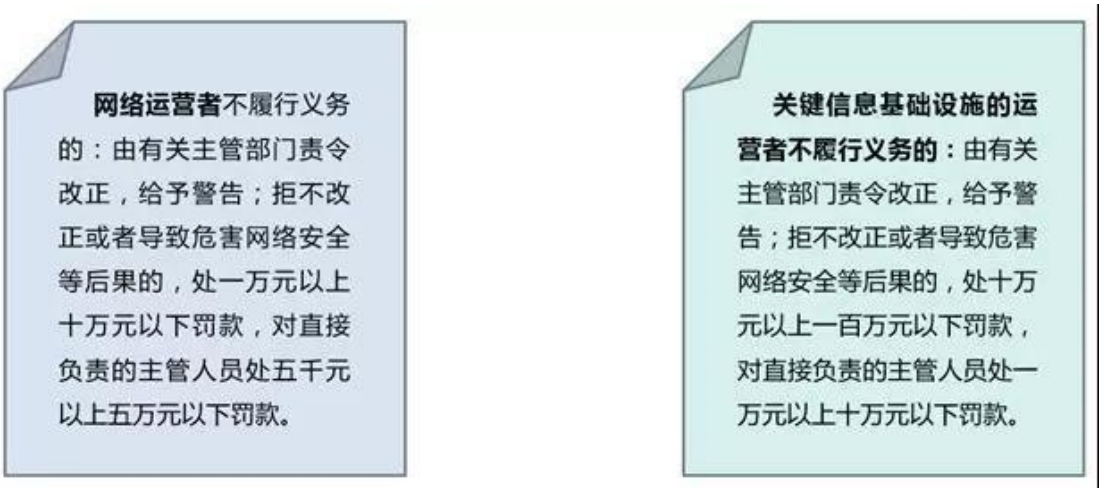
第二十一条规定：



第三十八条规定：



第五十九条规定：



（二）行业要求

在金融、电力、广电、医疗、教育等行业，主管单位明确要求从业机构的信息系统要开展等级保护工作。

（三）企业系统安全的需求

信息系统运营、使用单位通过开展等级保护工作可以发现系统内部的安全隐患与不足之处，可通过安全整改提升系统的安全防护能力，降低被攻击的风险。

三、等级保护涉及范围

（一）省辖市以上党政机关的重要网站和办公信息系统；

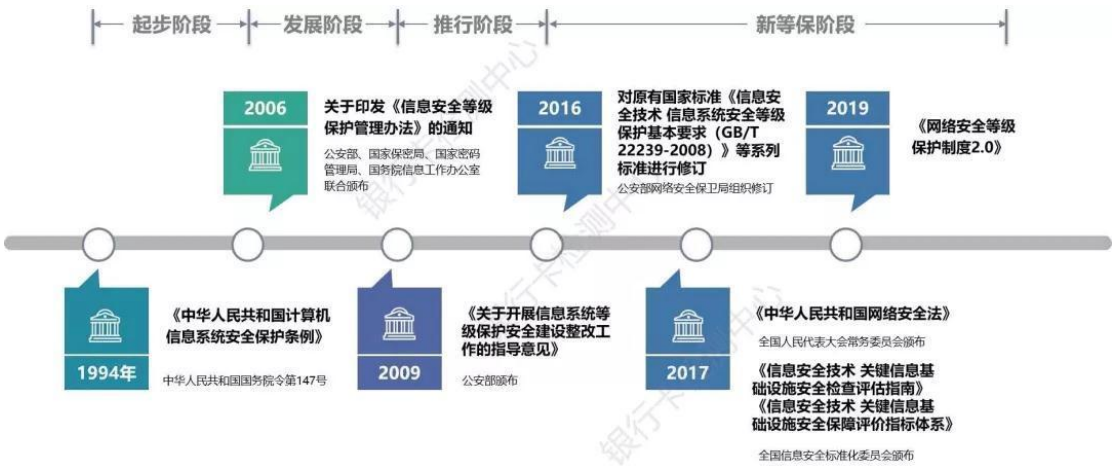
（二）电信、广电行业的公用通信网、广播电规传输网等基础信息网络，经营性公众互联网信息服务单位、互联网接入服务单位、数据中心等单位的重要信息系统；

（三）铁路、银行、海关、税务、民航、电力、证券、保险、外交、科技、发展改革、国防科技、公安、人事劳动和社会保障、财政、审计、商务、水利、国土资源、能源、交通、文化、教育、统计、工商行政管理、邮政等行业、部门的生产、调度、管理、办公等重要信息系统。

四、等级保护发展历程

1994 年，《中华人民共和国计算机信息系统安全保护条例》（国务院 147 号令）规定，“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”，等级保护制度正式被提出。

2016 年 10 月，公安部网络安全保卫局对原有国家标准《信息安全技术信息系统安全等级保护基本要求（GB/T 22239-2008）》等系列标准进行修订。2017 年 6 月，《网络安全法》正式出台，信息安全等级保护过渡到网络安全等级保护，法规明确要求国家实施等保制度。2019 年 5 月，随着《信息安全技术网络安全等级保护基本要求（GB/T 22239-2019）》《信息安全技术网络安全等级保护测评要求（GB/T 28448-2019）》等标准的正式发布，标志着等保 2.0 全面启动。

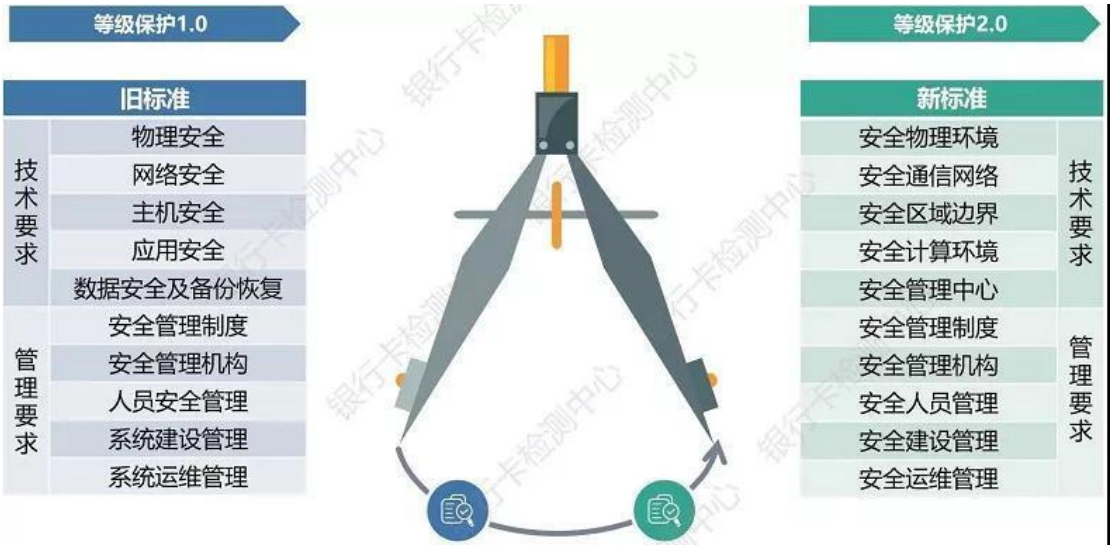


五、等保 1.0 与 2.0 对比

等保 2.0 将原来的标准《信息安全技术信息系统安全等级保护基本要求》改为《信息安全技术网络安全等级保护基本要求》，与《中华人民共和国网络安全法》中的相关法律条文保持一致。

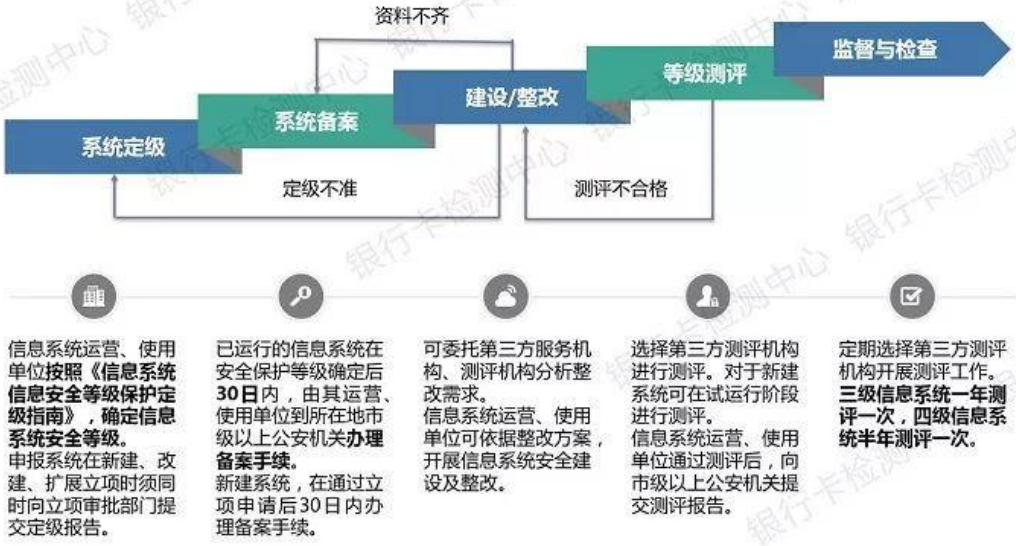
等保 2.0 调整各个级别的安全要求为安全通用要求、云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求和工业控制系统安全扩展要求。

下图为等保 1.0 和等保 2.0 控制措施分类结果的变化：



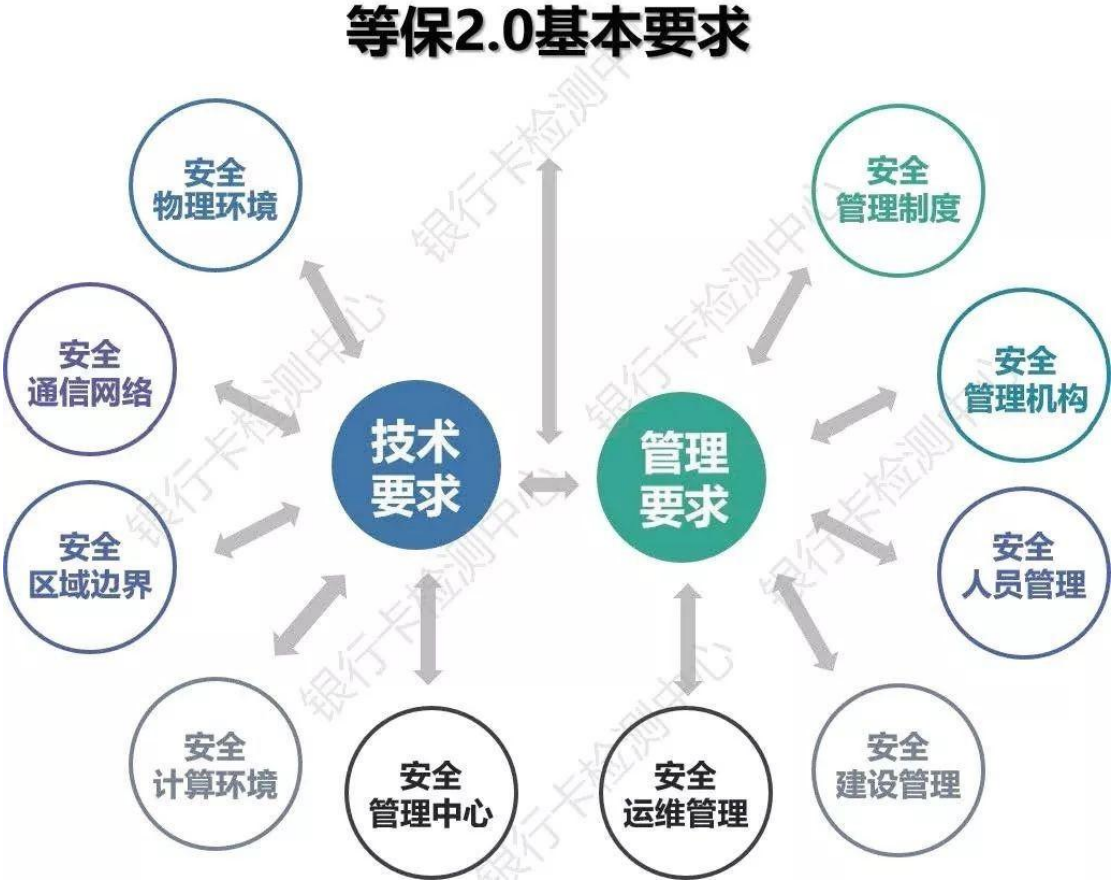
六、等级保护实施过程

等保 2.0 将落实到系统建设全生命周期的每个环节，从系统定级、系统备案、建设/整改、等级测评、再到监督与检查，每一环节都需要系统运营、使用单位重点留意。



七、等保 2.0 的测评内容

等级保护测评分为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全人员管理、安全建设管理、安全运维管理十个层面。



八、开展等级保护的难点

现阶段，信息系统运营、使用单位已意识到等级保护制度的必要性，但在开展等级保护的过程中仍会遇到各式各样的问题与挑战。

九、何种机构能实施等级保护测评

具备由国家网络安全等级保护工作协调小组办公室颁发的网络安全等级保护测评机构推荐证书的机构才能开展等级保护测评工作。

网络安全等级保护制度是国家网络安全领域的基本国策、基本制度和基本方法。随着信息技术的发展和网络安全形势的变化，等级保护制度 2.0 在 1.0 的基础上，注重全方位主动防御、动态防御、整体防控和精准防护，实现了对云计算、大数据、物联网、移动互联和工业控制信息系统等保护对象全覆盖，以及除个人及家庭自建网络之外的领域全覆盖。网络安全等级保护制度 2.0 国家标准的发布，对加强我国网络安全保障工作，提升网络安全保护能力具有重要意义。