广东省网络空间安全协会

网安联
Wang An Lian

抗“疫情”，我们在行动！

众志成城、共克时艰

认清网络安全等级保护2.0
打赢疫情保卫战

2019年12月1日，等级保护2.0正式实施，宣布等级保护2.0时代到来！

（一）

汇报人：张伟

目 录
CONTENTS

01 等保2.0时代来临

02 1.0与2.0的共同点

03 1.0与2.0的不同点

04 对企业或部门有何影响？

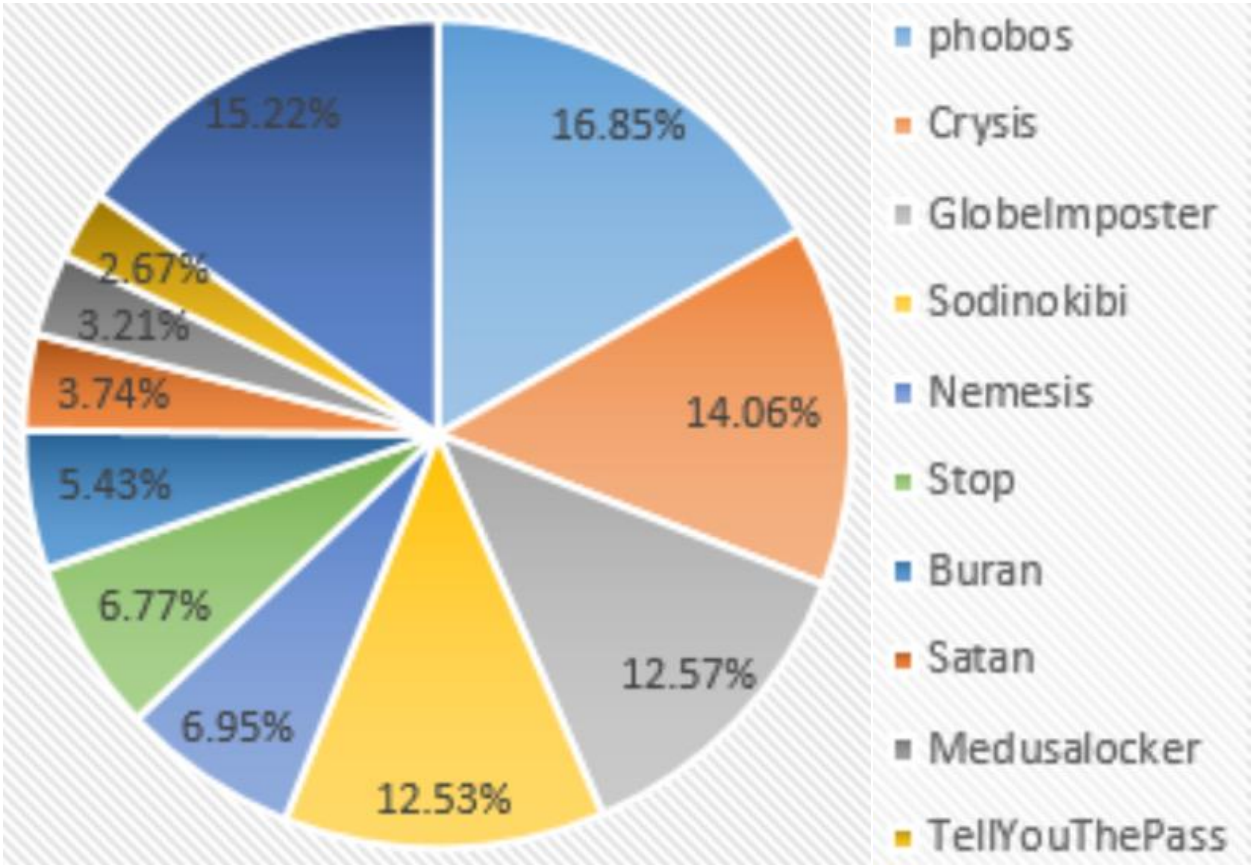
网安联
Wang An Lian

前 言

“疫”情来袭

2020年2月疫情蔓延流向分布

2020年1月勒索病毒家族占比分布



病毒持续发酵，网络安全防控工作如何做？

1月新型冠状病毒感染肺炎疫情的爆发，打响了一场全国人民共克时艰的防疫阻击战，众志成城，病毒疫情蔓延得到一定程度上的有效遏制。在**疫情还未结束、黑客却纷纷复工，网络“黑手”大肆横行，前有利用“冠状病毒”热词攻击外贸航运的间谍木马盗取信息，后有利用论坛传播的“已锁定”勒索病毒兴风作浪，非常时期网络安全隐患不断、网络犯罪日渐飙升，为全行业的网络安全防控带来无比严峻的考验。**

始终把等级保护作为一个部门制度遵守下去！

等保制度规范

等保相关重要标准：

《信息安全技术 网络安全等级保护基本要求》

《信息安全技术 网络安全等级保护定级指南》

《信息安全技术 网络安全等级保护实施指南》

《信息安全技术 网络安全等级保护测评要求》

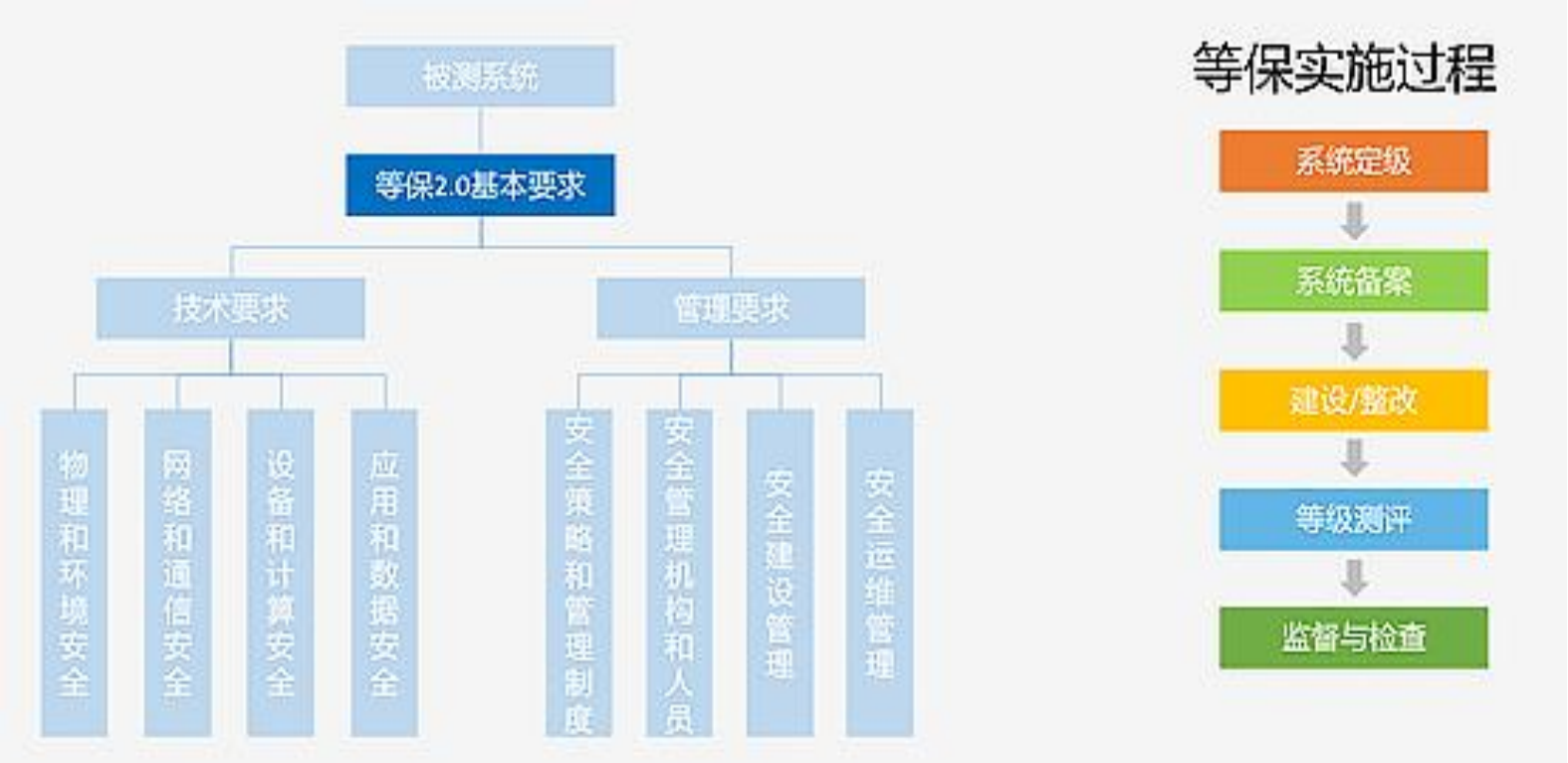
《信息安全技术 网络安全等级保护测评过程指南》

《信息安全技术 网络安全等级保护安全设计技术要求》

《信息安全技术 网络安全等级保护测试评估技术指南》

始终把等级保护作为一个管理要求落到实处！

等保基本要求



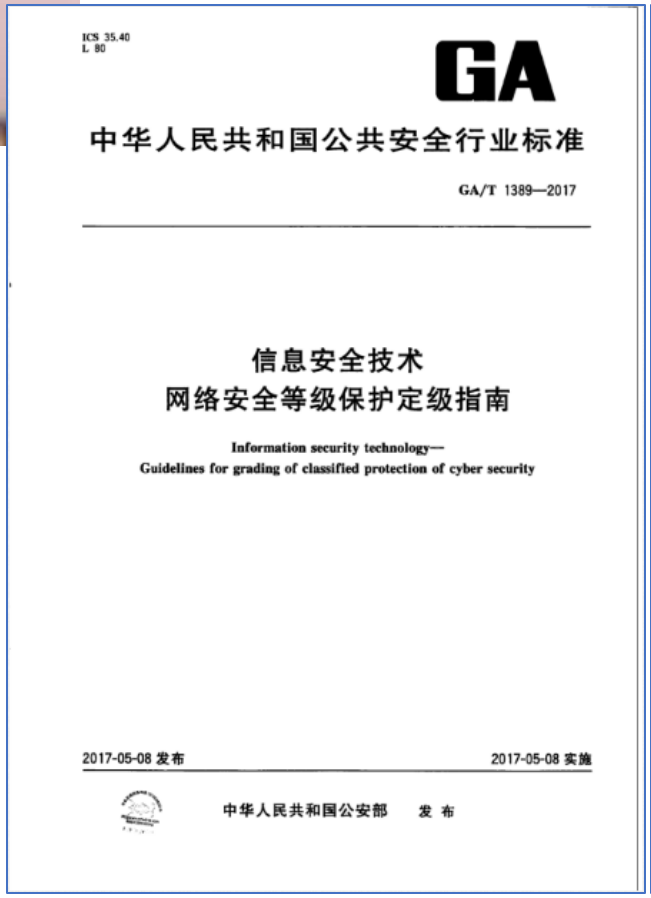
一、

等保2.0时代来临

网安联
Wang An Lian

2019年5月13日，国家市场监督管理总局、国家标准化管理委员会召开新闻发布会，正式发布了等保2.0 相关的国家标准，并于2019年12月1日开始正式实行，则从标准意义上宣告实施了25年的网络安全等级保护（1994年提出）从1.0 跨入2.0 时代。

等保2.0 定级指南



等保2.0 基本要求

等保2.0 安全设计技术要求

等保2.0 测评要求

网络安全等级保护2.0的重要特征

1. 基本的国策制度： 网络安全等级保护制度是我国网络安全领域的基本国策、基本制度；

2. 全流程积极防御： 等级保护标准在1.0时代被动防御的基础上，注重主动防御。从事前、事中、事后实施全流程的安全可信、动态感知和全面审计；

3. 等保对象全覆盖： 实现对传统信息系统、基础信息网络、云计算、大数据、物联网、移动互联网和工业控制信息系统等级保护对象的全覆盖。

二、

1.0与2.0的共同点

网安联
Wang An Lian

等保1.0 和2.0 标准的共同点

A

五个级别不变

B

五项规定动作不变

（定级、备案、整改、测评、监查）

C

主体责任不变

等级保护的概念自1994年提出后，经过20多年的发展和演进，已取得较大成功。从法律意义上看，网络安全法未发布之前称为等保1.0，2017年6月1日网络安全法实施后就成为等保2.0，在2.0时代产生了较大变化。但万变不离其宗，其中等保**五个等级不变、五项工作不变、主体责任不变。**

三、

1.0与2.0的不同点

网安联
Wang An Lian

近年来，随着信息技术的发展和网络安全形势的变化，等保1.0要求已无法有效应对新的安全风险和新技术应用所带来的新威胁，等保1.0被动防御为主的防御无法满足当前发展要求，因此急需建立一套主动防御体系。等保2.0适时而出，从**法律法规、标准要求、安全体系、实施环节**等方面都有了变化。

等保1.0 和2.0 标准的不同点

01

法律法规

02

标准要求

03

安全体系

04

实施环节

01. 标准依据的变化（法规➔ 法律）

从条例法规提升到法律层面 （违规➔犯法）

等保1.0的最高国家政策是国务院147号令，而等保2.0标准的最高国家政策是网络安全法，其中《中华人民共和国网络安全法》第二十一条要求，国家实施网络安全等级保护制度；第二十五条要求，网络运营者应当制定网络安全事件应急预案；第三十一条则要求，关键基础设施，在网络安全等级保护制度的基础上，实行重点保护；第五十九条规定不履行网络安全保护义务的，由有关主管部门给予处罚。**因此不开展等级保护等于犯法。**

02. 标准要求的变化（通用要求➔ 通用+扩展要求）

等级2.0在1.0基本上进行了优化，同时对云计算、大数据、物联网、移动互联网、工业控制新技术提出了新的安全扩展要求。在使用新技术的信息系统需要同时满足**“通用要求+扩展要求”**。且针对新的安全形势提出了新的安全要求，标准覆盖度更加全面，安全防护能力有很大提升。

通用要求方面，等保2.0标准的核心是优化。删除了过时的测评项，对测评项进行合理改写，新增对新型网络攻击行为防护和个人信息保护等新要求，调整了标准结构、将安全管理中心从管理层面提升至技术层面。

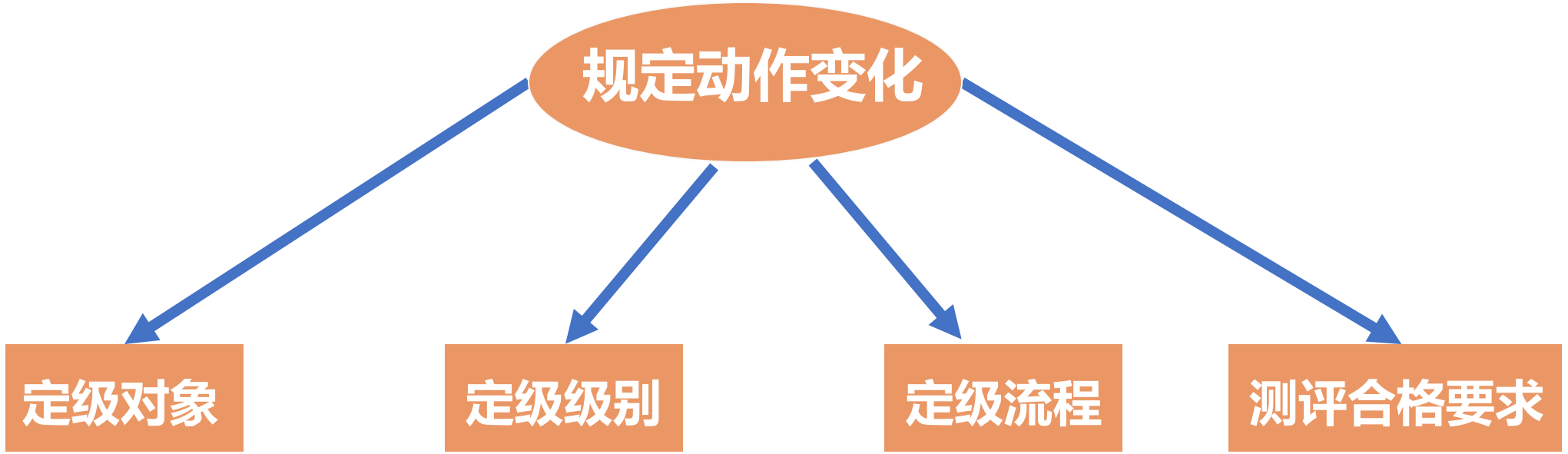
扩展要求扩展了云计算、大数据、物联网、移动互联网、工业控制。

03.安全体系的变化（静态被动防御➔ 主动综合防御体系）

等保2.0相关标准依然采用“**一个中心、三重防护**”的理念，从等保1.0被动防御的安全体系向事前防御、事中响应、事后审计的动态保障体系转变。建立安全**技术体系**和安全**管理体系**，构建具备相应等级安全保护能力的网络安全**综合防御体系**，开展**组织管理、机制建设、安全规划、通报预警、应急处置、态势感知、能力建设、监督检查、技术检测、队伍建设、教育培训和经费保障**等工作。

04.等保实施动作变化（五项规定动作➔优化调整➔内容变了要求高了）

保护**定级、备案、建设整改、等级测评、监督检查**的实施过程中，等保2.0相对1.0对此进行了**优化和调整：**



（04-1）定级对象的变化

等保1.0定级的对象是**信息系统**，等保2.0的定级对象扩展至**基础信息网络、工业控制系统、云计算平台、物联网、使用移动互联技术的网络、其他网络以及大数据**等多个系统平台，覆盖面更广。

（04-2）定级级别的变化

公民、法人和其他组织的合法权益产生**特别严重损害时**，相应系统的等级保护级别从1.0的**第二级调整**到了**第三级**（根据定级指南GA/T 1389-2017，级别调整见后面插图）。

（04-3）定级流程的变化

等保2.0标准不再有自主定级，二级及以上系统定级必须经过专家评审和主管部门审核，才能到公安机关备案，整体定级更加严格。

（04-4）测评合格条件提高

相较于等保1.0，等保2.0测评的标准发生了变化，2.0中**测评结论**分为：**优**（90分及以上）、**良**（80分及以上）、**中**（70分及以上）、**差**（低于70分），70分以上才算基本符合要求，**基本分调高了，测评要求更加严格。**

四、

对企业或部门有何影响？

网安联
Wang An Lian

4.1 责任压实——企业或部门的责任主体更明了、职责分工更细！

主管负责　　运营负责　　使用负责　　网络运营者负责

根据谁主管谁负责、谁运营谁负责、谁使用谁负责的原则，网络运营者成为等级保护的责任主体，如何快速高效地通过等级保护测评成为企业开展业务前必须思考的问题。

4.2 合格更难——等保2.0五个规定动作依旧、标准更高面更广！

等保2.0有**5个运行步骤：定级、备案、建设和整改、等级测评、检查。**同时对等级保护对象按其**重要程度**由低到高**分为5个等级**，并**分别实施不同的保护策略。**

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

4.3 处罚更严——自网络安全法颁布全国已有百起违反等保受罚案件！

自2017年6月1日《网络安全法》正式实施以来，全国各地已发生上百起因违反其中等级保护相关条令而受到执法机关行政处罚的案件。

网络运营者必须按照等级保护制度要求开展**定级备案、等级测评、安全建设、安全检查**等工作，必须**严格对照自身属性和等级分类**，积极开展网络安全等级保护工作，增强网络安全防护能力，切实保障网络运行安全。

4.4 等保2.0才刚开始——过保 =/= 安全免责牌

（临时应付、阶段终结 NO ！）

测评合格条件提高，测评要求更加严格。同时，**等保合规不完全等于信息安全，企业过保并不意味着在安全保障上拿到了免责牌。**

根据网络**安全法**及**等级保护相关要求，企业或单位**必须按照网络安全法要求**严格落实等级保护制度、履行网络安全责任、加强网络安全防护、不断提高网络抗攻击能力**。

4.5 正确认清等保2.0——长期性、策略性

- ✓ **长期性：** 企业或单位应坚持定期开展网络的等级测评、风险评估、渗透测试、安全培训、安全运维、重要时期的安全保障、日常的应急响应和安全通报等工作。通过这些工作夯实网络安全工作的各个层面，提高安全水平和防御能力，保障企业或单位的网络系统长期安全稳定运行；
- ✓ **策略性：**（还是那两句话——事半功倍）

把等级保护作为一个部门制度始终遵守下去！

把等级保护作为一个管理要求始终落到实处！

谢　谢　聆　听　！
打赢疫情安全保卫战！

网安联
Wang An Lian

广东省网络空间安全协会