“等保 2.0”新版本变化分析

e 安教育　2019-05-08 14:27:53

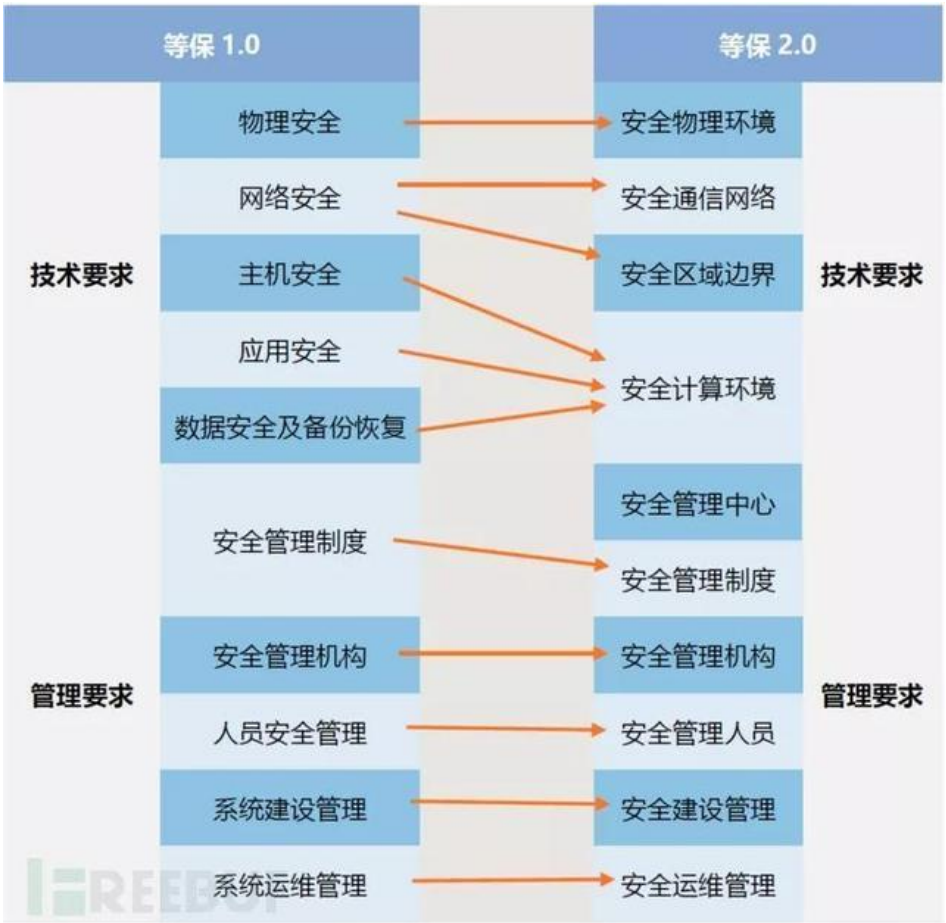
突然发现等保 2.0 最新报批稿的结构又进行了较大改动，和之前的送审稿终板存在较大差异，这里补充说明一下具体变化的情况。

通过和之前的 2.0 标准对比，细节变化其实不大，主要在控制项的结构变化，以及原先删除的一些内容又加回来了。我们先看下最新的结构是什么样的。

新版“等保 2.0”的变化

结构的变化

先看新标准安全通用要求和旧版的变化：



控制大项数量之前是 8 项，现在又变为了 10 项，网络安全拆分为安全通信网络和安全区域边界两个部分，主机安全、应用安全和数据及备份合并到安全计算环境中，新增安全管理中心控制项，经过 2 次改版后，最终是现在的结构。而且各控制大项名称全部变化，与之前的也不同，技术部分减少，管理部分要求增加。

要求项的变化

	等保 1.0			等保 2.0		
要求	基本要求子类	等保二级	等保三级	基本要求子类	等保二级	等保三级
技术要求	物理安全	19	32	安全物理环境	15	22
	网络安全	18	33	安全通信网络	4	8
				安全区域边界	11	20
	主机安全	19	32	安全计算环境	23	34
	应用安全	19	31			
	数据安全	4	8			
管理要求	安全管理制度	7	11	安全管理中心	4	12
				安全管理制度	6	7
	安全管理机构	9	20	安全管理机构	9	14
	人员安全管理	11	16	安全管理人员	7	12
	系统建设管理	28	45	安全建设管理	25	34
	系统运维管理	41	62	安全运维管理	31	48
要求项	/	175	290	/	135	211

新老等保 2.0 的变化

	等保 2.0（旧）			等保 2.0（新）		
要求	基本要求子类	等保二级	等保三级	基本要求子类	等保二级	等保三级
技术要求	物理和环境安全	15	22	安全物理环境	15	22
	网络和通信安全	16	33	安全通信网络	4	8
				安全区域边界	11	20
	设备和计算安全	17	26	安全计算环境	23	34
	应用和数据安全	22	34			
管理要求	安全策略和管理制度	6	7	安全管理中心	4	12
				安全管理制度	6	7
	安全管理机构和人员	16	26	安全管理机构	9	14
				安全管理人员	7	12
	安全建设管理	25	34	安全建设管理	25	34
	安全运维管理	30	48	安全运维管理	31	48
要求项	/	147	230	/	135	211

这其中要求项的细节变化可以对比新旧标准自己看一下，可见通用部分的要求项又减少了，三级减少了 19 项（230->211），二级减少了 12 项（147->135）。

个人信息保护保留，剩余信息保护又回来了，新增**安全管理中心**控制大项（之前是没有的）。

扩展要求的变化

新的版本不再分 5 个单独标准发布，而是整合到一个标准中，用序号标识各扩展要求部分，包括：

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。

经过 2 次改版，可以说扩展要求的 4 个部分又略微简化了，是这样一个结构：

云计算安全扩展要求	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 安全建设管理 安全运维管理
移动互联安全扩展要求	安全物理环境 安全区域边界 安全计算环境 安全建设管理 安全运维管理
物联网安全扩展要求	安全物理环境 安全区域边界 安全计算环境 安全运维管理
工业控制系统安全扩展要求	安全物理环境 安全通信网络 安全区域边界 安全计算环境 安全建设管理

扩展部分要求较之前的送审稿明显减少，也就是说新的标准在各个方面都简化了。

原文中的目录截图如下：

11

等保 2.0 要求项的变化

由于之前已详细解释过，这里只提一下，相较之前，等保 2.0 新版的一些明显要求项变化。

技术要求部分

安全物理环境	**物理和环境安全**变更为**安全物理环境**，要求项无变化。
安全通信网络	**网络和通信安全**变更为**安全通信网络**和**安全区域边界**两个部分，要求项由 33 变为 8+20 项。 将原来的**网络架构**和**通信传输**整合作为**安全通信网络**的要求子类，并新增**可信验证**要求项。 要求：可基于可信根对通信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。 有点类似之前设备和计算安全中对恶意代码防范的要求，不过有变化，这次说明了就是要搞可信计算。
安全区域边界	将原来的**边界防护、访问控制、入侵防范、恶意代码防范和安全审计**整合作为**安全区域边界**的要求子类，新增**可信验证**要求项（要求同上），去掉**集中管控**的要求。 **集中管控**按照之前的描述更像是安全域的划分和管理，所以重新定义安全区域更为合理一些，但这样一来，出现一个问题，要求项里就没有体现安全域划分这样的要求了，而把集中管控移动到了**安全管理中心**中，这个逻辑是怎么样的我也不好说，不过倒也说得通 o(*￣v￣*)o。
安全计算环境	**设备和计算安全**、**应用和数据安全**合并到一起，改为**安全计算环境**，控制项由 26+34 变为 34 项。 感觉可能一下缩减了很多项，应该是考虑到的去重的部分，比如身份鉴别、访问控制在主机和应用的要求是一样的。**身份鉴别**、**访问控制**要求项无变化。安全审计删除一条要求：要求审计记录必须要确定唯一时钟同步保持准确性。（本条现在是四级系统，安全管理中心的要求项） 恶意代码防范要求有所变化： 老版等保 2.0 要求：应采用免受恶意代码攻击的技术措施或采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性检测，并在检测到破坏后进行恢复。 新版等保 2.0 要求：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。 因为新版加入了可信计算的单独要求，所以这里不再重复，也不再要求完整性检测的，此外这里去掉了破坏后恢复的要求，更为合理一些。 同样，本控制项中也增加了可信验证，也就是技术部分除了物理的，都要求可信计算技术。 之前在设备和计算安全部分删除了剩余信息保护的要求，现在两部分合并后，作为统一要求了，不过从之前的老版 2.0 来看，这块其实主要还是重点针对应用部分的，对于主机层面的依旧关系不大。

管理要求部分

再来看管理上，可以说变化比较大的是管理要求，主要在前几个部分，后边的建设和运维基本没变化。

安全管理中心	属于新增的一个控制项，包括：**系统管理**、**审计管理**、**安全管理**和**集中管控**。共计12项要求。 **系统管理** a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计； b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。 **审计管理** a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计； b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。 **安全管理** a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计； b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。 这是新增的要求，强调了系统管理员、审计管理员和安全管理员的重要性，也明确了一些职责上的要求，估计再想兼职其他岗位怕是困难了。具体的要求写得很清楚了，就不在解释。 **集中管控** a）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； b）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； c）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； d）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； e）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； f）应能对网络中发生的各类安全事件进行识别、报警和分析。 这部分要说新增也算不上，就是把其他各部分的一些要求拿过来拼凑成了一个控制项，从整体的角度来要求。a和b就是之前安全域的2条要求，放到这里来了。cd是通信、设备的要求拿了过来，ef有点偏系统运维和应急的东西，之前也是见过，所以这部分为什么单独拿出来也不是很清楚，但也能够理解，现在都在搞统一管理平台，从全公司IT治理和管理的角度来看，也是合理的。
安全管理制度	安全策略和管理制度改为安全管理制度，要求项没有变化，还是7项。
安全管理机构 **安全管理人员**	**安全管理机构和人员**拆分开，成为两个部分，**安全管理机构**和**安全管理人员**。要求没有变化原来26项，现在是14+12项。不知道为什么又分为两个部分，是分久必合，合久必分的意思？
安全建设管理	无变化，名称和要求项数量不变（34项）。
安全运维管理	无变化，名称和要求项数量不变（48项）。

总的来看，变化比较大的是整体结构，其实细节上并没有太多变化，不过既然这么来调整，国家肯定有一定的考虑和道理。

结语

本以为最终送审稿就是最终的正式版，没想到短短几个月改动这么大，照此来看，年内颁布实施怕是不好说了，不过大体的方向和细节没有很大的变化，也不用太过担心，还是以最终发布的正式标准为准。

本文来源：默安科技合规研究小组发表于 FreeBuf