计算机行业专题报告

安全可控系列之一：等保 2.0，催生网络安全新需求

推荐（维持）

- **网络安全等级保护 2.0 标准颁布在即。**从 2015 年开始，国家安标委开始启动等级保护 2.0 标准的制定。2017 年 6 月 1 号开始实施的《网络安全法》第二十一条和第五十九条以网络安全领域基本法的形式确立了国家网络安全等级保护制度，规定了等级保护制度安全措施的基线要求并赋予强制力，同时第三十一条进一步要求关键信息基础设施必须落实国家安全等级保护制度，突出保护重点。2018 年 6 月 27 日，公安部发布《网络安全等级保护条例(征求意见稿)》。2018 年 11 月 9 日，公安部网络安全保卫局总工程师郭启全在 2018 合肥网络安全大会上提到，等保 2.0 标准已在国家安标委最终审批，不日出台。
- **等保 2.0 是网络安全的一次重大升级。**等级保护 2.0 较 1.0 相比，主要变化体现在等级保护工作内容扩展、保护对象扩展、保护力度提升这几个方面。从工作内容上来比较，除了满足等保 1.0 时代定级、备案、建设整改、等级测评和监督检查五个规定动作以外，把风险评估、安全监测、通报预警、案事件调查等方面的工作都纳入到等级保护的范围之内。另外，保护对象也从传统的网络和信息系统，向“云大物智移”上扩展。保护力度上，从原来等保 1.0 的十个安全控制域缩减为 2.0 的八个。总体控制要求，以三级为例控制数量从 290 个点，调整为 231 个点。这些诸多细粒度的变化，从制度层面给用户带来了一次知识更新的要求，同时也是为用户构建更加强大的安全能力提供了体系化的制度保障。
- **回溯等保 1.0 时代，等级保护政策极大促进了信息安全行业的发展。**2007 年《信息安全等级保护管理办法》的发布，标志着等保 1.0 时代正式开启。随后等级保护系列配套政策密集出台，推动信息安全行业景气度快速提升。根据对启明星辰、绿盟科技、卫士通、北信源、蓝盾股份五家信息安全上市企业收入增速（中位数法）的统计，从 2008 到 2011 年我国信息安全厂商收入增速快速提升，我们认为等级保护政策是重要驱动因素之一。
- **等保 2.0，料将催生网络安全新需求。**我们认为等保 2.0 给信息安全行业带来的增量空间主要来自两个方面：1）由于第三级以上的信息系统涉及地市级以上各级政府机关、金融和能源等国家重点行业，为符合等保 2.0 时代国家网络安全等级保护政策的新要求，将进一步加大信息安全产品和服务的投入。2）等保 2.0 把包括传统网络安全、云计算、物联网、移动互联、工业控制、大数据等在内所有新技术纳入监管，比等保 1.0 拓展了一个维度。随着等保 2.0 标准的逐步落实，国内信息安全市场有望迎来更大的发展。
- **投资建议：**等保 2.0 进入落地阶段，将助力网络安全行业景气度进一步提升，具有深厚攻防等核心技术积累及完整解决方案的龙头厂商有望充分受益。推荐启明星辰、深信服，关注北信源、绿盟科技、卫士通。
- **风险提示：**政策落地不及预期；市场竞争加剧。

重点公司盈利预测、估值及投资评级

简称	股价（元）	EPS（元）			PE（倍）			PB	评级
		2018E	2019E	2020E	2018E	2019E	2020E		
启明星辰	21.18	0.65	0.84	1.07	32.58	25.21	19.79	6.06	强推
深信服	84.32	1.75	2.25	2.87	48.18	37.48	29.38	19.53	强推
北信源	3.23	0.10	0.12	0.15	32.3	26.92	21.53	2.12	
绿盟科技	8.79	0.31	0.42	0.56	28.35	20.93	15.70	2.46	
卫士通	19.18	0.20	0.48	0.70	95.9	39.96	27.4	3.74	

资料来源：Wind，华创证券预测（其中，北信源、绿盟科技、卫士通盈利预测来自 wind 一致预期）

注：股价为 2018 年 12 月 10 日收盘价

华创证券研究所

证券分析师：陈宝健
电话：010-66500984
邮箱：chenbaojian@hcyjs.com
执业编号：S0360517060001

证券分析师：邓芳程
电话：021-20572565
邮箱：dengfangcheng@hcyjs.com
执业编号：S0360518080001

联系人：刘逍遥
电话：010-63214650
邮箱：liuxiaoyao@hcyjs.com

行业基本数据

		占比%
股票家数(只)	203	5.69
总市值(亿元)	16,437.41	3.24
流通市值(亿元)	10,886.3	3.0

相对指数表现

%	1M	6M	12M
绝对表现	-0.13	-21.88	-26.52
相对表现	0.58	-5.09	-5.07

相关研究报告

《计算机行业云计算与 AI 双周报:腾讯首次披露云收入超市场预期，云战略地位持续强化》
2018-11-28
《计算机行业周报（20181126-20181130）：等保 2.0，催生网络安全新需求》
2018-12-02
《计算机行业周报（20181203-20181207）：紧跟基本面，布局明年高景气》
2018-12-09

目 录

一、 初识等级保护：关于等级保护的六问六答 4
二、 等级保护制度步入 2.0 时代，保护对象和技术手段等全面升级 7
（一）网络安全等级保护 2.0 标准颁布在即 7
（二）等保 2.0VS 等保 1.0，多方面进行重大升级 8
三、等保 2.0 有望助力网络安全行业迈上新台阶 12
（一）回溯等保 1.0 时代，等级保护政策极大促进了信息安全行业的发展 12
（二）等保 2.0 时代，料将催生网络安全新需求 13
1、为满足等保 2.0 新要求，政府及重点行业有望加大信息安全产品和服务的投入 13
2、等保 2.0 将“云大物智移”纳入监管，进一步拓展了市场空间 14
四、投资建议 17
五、风险提示 17

图表目录

图表 1 等级保护 2.0 工作流程图.....4
图表 2 等保测评等级分类.....5
图表 3 典型关键信息设施定级范例.....5
图表 4 2015 年我国信息安全下游行业需求分布.....6
图表 5 网络安全等级保护制度发展历程.....7
图表 6 新形势下的等级保护.....8
图表 7 等保 2.0 管理策略维度变化.....8
图表 8 等保 2.0 工作内容变化.....9
图表 9 等保 2.0 具体对象.....9
图表 10 等级保护 2.0 标准体系.....10
图表 11 等保 2.0 基本框架变化.....10
图表 12 控制点变化对比表.....11
图表 13 要求项变化对比表.....11
图表 14 等保 2.0 部分技术措施.....11
图表 15 信息安全上市企业收入增速（中位数法）.....13
图表 16 近期部分典型等级保护整改、测评项目.....13
图表 17 信息安全防御体系的变化趋势.....15
图表 18 云服务商和云租户责任划分.....15
图表 19 等保 2.0 物联网扩展要求.....16
图表 20 物联网安全防护体系.....16
图表 21 工控安全控制项的变化.....17

一、初识等级保护：关于等级保护的六问六答

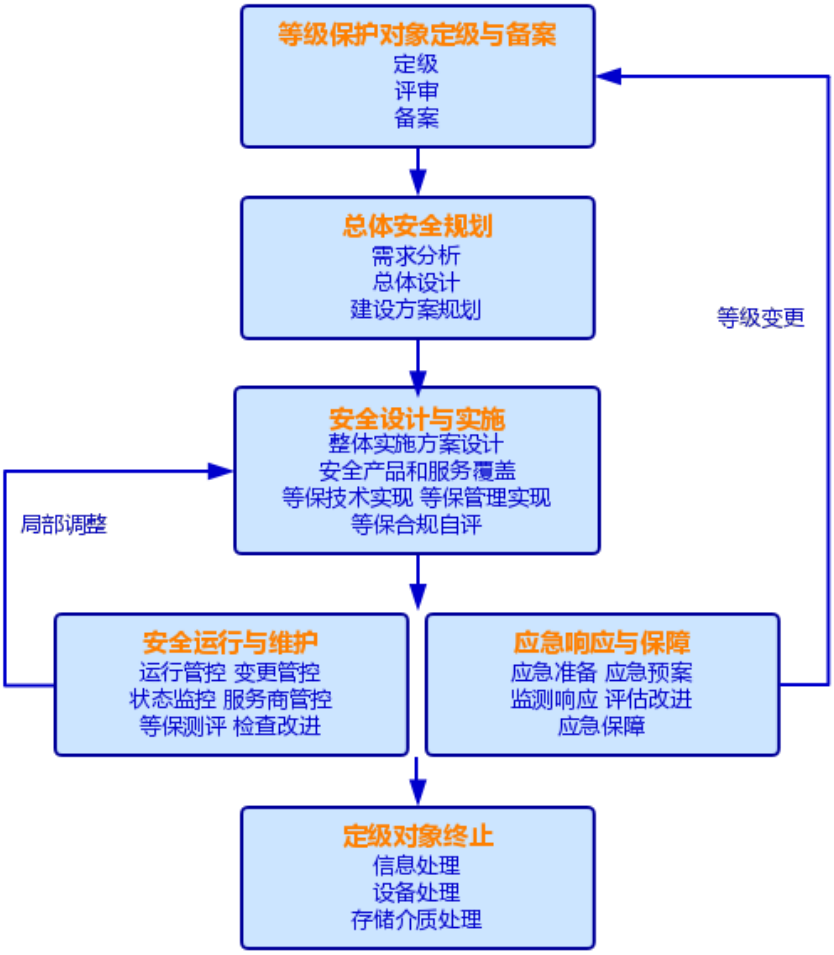
Q1：什么是等级保护？

信息安全等级保护是指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

Q2：等级保护包括哪些流程？

等保 1.0 时代的工作是五个规定动作，定级、备案、建设整改、等级测评和监督检查。在等保 2.0 时代，除了满足以上五个以外，把风险评估、安全监测、通报预警，案事件调查、数据防护、自主可控、供应链安全、效果评价、综治考核等方面的工作都纳入到等级保护的范围之内。

图表 1　等级保护 2.0 工作流程图



资料来源：e 安在线网站、华创证券

Q3：安全保护等级如何划分？

根据等保对象受到破坏时所侵害的客体和对客体造成侵害的程度，网络分为五个安全保护等级，五级是最高级别，系统等级越高，系统越重要，突发事故造成的损害越严重。

第一级，自主保护级。一旦受到破坏会对相关公民、法人和其他组织的合法权益造成损害，但不危害国家安全、社

会秩序和公共利益的一般网络。

第二级，指导保护级。一旦受到破坏会对相关公民、法人和其他组织的合法权益造成严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全的一般网络。

第三级，监督保护级。一旦受到破坏会对相关公民、法人和其他组织的合法权益造成特别严重损害，或者会对社会秩序和社会公共利益造成严重危害，或者对国家安全造成危害的重要网络。

第四级，强制保护级。一旦受到破坏会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害的特别重要网络。

第五级，专控保护级。一旦受到破坏后会对国家安全造成特别严重危害的极其重要网络。

图表 2 等保测评等级分类

等级	对象	侵害客体	侵害程度	各类系统定级参考
第一级（自主保护等级）	一般系统	合法权益	损害	适用于小型私营、个体企业、中小学、乡镇所属信息系统、县级单位中一般的信息系统。
第二级（指导保护等级）		合法权益	严重损害	适用于县级某些单位中的重要信息系统；地市级以上国家机关、企事业单位内部一般的信息系统。例如非涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统等。
		社会秩序和公共利益	损害	
第三级（监督保护等级）	重要系统	社会秩序和公共利益	严重损害	一般适用于地市级以上国家机关、企业、事业单位内部重要的信息系统，例如涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统；跨省或全国联网运行的用于生产、调度、管理、指挥、作业、控制等方面的重要信息系统以及这些系统在省、地市的分支系统；中央各部委、省（区、市）门户网站和重要网站；跨省联接的网络系统等。
		国家安全	损害	
第四级（强制保护等级）		社会秩序和公共利益	特别严重损害	一般适用于国家重要领域、部门中涉及国计民生、国家利益、国家安全，影响社会稳定的核心系统。例如电力生产控制系统、银行核心业务系统、电信核心网络、铁路客票系统、列车指挥调度系统等。
		国家安全	严重损害	
第五级（专控保护等级）	极端重要系统	国家安全	特别严重损害	一般适用于国家重要领域

资料来源：江苏省等级保护测评微信公众号、华创证券

总结来说，信息系统涉及到工作秘密、敏感信息的，信息泄露出去或者被非法篡改、破坏后造成比较大的影响的系统，建议定到三级，其他系统定到二级。另外，涉及到国家安全的，特别是全国性的系统定为四级。

图表 3 典型关键信息设施定级范例

名称	等级	名称	等级
能量管理系统	四级	**广东移动云**	三级

光传送网国际传送网	四级	业务运营支撑系统	三级
中国移动信令网	四级	大额实时支付系统	三级
数据及数据管理系统	四级	网上银行系统	三级
统一权限管理平台	三级	手机银行系统	三级
网站群平台	三级	网上税务系统	三级
生产控制系统	三级	中国疾病预防控制信息系统	三级
中国联通移动通信网	三级	央广网	三级
河南省政务云	三级	北斗星物联网平台	三级

资料来源：e 安在线网站、华创证券

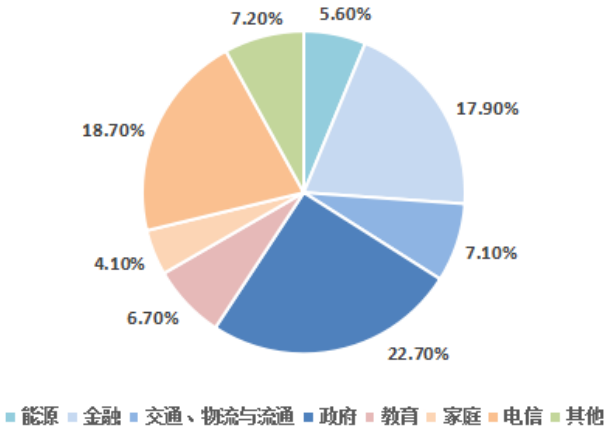
Q4：等保测评周期一般多长？

等保工作是一个持续性工作，等保测评也是周期性工作。**根据等保 2.0 最新要求，第三级以上网络的运营者应当每年开展一次网络安全等级测评，发现并整改安全风险隐患，并每年将开展网络安全等级测评的工作情况及测评结果向备案的公安机关报告。**

Q5：等保测评的重点行业包括哪些？

根据智研咨询 2015 年公布的数据显示，政府、电信以及金融领域分别占据我国信息安全行业下游需求的前三位，合计占比 59.3%，是需要进行等保测评的重点领域。另外由于能源行业的政策特殊性，也是进行等保测评的重点行业。

图表 4　2015 年我国信息安全下游行业需求分布



资料来源：智研咨询、华创证券

Q6：等级保护的主管部门是谁？

中央网络安全和信息化领导机构统一领导网络安全等级保护工作。国家网信部门负责网络安全等级保护工作的统筹协调。国务院公安部门主管网络安全等级保护工作，负责网络安全等级保护工作的监督管理，依法组织开展网络安全保卫。**国家保密行政管理部门**主管涉密网络分级保护工作，负责网络安全等级保护工作中有关保密工作的监督管理。**国家密码管理部门**负责网络安全等级保护工作中有关密码管理工作的监督管理。**国务院其他有关部门**依照有关法律法规的规定，在各自职责范围内开展网络安全等级保护相关工作。**县级以上地方人民政府**依照本条例和有关法律法规规定，开展网络安全等级保护工作。

二、等级保护制度步入 2.0 时代，保护对象和技术手段等全面升级

（一）网络安全等级保护 2.0 标准颁布在即

回顾我国等级保护制度的发展，大致可分为以下三个阶段：

第一阶段：等级保护确立和探索阶段。这个阶段从 1994 年确立计算机信息系统实行安全等级保护制度开始，到 2003 年等级保护从一项计算机信息系统安全保护制度提升至国家信息安全保障基本制度。2004 年至 2006 年，公安部联合四部委开展了涉及 6 万余家单位，共 11 万余信息系统的等级保护基础调查和等级保护试点工作。通过摸底调查和试点，探索开展等级保护工作领导、组织、协调的模式和办法，营造等级保护工作的政策环境，为全面开展等级保护工作奠定了坚实的基础。

第二阶段：等级保护全面实施阶段（等保 1.0 阶段）。历经十多年的探索，2007 年正式启动实施等级保护工作，陆续出台等级保护基本要求、安全设计和测评要求等一系列标准，实现了完善测评体系、开展三级以上系统测评、建设整改等有关等级保护工作的阶段性目标。2010 年以后，金融、电力、教育、医疗、交通等行业监管部门和企事业单位陆续配套相关制度，全面贯彻执行等级保护工作，标志着我国信息安全等级保护工作全面展开，等级保护工作进入规模化推进阶段。

第三阶段：等级保护创新发展阶段（等保 2.0 阶段）。我国网络安全威胁态势日益严峻，网络安全新形势新变化对等级保护工作提出了新要求，云计算、物联网、移动互联、工控系统等新技术新应用的发展不断催生等级保护的模式创新。从 2015 年开始，国家安标委开始启动等级保护 2.0 标准的制定。2017 年 6 月 1 号开始实施的《网络安全法》第二十一条和第五十九条以网络安全领域基本法的形式确立了国家网络安全等级保护制度，规定了等级保护制度安全措施的基线要求并赋予强制力，同时第三十一条进一步要求关键信息基础设施必须落实国家安全等级保护制度，突出保护重点。**2018 年 6 月 27 日，公安部发布《网络安全等级保护条例(征求意见稿)》，正式宣告等保进入 2.0 时代。公安部网络安全保卫局总工程师郭启全在 2018 年 11 月 9 日技术论坛上谈到关于等保最新情况：等保 2.0 标准已在国家安标委最终审批，不日出台。**

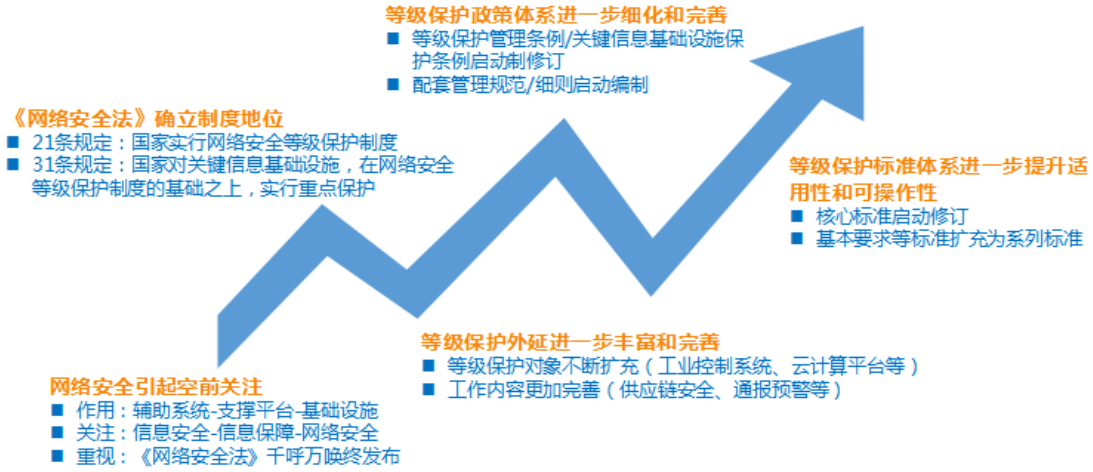
图表 5　网络安全等级保护制度发展历程

时间	事件
1994 年	国务院颁布《中华人民共和国计算机信息系统安全保护条例》（国务院令 147 号），首次提出“计算机信息系统实行安全等级保护”概念
2003 年	中办、国办转发《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）
2007 年	公安部会同国家保密局、国家密码管理局、国务院信息化工作办公室等四部委发布了《信息安全等级保护管理办法》，将信息安全等级保护工作写入法规中
2007 年	浙江省发布了《浙江省信息安全等级保护管理办法》，细化信息安全等级保护工作要求
2008 年	发布《GB/T22239-2008 信息安全技术 信息系统安全等级保护基本要求》，简称为等保 1.0，明确对于各等级信息系统的安全保护基本要求
2015 年	发布《公共安全业务连续性管理体系指南》，针对企业实施业务连续性管理体系中的方法和步骤给出了详细的指导
2016 年	全国人民代表大会常务委员发布《中华人民共和国网络安全法》，标志着网络空间安全治理方面从此有法可依
2017 年	信息安全等级保护制度改为网络安全等级保护制度
2018 年 6 月	公安部向社会发布了《网络安全等级保护条例（征求意见稿）》公开征求意见

资料来源：深信服官网、西部数码官网、华创证券

（二）等保 2.0VS 等保 1.0，多方面进行重大升级

图表 6 新形势下的等级保护



资料来源：深信服官网、华创证券

与等保 1.0 相比，等保 2.0 主要变化体现在以下方面：

➢ **《网络安全法》已经将等级保护制度上升为法律**

原信息安全等保标准叫做“信息安全等级保护制度”，现在叫“网络安全等级保护制度”，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，**等级保护从传统的信息系统层面上升到了网络空间安全的层面。**

➢ **定级方式更加规范化**

等保 2.0 的定级并不是 1.0 标准下的用户自主定级，而是要参照定级指南进行定级，等保工作更加规范化。

图表 7 等保 2.0 管理策略维度变化

资料来源：e 小安微信公众号

➢ **等级保护工作内容扩展**

除了满足等保 1.0 时代定级、备案、建设整改、等级测评和监督检查五个规定动作以外，等保 2.0 把风险评估、安全监测、通报预警、案事件调查等措施都将全部纳入等级保护制度并加以实施。

图表 8 等保 2.0 工作内容变化

资料来源：张振锋，《等级保护 2.0 时代的云等保合规与云安全基本要求解读》、华创证券

➢ **等级保护对象进一步扩展**

等保进入 2.0 时代，保护对象从传统的网络和信息系统，向“云大物智移”上扩展，大型互联网企业、基础网络、重要信息系统、网站、大数据中心、云计算平台、物联网系统、移动互联网、工业控制系统、公众服务平台等都纳入了等级保护的范围。

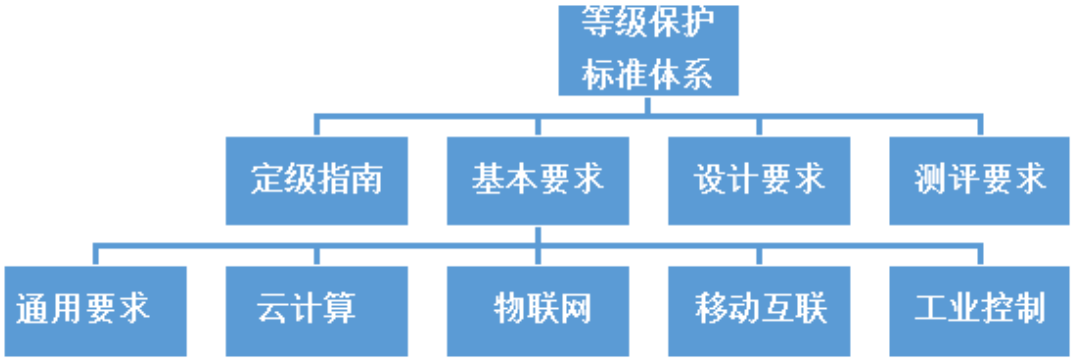
图表 9 等保 2.0 具体对象

资料来源：e 小安微信公众号

➢ **等级保护体系升级**

横向扩展了对云计算、移动互联、物联网、工业控制等新的安全要求；纵向延伸了对等保测评机构的规范管理。

图表 10　等级保护 2.0 标准体系

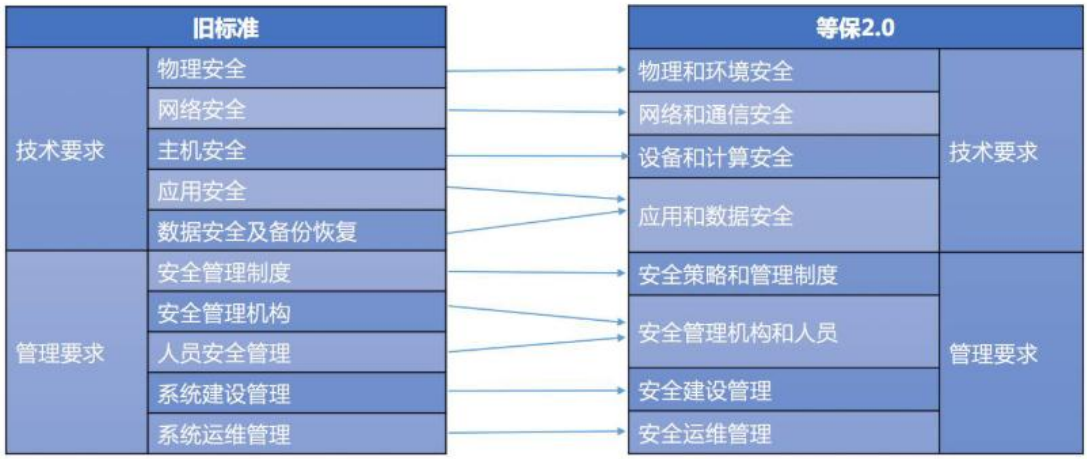


资料来源：华创证券整理

➢ **控制措施分类结构变化**

等保 2.0 依旧保留技术和管理两个维度，而具体要求由 10 个分类调整为 8 个分类。

图表 11　等保 2.0 基本框架变化



资料来源：深信服官网

➢ **标准控制点和要求项变化**

等保 2.0 在控制点要求上并没有明显增加，通过合并整合后相对旧标准略有缩减。

以三级为例，在物理和环境安全控制类下，等保 2.0 控制点未发生变化，要求项由原来的 32 项调整为 22 项；**在网络和通信安全类下，**新标准减少了结构安全、边界完整性安全、网络设备防护三个控制点，增加了网络架构、通信传输、边界防护、集中管控四个控制点，要求项总数还是 33 项，但内容有所变化。**在设备和计算安全类下，**新标准减少了剩余信息保护一个控制点，在测评对象上把网络设备、安全设备也纳入了此层面的测评范围，要求项由原来的 32 项调整为 26 项；**新标准将应用安全、数据安全及备份恢复两个层面合并为应用和数据安全一个层面，**减少了通信完整性、通信保密性、和抗抵赖三个控制点，增加了个人信息保护控制点，要求项则纳入了网络和通信安全层面的通信传输控制点，要求项由原来的 39 项调整为 33 项。

图表 12 控制点变化对比表

旧标准	控制类	二级	三级	四级	等保2.0	控制类	二级	三级	四级
	物理安全	10	10	10		物理和环境安全	10	10	10
	网络安全	6	7	7		网络和通信安全	6	8	8
技术要求	主机安全	6	7	9	技术要求	设备和计算安全	6	6	6
	应用安全	7	9	11		应用和数据安全	9	10	10
	数据安全及备份恢复	3	3	3					
	安全管理制度	3	3	3		安全策略和管理制度	4	4	4
	安全管理机构	5	5	5		安全管理机构和人员	9	9	9
管理要求	人员安全管理	5	5	5	管理要求				
	系统建设管理	9	11	11		安全建设管理	10	10	10
	系统运维管理	12	13	13		安全运维管理	14	14	14
合计	/	66	73	77	合计	/	68	71	71
级差	/	/	7	4	级差	/	/	3	/

资料来源：深信服官网

图表 13 要求项变化对比表

方面	控制类	二级	三级	四级	方面	控制类	二级	三级	四级
	物理安全	19	32	33		物理和环境安全	15	22	24
	网络安全	18	33	32		网络和通信安全	16	33	35
技术要求	主机安全	19	32	36	技术要求	设备和计算安全	17	26	27
	应用安全	19	31	36		应用和数据安全	22	34	38
	数据安全及备份恢复	4	8	11					
	安全管理制度	7	11	14		安全策略和管理制度	6	7	7
	安全管理机构	9	20	20		安全管理机构和人员	16	26	29
管理要求	人员安全管理	11	16	18	管理要求				
	系统建设管理	28	45	48		安全建设管理	25	34	35
	系统运维管理	42	62	70		安全运维管理	31	49	51
合计	/	175	290	318	合计	/	148	231	246
级差	/	/	115	28	级差	/	/	83	15

资料来源：深信服官网

➢ 技术保障体系升级

旧标准更偏重于对于防护的要求，而等保 2.0 标准，结合近些年网络与信息技术的新变化，补充提出了对云计算、物联网、移动互联网和工业控制系统的安全防护要求，更适应当前网络安全形势的发展，结合《网络安全法》中对于持续监测、威胁情报、快速响应类的要求提出了具体的落地措施。

图表 14 等保 2.0 部分技术措施

分类	安全控制点	等保三级要求内容	应对思路
网络和通信安全	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未知的新型网络攻击的检测和分析。	部署安全防护设备能够对新型网络攻击进行检测和分析，对未知威胁检测需具备云端未知威胁分析引

			擎，并实现本地防护设备能与云引擎进行联动的功能。具备**与云引擎联动分析的下一代防火墙**或安全感知平台可满足此要求。
	集中管控	应能对网络中发生的各类安全事件进行识别、报警和分析。	部署能够**对网络中发生的各类安全事件进行识别、报警和分析**的安全防护设备可以满足此要求，如安全感知平台。
	边界防护	应能够对内部用户非授权联到外部网络的行为进行限制或检查。	新提出从内到外网络的行为进行限制或检查，传统防火墙无法满足此类要求，必须采用**具有双向检测能力的下一代防火墙**或上网行为管理检测非法无线共享来满足。
		应限制无线网络的使用，确保无线网络通过受控的边界防护设备接入内部网络。	必须在无线网络边界增加安全防护设备。
	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。	新增对远程访问用户及互联网访问用户行为单独进行审计分析，数据中心的服务器如果可以访问互联网或需要进行远程管理或访问，徐亚在互联网出口单独部署上网行为管理或 VPN。
设备和计算安全	入侵防范	因能够检测到对重要节点进行入侵行为，并在发生严重入侵事件时提供报警。	应在**重要节点部署检测探针**，能够检测到对重要节点进行入侵的行为，将**日志汇总安全感知平台进行分析**，并在发生严重入侵事件时提供报警。

资料来源：深信服官网、华创证券

这些诸多细粒度的变化，从制度层面给用户带来了一次知识更新的要求，同时也是为用户构建更加强大的安全能力提供了体系化的制度保障。可以说，等级保护 2.0 是一次网络安全的重大升级。

三、等保 2.0 有望助力网络安全行业迈上新台阶

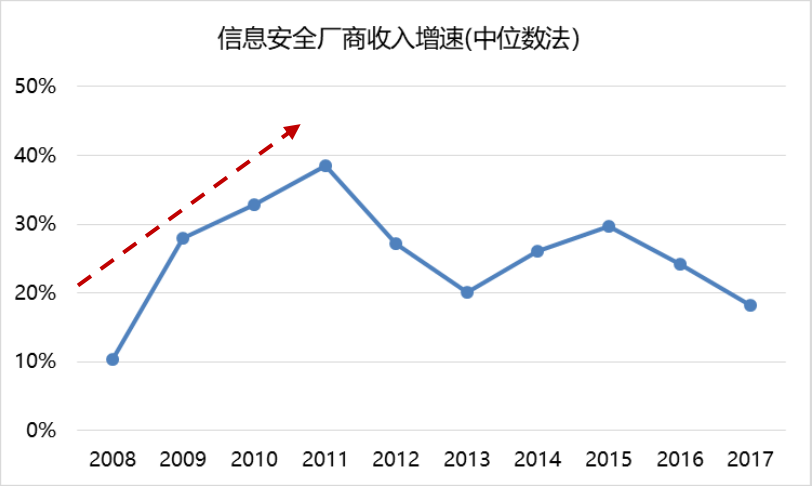
（一）回溯等保 1.0 时代，等级保护政策极大促进了信息安全行业的发展

等保 1.0 给信息安全行业带来广阔市场空间。由于第三级以上的信息系统涉及地市级以上各级政府机关、金融和能源等国家重点行业，为符合国家信息安全等级保护政策，其必然要加大信息安全产品和服务的投入。**根据卫士通的招股说明书中的阐述，“按照国家等级保护和分级保护相关政策要求，约有上万个等级、分级保护系统需要通过测评、认证和规划建设，这两个市场约有 100 亿以上的规模”**。

等级保护系列政策的密集出台，推动信息安全行业景气度提升。2007 年《信息安全等级保护管理办法》的发布，标志着等保 1.0 时代正式开启。此后配套政策、文件与标准密集出台，对等级保护的要求，流程，甚至时间节点做出了规定。例如 2010 出台的《关于推动信息安全等级保护测评体系和开展等级测评工作的通知》中，明确规定“2010 年底前完成测评体系建设，并完成 30%第三级（含）以上信息系统的测评工作，2011 年底前完成第三级（含）以上

信息系统的测评工作，2012 年底前完成第三级（含）以上信息系统的安全建设整改工作”。**随着等级保护系列政策的出台，信息安全行业的景气度也在快速提升。根据对启明星辰、绿盟科技、卫士通、北信源、蓝盾股份五家信息安全上市企业收入增速（中位数法）的统计和分析，我们发现：1）从 2008 到 2011 年我国信息安全厂商收入增速快速提升，我们认为等级保护政策是信息安全景气度提升的重要驱动因素之一。2）2014-2015 年信息安全行业再次迎来高速增长，一个重要原因就在于 2013 年斯诺登“棱镜门”事件爆发，“信息安全”和“自主可控”被提升到了国家战略高度，政府及企业对信息安全的重视程度空前，推动整个行业的高景气。**

图表 15　信息安全上市企业收入增速（中位数法）



资料来源：Wind、华创证券

（二）等保 2.0 时代，料将催生网络安全新需求

随着等保 2.0 标准的逐步落实，国内信息安全产品市场将迎来更大的发展。我们认为等保 2.0 给信息安全行业带来的增量空间主要来自两个方面：1）第三级以上的信息系统为符合等保 2.0 时代国家信息安全等级保护政策的新要求，将进一步加大信息安全产品和服务的投入。2）等保 2.0 把包括传统网络安全、云计算、物联网、移动互联、工业控制、大数据等新业态也纳入监管，实际上比等保 1.0 拓展了一个维度。

1、为满足等保 2.0 新要求，政府及重点行业有望加大信息安全产品和服务的投入

等保 2.0 对于等级保护工作提出新的要求，第三级以上的信息系统涉及地市级以上各级政府机关、金融和能源等国家重点行业，为符合国家信息安全等保 2.0 的要求，需要对信息系统重新进行定级、备案、建设整改、等级测评和监督检查等工作，将加大信息安全产品和服务的投入。**据了解，目前已经有一些政府机构及重点行业企业针对等保 2.0 的要求进行等级保护整改、测评。**

图表 16　近期部分典型等级保护整改、测评项目

项目名称	日期	项目金额（万元）	项目内容	中标厂商
财政部会计资格评价中心网络信息安全服务项目	2018.12.10	60.0	对会计评价中心现有网站、网上报名系统、考试监控平台等信息系统进行每年 4 次网络安全风险评估和安全加固。此外，还需要对会计评价中心信息系统进行网络安全监控，提供信息安全应急响应、预警通告等安全服务，**协助会计评价中心指导信息系统建设商开展等级保护三级测评工作。**	北京启明星辰信息安全技术有限公司
北京市教育网络和	2018.12.07	359.2	拟对运营使用的 38 个信息系统开展年度测评工作	公安部第三研

项目名称	日期	项目金额（万元）	项目内容	中标厂商
信息安全统筹建设				究所
黔南法院系统等级保护平台系统整改设备及运行服务	2018.12.07	357.7	包括等级保护整改设备和系统等级保护运维服务	贵阳昌南科技有限责任公司、贵阳宏图科技有限公司
广东省阳江监狱信息安全等级保护建设项目	2018.12.05	166.0	监管改造系统、刑罚执行系统达到信息系统安全等级保护“第三级基本要求”和“第三级安全保护能力”，罪犯考核系统、狱情排查与处置系统、狱务公开系统、罪犯生活信息系统、内网网站、罪犯危险性评估系统、会见系统、心理矫治系统等 8 套系统达到信息系统安全等级保护“第二级基本要求”和“第二级安全保护能力”，全面提高阳江监狱信息安全管理水平和控制能力	广东瑞普科技股份有限公司
西藏自治区省级审计数据分中心机房等级保护四级加固和审计指挥室建设项目	2018.12.05	333.53	-	北京天大清源通信科技股份有限公司
环保厅信息安全等级保护整改、测评及应急响应采购项目	2018.10.12	44.6	网站安全监测服务、源代码审计服务、渗透测试服务、新业务系统上线前安全检查服务、信息化管理制度的梳理建设服务等	北京启明星辰信息安全技术有限公司
徽商银行 2018 年互联网相关系统安全测评服务项目	2018.09.03	48.5	-	北京神州绿盟科技有限公司
汉中市政府网站群等系统等级保护安全服务采购项目	2018.06.22	56.2	政府网站群等系统等级保护安全测评服务	北京启明星辰信息安全技术有限公司

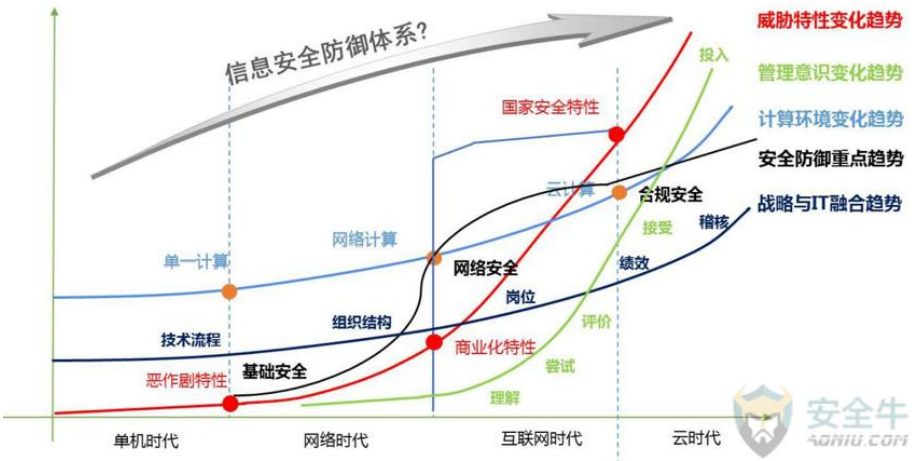
资料来源：政府采购网、华创证券

2、等保 2.0 将“云大物智移”纳入监管，进一步拓展了市场空间

➢ 云安全等级保护

等级保护工作进入 2.0 时代，等级保护对象从原来单纯的信息系统拓展到了很多个领域，其中云计算系统是等级保护重点要关注的领域。

图表 17 信息安全防御体系的变化趋势



资料来源：安全牛

云等保框架下，尤其需要对云计算环境中的安全责任进行明确。IaaS 服务下，云服务方责任硬件及虚拟化层的防护；云租户负责虚拟化以上的客户机的安全防护，数据库防护以及中间件和应用及数据的防护。PaaS 服务模式下，客户虚拟机的安全防护责任交给了云服务商，云租户负责软件开发平台中间件以及应用和数据本身的安全防护。SaaS 服务模式下，责任进一步上移，云租户只需要关心一些应用的简单的安全配置相关以及数据安全的防护。而数据安全防护，无论 IaaS、PaaS 到 SaaS，对于云租户来讲，是始终要面对的重要问题。

图表 18 云服务商和云租户责任划分

资料来源：安华金和官网

- **物联网安全等级保护**

等保 2.0 物联网部分主要扩展了感知层的安全要求，在物理和环境安全、网络和通讯安全、设备和计算安全，以及应用和数据安全做了扩展要求。

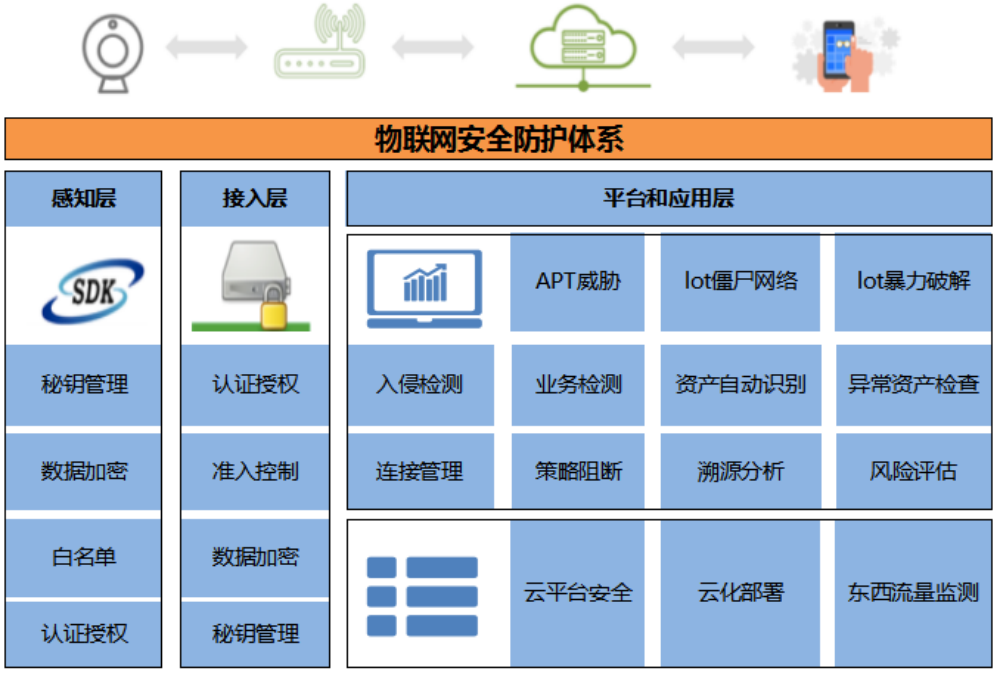
图表 19　等保 2.0 物联网扩展要求

等保2.0物联网扩展要求					
类别	子类	第一级	第二级	第三级	第四级
物理和环境安全	感知节点设备物理防护	增加	增加	增加	增加
网络和通讯安全	入侵防范	/	增加	增加	增加
	接入控制	增加	增加	增加	增加
设备和计算安全	感知节点设备安全	/	/	增加	增加
	网关节点设备安全	/	/	增加	增加
应用和数据安全	抗数据重放	/	/	增加	增加
	数据融合处理	/	/	增加	增加

资料来源：绿盟科技、华创证券

等保 2.0 物联网扩展要求，大部分条款是针对感知节点，然而，标准强调物联网系统定级的整体性。因此，物联网安全需要体系化建设，需要涵盖物联网的感知层、平台层、应用层和网络层。物联网安全防护体系，既包括等保 2.0 中所要求的传统安全，也能涵盖扩展后对感知设备层面的安全要求。

图表 20　物联网安全防护体系



资料来源：安全牛、华创证券

➢ **工控安全等级保护**

工业控制系统安全扩展要求：1）物理和环境安全：增加了对室外控制设备的安全防护要求，如放置控制设备的箱体或装置以及控制设备周围的环境；

2）网络和通信安全：增加了适配于工业控制系统网络环境的网络架构安全防护要求、通信传输要求以及访问控制要

求，增加了拨号使用控制和无线使用控制的要求；

3）设备和计算安全：增加了对控制设备的安全要求，控制设备主要是应用到工业控制系统当中执行控制逻辑和数据采集功能的实时控制器设备，如 PLC、DCS 控制器等；

4）安全建设管理：增加了产品采购和使用和软件外包方面的要求，主要针对工控设备和工控专用信息安全产品的要求，以及工业控制系统软件外包时有关保密和专业性的要求；

5）安全运维管理：调整了漏洞和风险管理、恶意代码防范管理和安全事件处置方面的需求，更加适配工业场景应用和工业控制系统。

图表 21　工控安全控制项的变化

安全要求	控制项	一级	二级	三级	四级
技术要求	物理和环境安全	7	15	22	23
	网络和通信安全	7	15	33	33
	设备和计算安全	7	17	26	26
	应用和数据安全	8	22	34	37
管理要求	安全策略和管理制度	1	6	7	7
	安全管理机构和人员	7	16	26	29
	安全建设管理	9	23	34	35
	安全运维管理	13	31	49	51
合计（等保 2.0）		**59**	**145**	**231**	**241**
合计（等保 1.0）		85	175	290	318
工业控制系统安全扩展要求		**10**	**18**	**26**	**27**

资料来源：安全牛、华创证券

四、投资建议

等保 2.0 进入落地阶段，将助力网络安全行业景气度进一步提升，具有深厚攻防等核心技术积累及完整解决方案的龙头厂商有望充分受益。推荐启明星辰、深信服，关注北信源、绿盟科技、卫士通。

五、风险提示

政策落地不及预期；市场竞争加剧。

计算机组团队介绍

组长、首席分析师：陈宝健

清华大学计算语言学硕士。曾任职于国泰君安证券、安信证券。2017 年加入华创证券研究所。2015 年新财富最佳分析师第 2 名团队成员，2016 年新财富最佳分析师第 6 名团队成员。

分析师：邓芳程

华中科技大学硕士。曾任职于长江证券。2017 年加入华创证券研究所。

助理研究员：刘逍遥

中国人民大学管理学硕士。2018 年加入华创证券研究所。

华创证券机构销售通讯录

地区	姓名	职　务	办公电话	企业邮箱
北京机构销售部	张昱洁	北京机构销售总监	010-66500809	zhangyujie@hcyjs.com
	杜博雅	销售经理	010-66500827	duboya@hcyjs.com
	侯春钰	销售经理	010-63214670	houchunyu@hcyjs.com
	侯斌	销售助理	010-63214683	houbin@hcyjs.com
	过云龙	销售助理	010-63214683	guoyunlong@hcyjs.com
	刘懿	销售助理	010-66500867	liuyi@hcyjs.com
广深机构销售部	张娟	所长助理、广深机构销售总监	0755-82828570	zhangjuan@hcyjs.com
	王栋	高级销售经理	0755-88283039	wangdong@hcyjs.com
	汪丽燕	高级销售经理	0755-83715428	wangliyan@hcyjs.com
	罗颖茵	销售经理	0755-83479862	luoyingyin@hcyjs.com
	段佳音	销售经理	0755-82756805	duanjiayin@hcyjs.com
	朱研	销售助理	0755-83024576	zhuyan@hcyjs.com
	杨英伟	销售助理	0755-82756804	yangyingwei@hcyjs.com
上海机构销售部	石露	华东区域销售总监	021-20572588	shilu@hcyjs.com
	沈晓瑜	资深销售经理	021-20572589	shenxiaoyu@hcyjs.com
	朱登科	高级销售经理	021-20572548	zhudengke@hcyjs.com
	杨晶	高级销售经理	021-20572582	yangjing@hcyjs.com
	张佳妮	销售经理	021-20572585	zhangjiani@hcyjs.com
	沈颖	销售经理	021-20572581	shenying@hcyjs.com
	乌天宇	销售经理	021-20572506	wutianyu@hcyjs.com
	汪子阳	销售经理	021-20572559	wangziyang@hcyjs.com
	柯任	销售经理	021-20572590	keren@hcyjs.com
	何逸云	销售经理	021-20572591	heyiyun@hcyjs.com
	张敏敏	销售经理	021-20572592	zhangminmin@hcyjs.com
	蒋瑜	销售助理	021-20572509	jiangyu@hcyjs.com

华创行业公司投资评级体系(基准指数沪深 300)

公司投资评级说明:

强推：预期未来 6 个月内超越基准指数 20%以上;
推荐：预期未来 6 个月内超越基准指数 10%－20%;
中性：预期未来 6 个月内相对基准指数变动幅度在-10%－10%之间;
回避：预期未来 6 个月内相对基准指数跌幅在 10%－20%之间。

行业投资评级说明:

推荐：预期未来 3-6 个月内该行业指数涨幅超过基准指数 5%以上;
中性：预期未来 3-6 个月内该行业指数变动幅度相对基准指数-5%－5%;
回避：预期未来 3-6 个月内该行业指数跌幅超过基准指数 5%以上。

分析师声明

每位负责撰写本研究报告全部或部分内容的分析师在此作以下声明:

分析师在本报告中对所提及的证券或发行人发表的任何建议和观点均准确地反映了其个人对该证券或发行人的看法和判断;分析师对任何其他券商发布的所有可能存在雷同的研究报告不负有任何直接或者间接的可能责任。

免责声明

华创证券研究所

北京总部	广深分部	上海分部
地址：北京市西城区锦什坊街 26 号 恒奥中心 C 座 3A	地址：深圳市福田区香梅路 1061 号 中投国际商务中心 A 座 19 楼	地址：上海浦东银城中路 200 号 中银大厦 3402 室
邮编：100033	邮编：518034	邮编：200120
传真：010-66500801	传真：0755-82027731	传真：021-50581170
会议室：010-66500900	会议室：0755-82828562	会议室：021-20572500