国盟信息安全通报

2020 年 3 月 30 日第 212 期

全国售后服务中心

国盟信息安全通报

（第 212 期）

国际信息安全学习联盟

2020 年 03 月 30 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 365 个，其中高危漏洞 103 个、中危漏洞 172 个、低危漏洞 90 个。漏洞平均分值为 5.49。本周收录的漏洞中，涉及 0day 漏洞 112 个（占 30%），其中互联网上出现“CentOS Web Panel SQL 注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2662 个，与上周（2537 个）环比增加 5%。

主要内容

一、概述 4
二、安全漏洞增长数量及种类分布情况 4
➢漏洞产生原因（2020 年 03 月 15 日—2020 年 03 月 30）.....4
➢漏洞引发的威胁（2020 年 03 月 15 日—2020 年 03 月 30）.....5
➢漏洞影响对象类型（2020 年 03 月 15 日—2020 年 03 月 30）.....5
三、安全产业动态 6
➢我国网络安全产业现状、问题与发展.....6
➢个人金融信息安全技防研究.....13
➢网络安全等级保护 2.0 云计算安全合规能力模型.....20
➢2019 全球数据与信息治理回顾与前瞻.....30
四、政府之声 37
➢2020 年网络扶贫工作要点印发实施.....37
➢工业和信息化部办公厅关于推动工业互联网加快发展的通知.....39
➢十一部门印发《整治虚假违法广告部际联席会议 2020 年工作要点》.....40
➢工业和信息化部关于推动 5G 加快发展的通知.....41
五、本期重要漏洞实例 44
➢Adobe ColdFusion 任意文件读取安全漏洞.....44
➢VMware Workstation vmnetdhcp.exe 组件资源管理错误漏洞.....44
➢WordPress-5.3.2 up***.php 文件存在文件上传漏洞.....45
➢Microsoft Edge 内存破坏漏洞.....45
六、本期网络安全事件 46
➢团伙冒充农商行行长行骗被识破！竟有银行“内鬼”协助.....46
➢工信部就新浪微博 App 数据泄露问题开展问询约谈.....47
➢京沪 50 余万条学生个人信息遭侵犯.....48
➢自贡 11 万条小区业主信息被卖 男子获刑并处罚金.....49
➢女黑客盗取 GPU 源码勒索 AMD 开口就是 1 亿美元.....51
➢信息安全又现漏洞，智能手机传感器竟成“窃听器”.....53

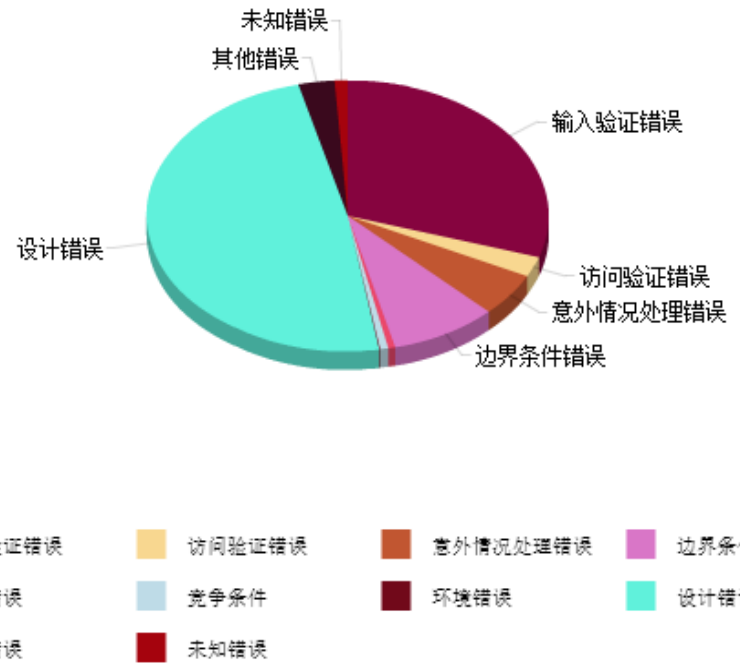
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

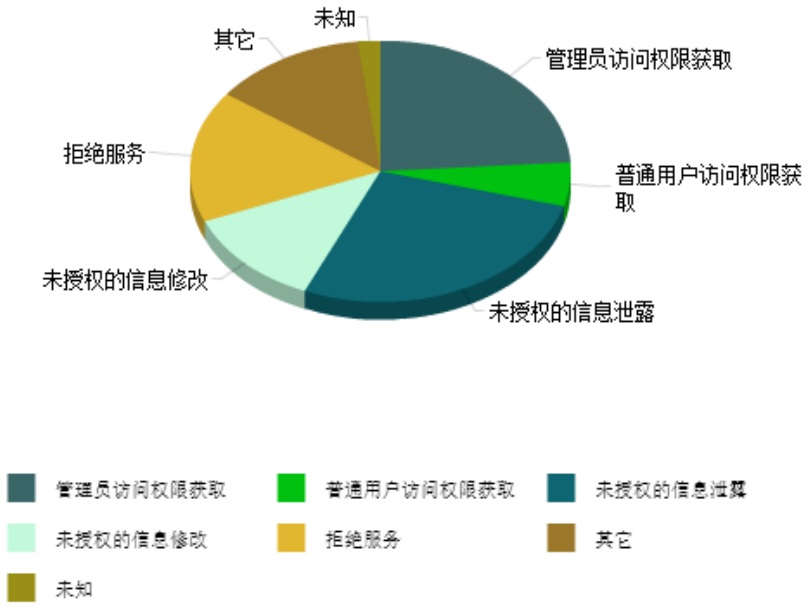
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 365 个，其中高危漏洞 103 个、中危漏洞 172 个、低危漏洞 90 个。漏洞平均分值为 5.49。本周收录的漏洞中，涉及 0day 漏洞 112 个（占 30%），其中互联网上出现“CentOS Web Panel SQL 注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2662 个，与上周（2537 个）环比增加 5%。

二、安全漏洞增长数量及种类分布情况

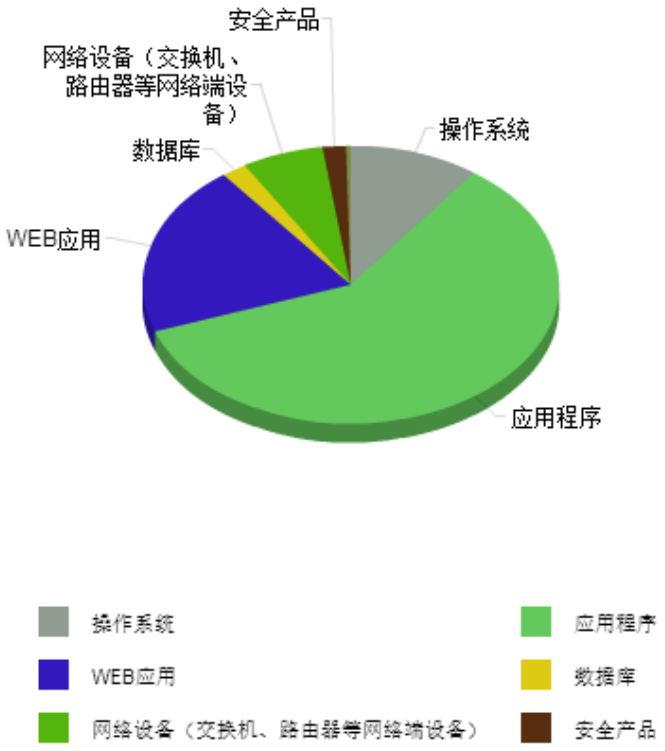
➢ 漏洞产生原因（2020 年 03 月 15 日—2020 年 03 月 30）



➢ 漏洞引发的威胁（2020 年 03 月 15 日—2020 年 03 月 30）



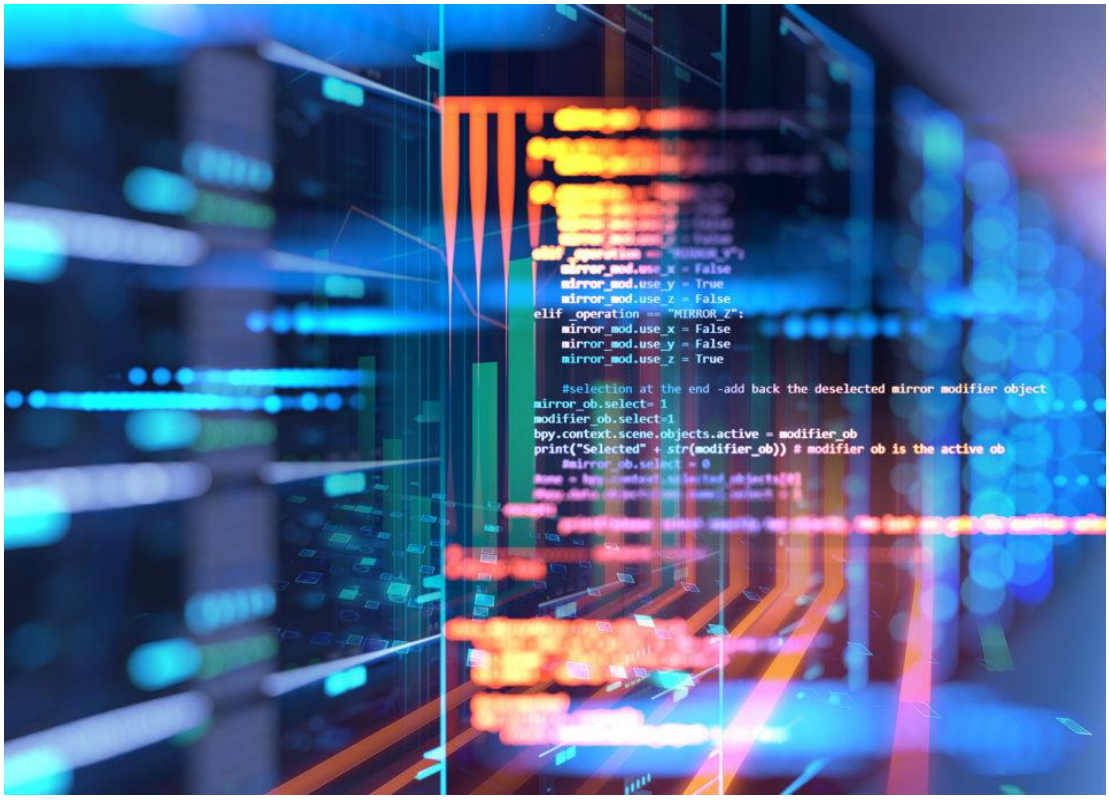
➢ 漏洞影响对象类型（2020 年 03 月 15 日—2020 年 03 月 30）



三、安全产业动态

➢ 我国网络安全产业现状、问题与发展

近年来，我国网络安全产业在政策、需求、资本的多重驱动下，迎来了更加快速稳定的发展，产业规模不断增长，资本的持续投入也助力了产业整合的加速发展。



一、我国网络安全产业的内涵和外延

从传统意义上说，网络安全产业的目标主要是针对保障网络的可用性、可靠性和安全性，提供产品和服务。随着网络技术的演变与安全形势日趋复杂，在技术发展和用户需求的双重驱动下，新技术、新产品不断出现，安全产品和安全服务的融合日益紧密，网络安全产业的内涵由此得到了丰富；同时，新应用场景不断被新的网络安全技术和产品所覆盖，网络安全产业的外延也得到了充分的扩展。

2016 年 12 月发布的《国家网络空间安全战略》指出，网络空间由互联网、通信网、计算机系统、自动化控制系统、数字设备及其承载的应用、服务和数据等组成。如今，网络安全产业已经演化为以满足网络空间的可用性、可靠性和安全性为目标，融合了技术研究开发、产品生产经营和提供相关安全服务的完整产业生态链。

由此，我们认为，网络安全产业是指为保障网络空间安全提供技术、产品和服务的相关

行业的总称。具备网络安全产品、服务和解决方案销售收入的我国网络安全企业，是我国网络安全产业的主要支撑力量。

二、我国网络安全产业的分类

网络安全产业的发展是一个升维的过程，网络安全从最初的基础安全产品及服务延伸到云、移动、物联网和工业控制等不同的应用场景。原来的问题是“如何做网络安全”，而新问题是“如何在不同场景下做网络安全”。新问题的提出就意味着新的市场机会。可以从基础安全、应用场景、业务、服务四个维度，描述我国网络安全产业的分类。

其中，基础安全主要解决传统网络安全领域的核心问题，主要包括端点安全、网络安全、应用安全、数据安全、身份与访问管理、安全管理等六类。应用场景主要包括云计算、移动互联网、工业控制、物联网等四个场景。信息技术应用创新和业务安全均属于在产品与应用场景基础上的业务维度。网络安全服务初步定义了管理安全服务、管理检测与响应和安全教育培训三个类别。无论是传统领域还是新应用场景，或是业务，都需要有服务体系支撑。

图 1 我国网络安全产业分类

我国网络安全产品的细分程度较高，不同的细分市场领域聚集着相应的数量庞大的专业厂商。网络安全产业正在呈现分散格局。造成的这种现象的主要原因是，网络安全贯穿整个信息流链条涉及几乎所有信息设备与软件，单个网络安全企业无法掌握全部网络安全技术，只能根据自身技术优势和渠道特点进行差异化定位，选择部分细分领域参与市场竞争。

表 1 我国网络全产品与服务分类

类别	项目	子项目
基础安全	网络安全	防火墙、上网行为管理、入侵检测与防御、网络隔离和单向导入、防病毒网关、网络安全审计、VPN/ 加密机、抗拒绝服务攻击（设备）、网络准入与控制、高级持续性威胁、网络流量分析
	终端安全	恶意软件防护、终端安全管理、主机 / 服务器加固
	应用安全	Web 应用防火墙、Web 应用安全扫描及监控、网页防篡改、邮件安全
	数据安全	数据库安全、安全数据库、数据脱敏、数据泄露防护、电子文档管理与加密、数据备份与恢复
	身份与访问管理	运维审计堡垒机、身份认证与权限管理、硬件认证、数字证书
	安全管理	安全管理平台、日志分析与审计、脆弱性评估与管理、安全基线与配置管理、合规检查工具、网络安全资产管理、威胁管理
应用场景	云计算	云基础设施安全、云负载保护平台、云操作系统、云身份认证、云抗 D、云 WAF
	移动互联网	移动终端安全、移动应用安全、移动设备管理
	物联网	车联网、视频专网
	工业控制网络	工控安全
业务	信息技术应用创新	安全产品、操作系统、芯片
	业务安全	舆情分析、反欺诈与风控、区块链安全、电子取证
服务	管理安全服务	网络安全系统集成、安全运维
	管理检测与响应	风险评估、渗透测试、应急响应等
	安全教育与培训	人才培养、网络靶场等

三、我国网络安全产业规模、增速与集中度

2019 年，我国研究机构以具备网络安全产品、服务和解决方案销售收入的我国网络安全企业作为目标研究对象，调研超过 200 家网络安全企业。通过对确定的 120 多家企业的有效数据为基础进行统计分析，可以看出 2018 年我国网络安全产业规模、增速与集中度情况。

（一）网络安全产业发展态势整体良好，总体规模仍较小

2018 年，我国网络安全产业规模约为 393 亿元人民币，同比增长率约 17.8%，增速相比上一年有所放缓。我国网络安全市场现已进入调整期，一方面，传统安全业务增长触及天花板，另一方面，新兴安全业务市场空间尚未有效释放，导致整体市场增速有所放缓。随着关键基础设施保护、等级保护 2.0 系列标准等政策标准的推动，信息技术应用创新、安全可控市场需求的逐步释放，将有望推动整体网络安全产业进入下个上升周期。预计，未来三年，网络安全产业整体市场依然会保持 20%左右的高速增长，到 2021 年，我国网络安全产业规模将达到 668 亿元。

图 2 2016–2021 年我国网络安全产业规模及增速

（二）网络安全产业向低集中寡占型市场转变

行业集中度指数(CRn 指数)，又称“行业集中率”，是指该行业的相关市场内前 N 家最大的企业所占市场份额，例如，CR1、CR4、CR8 分别代表行业内排名第 1 位、前 4 位、前 8 位的企业所占的市场份额。2018 年，我国网络安全市场 CR1 为 6.41%，CR4 为 21.71%，CR8 为 38.75%。根据美国经济学家贝恩对产业集中度的划分标准，我国网络安全产业 CR8 小于 40%，属于竞争型市场。但是，通过对过去三年市场集中度情况进行数据统计，我国网络安全产业的 CR4 和 CR8 都呈现增长态势，说明行业市场份额在向头部企业聚集，我国网络安全产业正在由竞争型市场向低集中寡占型市场转变。

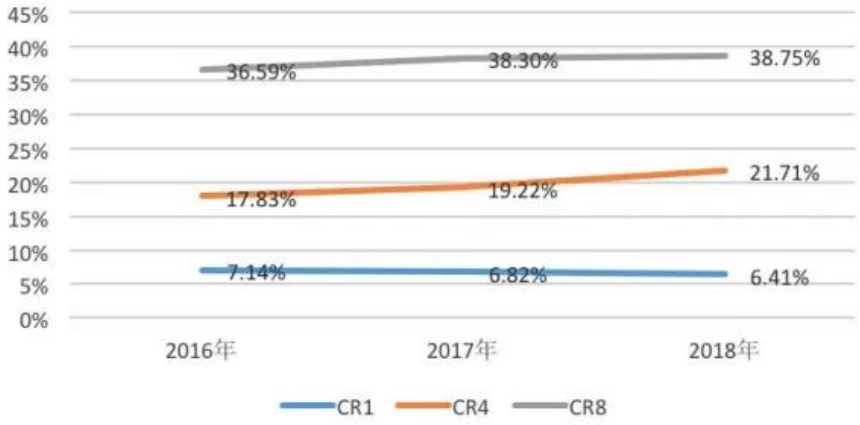


图 3 2016–2018 年我国网络安全产业集中度

（三）网络安全市场仍然主要依靠内需驱动

我国网络安全企业收入主要来自于华北、华东和华南三个区域，三个区域合计收入占比超过 70%。可见，我国网络安全区域市场规模与我国区域经济发展水平强相关。其中，华北区域由于政府及央企的垂直效应，多年以来一直占据区域收入首位，也是网络安全企业的必

争之地。虽然部分大型企业努力尝试海外业务拓展，但是，收效甚微，海外收入占行业总体市场份额仍不足 1%，我国网络安全市场仍然主要依靠内需驱动。

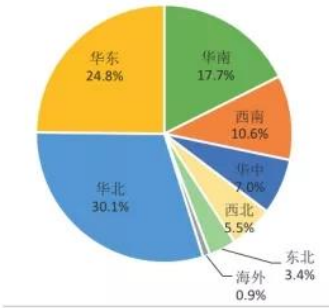


图 4 我国网络安全市场区域分布

四、我国网络安全企业竞争格局

我国网络安全产业近年来快速增长，但是，由于网络安全市场细分领域众多，竞争较为激烈，导致产业集中度偏低，目前，市场上缺少真正的龙头企业。我国网络安全企业按照规模主要分为三种类型：大规模头部企业、中等规模企业和小规模初创型企业。

大规模头部企业以启明星辰、深信服、奇安信、天融信和绿盟科技等为代表的综合型网络安全企业为主。它们在网络安全产业深耕多年，在品牌、营销及服务网络、资质认证等方面构建了较高的竞争壁垒。未来，头部企业之间的竞争将会更加激烈，竞争将从业务和资本两个维度展开。预计，三至五年内，将会出现 1-3 家具备一定领先优势的龙头企业。

中等规模网络安全企业随着科创板快速落地开板，预计，未来两三年内进入上市潮。上市后由于资本加持，这些企业将会进入一段高速发展期，向头部企业发起冲击。在这个过程中，一些企业有望突围成功，也会有企业将进入较为平稳的成熟期。

小规模初创型网络安全企业一般业务方向较为单一。由于市场细分领域众多导致单一细分市场天花板较低，加之行业竞争壁垒较高，当业务规模逐渐触及天花板时，初创企业一般有两个选择，一是适时退出，被大中型网络安全企业并购，利用买方的品牌、营销网络和资源等方面优势快速占据该细分市场份额；二是独立发展，独立发展过程中必然会伴随扩展企业人员规模，构建完整营销服务网络、扩充产品线等动作，在这个过程中，也将会面临一定的经营风险，最终只有少数优秀团队能够成功突围，成为中等规模企业。

五、我国网络安全产业发展面临的主要问题

面对当前网络安全发展的新形势新格局，我国网络安全产业的发展仍然面临着更加复杂严峻的挑战，在产业发展顶层设计、完善产业发展环境、市场准入与监督、人才、服务保障以及融资等方面还存在着不少问题，有待进一步完善和提高，主要表现在以下几个方面。

（一）网络安全产业总体规模较小，投入严重不足

根据 IDC 的统计数据，全球 IT 安全占 IT 市场比例为 3.74%，美国 IT 安全占 IT 市场比例为 4.78%，而我国 IT 安全占 IT 市场比例仅为 1.84%，严重低于国际平均水平。目前，我国的网络安全总体投入还缺乏刚性投入要求，导致网络安全市场规模增长缓慢，我国网络安全产业总体规模尚未达到千亿级，网络安全与信息化发展还存在一定的不平衡。

（二）网络安全行业资质要求多、重复测评认证现象严重

网络安全行业各种合规性要求与资质种类繁多，除基本市场准入要求以外，进入政府采购、保密、军工、金融、电力、通信等领域，均需各种企业资质和产品测评认证证书。但是，测评认证技术要求内容基本一致，重复检测现象严重，繁多的合规性和资质要求给企业增加了大量的时间、人力和经费成本。

（三）网络安全人才缺失，培养模式单一、周期长、成本高

随着 IT 和网络安全产业发展，人才竞争越来越激烈，未来中高端人才需求持续增长，特别是网络安全系统总体人才、售前方案人才和高级研发人才需求量会比较大，目前，这类人才缺失严重。然而，网络安全企业人员素质要求门槛高，需具有互联网、通信、安全等方面的知识体系，但是，高校人才培养模式单一，学校、企业和产业之间缺乏合作交流，学生在校期间对网络安全行业实际了解少。网络安全企业需用至少一至两年时间才能将应届毕业生培养为适应工作要求的网络安全人才，培养周期长，企业花费成本高。

（四）网络安全企业同质化竞争严重、国家缺乏体系化引导

由于整体网络安全行业市场空间有限，单一细分市场规模小，难以满足网络安全企业增长需求，行业内越来越多的企业向综合型安全厂商转型。大家的战略选择比较趋同，产品线不断扩张，覆盖越来越多的细分领域，同质化竞争严重。

（五）网络安全企业融资难，融资贵问题依然存在

我国大部分网络安全企业规模小，研发投入巨大，企业为了提升核心竞争力不断加大研发投入，从初创达到盈利周期很长，在拿到 IPO 资质之前，证监会要求企业必须弥补前期亏损，致使企业融资成本增多，转亏为盈时间过长，转型后，还将面临如何快速获取利润的压力。在理财方面，中央网信办、工信部、证监会都出台了针对促进网络安全企业发展的政策措施，引导企业融资合作，但是，政策落实举步维艰。国家对主板企业的利润要求高，虽然没有硬性条件，却有基准条件、指标。网络安全企业毛利率、周转率、现金流等与传统制造业甚至互联网企业都处在相对较弱的地位，投资周期长，债权融资和股权融资都缺乏吸引力，相关部门出台的引导企业融资合作政策落实困难。

六、我国网络安全产业发展建议

为进一步促进我国网络安全产业健康、高质量发展，针对我国网络安全产业发展现状以及目前面临的主要问题，建议如下。

（一）大幅提高国家信息化建设中网络安全投入比重，扩大网络安全产业规模

促进网络安全需求释放，切实增加投入。明确在国家信息化建设重大项目、重大工程、政府及企事业信息化建设和运维中网络安全投入的硬性比例要求，实施一系列重大工程项目，地方政府结合自身情况出台相关配套政策，扩大我国网络安全产业市场规模。

（二）减少网络安全行业重复检测认证，切实减轻企业负担

统筹规划网络安全测评认证工作，推进多证合一及互认，简化流程，提高效率，降低企业测评成本；推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

（三）加强统筹规划，形成产业合力，提升国家网络安全保障服务能力

加强统筹规划，充分发挥央企、互联网企业、网络安全民营企业各自优势，形成产业合力，兼顾安全和发展，实现国家需求和产业能力的良性促进，切实提升国家网络安全保障服务能力。

针对我国网络安全企业同质化竞争严重的现象，面向各技术领域的网络安全产品、服务建立一套公平、公正、科学的评判机制，推选出在专业细分领域领先的优质企业，做好“评优、选优、扶优”工作，加强宣传推广，鼓励在政府采购、重大科技项目立项评审等工作中优先选用推选出的产品和服务，引导企业在专业细分领域做深做专做优。

（四）创新人才培养模式，建立健全人才激励机制

实施针对性的网络安全人才培养工程，鼓励学校、企业、产业开展合作交流，必要时可以以产业联盟或协会为主体与高校开展对接工作，根据企业对网络安全技术研发、产品研制的实际工作需求，完善在校学生的网络安全知识体系、专业技能和相关素质，培养适应企业实际工作需求的网络空间安全人才队伍。

（五）拓宽网络安全企业融资渠道

针对网络安全企业“轻资产、重研发、人力成本高”的实际情况，国家出台相关政策鼓励金融机构开展知识产权质押、信用保险保单质押贷款等服务，加大对网络安全企业特别是中小企业的信贷投放力度，提高低息、无息贷款投放比例；适当降低对在市值、盈利情况、利润额、现金流等方面的上市资格要求，支持网络安全企业优先上市融资。

（六）鼓励网络安全技术创新，适应信息化新技术、新应用、新业态的发展趋势

设立网络安全科技研发专项基金，鼓励企业密切跟踪云计算、大数据、物联网、移动互联、5G、区块链、人工智能、量子计算等新技术的发展趋势，加大对企业开展安全可控相关研发工作的扶持力度，引导企业积极深入研究信息化新技术、新应用、新业态发展带来的安全隐患，加快网络安全相关技术创新和产品研制速度。（来源：《中国信息安全》杂志 2020 年第 3 期）

➢ 个人金融信息安全技防研究

个人金融信息是金融机构在提供金融产品和服务过程中积累的重要基础数据，也是涉及金融消费者信息安全的重要内容。如何收集、使用、对外提供个人金融信息，既涉及金融机构业务的正常开展，也涉及客户信息、个人隐私的保护。随着大数据、移动互联网和云计算等技术在金融行业的广泛应用，个人金融信息呈爆发式增长，海量汇聚，一方面通过海量数据的搜集、整理以及分析，可以高效地归纳和总结人们的活动特点，为用户提供精准化、个性化的服务，大大提升了用户体验和生活效率，另一方面大数据分析使个人金融信息泄密的威胁日益凸显。本文通过梳理个人金融信息安全保护现状，研究当前主流的隐私保护技术，并从法律、技术、内控等多角度、多层次提出加强个人金融信息保护的政策建议。

个人金融信息相关概述

1.个人金融信息概念界定。个人金融信息是指金融机构在为个人消费者提供金融产品和服务的过程中，获取到的个人信息，包括但不限于个人基本身份信息、交易记录信息以及其

他信息。2011 年下发的《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》(银发〔2011〕17 号)，首次给出个人金融信息的概念界定。2016 年 12 月出台的《中国人民银行金融消费者权益保护实施办法》（银发〔2016〕314 号）将个人金融信息定义为金融机构通过开展业务或者其他渠道获取、加工和保存的个人信息，包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他反映特定个人某些情况的信息。2020 年 2 月人民银行发布的《个人金融信息保护技术规范》（JR/T 0171-2020）将个人金融信息内容界定为七类，包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息和其他反映特定个人金融信息主体某些情况的信息等（见表 1）。《规范》同时根据信息遭到未经授权的查看或未经授权的变更后所产生的影响和危害，将个人金融信息按敏感程度从高到低分为 C3、C2、C1 三个类别（见表 2）。

信息类型	包括范围
账户信息	账户及账户相关信息，包括但不限于支付账号、银行卡磁道数据（或芯片等效信息）、银行卡有效期、证券账户、保险账户、账户开立时间、开户机构、账户余额以及基于上述信息产生的支付标记信息等
鉴别信息	用于验证主体是否具有访问或使用权限的信息，包括但不限于银行卡密码、预付卡支付密码；个人金融信息主体登录密码、账户查询密码、交易密码；卡片验证码（CVN 和 CVN2）；动态口令、短信验证码、密码提示问题答案等
金融交易信息	个人金融信息主体在交易过程中产生的各类信息，包括但不限于交易金额、支付记录、透支记录、交易日志、交易凭证；证券委托、成交、持仓信息；保单信息、理赔信息等
个人身份信息	个人基本信息、个人生物识别信息等。（1）个人基本信息包括但不限于客户法定名称、性别、国籍、民族、职业、婚姻状况、家庭状况、收入情况、身份证和护照等证件类信息、手机号码、固定电话号码、电子邮箱、工作及家庭地址，以及在提供产品和服务过程中手机的照片、音视频等信息；（2）个人生物识别信息包括但不限于指纹、人脸、虹膜、耳纹、掌纹、静脉、声纹、眼纹、步态、笔迹等生物特征样本数据、特征值与模板
财产信息	金融机构在提供金融产品和服务过程中，收集或生成的个人金融信息主体财产信息，包括但不限于个人收入状况、拥有的不动产状况、拥有的车辆状况、纳税额、公积金存缴金额等
借贷信息	个人金融信息主体在金融业机构发生借贷业务产生的信息，包括但不限于授信、信用卡和贷款的发放及还款、担保情况等

表 1《个人金融信息保护技术规范》对个人金融信息的界定

信息类别	包括范围
C3	主要为用户鉴别信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成严重危害
C2	主要为可识别特定个人金融信息主体身份与金融状况的个人金融信息，以及用于金融产品与服务的关键信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成一定危害
C1	主要为机构内部的信息资产，主要指金融业机构内部使用的个人金融信息。该类信息一旦遭到未经授权的查看或未经授权的变更，可能会对个人金融信息主体的信息安全与财产安全造成一定影响

表 2《个人金融信息保护技术规范》对个人金融信息的类别界定

2.个人金融信息与个人信息、个人隐私的关系。个人金融信息保护涉及消费者、金融机构、互联网平台、监管部门等多方面要素，而探讨个人金融信息、个人信息、个人隐私之间的关系，将有助于我们圈定个人金融信息保护的边界，明确参与其中的各个主体的责任问题，从而构建有效的保护模式。

个人金融信息是个人信息在金融产品和服务中的细化，两者之间是特殊和一般的关系。个人信息在 2018 年 5 月开始实施的国家标准 GB/T 35273-2017《信息安全技术个人信息安全规范》中有明确定义，只要是能够识别自然人身份或者反映自然人特定活动的信息都划为个人信息的范畴，包括个人基本信息、个人生物识别信息、财产信息、征信信息、交易信息、行踪轨迹信息、住宿信息、健康生理信息等。可见个人信息范围较为广泛，对比两者包含的信息范畴，存在大量的信息重叠，如个人身份信息、财产信息、征信信息以及交易信息，这些信息在金融活动中非常重要。

个人金融信息与个人隐私有非常密切的关系。隐私权是一种基本人格权，同肖像权、姓名权一样是公民拥有的基本人格权利。2017 年 6 月 1 日正式实施的《网络安全法》中就明确规定任何个人和组织在使用网络时不得侵犯他人隐私。个人金融信息中的财产信息、交易信息、征信信息以及账户信息直接关系到消费者的人格权利和财产权利，个人金融信息一旦泄露直接威胁到信息主体的财产安全。因此，笔者认为个人金融信息应该纳入个人隐私保护的范畴。

个人金融信息保护的发展现状

1.个人金融信息保护的法律、法规和规章情况。相比美国、欧盟等发达地区，我国关于个人金融信息的立法保护相对滞后。2018 年全国两会期间，全国人大代表、人民银行南京分行行长周学东就提出，应加快个人信息保护立法进程，制定个人信息保护法的建议。但截至目前，个人信息保护法的制定并没有被提上立法日程，这与我国在社会主义建设关键阶段，互联网产业处于上升时期不无关系。我国关于个人金融信息保护的法规分散体现在多个部门法中。我国《刑法》《消费者权益保护法》《中国人民银行法》《商业银行法》《证券法》《保险法》《反洗钱法》中的部分条款间接或直接涉及个人金融信息保护，但是除了《刑法》中关于侵犯公民个人信息等犯罪的规定及其司法解释以外，其他的法律法规都是较为笼统和抽象的原则性规定，在个人信息保护的司法实践中不能起到有效的保护或惩戒作用。

近年来，因个人金融信息泄露而引发的金融诈骗行为日益严重，为加强个人金融信息保护，国家先后出台了一系列法律法规、行业新标准。《网络安全法》对网络运营者提出个人信息保护的相关要求；《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案

件适用法律若干问题的解释》定义了公民个人信息，并对个人信息泄露情形提出量刑标准；《民法总则》规定自然人的个人信息安全受到法律的保护。以上法律法规的制定主要是以不侵犯个人隐私为前提，所形成的法律规定也是以限制或禁止个人信息流转为原则，都是对个人信息保护进行规范要求，无法兼顾到个人金融信息保护的特殊情况。此外，国家标准《信息安全技术个人信息安全规范》提出个人信息收集、使用、传输、存储的相关要求；新推出的金融行业标准《个人金融信息保护技术规范》明确对个人金融信息做出分类，规定了金融支付机构在数据全生命周期环节中应做到的技术要求。人民银行出台的《个人信用信息基础数据库管理暂行办法》和《关于银行业金融机构做好个人金融信息保护工作的通知》，对个人金融信息收集、保存、使用等过程做了规定，《个人信息安全规范》和《个人金融信息保护技术规范》是标准，《办法》属于部门规章，《通知》是规范性文件，均不属于广义法律范畴，囿于效力层级低，不能设立行政检查权和处罚权。

2.信息安全技术防范情况。互联网金融、大数据以及金融业云计算的发展，使金融消费者在享受便捷金融服务的同时，个人金融信息泄露事件屡屡发生。2014 年欧洲中央银行 1.5 亿注册者的电子邮件和联络人的细节信息被黑客窃取；2016 年京东 struts2 安全漏洞被黑客攻击，12GB 的客户信息在黑市流通；2017 年广东知名网贷平台 PPmoney 百万借款人信息被泄露。

个人金融信息在金融企业内部以及金融企业之间流转和共享已经成为常态，数据共享可以节约成本，提高金融机构服务水平，对科学发展有着积极的促进作用。但因其信息系统管理水平和应对网络攻击能力未能同步，其信息安全管控能力不足，存在信息泄露、篡改、滥用的风险。目前学术界和工业界加强了数据安全和隐私保护研究和技术落地，关于数据安全和隐私保护的技术研究进展将在下一章节中详细分析。

3.外部监管和内部管理情况。从外部监管的情况看，当前我国个人信息保护基础立法的缺位，对个人金融信息保护履行监管职责的部门较多，中国人民银行、银保监会、证监会等都在各自的监管领域开展工作，但监管标准不一致，沟通协调不足，导致个人金融信息保护工作存在多方监管、监管重叠、监管漏洞等问题。另一方面，由于缺乏明确的法律支持，监管部门执法时，对违法行为的认定和处理存在较大困难，缺乏有效处理手段，只能运用通报、约谈等惩罚性不强的手段，不能对违法机构产生威慑力。

从金融企业内部管理看，一是关于个人金融信息保护相关制度散见于各类管理制度中，未形成系统化的个人信息管理框架，使得制度不能完全实现对个人金融信息采集、使用、共享等环节的约束。二是没有组建专门的个人信息管理机构，导致各部门在个人信息保护领域

杂乱无章，缺乏统一管控。

隐私保护技术研究进展

1.基于加密技术的隐私保护。数据加密是信息安全的核心技术之一，用于保障数据不被泄露和篡改。数据加密有两个过程：第一个过程是加密，将可识别的数据（即明文）通过加密函数和加密密钥为无法识别的形式（即密文）；第二个过程是解密，是通过解密算法和解密密钥将密文恢复为明文。

数据加密技术分为两类：一类是对称加密，另一类是非对称加密。对称加密,多采用置换、替换、移位、异或等运算操作，优点在于效率高，算法简单，系统开销小，适合加密大量数据。非对称加密，运算复杂，计算速度慢，用于加密少量重要数据或者是用于分发对称加密算法的密钥。数字签名技术就是一种应用非对称加密技术实现的，是类似写在纸上的普通物理签名，具有不可抵赖性，用于身份鉴别。

数据加密技术的特征，一是始终保障数据的安全性，数据在金融企业内部以及金融企业之间流转和共享已经成为常态，在数据转移和共享过程中采用加密技术，能够让敏感数据得到更安全的保障；二是有效保证数据的完整性，数据加密技术可以有效阻止黑客改变数据信息，最大限度保证数据不被篡改；三是有效保护用户隐私和财产，对金融机构而言，保护好客户数据，对这些数据进行加密处理，才能对自己更加有利。

数据加密技术在金融领域具有广泛的应用，一是数据存储加密，采用存储层的加密技术，被加密的数据以密文的形态存储在磁盘上，在缺乏密钥的情况下，即使黑客冲破防护获得数据信息文件，也不会导致敏感数据泄露；二是应用数字签名技术，数字签名无论在提升合同处理效率，还是降低管理成本、优化服务体验方面，均具有传统业务模式不可比拟的先进性。

2.基于隐私计算技术的隐私保护。2016 年，中国科学院信息工程研究所副总工程师李凤华提出隐私计算的概念，由于其兼顾隐私保护和数据利用的计算方式，一经推出就成为学术界和工业界研究的重点。作为密码学的一个前沿发展方向，隐私计算填补了数据在计算环节隐私性问题的空白，将基于密码学的信息安全体系打造成完整的闭环。

隐私计算是面向隐私信息全生命周期保护的计算理论和方法，具体指对所涉及的隐私信息进行描述、度量、评价和融合等操作，形成一套符号化、公式化且具有量化评价标准的隐私计算理论、算法及应用技术、支持多系统融合的隐私信息保护。隐私信息的全生命周期如图 1 所示。

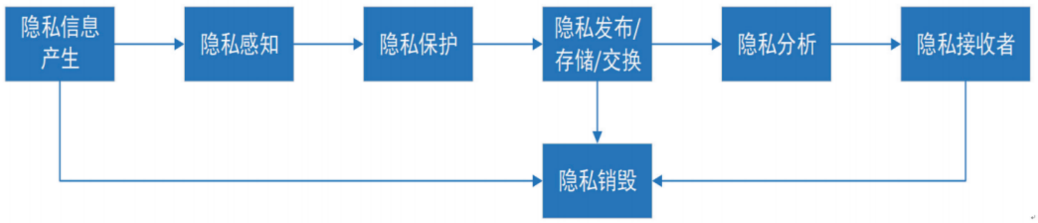


图 1 隐私信息的全生命周期

隐私计算中，将隐私信息抽象为符号化 n 维变量 x=(x1,x2,⋯,xn),每个分量 xi 表示一类隐私信息，如姓名或联系方式，不同分量的取值集合组成了整个隐私信息的取值集合。集合的运算以及定义在集合上的测度运算可应用于隐私的计算模型。根据取值集合上定义的隐私度量来定义隐私运算的规则，形成隐私计算的公理化体系。

目前阶段，密码学层面的隐私计算主要有全同态加密、安全多方计算、零知识证明等技术方向。其中，安全多方计算是隐私计算技术主要研究方向之一。

2009 年，Gentry 构造出了第一个全同态加密方案，全同态加密被认为是解决云计算安全的最好方法，利用全同态加密方案对用户数据进行加密，再将密文发送到云端，云端可以在不解密的情况下进行检索和比较等操作，避免了数据存储方泄露数据的危险。但现有的全同态加密方案计算复杂度相对较高，还无法在实际系统中应用。

安全多方计算（MPC）最初由图灵奖获得者、中国科学院院士姚期智教授提出。它主要解决一组互不信任的参与方之间保护隐私的协同计算问题，即如何在参与计算的各方不泄露自身输入、且没有可信第三方的情况下安全地计算约定的函数并得到可验证结果。

当一个 MPC 节点计算任务发起时，枢纽节点传输网络及信令控制。每个数据持有方可发起协同计算任务。通过枢纽节点进行路由寻址，选择相似数据类型的其余数据持有方进行安全的协同计算。参与协同计算的多个数据持有方的 MPC 节点根据计算逻辑，从本地数据库中查询所需数据，共同就 MPC 计算任务在数据流间进行协同计算。在保证输入隐私性的前提下，各方得到正确的数据反馈，整个过程中本地数据没有泄露给其他任何参与方。

当前，金融机构普遍面临着数据隐私安全导致的数据孤岛问题。借助于 MPC 等隐私计算技术，金融机构可以在不泄露自身数据的前提下实现与电商、社交、交通等多领域数据协同计算，深度挖掘，构建基于多元化数据的客户需求分析模型，准确刻画用户画像，预测客户潜在需求，精准推送个性化金融产品和服务，彻底改变传统营销模式，提升金融业个性化服务水平。

加强我国个人金融信息保护的建议

1.建立健全信息保护法律体系，提供刚性约束。从长远看，应制定专门的《个人信息保护法》，应设立专门章节来规定个人金融信息的保护，全面规定个人金融信息保护的相关定义、信息处理的基本原则、数据主体的权利、控制者和处理者的义务、安全保障措施、信息转移的规则、监管机构、救济途径、责任承担方式、处罚措施等内容。

除制定《个人信息保护法》作为基本法外，还应完善配套的法律制度。金融机构管理层须将个人信息保护纳入整体风险管理框架，依据《网络安全法》《信息安全技术个人信息安全规范》等，因地制宜制定符合本机构个人金融信息保护的内部规章，对易发生个人金融信息泄露的环节进行充分排查，明确规定各部门、岗位和人员的管理责任，加强个人金融信息管理的权限设置，形成相互监督、相互制约的管理机制。

当然，有效监管是保障个人金融信息安全的必要之举，立法应该明确监管机构、监管职责和监管措施，并授权监管机构对金融机构个人金融信息保护工作开展非现场监测和现场检查，对金融机构违规泄漏个人金融信息，造成客户损失或引发不良社会影响的，可视情形实施行政处罚或采取其他监管措施。

2.建立个人信息风险评估机制，夯实安全根基。开展个人信息风险评估是《网络安全法》明确规定企业的一项法定责任，不仅是企业降低个人信息风险的一道重要关卡，同时也是发生安全事件后，企业网络安全责任划分的一个重要抓手。因此企业应当确立符合自身特点的个人信息评估体系，建立一个科学的评估组织议事规则和责任机制，必要时可以引入外部专业机构评估或出具专项的法律意见。

3.注重隐私保护技术应用，提升技防能力。一方面，应采用安全认证网关保障网络资源的安全访问，使用 IPSecVPN 或 SSLVPN 建立虚拟安全传输通道，确保信息在网络中的安全稳定传输。另一方面，应注重密码技术的应用，调用服务器密码机实现对数据的加密保护，利用数字签名技术实现信息来源真实性和数据完整性。第三方面，加强隐私计算技术在金融领域应用层的落地，打破数据壁垒，使金融机构内外部之间既分享数据，又保证数据安全，使个人金融信息实现更大的应用价值。

4.强化内控管理，提升安全责任意识。确保金融机构的责任与义务，强化内部管理。一是金融机构管理层要加强认识，积极营造个人金融信息的保护环境，注重隐私保护技术的落实工作，确保个人金融信息风险评估形成长效机制。二是加强对从业人员的培训，强化从业人员个人金融信息安全意识，上岗前应当签署保密承诺书。三是注重网络安全人才的引进和培养，发现漏洞，填补漏洞，根源上杜绝黑客入侵，保障业务系统不受侵犯。（来源：金融电子化 作者：中国人民银行太原中心支行副行长王山松）

➢ 网络安全等级保护 2.0 云计算安全合规能力模型

2019 年，网络安全等级保护系列标准正式发布，网络安全等级保护从此由 1.0 时代迈入 2.0 时代。网络安全等级保护制度在 2.0 时代着重于全方位的主动防御、动态防御、精准防护和整体防控的安全防护体系，将云计算、物联网、移动互联、工业控制信息系统和大数据等新应用、新技术纳入等级保护扩展要求。云计算是以网络技术及分布式计算为基础的一种新计算模式，通过互联网实现按需服务、泛在接入、多租户和资源池、快速弹性、可度量性五大特征。随着云计算的迅速发展，云计算安全已成为制约云计算发展的重要一环，使得云计算安全成为 IT 界的热点研究方向之一。大量存储或运行在云端的数据面临数据丢失、泄露及非法访问等风险，为确保云端数据在存储、共享、查询和计算等云计算服务中数据的安全性，规避云数据面临的安全威胁，国家发布了《信息安全技术 云计算服务安全能力要求》、《信息安全技术 网络安全等级保护基本要求》等系列合规性要求，合理、有效地应用这些合规性要求对提升云计算安全具有重要的作用。因此，建立云计算环境下的合规能力评估模型有着重大的探索意义和参考价值。与此同时，基于云环境下合规能力的要求，可进一步强化云计算安全性及可用性，有利于云计算安全合规体系的发展。相应的合规体系与防护技术也可以为一些云服务商提供参考与借鉴，具有一定的实际应用性。

区别于传统信息系统，云计算环境中通常有一个或多个安全责任主体，各安全责任主体根据管理权限的范围划分安全责任边界。云计算环境中多个安全责任主体的安全保护能力之和共同构成了整个云计算环境的安全防护能力。当云服务商与云服务客户为同一类实体机构或自然人时，云计算环境的安全责任主体只有一个，就是该系统的建设运行使用单位或个人。云计算环境中可能承载一种或多种云服务模式，每种云服务模式下提供了不同的云计算服务及相应的安全防护措施，在对云计算系统测评时，应关注每种特定云服务模式下，与其提供的云服务相对应的安全防护措施的有效性。

不同的云服务模式下，云服务商与云服务客户的责任边界会发生变化，在确定具体的安全责任时，应根据系统的实际运行情况而定。在明确云计算平台保护等级的情况下，按照等级保护对象在云计算环境中的角色、云计算的服务模式、云计算环境中的责任主体及云计算实现方式对测评指标选取的影响对等级保护对象和等级测评指标进行选取。

本文基于《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），通过对云计算系统/平台保护对象、安全措施及安全能力的识别，构建云计算等级保护 2.0 合规能力模型，并介绍了模型的应用

方法。

1、云计算保护对象

基于云计算等级保护防护体系和云计算的实现机制可将云计算平台分为基础架构层、云服务层、云访问层、云用户层、应用/数据层及管理层 6 个层次，如图 1 所示。

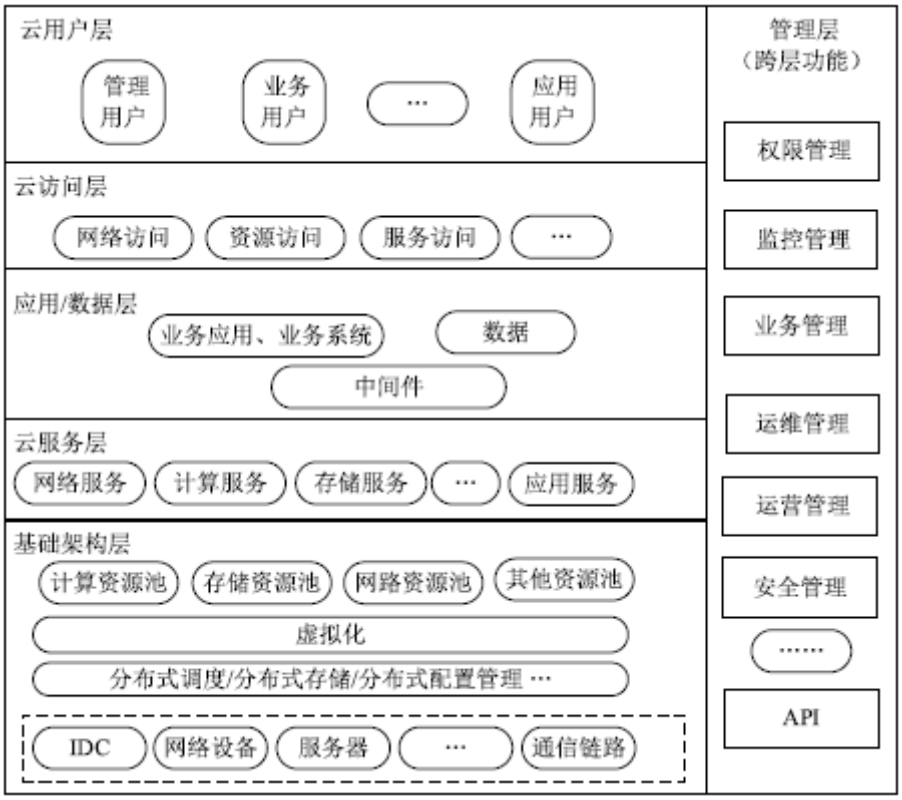


图 1 云计算功能架构

云用户层包括云计算服务提供者和云计算服务使用者各类用户。云用户层是云服务提供者与云服务客户间的交互界面。云访问层主要面向云计算服务提供者、云计算服务使用者，为其提供访问和管理功能，包括网络通信访问、面向云计算服务提供者和使用者的服务访问以及面向最终用户的应用访问等。应用/数据层为用户提供应用软件开发平台中间件、业务应用和数据。云服务层面向云服务客户提供虚拟机、数据库等基础服务，也可以分为网络服务、弹性计算服务、云存储服务及面向用户的应用服务，主要的服务包括但不限于负载均衡、虚拟主机、对象存储服务、分布式数据库与大数据计算服务等。基础设施层为云服务层或者用户提供其所需的计算和存储等资源，并通过虚拟化等技术将资源池化，以实现资源的按需分配和快速部署，包括网络资源、计算资源和存储资源等的资源池，并实现资源管理、任务调度和服务管理等方面功能；还包括主要的硬件设施，如存储设备、网络设备、安全设备和服务器等硬件设备及硬件设备的运行环境等。管理层主要是跨层访问功能

的集合，包括对云服务的业务管理、云平台和云服务的运维运营管理以及云平台系统和服务的安全管理。

云计算平台由基础设施、设备硬件、资源抽象控制层、虚拟化计算资源、软件平台和应用软件等组成，根据云计算服务模式可分为基础设施即服务（IaaS）、平台即服务（PaaS）、软件即服务（SaaS）。在不同的云计算服务模式下，云服务商和云服务客户对计算资源拥有不同的控制范围，如图 2 所示，控制范围决定其安全责任的边界。在 IaaS 模式下，云计算平台/系统由设施、硬件、资源抽象控制层组成；在 PaaS 模式下，云计算平台/系统包括设施、硬件、资源抽象控制层、虚拟化计算资源和软件平台；在 SaaS 模式下，云计算平台/系统包括设施、硬件、资源抽象控制层、虚拟化计算资源、软件平台和应用软件。

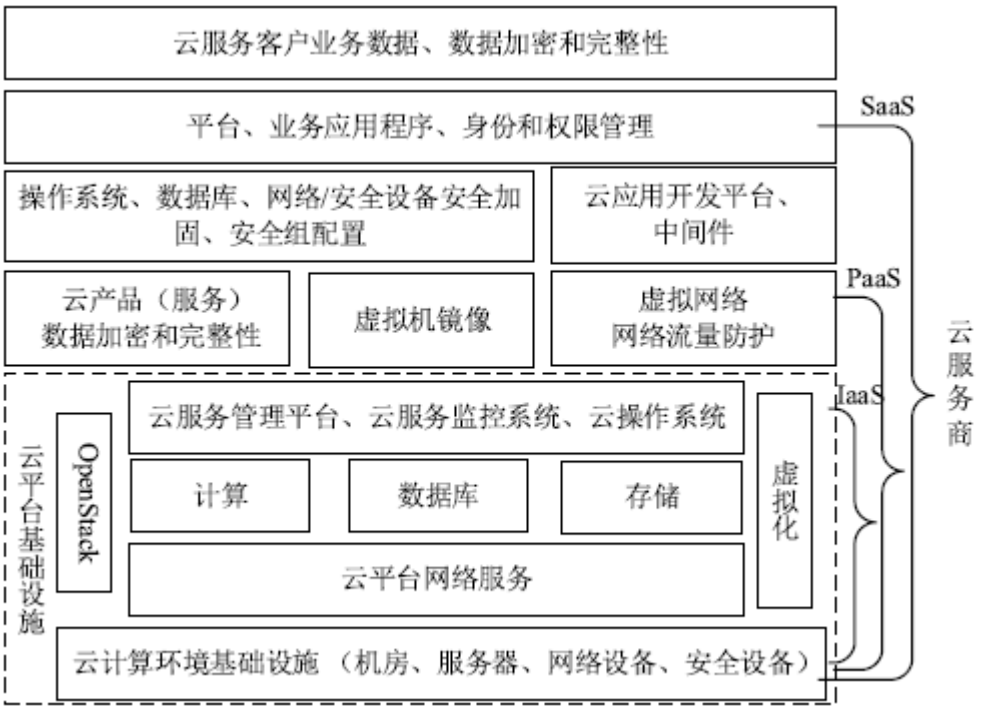


图 2 云计算服务模式与控制范围的关系

云计算环境采用的部署模式不同安全责任边界也不同，在确定具体安全责任时，应视系统具体运行情况而定。例如，自建私有云并独立承担云上业务的应用系统，云计算平台及其上的云服务应用责任主体一致。云安全责任规定任何一个云服务参与者都应承担相应的职责。云计算是一种共享技术模式，不同的云平台通常会承担实施和管理不同部分的责任。因此，安全职责也由不同的云平台分担，所有的云平台都包含在其中，即分担责任模型，它依赖于特定的云提供商和功能/产品、服务模式和部署模式的责任矩阵，基于“ 权责一致” 、“ 安全管理责任不变，数据归属关系不变” 的原则，即对数据有什么管理权就应负相应的责任。

对于 IaaS 服务模式，云服务商的责任对象主要包括网络设备、安全设备、云产品（服务）服务器（虚拟机）、宿主机、终端、云管平台服务器；云操作系统、云产品（服务）、虚拟机监视器、虚拟网络/安全设备、虚拟机镜像；鉴别数据、系统数据、审计数据、快照数据、个人信息等。云租户的责任对象包括虚拟机、数据库、中间件、业务应用和数据的安全防护、云服务安全策略配置。

对于 PaaS 服务模式，云服务商的责任对象主要包括网络设备、安全设备、云产品（服务）服务器（虚拟机）、宿主机、终端、云管平台服务器；云操作系统、云产品（服务）、虚拟机监视器、虚拟网络/安全设备、虚拟机镜像；虚拟机、数据库；鉴别数据、系统数据、审计数据、快照数据、个人信息。云租户责任对象包括软件开发平台中间件以及应用和数据的安全防护、云服务安全策略配置。

对于 SaaS 服务模式，云租户仅需关心业务应用相关的安全配置、用户访问、用户账户以及数据安全的防护、云服务安全策略配置。云服务商的责任对象包括网络设备、安全设备、云产品（服务）服务器（虚拟机）、宿主机、终端、云管平台服务器；云操作系统、云产品（服务）、虚拟机监视器、虚拟网络/安全设备、虚拟机镜像；虚拟机、数据库、中间件、业务应用；鉴别数据、系统数据、审计数据、快照数据、个人信息。

无论 IaaS 服务模式、PaaS 服务模式还是 SaaS 服务模式，对于云租户而言，数据安全的防护始终由其自己负责，但云计算平台提供的数据传输、存储完整性和保密性的安全功能决定了用户数据安全防护措施能否实现。

基于重要性、安全性、共享性、全面性和符合性的原则，云计算平台/系统的安全保护对象除网络互联与安全设备操作系统、应用软件系统、主机操作系统、数据库管理系统、安全相关人员、机房、介质及管理文档外，基于云计算平台/系统的服务模式考虑，还应包括虚拟设备（虚拟机、虚拟网络设备、虚拟安全设备）、云操作系统、云业务管理平台、虚拟监视器、云产品（服务）及云服务客户网络控制器、云应用开发平台等。

当保护系统为云计算平台时，保护对象如表 1 所示。

服务模式	安全层面	测评对象
SaaS、PaaS、IaaS	安全计算环境	云产品（服务）
		云产品（服务）数据
SaaS、PaaS	安全计算环境	虚拟机、数据库服务、中间件、容器、云应用开发平台、云产品（服务）等
SaaS、PaaS、IaaS	安全计算环境	云操作系统、虚拟机监视器、云业务管理系统、云产品（服务）
		虚拟网络 / 安全设备、虚拟机镜像
		云产品（服务）服务器（虚拟机）、宿主机、终端、云管平台服务器
		网络设备、安全设备
		配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据、个人信息
SaaS、PaaS、IaaS	安全通信网络	网络架构、物理链路、通信数据
SaaS、PaaS、IaaS	安全区域边界	物理网络边界、虚拟网络边界
SaaS、PaaS、IaaS	安全管理中心	云管理平台、云平台监控系统
SaaS、PaaS、IaaS	安全管理	安全相关人员、机房、介质及管理文档
SaaS、PaaS、IaaS	安全物理环境	物理机房、云计算基础设施部署的相关机房及基础设施

表 1 云计算平台保护对象

2、云计算安全措施

区别于传统的信息系统，在云计算环境中，边界可信日益削弱，源自不同平面的攻击日趋增多。传统分层面单层防御体系对确保云计算系统安全性显得尤为困难，基于等级保护 2.0“ 一个中心，三重防护” 的纵深防护思想，即从通信网络到区域边界再到计算环境进行重重防护，通过安全管理中心进行集中监控、调度和管理，构建云计算安全措施，如图 3 所示。

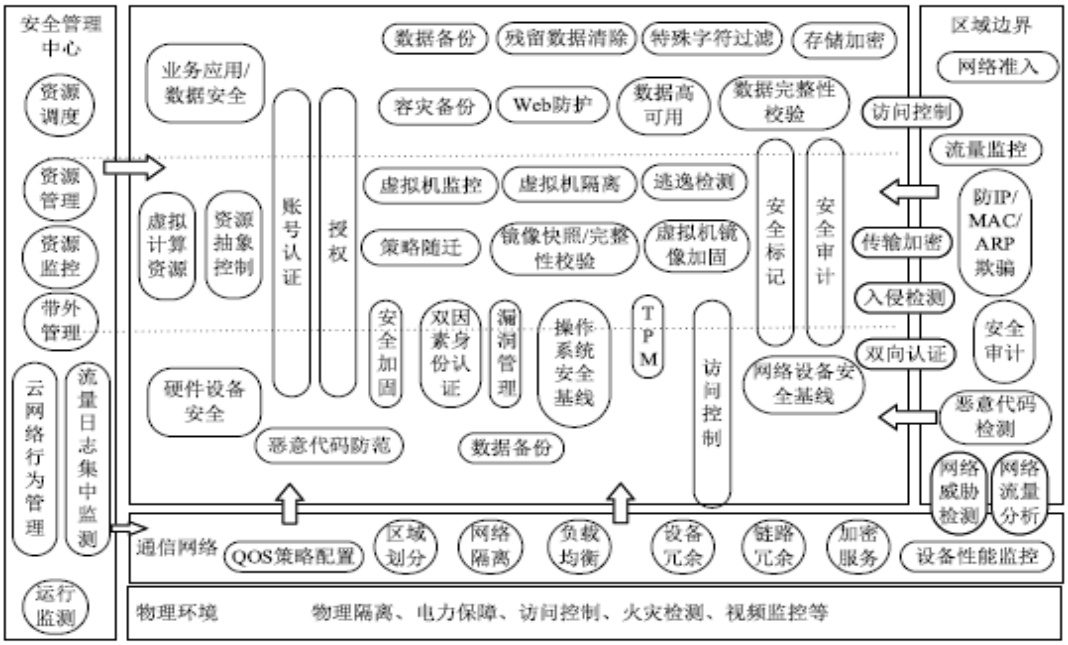


图 3 网络安全等级保护云计算环境安全防护措施

用户通过安全的通信网络跨越安全的区域边界以网络直接访问、API 接口访问或 Web 服务访问等方式访问安全的云计算环境。安全云计算环境包括基础架构层安全、云服务层安全以及业务应用和数据安全。基础架构层分为云计算硬件设备和虚拟化计算资源，云服务层包括云产品及资源抽象控制等。云计算环境的系统管理、安全管理和安全审计由安全管理中心统一管控。

《信息安全技术网络安全等级保护基本要求》在安全计算环境方面主要增加了虚拟化安全、镜像和快照安全等云计算相关的控制点，安全的云计算环境应提供安全加固（操作系统、镜像）、虚拟机隔离、双因素身份认证以及访问控制、安全审计等安全措施。在安全区域边界方面，除了传统物理区域的边界安全外，增加了虚拟网络区域边界、虚拟机与宿主机之间的区域边界等安全防护要求，安全的云计算环境区域边界应提供网络隔离、流量监控、虚拟机隔离等安全措施。在安全通信网络方面，在物理通信网络基础上增加了虚拟网络通信的安全保护要求，安全的通信网络应提供区域划分（物理网、虚拟网）、入侵检测、设备性能（物理网络设备、虚拟网络设备）监控等安全措施。在安全管理中心方面，应提供权限划分、授权、审计日志集中收集（分析）、时间同步等安全措施。

3、云计算安全技术能力

安全技术能力是云计算系统安全措施作用于保护对象上形成的抵抗外部攻击的一种防护能力。云安全措施是根据广泛的经验和学识为对抗云计算系统面临的威胁而采取的防护措施，有的安全措施是云计算平台原生的，有些则是云服务商为应对威胁而自研或由云生态合作伙伴提供的。本文引入安全能力定量和变量的定义。定量指云服务商不依赖于用户选择而原生提供的安全能力，如 VPC、安全组防火墙等。变量指云服务商依据用户需求，为应对系统威胁而选择性提供的安全能力，该能力既可由云服务商提供，也可由云服务生态合作伙伴提供，如网络设备加固、第三方硬件加密机等。

1）安全通信网络

（1）网络隔离

网络隔离措施作用于安全保护对象后，使得云计算平台在通信网络方面形成安全能力：云平台对云平台网络环境中的管理网络（OPS）、业务网络、物理网络进行了三网安全隔离。OPS 网络、业务网络、物理网络之间通过网络访问控制策略实现三网逻辑隔离，彼此之间不能相互访问；同时，采取网络控制措施防止非授权设备私自连接云平台内部网络，并防止云平台物理服务器主动外连。

（2）流量安全监控

流量安全监控作用于安全保护对象后，使得云计算平台在通信网络方面形成安全能力：通过对云平台入口镜像流量进行安全监控、深度解析流量包，实时检测各种攻击和异常行为。

2）安全区域边界

IP、MAC、ARP 防欺骗安全措施作用于安全保护对象后，使得云计算平台在区域边界方面形成安全能力。在传统网络环境中，IP、MAC、ARP 欺骗一直是网络面临的严峻考验，通过 IP、MAC、ARP 欺骗，黑客可以扰乱网络环境，窃听网络机密。云平台通过物理服务器上的网络底层技术机制，彻底解决地址欺骗问题。云平台在物理服务器数据链路层隔离由服务器向外发起的异常协议访问，阻断服务器的 MAC、ARP 欺骗，并在宿主机网络层防止服务器 IP 欺骗。

3）安全计算环境

（1）账号安全：账号安全作用于安全保护对象后，使得云计算平台在计算环境方面形成安全能力：针对网络设备、物理服务器账号的口令长度、复杂度、密码长度、口令生命期进行安全策略设置，删除空口令的账号，设置登录超时（TIMEOUT）时间等。

（2）主机入侵检测：主机入侵检测作用于安全保护对象后，使得云计算平台在计算环境方面形成安全能力：在物理服务器上部署主机入侵检测（HIDS）模块，其主要功能包括异常进程检测、异常端口检测、异常行为检测等。

（3）网络隔离：网络隔离作用于安全保护对象后，使得云计算平台在计算环境方面形成安全能力：为了支持虚拟机实例使用网络连接，将虚拟机实例连接到云平台的虚拟网络。虚拟网络是建立在物理网络结构之上的逻辑结构，每个逻辑虚拟网络与其他虚拟网络隔离。这种隔离有助于确保部署中的网络流量数据不被其他虚拟机访问。

（4）逃逸检测：逃逸检测作用于安全保护对象后，使得云计算平台在计算环境方面形成安全能力：云平台虚拟化管理程序通过使用高级虚拟机布局算法防止恶意用户的虚拟机运行在特定物理机上。同时，在虚拟化管理软件层面还提供了虚拟化管理程序加固、虚拟化管理程序下攻击检测、虚拟化管理程序热修复三大核心技术来防范恶意虚拟机的攻击。

4）安全管理中心

日志集中化作用于安全保护对象后，使得云计算平台在管理中心方面形成安全能力：将网络设备、宿主机、虚拟机等产生的日志进行集中化收集和管理。

5）安全物理环境

云机房物理环境安全措施主要包括但不限于火灾检测、双路供电、访问控制、视频监控、机房热备等。

（1）火灾检测：火灾检测作用于机房后形成安全能力：云数据中心机房配备火灾自动报警系统，包括火灾自动探测器、区域报警器、集中报警器和控制器等，能够对火灾发生的部位以声、光或点的形式发出报警信号，并启动自动灭火设备，切断电源、关闭空调设备等。

（2）访问控制：访问控制作用于机房后形成安全能力：云数据中心的物理设备和机房的访问要具备访问控制策略，包括机房的进出访问控制。例如，进出机房或者携带设备进出机房，物理设备的配置、启动、关机、故障恢复等，均需具备相应的访问控制策略。

（3）视频监控：视频监控作用于机房后形成安全能力：云数据中心机房装设视频监控系统或者有专人 24 小时值守，对通道等重要部位进行监视。例如，对出入通道进行视频监控，同时报警设备应该能与视频监控系统或者出入口控制设备联动，实现对于监控点的有效监视。

4、云等保 2.0 合规能力模型

首先，明确云计算保护对象；其次分析云计算系统所拥有的原生安全措施以及为应对可能面临的威胁建设的安全防护措施，并分析云平台安全措施作用于保护对象后所形成的安全技术能力；最后比较云平台安全技术能力与网络安全等级保护 2.0 基本要求间的差距，分析云平台的合规情况，构建云等保 2.0 合规能力模型。

1）模型建立

安全技术能力是云计算系统安全措施作用于保护对象上形成的抵抗外部攻击的一种防护能力，构建 SMO 矩阵模型，如表 2 所示。

	保护对象 1	保护对象 2	……	保护对象 *m*
安全措施 1	√	N/A	√	N/A
安全措施 2	√	√	N/A	√
……	N/A	√	√	√
安全措施 *n*	√	N/A	√	√

表 2 SMO 矩阵模型

表 2 中，“ √ ” 表示安全措施在保护对象上能够起到相应的安全作用；N/A 表示安全措施无法作用于保护对象或作用于保护对象时无法起到相应的安全作用。根据不同的安全措施作用于不同的保护对象形成的安全能力，构建 SCMO 矩阵模型，如表 3 所示。

	保护对象 1	保护对象 2	……	保护对象 *m*
安全措施 1	1	—	0	—
安全措施 2	–1	0	—	–1
……	—	1	1	0
安全措施 *n*	0	—	–1	–1

表 3 SCMO 矩阵模型

表 3 中，“ 0” 表示云平台原生安全措施作用于保护对象后提供的安全能力，在云平台交付时，默认交付；“ 1” 表示云平台提供的安全能力，在云平台交付时，用户根据业务需求，考虑系统所面临的威胁，需按需购买；“ -1” 表示根据业务需求，用户自行部署安全产品或安全加固后所形成的安全能力。“ 0” 为定量，“ 1” 和“ -1” 为变量。“ — ” 表示安全措施无法作用于保护对象或作用后未形成安全能力。

综合云平台保护对象、安全措施、安全能力间的关系，构建云网络安全等级保护 2.0 合规模型，根据模型分析得出云安全技术能力，与网络安全等级保护 2.0 基本要求项进行对比，进行合规性评估，如图 4 所示。对于不符合项，识别云计算平台脆弱性，及时作出相应的加固，增强抵御风险的防护能力。

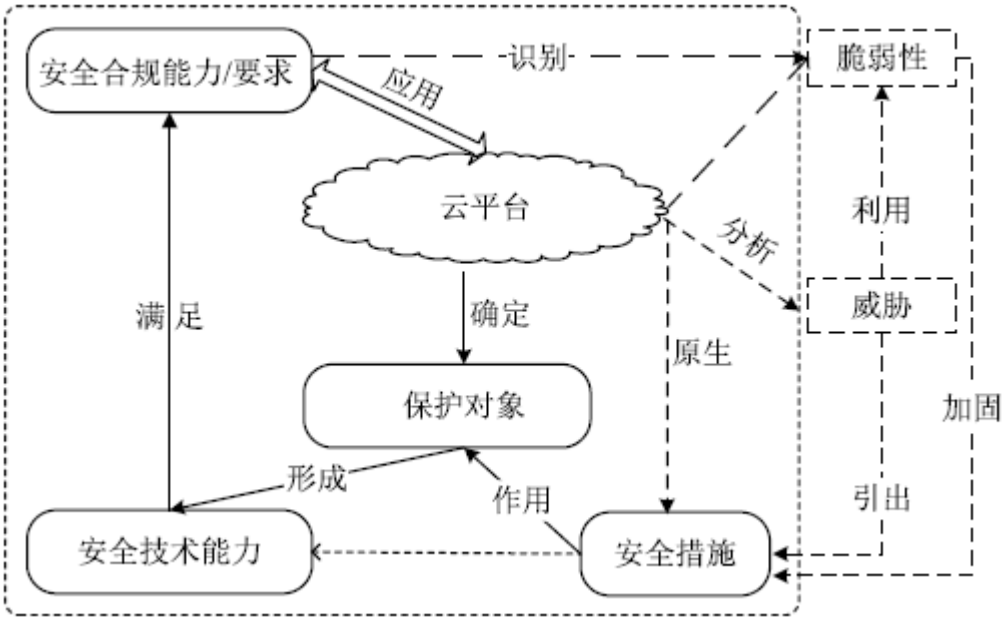


图 4 云平台网络安全等级保护 2.0 合规模型

2）模型应用

识别云计算保护对象、安全措施，分析得到云计算安全技术能力，基于云平台网络安全等级保护合规能力模型，与网络安全等级保护 2.0 基本要求项进行对比，进行安全合规性评估，如图 5 所示。对于不符合项，识别云计算云平台脆弱性，及时作出相应的加固，增强抵

御风险的防护能力。

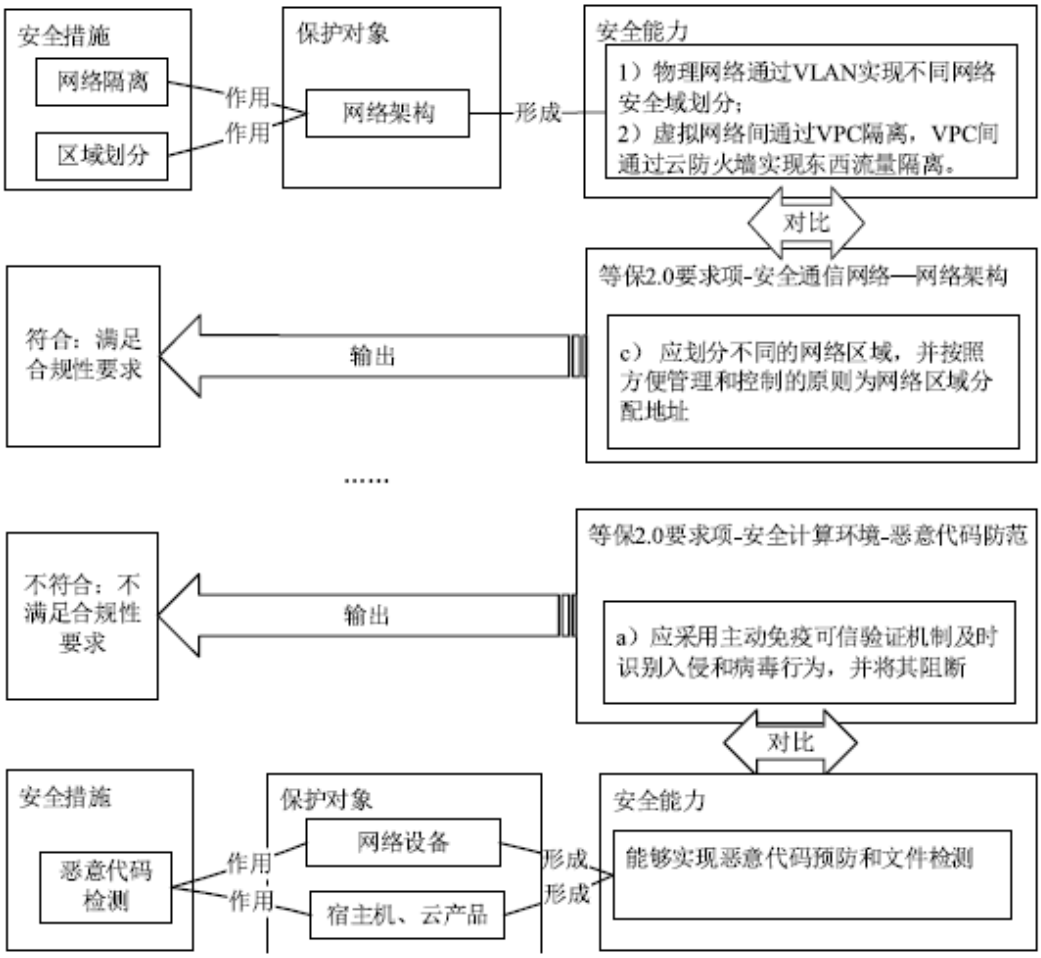


图 5 云平台网络安全等级保护 2.0 评估方法

5、结束语

本文基于网络安全等级保护 2.0 安全架构防护体系和云计算的实现机制，首先对云计算平台的保护对象进行识别；然后基于网络安全等级保护“ 一个中心，三重防御” 的主动防御、动态防护的思想，分析了云计算平台当前具有的安全措施，并对安全措施作用于保护对象后形成的安全能力进行分析、识别，从而构建网络安全等级保护 2.0 合规能力模型。本文对模型的使用进行了简要说明，该模型可有效帮助云服务商了解自身云平台所具备的安全技术能力与合规性要求间的差距，便于及时发现云计算平台的脆弱性，以便能够及时进行安全性加固，进而为用户提供更加安全的云计算服务。（来源：信息网络安全杂志 2019 年 12 期）

➢ 2019 全球数据与信息治理回顾与前瞻

如果说 2018 年因欧盟《通用数据保护条例》（GDPR）生效而被称为世界数据治理元年，那么 2019 年就是延续与反思之年。从美欧到中国，从立法到执法，全球数据治理格局呈现“不变中的变化”与“变化中的不变”。

一、个人数据保护执法：一山更比一山高

2019 年，英国信息专员办公室（ICO）凭借 GDPR 利剑，对英国航空（British Airways）和万豪国际（Marriot）分别开出 1.8339 亿英镑和 9920.0396 万英镑的巨额罚单。而在大西洋的彼岸，美国联邦贸易委员会对 Facebook 开出了 50 亿美元的罚单，可谓前无古人。在中国，2019 年伊始，中央网信办、工信部、公安部、市场监管总局即联合发布《关于开展 App 违法违规收集使用个人信息专项治理的公告》，在全国范围开展专项治理。在联合治理之外，公安部开展的“净网 2019”专项行动、市场监管总局开展的“守护消费”暨打击侵害消费者个人信息违法行为专项执法行动、工信部网安局开展的“电信和互联网行业提升网络数据安全保护能力专项行动”、工信部信管局开展的“信息通信领域 App 侵害用户权益专项整治行动”，亦前赴后继，形成了具有中国特色的个人信息保护执法格局。与美欧相比，中国的执法机关更分散，法律依据更多样，处置措施也更复杂。

事件 1：英国航空和万豪国际因违反 GDPR 遭受巨罚

2019 年 7 月 8 日，英国 ICO 宣布其拟就英国航空违反 GDPR 的行为对其处以 1.83 亿英镑的罚款。在该事件中，访问英国航空网站的用户流量被导向了一个欺诈性网站，大约 50 万名消费者的姓名、电子邮件地址、信用卡等信息遭到泄露。2019 年 7 月 9 日，ICO 宣布就万豪国际违反 GDPR 的行为对其处以 9920 万英镑的罚款。

事件 2：因 8700 万数据被滥用 Facebook 被罚 50 亿美元

2018 年 3 月，《卫报》和《纽约时报》曝出英国政治咨询公司剑桥分析（Cambridge Analytica）在未获得用户授权的情况下，通过在线性格测验的方式获取 8700 万 Facebook 用户的个人信息，在 2016 年的美国总统大选中，这些数据被用于新闻或观点的精确投放，以帮助特朗普团队。“剑桥分析”事件后，美国联邦贸易委员会（FTC）重启对 Facebook 的调查，旨在探明其是否违反了和解令，并对 Facebook 处以 50 亿美元的罚款。但是，Facebook 的代价绝不限于罚款，此次针对 Facebook 的新和解令象征 FTC 在隐私与网络安全方面监管公司的重大变化。

事件 3：中国 App 专项治理

2019 年，中国四部委开展 App 专项治理工作，对 1000 余款 App 的协议文本、使用体验、技术细节三方面进行测试，督促问题严重的近 300 款 App 进行整改，整改问题达 800 余个，并制定和实施了《App 违法违规收集使用个人信息行为认定方法》，明确“未明示收集使用个人信息的目的、方式和范围”“未经用户同意收集使用个人信息”“违反必要原则，收集与其提供的服务无关的个人信息”等违法行为的具体含义。

二、个人数据保护立法：美国的宪法时刻

在 GDPR 影响下，2018 年，美国加州率先出台了《加州消费者隐私法案》（CCPA），但是，加州并非独行者。在美国，激烈的公众讨论和行动将可能导致传统隐私权的结构性变化，以至于 2019 年成为美国个人数据保护的宪法性时刻（Privacy’s Constitutional Moment）。

事件 4：《加州消费者隐私法案》的重大发展

2019 年 10 月 10 日，加利福尼亚州总检察长 Xavier Becerra 宣布发布 CCPA 实施条例草案，为 2020 年 1 月 1 日生效的 CCPA 铺平了道路。尽管 CCPA 相对宽松，但是，在有些方面，它比 GDPR 走得更远。CCPA 实施条例特别规定了企业在收集个人信息之时或之前向消费者履行的告知义务；关于选择退出出售个人信息之权利的告知义务（如设置“请勿出售”按钮）；关于为收集、出售或删除个人信息而可能提供的财务激励或者价格或服务差异的告知义务；以及企业隐私政策必须包含的内容。此外，它还强调“无区别对待”原则。企业不得因消费者行使其在 CCPA 下的权利而区别对待该等消费者。但是，这不意味着企业不能提供差异化的价格或服务，前提是该等差异与相应消费者数据向企业提供的价值“直接相关”。

事件 5：美国联邦隐私法案的提出

在 CCPA 的刺激下，伊利诺伊州、纽约州和华盛顿州都在筹备自己的个人信息保护法，层出不穷的立法使科技公司开始支持联邦层面的统一立法。2019 年 11 月 26 日，多名民主

党参议员联合提出《消费者线上隐私权法》（COPRA）。这份综合性隐私法案将向个人授予对他们数据的广泛控制权、设置关于数据处理的新义务以及扩大美国联邦贸易委员会（FTC）在数字隐私方面的执法职能。

与 CCPA 相比，COPRA 首先明确了个人一系列数据权利，包括访问权、删除权、更正权和可携带权以及反对数据转移给第三方的权利。其次，它指示 FTC 成立一个新的部门专门负责隐私和数据安全问题，并设立一个“数据隐私和安全救济基金”，用于补偿受影响的个人。COPRA 还指示 FTC 发布实施条例，例如进一步定义敏感的涵盖数据，并建立相应流程以供个人反对涵盖数据的转移。最后，COPRA 向个人赋予了私人诉讼权，个人每天就每一侵权行为可以获得的一般损害赔偿从 100 美元至 1000 美元不等。

三、数据跨境流动：云深不知处

不论是 GDPR，还是《澄清域外合法使用数据法案》（CLOUD 法案），均尝试确立数据跨境流动的新规则。不过，GDPR 所规制的主要是贸易场景下大规模而持续的数据流动，而 CLOUD 法案所讨论的则是执法协作场景中跨境电子证据调取机制。自 2018 年 3 月出台以来，CLOUD 法案引发了无穷争议，也迫使相关国家启动与美国的双边谈判，重构数字时代的数据流动框架。

事件 6: 欧洲数据保护委员会发布关于美国 CLOUD 法案以及对 GDPR 之域外效力的意见

2019 年 7 月 10 日，欧洲数据保护委员会（EDPB）和欧洲数据保护监督机构（EDPS）发表了一项联合评估，指出 CLOUD 法案的域外效力可能导致服务提供商“较易面临美国法律与 GDPR 及其他适用的欧盟法律或成员国国内法律之间的法律冲突”。两部门指出，GDPR 第 48 条规定，非欧盟权力机构要求在欧盟以外转移个人数据的任何命令都必须得到司法互助条约（MLAT）等国际协议的承认，方才有效。因此，两部门称，“欧盟企业通常应当拒绝直接的请求并且请发出请求的第三国权力机构依照现行有效的法律互助条约或协议行事”。另一方面，这并不意味着 GDPR 与 CLOUD 法案绝对不相容，在保护生命或人身安全等个人“重要利益”的情形下，相关数据可以跨境传输。这显然是不够的，两部门建议欧盟和美国就一项新的国际协议开展谈判，该协议应包含强有力的程序保障措施并保护基本权利，同时支持“双重犯罪”原则。

四、平台数据之争：公地还是私域

2019 年 10 月 31 日，第十九届中央委员会第四次全体会议通过的《推进国家治理体系和治理能力现代化若干重大问题的决定》首次将“数据”纳入与劳动、资本、土地并驾齐

驱的生产要素，这凸显了数据的经济地位。由于数据自身的特殊性，数据在“使用上的排他性”和“享有上的竞争性”方面与传统财产迥异，使确立数据使用规则困难重重。2019 年，围绕网络平台数据的中外诉争恰恰显示了这一分歧。

事件 7：hiQ Labs 诉 LinkedIn 案上诉判决出炉

2019 年 9 月 9 日，美国第九巡回上诉法院对“hiQ 诉 LinkedIn 案”做出裁决，认定 hiQ Labs 公司从领英（LinkedIn）抓取公开的个人信息数据的行为并未违反《计算机欺诈和滥用法案》，维持此前做出的对 hiQ Labs 公司有利的裁决。在本案中，hiQLabs 对公开信息的爬取行为是否构成 CFAA 下“未经授权访问”，是核心争点。对此，上诉法院着重指出，CFAA 此处禁止的是类似“破坏并闯入”计算机的行为，而非仅仅“使用”计算机的行为。因此，CFAA 是一部“反侵入”法，而非反“滥用数据”法。领英网站数据默认对所有人公开，人人得以访问，不适用 CFAA，hiQLabs 不构成“未经授权访问”。

事件 8：腾讯诉今日头条不正当竞争案

2019 年 1 月 15 日，今日头条推出短视频社交产品多闪，其下载链接短时间内被微信屏蔽，理由是“网页包含不安全内容”。三天后，今日头条母公司字节跳动官网的链接（bytedance.com）步其后尘，微信页面显示“网页包含诱导分享、关注等诱导行为内容，被多人投诉，为维护绿色上网环境，已停止访问”。一周后，事态进一步升级，抖音的新用户无法以微信授权的方式登录抖音 App。2019 年 2 月 28 日，腾讯一纸诉状，将头条诉诸法院。2019 年 3 月 20 日，天津市滨海新区人民法院公布了对腾讯起诉字节跳动旗下抖音、多闪涉嫌违规使用用户数据一事的裁定结果。法院裁定，抖音立刻停止在抖音中向抖音用户推荐好友时使用来源于微信/QQ 开放平台的微信用户头像、昵称；立刻停止将微信/QQ 开放平台为抖音提供的已授权微信/QQ 的登录服务提供给多闪使用，并不得以类似方式将其提供给抖音以外的应用使用；抖音、多闪立刻停止在多闪中使用来源于微信/QQ 开放平台的微信用户头像、昵称。

与 hiQ Labs 诉 LinkedIn 案不同，本案并不涉及数据爬取，而是经由腾讯开放平台应用编程接口（Open API）的数据调取，故此，法院所审查的重心自然落在 Open API 的数据调取规则，也就是双方签署的开放平台《开发者协议》上。根据《开发者协议》，抖音和多闪是由不同的企业主体运营的独立应用，多闪并未申请接入微信/QQ 开放平台，也并未与腾讯达成《开放者协议》，并非合同的一方，不享有通过 Open API 调取任何数据的权利。同时，根据《开发者协议》第 2.7.6 条，它也不能从抖音那里间接获取数据，因而，多闪应当将非法获取的头像和昵称删除。其次，对于抖音而言，其固然有权调取数据，但是，必须在《开发

者协议》授权的范围内。《开发者协议》第 2.7.2 和 2.7.3 条明确规定，抖音不得将所合法获得的前述数据自行或提供给其用户、客户用于创建、补充或维护自身关系链，不得利用合法获得的数据（包括但不限于微信用户关系链等）实施或变相实施任何形式的推广、营销、广告行为。因此，尽管抖音获取数据并未违约，可它展示头像和昵称进行推广的数据使用方式却违反了《开发者协议》。

五、迈向公共治理的数据治理

数据不仅仅是企业的投入品，更是国家经济运行机制的重要生产要素，是国家治理能力的“基础性战略资源”；数据亦不仅仅是企业的产出品，更关乎世界范围内的生产、流通、分配、消费活动，具有全球化和跨国界的天然属性；数据也不仅仅限于企业，在数字化生存的时代，它改变了普罗大众对自我和对隐私的观念，同时塑造了人与人交往的方式。随着整个社会的数字化转型，在过去一年，数据治理开始从个人和企业的私领域日益向公共领域迈进。

事件 9 ：公共的“人脸”

浙江理工大学特聘副教授郭兵于 2019 年 10 月 28 日向杭州市富阳区人民法院提起诉讼。这一案件肇始于一封短信。作为杭州野生动物世界的年卡用户，杭州野生动物世界通过短信的方式告知郭兵“园区年卡系统已升级为人脸识别入园，原指纹识别已取消，未注册人脸识别的用户将无法正常入园，同时也无法办理退费”。郭兵认为，人脸识别等个人生物识别信息属于个人敏感信息，一旦泄露、非法提供或者滥用，将极易危害消费者人身和财产安全。

事件 10：《数据安全管理办法（征求意见稿）》和《网络信息内容生态治理规定》发布

数据是个人、企业、社会、国家利益的聚合点，2019 年 5 月 28 日发布的《数据安全管理办法（征求意见稿）》回应了这一趋势，将个人信息、国家重要数据和企业数据资源均囊括其中，形成了“狭义数据安全”（保密性、完整性、可用性、可控性）和“广义数据安全”（避免因数据的收集、存储、处理和使用给个人、社会和国家造成危害）的复合结构。12 月 25 日发布的《网络信息内容生态治理规定》进一步提升了数据治理的公共性。遵循网络空间共享共治的理念，该规定以建立健全网络综合治理体系、营造清朗的网络空间、建设良好的网络生态为目标，要求政府、企业、社会、网民等各个主体各负其责，开展弘扬正能量、处置违法和不良信息等相关活动。这一规定站在网络空间的宏观视角重新思考数据解决之道，未尝不能成为数据公共治理的新思路。

六、2020 年新趋势

在一本 25 年前的书《未来之路》中，比尔·盖茨畅想了互联网带来的虚拟现实、智能助手、定向广告和 P2P 金融革新，同时，他也提出对个人隐私、商业秘密和国家安全的忧虑。如今，未来已来，答案还需要每个人思考，人类只有在科技、伦理与法律的互动之中寻找正确的方向。

（一）个体对数据保护的关注度持续提升

在欧洲，GDPR 的实施让欧盟民众的个人数据权利意识飙升。欧盟的调查显示，2015 年，大约只有 20%的人知道政府保护个人数据，而现在有 57%的人了解到国家专设了数据保护局，提供个人数据权的缜密保障，有 67%的人听说过 GDPR 这部法律。同时，向各成员国数据保护局咨询 GDPR 和提出申诉的人日益增多，非营利组织代表个人发起的申诉也开始出现。

在美国，IBM 商业价值研究院的一项隐私调查显示：消费者强烈关注个人数据问题。其中，有 81％的消费者表示，他们已经更加关注公司如何使用其数据，而 87％的消费者则认为，公司应在个人数据管理方面受到更严格的监管。

在中国，利用百度关键词的趋势研究，可以发现，2019 年，主要测量网民关注的“资讯指数”（其将网民的阅读、评论、转发、点赞、不喜欢等行为的数量加权求和得出）在个人信息/隐私上录得新高，这与两年前主要是各大新闻报告关注的局面截然不同；因传播需要或界定不清，网民主要使用“隐私”而非“个人信息”一词，相反，专业的新闻机构已区分两者，自 2018 年起基本使用“个人信息”的概念。中国公众对个人信息/隐私的关注并非空穴来风。过去一年，人脸识别、视频监控、监控摄像头的普遍使用，从反面提升了大众的权利意识。根据欧洲专利办公室的统计，全球在上述领域的专利申请在 2019 年飙升，而中国又独占鳌头。

民众权利意识的提升亟待法律回应。2020 年即将出台的《民法典》将单辟“隐私权和个人信息保护”一章，对私密信息和个人信息加以规定。不仅于此，2020 年也是我国《个人信息保护法》制定的关键时刻，如何在满足民众对个人信息保护诉求的同时，平衡企业和政府对个人数据的利用，是一个棘手而复杂的问题。

（二）对产业“科技抵制”的思潮依然持续

大西洋两岸对大科技公司的调查和执法均日益趋紧。2019 年 6 月，美国司法部和联邦贸易委员会对苹果、亚马逊、Facebook 和 Alphabet（Google 母公司）的反垄断管辖权进行了划分，从而为 2020 年的正式调查奠定了基础。在国会层面，由美国司法部前官员、耶鲁大学经济学教授莫顿（Fiona Morton）提出“成立一家数据联邦通信委员会”（Digital FCC）的建议日益赢得支持，这一新的机构将监督大型科技企业的运作，从而保护竞争。可以预见，

在 2020 年，大科技公司个人信息保护以及数据垄断行为仍是持续发酵的核心议题。

如果说中国在 2019 年持续一年的 App 专项治理以个人信息收集为焦点，那么,在 2020 年，执法有可能延伸到个人数据的保存、处理、共享和删除环节，人脸信息等生物识别信息也会被严肃对待。随着《关键信息基础设施安全保护条例》的发布和《数据安全管理办法》的制定，大科技公司以及手握影响国家安全、公共利益的“重要数据”的企业，将面临更严峻的监管态势。此外，2020 年 1 月 2 日，国家市场监管总局公布《<反垄断法>修订草案(公开征求意见稿)》，新增“认定互联网领域经营者具有市场支配地位还应当考虑网络效应、规模经济、锁定效应、掌握和处理相关数据的能力等因素”一条，为我国开启数据领域反垄断执法铺平了道路。

（三）不断完善“通过数据”的政府治理

在“对数据治理”和“用数据治理”的二分法下，政府更偏向后者，即通过数据实现政府治理的一般目标。放宽视野看，这也是推进国家治理体系和治理能力现代化的重要一环，或者用国务院《促进大数据发展行动纲要》的表述，建立一个“用数据说话、用数据决策、用数据管理、用数据创新”的管理机制。通过数据治理，可以在如下方面发挥作用，一是公共服务的开放化、个性化和便捷化；二是行政决策的回应化和智能化；三是行政监管和个案调查的主动化和敏捷化。上述内容落实到数据治理环节，即公共数据开放、公共数据共享、公共数据报送。

公共数据共享是“用数据治理”的“基础设施”。如何在不同政府部门之间打破数据孤岛，促进数据安全合规的流通是数据驱动型治理的症结所在。尽管我国“通过数据的治理”已取得显著成绩，但是，其所带来的侵害个人、企业权益的风险还未被充分重视。2019 年，“社会信用体系建设”的争议反映出公众对于“一处失信，处处受限”的不满，其实质是公共数据在政府内部之间共享导致的“与事件无关之考虑”，涉嫌违反不当联结禁止原则。2019 年，在数据开放环节，因数据公开导致个人诉请删除个人信息的案件已经出现，如何在公众知情权和个人信息权益之间达到平衡，值得认真对待。此外，公共数据报送也频频遭受数据事项过多、范围过宽、报送目的不明确、报送程序不健全等诟病。如何在数据报送过程中落实依法报送、权利保障、正当程序和比例原则，必将成为未来制度的关键。（来源:《中国信息安全》杂志 2020 年第 2 期）

四、政府之声

➢ 2020 年网络扶贫工作要点印发实施

2020 年 3 月 18 日，近日，中央网信办、国家发展改革委、国务院扶贫办、工业和信息化部联合印发《2020 年网络扶贫工作要点》。通知要求，坚持以习近平新时代中国特色社会主义思想为指导，深入学习贯彻习近平总书记关于扶贫工作的重要论述，贯彻落实习近平总书记在决战决胜脱贫攻坚座谈会上的重要讲话精神，认真落实《中共中央、国务院关于打赢脱贫攻坚战三年行动的指导意见》，咬定目标，坚持标准，集中兵力打好深度贫困歼灭战，全面完成剩余脱贫任务，把网络短板补得更扎实一些，把信息基础打得更牢靠一些，推动网络扶贫行动再上新台阶，不断激发贫困地区内生动力，坚决打赢脱贫攻坚战。

《工作要点》明确了工作目标：2020 年底前，《网络扶贫行动计划》目标任务全面完成并巩固提升。网络覆盖质量进一步提升，全国行政村通光纤、通 4G 比例达到 99%，贫困村通宽带比例达到 99%。电商服务通达所有乡镇，快递服务基本实现乡乡有网点，电商帮扶贫困户增收作用更加明显。全国中小学（含教学点）宽带接入率达到 99%，出口带宽达到 100Mbps 以上，探索采用卫星通信等多种技术手段实现学校互联网全覆盖，“互联网+教育”显著增强贫困人口内生动力。县级以上医院普遍具备千兆网络接入能力，远程医疗覆盖所有贫困县。信息服务体系更加完善，网络公益持续深化，构建起人人参与的网络扶贫大格局。

《工作要点》部署了 8 个方面 28 项重点任务。

一是坚决打赢疫情防控阻击战。主要任务有：充分利用信息化手段做好贫困地区疫情防控，利用云计算、大数据等手段，为疫情防控提供数据支撑；积极开拓网络扶贫信息惠民服

务，充分依托已有资源，鼓励相关机构开展远程教育、远程医疗、远程心理健康疏导，及时提供就医、交通和生活服务信息等。

二是集中力量打好深度贫困歼灭战。主要任务有：扎实开展网络扶贫深度行活动，动员更多资源和力量向深度贫困地区倾斜；开展网络促进稳边富民行动，带动民族地区贫困人口脱贫增收；持续加大对深度贫困地区支持力度，积极引导政策性银行加大对网络扶贫项目的支持，扎实推进一批网络扶贫项目。

三是优先帮扶特殊贫困群体。主要任务有：完善特殊贫困群体信息服务，推进“互联网+公共就业服务”；加强因病致贫返贫群众救助，推进“互联网+医疗健康”；完善留守人员信息服务，实施精准帮扶；带动贫困妇女脱贫增收，打造适合妇女特点的电商品牌；加强对贫困残疾人帮扶，持续推进贫困残疾人康复、教育、就业、社保等数据部门间共享；搭建普通话培训学习远程平台，完善少数民族语言智能翻译软件。

四是以信息化支撑返贫人口和新发生贫困人口的监测预警。主要任务有：加强扶贫开发数据整合运用，进一步完善全国扶贫开发信息系统，加强行业部门扶贫数据共享和比对分析；探索大数据技术在返贫监测预警中的应用，开展返贫人口和新发生贫困人口精准动态帮扶。

五是深化网络扶贫东西部协作。主要任务有：加大网络扶贫东西部协作组织实施力度，督促帮扶双方做好网信资源汇聚和对口帮扶项目实施，促进沟通对接，细化帮扶举措；围绕网信产业合作、劳务协作、网信人才培训、电子商务、远程医疗等领域，实施一批东西部协作项目，加强项目跟踪问效。

六是巩固提升网络扶贫工程成效。主要任务有：推进电信普遍服务项目建设，提升4G和宽带网络覆盖水平；深入推进电子商务进农村综合示范，推动消费扶贫线上线下相结合，推进“互联网+”农产品出村进城工程，提升农村物流服务覆盖面和服务质量；扎实推进网络扶智工程攻坚行动，实施学校联网攻坚行动，开展“网联优教”教育信息化精准扶贫项目；健全网络扶贫信息服务体系，支持贫困地区大学生村官和大学生反哺归乡创业创新；积极开展网络公益扶贫，动员更多社会力量参与，助力精准扶贫。

七是建立网络扶贫长效机制。主要任务有：引导网信企业与贫困地区深化结对帮扶，强化结对帮扶项目的跟踪督促；接续推进数字乡村建设，支持已摘帽并稳定脱贫的贫困县纳入国家数字乡村试点；提升贫困群众网络技能和信息素养，持续开展农民手机应用技能培训，开展深度贫困地区教育信息化“送培到家”活动；加强网络扶贫人才队伍建设，引导贫困村党组织书记及村“两委”成员发挥网络扶贫带头人作用。

八是压实工作责任，狠抓任务落实。主要任务有：强化组织领导和统筹协调，加强部门

间政策协同和资源整合，共同推动重点任务和项目实施，形成工作合力；加强监测评估，推动项目取得实效；开展经验交流，遴选网络扶贫典型案例，鼓励基层和网信企业运用互联网创新扶贫模式；加强宣传推广，利用各类网络平台，以生动的事实反映贫困群众脱贫致富后的喜人变化，增强传播效能。（来源：中国网信网）

➢ 工业和信息化部办公厅关于推动工业互联网加快发展的通知

2020 年 3 月 20 日，工业和信息化部办公厅正式发布《关于推动工业互联网加快发展的通知》。《通知》包含 6 方面 20 项措施。其中，“加快新型基础设施建设”被排在最首要的位置。

工业互联网新型基础设施主要包括工业互联网内外网、标识解析体系、工业互联网平台、安全态势感知平台、工业互联网大数据中心等。《通知》要求，推动基础电信企业建设覆盖全国所有地市的高质量外网，利用 5G 改造工业互联网内网。出台工业互联网标识解析管理办法，新增标识注册量 20 亿，进一步增强网络基础资源支撑能力。引导平台增强 5G、人工智能、区块链、增强现实、虚拟现实等新技术支撑能力，发展 50 家重点工业互联网平台，推动重点平台工业设备连接数达到 80 万台。加快国家工业互联网大数据中心建设，建立工业互联网数据资源合作共享机制。

中国工业互联网研究院院长 徐晓兰：工业互联网它是实现全要素、全产业链、全价值链的全面的连接，它对我们的生产的组织方式和生产范式，都带来了一个变革性的发展，它不仅仅带动我们数字经济的发展，还带动我们社会的数字化转型。

中国信息通信研究院数据显示，工业互联网融合带动的经济影响正在快速扩张。2019 年我国工业互联网产业经济增加值规模为 2.13 万亿元，带动新增就业岗位 206 万个。预计 2020 年，我国工业互联网产业经济增加值规模将达到 3.1 万亿元，占 GDP 比重 2.9%，对经济增长的贡献将超过 11%，带动新增就业岗位 255 万个。（来源：工业和信息化部办公厅）

- **工业和信息化部办公厅关于推动工业互联网加快发展的通知 工信厅信管〔2020〕8 号**
- http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757016/c7828839/content.html

➢ 十一部门印发《整治虚假违法广告部际联席会议 2020 年工作要点》

2020 年 3 月 18 日，国家市场监管总局、中央宣传部、中央网信办、工业和信息化部、公安部、国家卫生健康委、人民银行、广电总局、银保监会、中医药局、国家药品监督管理局等十一部门联合印发《整治虚假违法广告部际联席会议 2020 年工作要点》（以下简称《工作要点》）和修订后的《整治虚假违法广告部际联席会议工作制度》（以下简称《工作制度》），以进一步加强广告市场协同监管，严厉打击虚假违法广告，维护良好广告市场秩序。

《工作要点》明确了 2020 年整治虚假违法广告工作的五项重点任务。其中明确要求加强重点产品、重点行业广告监管，严厉打击医疗、药品等事关人民群众健康和财产安全的虚假违法广告。在新冠肺炎疫情防控工作期间，统筹抓好疫情防控与广告监管执法工作，重点针对涉及口罩等防护用品广告以及涉及借疫情宣传疫病防治内容的虚假违法广告开展监测，依法从严从快查处。要治理规范移动端互联网广告，坚决遏制移动 APP、自媒体账号等虚假违法广告多发、易发态势。同时，要强化广告协同监管，加强部门间沟通及信息共享，强化联合部署、联合约谈告诫、联合执法、联合调研，提升部际联席会议协调调度能力；并健全完善重点案件联合督办机制，对重大违法案件实行统一挂牌督办；研究建立广告领域失信联合惩戒机制，推动形成一处违法、处处受限的广告信用监管格局。

《工作要点》明确，市场监管部门要严格药品、医疗器械、保健食品、特殊医学用途配方食品广告审查工作，严把广告审查准入关。药品监管部门要加强与市场监管等部门的沟通协作，充分发挥整治虚假违法广告部际联席会议机制作用。对发现的违法广告，及时移交相关部门处理，对涉及严重失信的企业，实施联合惩戒，并加大对药品、医疗器械生产企业监督检查力度，依法从严监管。

根据《工作制度》，各成员单位要发挥职能作用。国家药监局要加强药品、医疗器械、

化妆品生产企业监督管理，对相关部门移送的除发布虚假违法广告外，还涉嫌其他违法生产经营行为的，要将相关生产经营者列为重点监管对象，加大惩治力度。（来源：国家市场监管总局）

- **市场监管总局等十一部门关于印发《整治虚假违法广告部际联席会议 2020 年工作要点》和《整治虚假违法广告部际联席会议工作制度》的通知**
- http://gkml.samr.gov.cn/nsjg/ggjgs/202003/t20200318_313133.html

➢ 工业和信息化部关于推动 5G 加快发展的通知

2020 年 3 月 24 日，为深入贯彻落实习近平总书记关于推动 5G 网络加快发展的重要讲话精神，工业和信息化部发布（以下简称《通知》），要求各地各单位在做好疫情防控工作的同时，全力推进 5G 网络建设、应用推广、技术发展和安全保障，充分发挥 5G 新型基础设施的规模效应和带动作用，支撑经济社会高质量发展。就此，请中国信息通信研究院副院长王志勤对《通知》进行了解读。

问：当前时期，加快 5G 发展有什么重要意义？

答：5G 是全球科技革命中的引领性技术，是支撑经济社会高质量发展的新型基础设施，具有战略性、基础性和先导性。5G 也是新一轮产业革命的关键要素，不仅将激发新型消费和投资、促进就业创业、解放生产力，还将重构生产关系和社会关系、促进社会治理，对人们生产生活带来重大而深远的影响。

2020 年是 5G 商用突破的关键之年，也是我国全面建成小康社会的收官之年。党中央、国务院高度重视 5G 发展。近期，习近平总书记就加快 5G 发展多次做出重要指示，强调要“推动 5G 网络加快发展”“加快 5G 网络、数据中心等新型基础设施建设进度”。为贯彻落实习近平总书记指示精神，工业和信息化部发布《关于推动 5G 加快发展的通知》（以下简称《通知》），对于加快 5G 建设及应用、推动产业创新发展、助力经济平稳运行具有重要意义。具体来看：

一是有利于升级基础设施，赋能产业转型新时代。交通、电力等传统基础设施造就了工业化时代的奇迹，新一轮工业革命则需要新型基础设施的赋能。5G 新型基础设施建设不仅将从根本上改变移动网络的现状，促进数据要素的生产、流动和利用，还将让各行各业能够更便于联通协同、提供服务，带动形成万亿级 5G 相关产品和服务市场。

二是有利于拓展新型消费，创造美好生活新体验。5G 时代的到来，将让人们不仅享受到更高速、更低流量资费的网络，在智能终端、可穿戴设备、智能家居等方面创新出多样的消费产品，还将极大丰富消费场景，在电子商务、政务服务、网络教育、网络娱乐等方面创造出大量新消费。据中国信息通信研究院测算，2020-2025 年，5G 商用将带动超过 8 万亿元的新兴消费。

三是有利于稳定国内投资，打造经济发展新动能。5G 建设投资呈现出回收期长、带动性强、回报率高等特点。5G 网络建设不仅涉及大量的工程、基站、供电等基建投资，还将激发各行业转型升级，引致工厂改造、建设运营、系统升级、技术培训等诸多投资。预计到 2025 年 5G 网络建设投资累计将达到 1.2 万亿元，累计带动相关投资超过 3.5 万亿元。

四是有利于带动就业创业，形成社会发展稳定器。一是带动科研试验、生产建设、运营服务等产业就业，二是在工业、能源等诸多行业领域创造新的融合型就业需求，三是让随时随地工作、在家办公等更为便捷，拓展共享经济下的灵活就业。根据中国信息通信研究院的测算，预计到 2025 年，5G 将直接创造超过 300 万个就业岗位。

五是有利于提升政府服务，促进国家治理体系和治理能力现代化。5G 时代的到来，将可以利用对生态环境、经济社会的立体感知，为政务协同和全方位贴身服务的创新提供强大动力，加速治理模式、治理手段和治理过程的网络化智能化变革，助力国家治理体系和治理能力现代化。

问：《通知》提出了哪些重点任务？

答：《通知》面向近期的产业和经济社会发展目标，坚持问题导向，聚焦“网络、应用、技术、安全”四个重点环节，以网络建设为基础，以赋能行业为方向，以技术创新为主线，以信息安全为保障，系统推进，充分发挥 5G 的规模效应和带动作用，积极构建“5G+”新经济形态。

（一）加大支持力度，打造新型基础设施

当前处于 5G 网络集中建设初期，面临着投资成本、建设协调等多方面问题，需统筹布局，加大地方政策支持和落地实施，进一步发挥电信运营企业的建设运营主体作用。对于政策支持力度大、落实好的地区，运营企业应加大投资力度，优先开展 5G 建设；政策环境尚不完善的地区，需加快研究落实支持举措。一方面是加快建设部署。重点做好 5G 网络统筹部署规划，加快推进主要城市的网络建设，加快数据中心等新型基础设施建设，提升用户端到端的网络感知体验。另一方面是加大资源统筹支持。要加大基站站址资源支持，加强 5G 用电和频率保障，保障网络快速建设运营，同时深化共建共享和 5G 异网漫游，降低运营企

业运营的边际成本。

（二）深化融合应用，构建繁荣生态体系

我国 5G 融合应用仍处于探索期，需尽快从单点应用向规模应用转变。加快 5G 融合应用发展，需从丰富应用场景着手，打造重点应用领域，建设应用产业生态系统。具体来看，在产业领域，实施“5G+工业互联网”等工程，推动 5G 融合工业互联网、边缘计算等新一代信息技术，加快在制造业、医疗健康、车联网等垂直行业领域的应用，探索形成互利共赢的各种新业态、新模式。在消费领域，利用 5G 套餐优惠、信用购机举措，加快用户向 5G 服务迁移，鼓励终端消费；推广 5G+VR/AR、赛事直播、游戏娱乐、虚拟购物等应用，培育新兴消费模式，拓展新型消费领域。

（三）加强技术研发，健全产业创新体系

针对我国 5G 产业链的不足，加快 5G 技术创新，是带动通信产业转型升级、推动传统产业数字化转型的根本保障。具体来看，一是加强 5G 技术和标准研发。需把提升技术创新能力摆在更加突出位置，加快 5G 基础架构研究，加快关键元器件、软件、仪器仪表、模组等研发及应用，发展壮大 5G 产业集群。二是开展 5G 测试验证。持续开展 5G 增强技术研发试验，加快毫米波设备、5G SA 设备等的测试迭代，促进系统间互操作，加速技术和产业成熟。三是强化 5G 技术创新支撑能力。支持领先企业基于 5G 打造并提供行业云服务、能力开放平台、应用开发环节等共性平台，搭建检测认证平台，鼓励开源生态建设，促进开放式创新。

（四）强化能力建设，建立安全保障体系

5G 引入了网络功能虚拟化、边缘计算、网络切片、服务化架构等新技术新特征，也带来了新的安全风险，必须打造 5G 安全保障体系，为产业健康发展保驾护航。一是加强基础设施安全保障。建立 5G 关键设备检测认证等网络基础设施安全保障机制，开展 5G 安全检测，建设网络安全态势感知、威胁治理、事件处置、追踪溯源的安全防护体系。二是强化数据安全保护。围绕 5G 典型应用场景，建立网络数据安全管理制度与标准规范，加快形成事前、事中、事后的全环节数据安全技术监管能力。三是培育安全产业和治理生态。培育 5G 网络安全产业生态，积极创新 5G 安全治理模式，推动建设多主体参与、多部门联动、多行业协同的安全治理机制。（来源：工信微报）

- **《工业和信息化部关于推动 5G 加快发展的通知》工信部通信〔2020〕49 号**
- http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c7832258/content.html

五、本期重要漏洞实例

➢ Adobe ColdFusion 任意文件读取安全漏洞

发布日期：2020-03-18
更新日期：2020-03-27
受影响系统：
Adobe ColdFusion <= 2018 Update 7
Adobe ColdFusion <= 2016 Update 13
描述：

CVE(CAN) ID: CVE-2020-3761
Adobe ColdFusion 是一套快速应用程序开发平台。
Adobe ColdFusion 2016 Update 13 及之前版本、ColdFusion 2018 Update 7 及之前版本，在实现中存在远程文件读取安全漏洞。攻击者可利用该漏洞从 Coldfusion 安装目录中读取任意文件。
链接：https://helpx.adobe.com/security/products/coldfusion/apsb20-16.html
建议：

厂商补丁：
Adobe
Adobe 已经为此发布了一个安全公告（APSB20-16）以及相应补丁：
APSB20-16：Security updates available for ColdFusion
链接：https://helpx.adobe.com/security/products/coldfusion/apsb20-16.html

➢ VMware Workstation vmnetdhcp.exe 组件资源管理错误漏洞

发布日期：2020-03-17
更新日期：2020-03-17
受影响系统：
VMware Workstation
描述：

CVE(CAN) ID: CVE-2020-3947
VMware Workstation 是 VMware 公司推出的一款桌面虚拟计算软件。VMware Workstation 中的 vmnetdhcp.exe 组件存在资源管理错误漏洞，该漏洞源于程序在对对象进行操作之前未能验证该对象是否存在。攻击者可利用该漏洞提升权限并执行任意代码。
建议：

厂商补丁：
VMware

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://www.vmware.com/security/advisories/VMSA-2020-0004.html

➢ WordPress-5.3.2 up***.php 文件存在文件上传漏洞

发布日期：2020-3-19
更新日期：2020-3-19
受影响系统：
WordPress WordPress 内容管理系统 5.3.2
描述：

CVE(CAN) ID: CNVD-2020-10532
WordPress 是使用 PHP 语言开发的博客平台，用户可以在支持 PHP 和 MySQL 数据库的服务器上架设属于自己的网站。Wordpress 5.3.2 版本 up***.php 文件存在文件上传漏洞，攻击者可利用该漏洞上传恶意文件。
建议：

厂商补丁：
WordPress
目前厂商尚未提供相关漏洞补丁链接，请关注厂商主页随时更新：
https://www.wordpress.com/

➢ Microsoft Edge 内存破坏漏洞

发布日期：2020-03-11
更新日期：2020-03-11
受影响系统：
Microsoft Edge
描述：

CVE(CAN) ID: CVE-2020-0816
Edge 是 Microsoft 公司为 Windows 10 打造的浏览器，特点是快速、安全。Microsoft Edge 存在内存破坏漏洞。该漏洞源于 Microsoft Edge 未能正确访问内存中的对象。攻击者可利用该漏洞在当前用户的上下文中执行任意代码，从而可获得与当前用户相同的用户权限。
建议：

厂商补丁：
Microsoft
厂商已发布了漏洞修复程序，请及时关注更新：
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0816

六、本期网络安全事件

➢ 团伙冒充农商行行长行骗被识破！竟有银行“内鬼”协助

2020 年 3 月 15 日报道：2019 年 4 月 20 日，一对男女在商水农商行营业大厅冒充该行行长和工作人员行骗，被商水农商行工作人员当场识破。

值得注意的是，在此次颇为拙劣的团伙行骗过程中，竟有银行“内鬼”从旁策应。根据裁判文书网 3 月 9 日披露的刑事判决书，3 名涉案的犯罪嫌疑人中，苗广福、郭改正均为河南省周口市商水县农民，而郭长征为商水农商行汤庄支行内退员工。

苗广福、郭改正诈骗二审刑事判决书

发布日期：2020-03-09　　浏览：50次

河南省周口市中级人民法院

刑 事 判 决 书

（2020）豫16刑终108号

原公诉机关商水县人民检察院。

上诉人（原审被告人）苗广福，男，汉族，1957年12月9日出生，初中文化，农民，户籍所在地河南省驻马店市西平县，捕前住河南省西平县。因犯诈骗罪，于2007年12月21日被河南省漯河市源汇区人民法院判处有期徒刑一年零六个月，并处罚金人民币一万元。因涉嫌诈骗犯罪，于2019年4月20日被商水县公安局刑事拘留，同年5月25日被逮捕。

经法院审理查明，2018 年 12 月份，郭改正经人介绍与被害人罗某相识，郭改正自称是商水农商行主任，能办理企业借款保函。后郭改正、郭长征预谋给罗某办假“借款保函”。

2019 年 4 月 19 日上午，“张玉梅”（女）和郭改正、苗广福、郭长征四人在商水农商行南见面，郭改正将事先准备的假身份证、文件和印章交给苗广福，后张玉梅和苗广福、郭长征协商，让郭改正向罗某索要现金人民币 4 万元，当日下午 14 时许，被告人郭改正以办理保函需要费用为由，在商水县“金汇国际酒店”511 房间内，骗取被害人罗某现金人民币 4 万元。后由苗广福和“张玉梅”分别冒充商水农商行行长李楠和银行工作人员，在商水农商行营业大厅与被害人罗某等人见面，在办理假借款保函过程中，被告人苗广福身份被识破，银行工作人员报警后，苗广福被抓，“张玉梅”趁机逃走。

据悉，侦察机关从苗广福携带的档案袋里发现伪造的李楠的身份证一个、商水农商行的

公章一枚、商水农商行的部分红头文件。郭改正于案发当晚和次日凌晨通过 ATM 机退款给罗某 39000 元。经鉴定，印章与商水农商行印章不是同一枚印章。

根据上述事实和证据，法院作出如下判决：被告人苗广福犯诈骗罪，判处有期徒刑二年，并处罚金人民币一万五千元；被告人郭改正犯诈骗罪，判处有期徒刑二年，缓刑三年，并处罚金人民币一万五千元；被告人郭长征犯诈骗罪，判处有期徒刑二年，缓刑三年，并处罚金人民币一万五千元。（来源：北青金融）

➢ 工信部就新浪微博 App 数据泄露问题开展问询约谈

2020 年 3 月 21 日，针对媒体报道的新浪微博因用户查询接口被恶意调用导致 App 数据泄露问题，工业和信息化部网络安全管理局对新浪微博相关负责人进行了问询约谈，要求其按照《网络安全法》《电信和互联网用户个人信息保护规定》等法律法规要求，对照工信部等四部门制定的《App 违法违规收集使用个人信息行为认定方法》，进一步采取有效措施，消除数据安全隐患：一是要尽快完善隐私政策，规范用户个人信息收集使用行为;二是要加强用户信息分类分级保护，强化用户查询接口风险控制等安全保护策略;三是要加强企业内部数据安全管理，定期及新业务上线前要开展数据安全合规性自评估，及时防范数据安全风险;四是要在发生重大数据安全事件时，及时告知用户并向主管部门报告。

新浪微博表示:公司高度重视数据安全和个人信息保护，针对此次事件已采取了升级接口安全策略等措施，后续将按照工信部要求，落实企业数据安全主体责任，切实做好用户个

人信息保护工作。

事件回顾：2020 年 3 月 19 日消息，微博名为“安全_云舒”的用户转发微博时称：“很多人的手机号码泄露了，根据微博账号就能查到手机号……已经有人通过微博泄露查到我的手机号码，来加我微信了。”在其微博下，有不少网友留言表示自己也疑似遭遇了数据泄露。更有用户表示，发现 5.38 亿条微博用户信息在暗网出售，其中，1.72 亿条有账户基本信息，售价 0.177 比特币。涉及到的账号信息包括用户 ID、账号发布的微博数、粉丝数、关注数、性别、地理位置等。

经查证，在“安全_云舒”的用户主页上，目前已经找不到上图微博内容，只留有昨晚其转发的一条微博表示：“btw，我只是说数据泄露，没说是脱裤哈。看来 2019 年是通过接口被人薅走了一些数据”。

对此，微博安全总监罗诗尧回应称：“泄漏的手机号是 19 年通过通讯录上传接口被暴力匹配的，其余公开信息都是网上抓来的。”罗诗尧表示：“19 年被刷的部分数据，内部突发现异常后马上堵住了口子。我们第一时间报了警，取证后把相关信息递到了警方，同时一直也在追查网上售卖信息的黑灰产。用户的隐私至关重要，尤其还是涉及到手机号。”

针对“数据泄露”事件，微博方面向搜狐科技回应称，微博一直提供根据通讯录手机号查询微博好友昵称的服务，用户授权后可以使用该服务，但微博不提供用户性别和身份证号等信息，也没有“根据用户昵称查手机号”的服务。

微博表示，2018 年底，有用户通过微博相关接口通过批量手机批量上传通讯录，匹配出几百万个账号昵称，再加上通过其他渠道获取的信息一起对外出售。此次非法调用微博接口匹配出的信息为微博账号昵称，不涉及身份证、密码，对微博服务没有影响。“发现异常后，我们及时加强了安全策略，今后还将不断强化。 （来源：互联网综合整理）

➢ 京沪 50 余万条学生个人信息遭侵犯

2020 年 3 月 18 日报道，日前，虹口区检察院提起的教育培训行业从业人员侵犯公民个人信息刑事附带民事公益诉讼案件在虹口法院开庭审理，并当庭宣判，法院的判决支持检察机关作为公益诉讼起诉人提出的包括民事公益诉讼赔偿在内的全部诉讼请求。这也是上海市检察院集中通过公益诉讼加强公民信息保护的系列案件。

2019 年底，虹口区检察院公益诉讼检察官对公民信息保护案件筛查时注意到，有起 3

人侵犯学生个人信息的案子：3 名犯罪嫌疑人皆是教育培训机构从业人员，且其中 1 人是名校硕士生，而被侵犯的学生信息涉及京沪两地，数量巨大。2017 年上海某教育机构从业人员刘某花费 5000 元从他处购买上海各区大量学生个人信息 13 万余条;2018 年刘某通过微信认识了在北京从事教育培训的周某，用上海学生信息与周某交换，换取北京各区学生信息 38 万余条;2019 年年初，刘某又将 52 万余条学生信息中的一部分分别出售给两人，共获利 1.6 万元。这些学生信息包含了学生的姓名、身份证号码、所在学校、户籍地址、家长姓名电话等等。2019 年，周某还通过网络，从曾经的同事、上海某教育培训机构总经理李某处获取上海学生信息 3 万余条。经查，李某 2015 年通过网络花 200 元购买上海市部分高中生信息 13 万余条，将其中一部分提供给周某。

公益诉讼检察官认为：刘某非法购买、交换、出售公民个人信息，周某非法收受、交换公民个人信息，李某非法购买、提供公民个人信息，3 人的行为均已违反国家侵权法规的规定，侵害不特定公民的隐私权，损害社会公共利益。因此对 3 人以侵犯公民个人信息罪提起刑事诉讼同时附带民事公益诉讼。

最终，法院以侵犯公民个人信息罪分别判处刘某有期徒刑 3 年，缓刑 4 年，并处罚金 2 万元;周某有期徒刑 3 年，缓刑 3 年，处罚金 2 万元;李某有期徒刑 2 年 6 个月，缓刑 2 年 6 个月，处罚金 1 万元。同时，依法判令 3 人在国家级新闻媒体上公开赔礼道歉，并要求刘某按照其侵犯公民个人信息的获利赔偿民事公益诉讼费用 1.6 万元。（来源：新民晚报）

➢ 自贡 11 万条小区业主信息被卖 男子获刑并处罚金

2020 年 3 月 21 日报道：王哥，您位于 XX 小区的房子要装修吗?我们可以提供优质的服务。”刚买房的王先生百思不得其解，自己刚买了新房，装修公司、家具公司、电器公司等各式各样的推销电话就不约而至，让王先生不胜其烦、不堪其扰。您是否也遇到过类似的个

人信息泄露呢?

3 月 19 日，富顺县人民法院对一起侵犯公民个人信息案进行了审理并当庭宣判，被告人梁某因侵犯公民个人信息罪被判处有期徒刑三年，缓刑四年，并处罚金二万元。

2017 年以来，梁某伙同吴某(已判决)等人分工协作贩卖公民个人信息牟取利益。其中，梁某提供自贡市部分小区业主公民个人信息给吴某，吴某将这些小区业主公民的个人信息与他人交换新的小区业主公民的个人信息，再通过网络贩卖给郑某、何某、唐某等二十名不同装修公司人员用于推销房屋装修业务。二人合伙非法贩卖小区业主公民个人信息 111147 条，获利 5 万余元，其中梁某非法获利 2 万元。2020 年 2 月 27 日，梁某退缴违法所得 2 万元。

我国《刑法》第二百五十三条之一规定，违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金;情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。梁某与他人合伙贩卖公民个人信息达 50000 条以上，属于情节特别严重，法院考虑其如实供述自己的罪行、认罪认罚、退缴违法所得并积极缴纳罚金保证金，法院采纳检察机关的量刑建议，作出了上述判决。

法官提醒：随着大数据时代的来临，房地产、教育、医疗等领域泄露消费者个人信息的事件频发多发，个人信息安全问题日益严峻。与信息泄露相伴的垃圾短信、骚扰电话、精准诈骗日益威胁着人们的隐私、财产甚至生命安全，严重侵害社会公共利益。部分掌握公民个人信息的从业者抵挡不住金钱的诱惑，加之法律意识淡薄，以为交换、贩卖个人信息对当事

人生活的影响不大，行为后果不严重。殊不知，这样的行为不仅打扰了他人的正常工作生活，还可能会触犯刑法。

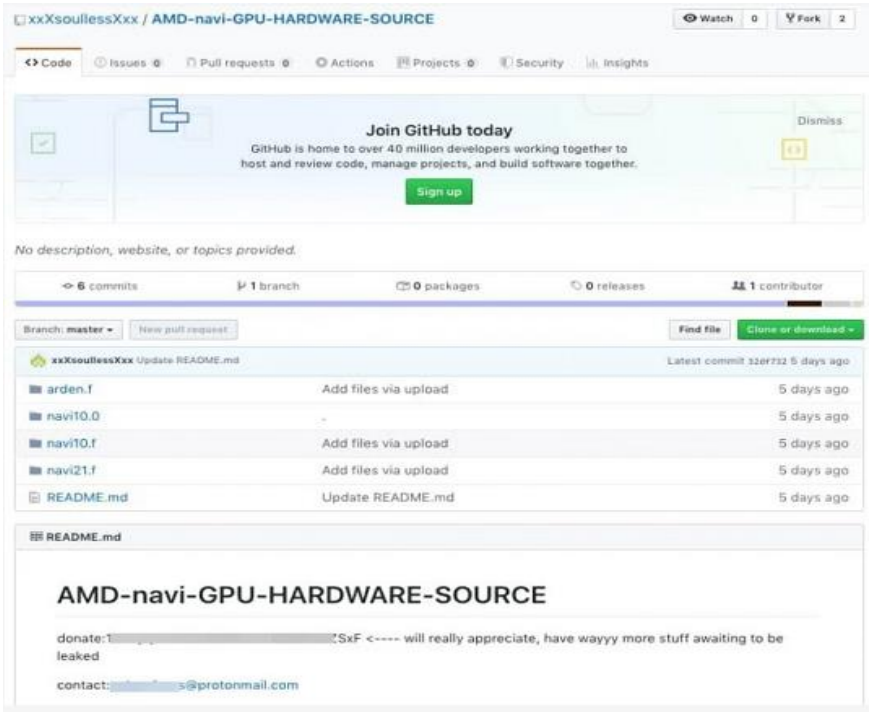
其中，尤其是房地产、教育、医疗、快递等行业，要提高防范意识和安全防范等级，建立自查、督察和责任制度，堵塞监管漏洞。同时加强对从业人员的管理教育，严防内部人员利用职务便利泄露公民个人信息。公民在日常生活中要增强个人信息安全保护意识，养成良好的上网习惯，不轻易提供个人信息，不点击陌生链接，不扫描陌生二维码，不轻信陌生电话。（来源：四川日报）

➢ 女黑客盗取 GPU 源码勒索 AMD 开口就是 1 亿美元

2020 年 3 月 27 日，黑客可不是好惹的。即便在疫情期间，黑客也是毫不留情地攻击了 WHO 网站。不过，最近深受黑客困扰的不止 WHO，还有 AMD。值得一提的是，和 AMD 纠缠的，还是个女黑客。

GPU 源代码被窃取，AMD 正面回应

据 TorrentFreak 报道，一位女黑客从一些不受保护的计算机/服务器中获得了 AMD 公司 Navi10（RadeonRX5700 系列），Navi21 和 Arden 设备（据称为 XboxSeriesX 的 12 浮点运算 GPU）的源代码，其中一部分源代码包已在 GitHub 上公开。



该黑客补充称，这些 GPU 源代码是 2019 年 11 月在一台被黑的电脑中发现的，电脑用户并未对这些泄露的代码实施保护。并且，黑客表示关于源代码公开之事并无事先与 AMD 方面沟通。她认为，AMD 不会承认并改正错误，而是会起诉她，那何不将源代码公之于众呢？

不过，这位黑客并不是只想警告一下 AMD，而想借此大赚一笔。在代码库页面上，黑客以 1 亿美金拍卖 GPU 源代码，并威胁称，如果没有买家，将会在网上公开所有代码信息。

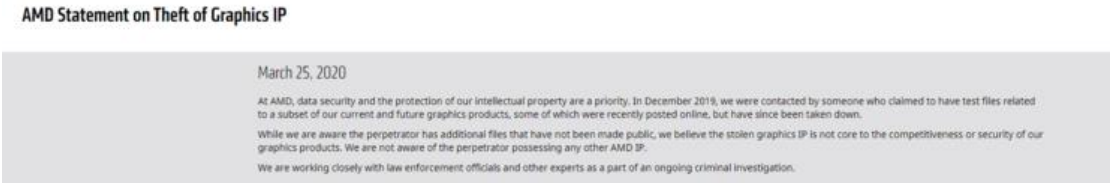
被认为应用了 Navi10 核心的 RX5700 系列对标 NVIDIA 的甜品卡；Navi21 据称是与 NVIDIA 旗舰卡抗衡的产品核心之一。不难得知，CPU 源代码的泄露对 AMD 影响不小。

```
+ **Please describe the nature of your copyright ownership or authorization to act on the owner's behalf.**
+
+ This repository contains intellectual property owned by and stolen from AMD.
+
+ **Please provide a detailed description of the original copyrighted work that has allegedly been infringed. If possible, include a
 URL to where it is posted online.**
+
+ The original IP is held privately and was stolen from AMD.
```

面对黑客公开源代码的行径，AMD 向 GitHub 多次提交 DMCA（Digital Millennium Copyright Act，数字千年版权法），要求 GitHub 删除与 AMD Navi 和 Arden GPU 有关的“被盗”源代码。

在发给 Github 的 DMCA 通知中，AMD 将最近创建的“xxXsoullessXxx”存储库和“AMD-navi-GPU-HARDWARE-SOURCE”的项目标识为 AMD 被盗的知识产权。AMD 表示，这些存储库的知识产权归 AMD 所有，存储库资源是从 AMD 盗取的。目前，GitHub 已删除相关信息，且其它四个分支资源也已被 AMD 回溯并要求删除。

除了删库处理，AMD 也进行了正面回应，表示在 2019 年 12 月就已知情此事，但被盗图形 IP 非其产品竞争力和安全性的核心，目前已报警，正与警方合作中。在 AMD 正式回应之后，该黑客又在 GitHub 上发布了第二部分源代码，并在文件名中特意注明了“pt.2”，尚不清楚后续是否会继续放出更多源代码。截至目前，AMD 暂未发布进一步评论。


AMD Statement on Theft of Graphics IP

March 25, 2020

At AMD, data security and the protection of our intellectual property are a priority. In December 2019, we were contacted by someone who claimed to have test files related to a subset of our current and future graphics products, some of which were recently posted online, but have since been taken down.

While we are aware the perpetrator has additional files that have not been made public, we believe the stolen graphics IP is not core to the competitiveness or security of our graphics products. We are not aware of the perpetrator possessing any other AMD IP.

We are working closely with law enforcement officials and other experts as a part of an ongoing criminal investigation.

以下是 AMD 关于该事件的回应声明：在 AMD，数据安全和知识产权保护是重中之重。2019 年 12 月，有人联系我们，声称拥有与我们当前和未来图形产品子集相关的测试文件，其中的一些文件近期被公开在网上，但后来被删除了。

尽管我们知道犯罪者还有其他文件没公开，但我们认为，被盗的图形 IP 并不是我们图形产品的竞争力和安全性的核心。至于犯罪者是否还有其他 AMDIP，我们目前尚不知晓。作为正在进行的刑事调查的一部分，我们正在与执法官员和其他专家密切合作。（来源：雷锋网）

➢ 信息安全又现漏洞，智能手机传感器竟成“窃听器”

2020 年 3 月 25 日，加速度计，又称加速度传感器，目前在智能手机上被广泛地应用，可以通过测量手机在各个方向上的“应力”来得出加速度，像手机中的计步器、“摇一摇”等许多功能都基于这些传感器来实现。以往业界普遍认为其和个人隐私信息无关，因此在功能设置上，手机 APP 可以“无门槛”调用加速度计读数或是获取相应权限。

但是近日，在国际四大信息安全会议之一的 “网络与分布式系统安全会议”上，一项来自浙江大学、加拿大麦吉尔大学、多伦多大学学者团队的最新研究成果显示：部分智能手机 APP 可在用户不知情且无需系统授权的情况下，利用手机内置的加速度传感器来采集手机扬声器所发出声音的震动信号，实现对用户语音的窃听。

利用通话时的手机震动实现窃听

“加速度传感器是目前智能手机中最常见的一种嵌入式传感器，它主要用于探测手机本身的移动，常见的应用场景包括移动检测，步数统计和游戏控制等。”浙江大学网络空间安全学院院长、教授任奎告诉科技日报记者，它之所以能被用来监听电话，主要是由于声音信号是一种由震动产生的、可以通过介质传播的声波，手机扬声器发出的声音会引起手机的震动，而加速度传感器可以灵敏地感知这些震动，因此攻击者可以通过它来捕捉手机

震动进而破解其中所包含的信息。

通过加速度传感器窃听语音的准确率有多高？“窃听语音的准确率与具体的窃听任务有关。根据我们的实验结果，在关键字检测任务中，这种窃听攻击识别用户语音中所携带的关键字的平均准确率达到了 90%。”任奎说，在实际攻击中，攻击者还可以结合上下文信息和实际语言中各个词汇的使用频率，进一步提升语音窃听的准确率。

手机加速度计可以收集语音信息，这意味着攻击者可以从用户的手机中窃取多种隐私数据。“比如，攻击者也许可以从语音信息中提取出用户的家庭住址、信用卡信息、身份证号、用户名密码等一系列重要信息；通过窃听手机地图的语音导航系统，攻击者也许能提取出一些跟位置有关的关键字，推断出用户目前的位置以及目的地；通过窃听用户手机播放的音乐和视频，攻击者可以推断出用户在这些方面的偏好。”任奎总结说，这种攻击方式对用户隐私安全具有很大威胁。

此外，任奎进一步强调，这种攻击对场景并没有特别的要求，无论手机用户将手机放在桌子上还是拿在手中，“甚至边使用手机边走路，攻击者都可以准确地识别出手机扬声器所播放的语音信息。”

“传感器数据”亟待重新审视

据了解，现行的法律法规对个人敏感信息的保护，主要是针对证件号码、金融账户等具体的个人敏感信息。由于加速计数据本身并不属于个人敏感信息，攻击者可以利用计步软件等必须用到加速计的 APP“合理”地对加速计数据进行收集，因此采集加速计数据这种行为本身并不违法。这就意味着，这种攻击方式目前仍处于法律法规的灰色地带。“但使用或贩卖分析出的个人敏感信息应该是违法的。”任奎说。

为有效防御此类攻击，任奎建议，首先应该从技术层面加大对移动设备物理层安全的研究投入，了解各类传感器的实际数据采集能力以及它们可能造成的隐私问题，对可能存在的各类攻击做到心中有数。然后依此重新设计智能手机操作系统中各类传感器的权限使用机制，从技术的角度尽可能地降低数据被滥用的可能性。

此外，任奎还补充道：“我们应当从法律法规上细化对敏感信息的定义和使用规范。除了对证件号码、银行账户、通信记录和内容等具体的个人敏感信息进行保护外，还应对可能包含这些信息的原始传感器数据进行保护，规范和限制这类数据的采集和使用方式。”

那么作为普通消费者，我们目前有机会防止自己的手机被窃听吗？在任奎看来，各大手机厂商提出进一步解决方案之前，消费者能够采取的最有效也最便捷的防御方式，就是通过耳机来接听电话或语音信息。手机中的加速计与耳机间存在着物理隔离，使其无法监

测到耳机发出的震动，所以通过耳机播放的声音是不会被这种攻击窃听的。（来源：新华网）