国盟信息安全通报

2022 年 1 月 31 日第 247 期

国盟信息安全通报

（第 247 期）

国际信息安全学习联盟

2022 年 01 月 31 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 607 个，其中高危漏洞 186 个、中危漏洞 367 个、低危漏洞 54 个。漏洞平均分值为 5.92。本周收录的漏洞中，涉及 0day 漏洞 282 个（占 46%），其中互联网上出现“SeedDMS 跨站脚本漏洞（CNVD-2022-05448）、Auerswald COMpact 5500R 权限提升漏洞”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 5941 个，与上周（33637 个）环比减少 82%。

主要内容

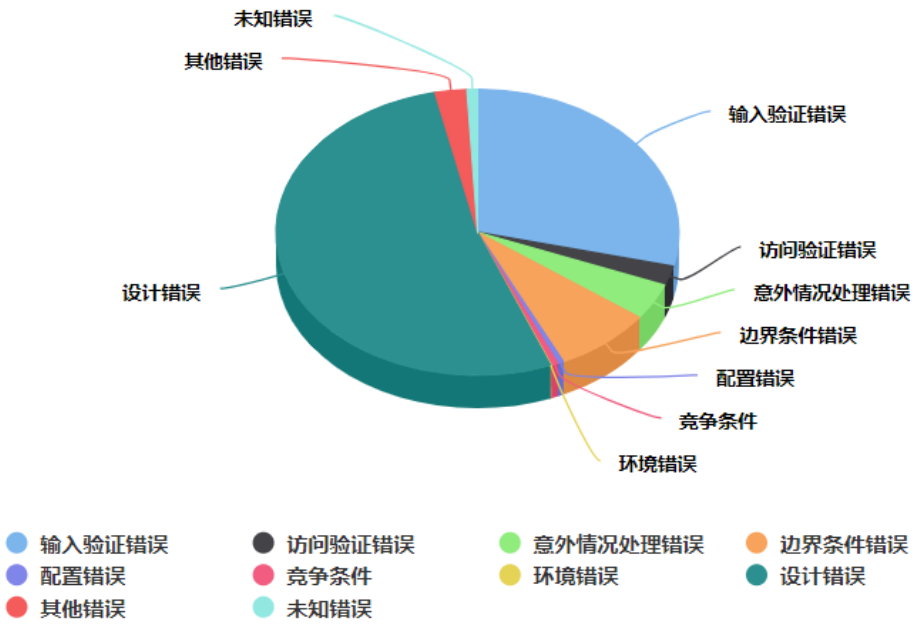
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

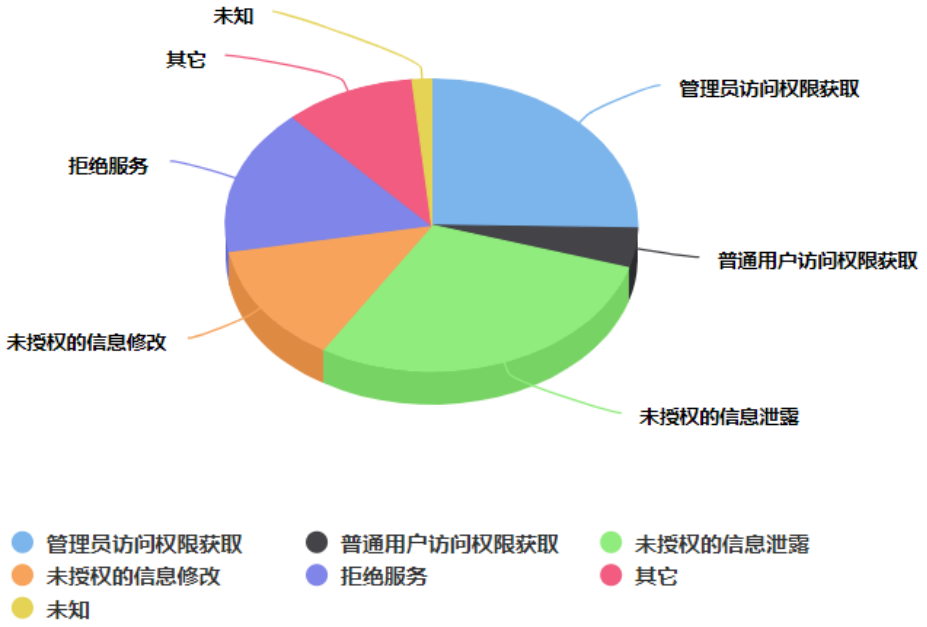
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 607 个，其中高危漏洞 186 个、中危漏洞 367 个、低危漏洞 54 个。漏洞平均分值为 5.92。本周收录的漏洞中，涉及 0day 漏洞 282 个（占 46%），其中互联网上出现“SeedDMS 跨站脚本漏洞（CNVD-2022-05448）、Auerswald COMpact 5500R 权限提升漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 5941 个，与上周（33637 个）环比减少 82%。

二、安全漏洞增长数量及种类分布情况

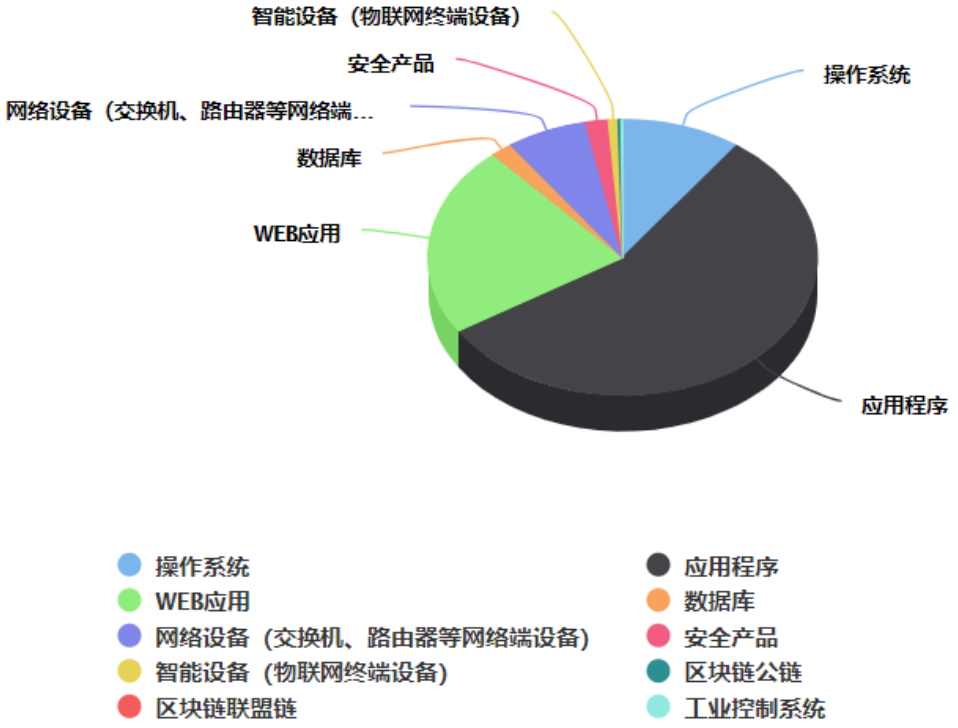
➢ 漏洞产生原因（2022 年 1 月 1 日—2022 年 1 月 31）



➢ 漏洞引发的威胁（2022 年 1 月 1 日—2022 年 1 月 31）



➢ 漏洞影响对象类型（2022 年 1 月 1 日—2022 年 1 月 31）



三、安全产业动态

➢ 习近平：不断做强做优做大我国数字经济

近年来，互联网、大数据、云计算、人工智能、区块链等技术加速创新，日益融入经济社会发展各领域全过程，各国竞相制定数字经济发展战略、出台鼓励政策，数字经济发展速度之快、辐射范围之广、影响程度之深前所未有，正在成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量。

长期以来，我一直重视发展数字技术、数字经济。2000 年我在福建工作期间就提出建设“数字福建”，2003 年在浙江工作期间又提出建设“数字浙江”。党的十八大以来，我多次强调要发展数字经济。2016 年在十八届中央政治局第三十六次集体学习时强调要做大做强数字经济、拓展经济发展新空间；同年在二十国集团领导人杭州峰会上首次提出发展数字经济的倡议，得到各国领导人和企业家的普遍认同；2017 年在十九届中央政治局第二次集体学习时强调要加快建设数字中国，构建以数据为关键要素的数字经济，推动实体经济和数字经济融合发展；2018 年在中央经济工作会议上强调要加快 5G、人工智能、工业互联网等新型基础设施建设；2021 年在致世界互联网大会乌镇峰会的贺信中指出，要激发数字经济活力，增强数字政府效能，优化数字社会环境，构建数字合作格局，筑牢数字安全屏障，让数字文明造福各国人民。

党的十八大以来，党中央高度重视发展数字经济，将其上升为国家战略。党的十八届五中全会提出，实施网络强国战略和国家大数据战略，拓展网络经济空间，促进互联网和经济社会融合发展，支持基于互联网的各类创新。党的十九大提出，推动互联网、大数据、人工

智能和实体经济深度融合，建设数字中国、智慧社会。党的十九届五中全会提出，发展数字经济，推进数字产业化和产业数字化，推动数字经济和实体经济深度融合，打造具有国际竞争力的数字产业集群。我们出台了《网络强国战略实施纲要》、《数字经济发展战略纲要》，从国家层面部署推动数字经济发展。这些年来，我国数字经济发展较快、成就显著。根据 2021 全球数字经济大会的数据，我国数字经济规模已经连续多年位居世界第二。特别是新冠肺炎疫情暴发以来，数字技术、数字经济在支持抗击新冠肺炎疫情、恢复生产生活方面发挥了重要作用。

2022 年 1 月 4 日，中共中央总书记、国家主席、中央军委主席习近平在北京考察 2022 年冬奥会、冬残奥会筹办备赛工作。这是 4 日上午，习近平在北京冬奥会、冬残奥会主媒体中心智慧餐厅，察看智能餐饮设备运行情况。新华社记者 谢环驰/摄

同时，我们要看到，同世界数字经济大国、强国相比，我国数字经济大而不强、快而不优。还要看到，我国数字经济在快速发展中也出现了一些不健康、不规范的苗头和趋势，这些问题不仅影响数字经济健康发展，而且违反法律法规、对国家经济金融安全构成威胁，必须坚决纠正和治理。

综合判断，发展数字经济意义重大，是把握新一轮科技革命和产业变革新机遇的战略选择。一是数字经济健康发展，有利于推动构建新发展格局。构建新发展格局的重要任务是增强经济发展动能、畅通经济循环。数字技术、数字经济可以推动各类资源要素快捷流动、各类市场主体加速融合，帮助市场主体重构组织模式，实现跨界发展，打破时空限制，延伸产

业链条，畅通国内外经济循环。二是数字经济健康发展，有利于推动建设现代化经济体系。数据作为新型生产要素，对传统生产方式变革具有重大影响。数字经济具有高创新性、强渗透性、广覆盖性，不仅是新的经济增长点，而且是改造提升传统产业的支点，可以成为构建现代化经济体系的重要引擎。三是数字经济健康发展，有利于推动构筑国家竞争新优势。当今时代，数字技术、数字经济是世界科技革命和产业变革的先机，是新一轮国际竞争重点领域，我们一定要抓住先机、抢占未来发展制高点。

面向未来，我们要站在统筹中华民族伟大复兴战略全局和世界百年未有之大变局的高度，统筹国内国际两个大局、发展安全两件大事，充分发挥海量数据和丰富应用场景优势，促进数字技术和实体经济深度融合，赋能传统产业转型升级，催生新产业新业态新模式，不断做强做优做大我国数字经济。

第一，加强关键核心技术攻关。要牵住数字关键核心技术自主创新这个“牛鼻子”，发挥我国社会主义制度优势、新型举国体制优势、超大规模市场优势，提高数字技术基础研发能力，打好关键核心技术攻坚战，尽快实现高水平自立自强，把发展数字经济自主权牢牢掌握在自己手中。

第二，加快新型基础设施建设。要加强战略布局，加快建设以 5G 网络、全国一体化数据中心体系、国家产业互联网等为抓手的高速泛在、天地一体、云网融合、智能敏捷、绿色低碳、安全可控的智能化综合性数字信息基础设施，打通经济社会发展的信息“大动脉”。要全面推进产业化、规模化应用，培育具有国际影响力的大型软件企业，重点突破关键软件，推动软件产业做大做强，提升关键软件技术创新和供给能力。

第三，推动数字经济和实体经济融合发展。要把握数字化、网络化、智能化方向，推动制造业、服务业、农业等产业数字化，利用互联网新技术对传统产业进行全方位、全链条的改造，提高全要素生产率，发挥数字技术对经济发展的放大、叠加、倍增作用。要推动互联网、大数据、人工智能同产业深度融合，加快培育一批“专精特新”企业和制造业单项冠军企业。当然，要脚踏实地、因企制宜，不能为数字化而数字化。

第四，推进重点领域数字产业发展。要聚焦战略前沿和制高点领域，立足重大技术突破和重大发展需求，增强产业链关键环节竞争力，完善重点产业供应链体系，加速产品和服务迭代。要聚焦集成电路、新型显示、通信设备、智能硬件等重点领域，加快锻造长板、补齐短板，培育一批具有国际竞争力的大企业和具有产业链控制力的生态主导型企业，构建自主可控产业生态。要促进集群化发展，打造世界级数字产业集群。

第五，规范数字经济发展。推动数字经济健康发展，要坚持促进发展和监管规范两手抓、

两手都要硬，在发展中规范、在规范中发展。要健全市场准入制度、公平竞争审查制度、公平竞争监管制度，建立全方位、多层次、立体化监管体系，实现事前事中事后全链条全领域监管，堵塞监管漏洞，提高监管效能。要纠正和规范发展过程中损害群众利益、妨碍公平竞争的行为和做法，防止平台垄断和资本无序扩张，依法查处垄断和不正当竞争行为。要保护平台从业人员和消费者合法权益。要加强税收监管和税务稽查。

第六，完善数字经济治理体系。要健全法律法规和政策制度，完善体制机制，提高我国数字经济治理体系和治理能力现代化水平。要完善主管部门、监管机构职责，分工合作、相互配合。要改进提高监管技术和手段，把监管和治理贯穿创新、生产、经营、投资全过程。要明确平台企业主体责任和义务，建设行业自律机制。要开展社会监督、媒体监督、公众监督，形成监督合力。要完善国家安全制度体系，重点加强数字经济安全风险预警、防控机制和能力建设，实现核心技术、重要产业、关键设施、战略资源、重大科技、头部企业等安全可控。要加强数字经济发展的理论研究。

第七，积极参与数字经济国际合作。要密切观察、主动作为，主动参与国际组织数字经济议题谈判，开展双多边数字治理合作，维护和完善多边数字经济治理机制，及时提出中国方案，发出中国声音。

数字经济事关国家发展大局。我们要结合我国发展需要和可能，做好我国数字经济发展顶层设计和体制机制建设。要加强形势研判，抓住机遇，赢得主动。各级领导干部要提高数字经济思维能力和专业素质，增强发展数字经济本领，强化安全意识，推动数字经济更好服务和融入新发展格局。要提高全民全社会数字素养和技能，夯实我国数字经济发展社会基础。（来源:《求是》 ※这是习近平总书记 2021 年 10 月 18 日在十九届中央政治局第三十四次集体学习时讲话的主要部分。）

➢ 激发数据要素价值 赋能数字中国建设

编者按：党中央、国务院高度重视信息化工作，习近平总书记强调，没有信息化就没有现代化。信息化为中华民族带来了千载难逢的机遇，必须敏锐抓住信息化发展的历史机遇。“十四五”时期，信息化进入加快数字化发展、建设数字中国的新阶段。近日，中央网络安全和信息化委员会印发《“十四五”国家信息化规划》（以下简称《规划》），对我国“十四五”时期信息化发展作出部署安排。为使社会各界更好理解《规划》的主要内容，中央网信办组

织有关专家学者对《规划》各项重点任务进行研究解读，共同展望数字中国建设新图景。

数据要素是参与社会生产经营活动，带来经济效益，以电子方式记录的数据资源，是国家发展的战略性基础性资源，也是驱动数字经济发展的强大动力。加强数据治理、深化数据开发、保障数据安全是释放数据资源价值的关键环节。近日，中央网络安全和信息化委员会发布《“十四五”国家信息化规划》（以下简称《规划》），作为指导未来五年的国家信息化发展的纲领性文件，《规划》提出建立高效利用的数据要素资源体系。“十四五”时期，要充分发挥数据的基础资源作用和创新引擎作用，精准谋划、有序推进我国数据资源开发利用、数据要素价值释放迈上新台阶，为网络强国、数字中国、智慧社会建设奠定坚实基础。

一、深刻认识数据要素价值

数字经济事关国家发展大局，数据要素已成为数字经济时代影响全球竞争的关键战略性资源。释放数据要素价值，有助于提升全要素生产率，赋能现代化经济体系高质量发展；有助于提升政府治理效能，推动国家治理体系和治理能力现代化。

（一）数据要素是国家发展的战略性基础性资源

数据要素具有非竞争、可共享、无限增长的特性，贯穿生产、分配、流通、消费等各环节，对经济社会变革产生深远影响，已经成为国家关键战略性基础性资源。当前，全球数据量指数级增长，世界各国抢占数据发展先机。美国、欧盟、英国、日本等全球主要经济体均通过出台国家数据战略、完善国内数据立法、加强国际数据合作等多种方式，将数据作为战略资源进行开发利用。2020 年，我国数据总规模达到 3.9ZB，同比增长 29.3%，占全球数据总量 9.3%，居全球第二位。党的十九届四中全会首次提出将数据作为与土地、劳动力、资

本、技术等同等重要的生产要素参与分配。数据要素通过融入生产生活各环节，大幅提升传统要素资源的资源配置效率，助力城市管理、公共服务和经营决策实现全局优化，对农业、工业、政务、交通、教育、城市管理等领域形成倍增作用，为经济社会发展提供不竭动力。

（二）数据要素是驱动数字经济发展的动力引擎

数据要素的高效利用与合理开发，提高全社会劳动生产率，有助于实现生产率跃升、产业链优化和竞争力重塑，正成为驱动数字经济发展的动力引擎。习近平总书记指出，“要构建以数据为关键要素的数字经济。建设现代化经济体系离不开大数据发展和应用”“数字技术、数字经济可以推动各类资源要素快捷流动、各类市场主体加速融合”。数据要素将对劳动力、资本等其他要素资源形成乘数作用，放大各类生产要素在社会流转中产生的价值。例如，数据要素在工业企业和金融机构间的共享互通，为中小企业低成本融资提供可能；数据要素在劳动力供需市场的有效流转，缓解疫情下企业用工难题。OECD 发布的《数据和数据流动的映射方法》指出，数据利用有助于产品、流程和组织的改善和创新，促进企业劳动生产率增长 5%-10%。此外，数据要素与其他要素的深度融合，催生出金融科技等“新资本”、智能机器人等“新型劳动力”，不断释放创新活力。

（三）数据要素是推动治理能力现代化的重要抓手

数据要素价值释放将助力数字政府、数字社会建设，推动我国治理体系和治理能力现代化。习近平总书记在主持“实施国家大数据战略”集体学习时强调，要建立健全大数据辅助科学决策和社会治理的机制，推进政府管理和社会治理模式创新。例如，在疫情防控中，基于政府与社会数据融合开发的“健康码”，为疫情防控精准施策提供了巨大帮助，成为疫情防控“中国经验”的重要组成。政务数据与社会数据融合，打破原有数据壁垒，充分发挥多方数据资源的专业化、全覆盖、公信力强显著优势，在疫情防控、医疗卫生、交通出行、文化教育、城市服务等方面发挥巨大作用，提升政府组织运行效率、推动社会治理模式创新、丰富数字化便捷服务场景，全面提高治理和服务效能。

二、建立数据要素资源体系

“十四五”时期，要充分发挥数据作为新生产要素的关键作用，以数据治理为突破提升数据质量，以数据开发利用为抓手激活要素价值，以立法规范为重点保障数据安全，加快完善与我国发展实际相符合的数据要素资源体系，释放数据要素价值。

（一）以数据治理为突破推动数据质量提升

数据治理是释放数据价值的首要环节，准确及时、完整一致的数据资源是数据要素价值释放的重要前提。近年来，我国不断完善数据治理标准规范，出台了《政务信息资源共享管

理暂行办法》等政策提升政务数据质量，发布了国家标准《数据管理能力成熟度评估模型》，帮助企业评价、提升自身数据管理能力。“十四五”时期数据互联互通互操作要求进一步提升，数据治理综合性、跨行业、跨区域等特点更加突出，但各级各部门数据治理统筹推进不足、数据责任主体多样、跨层级跨区域数据共享困难，需要建立完善央地协同、职责清晰、分工有序、协调有力的数据治理协同工作格局。要加快推进数据标准规范体系建设，制定数据采集、存储、加工、流通、交易、衍生产品等标准规范；建立完善数据治理能力评估体系；探索多主体协同治理机制，聚焦数据管理、共享开放、数据应用、授权许可、安全和隐私保护、风险管控等方面，加强“政产学研用”各方数据治理协同。

（二）以开发利用为抓手激活数据要素价值

数据开发利用是激活数据要素价值的关键。当前，我国围绕“数据资源、基础硬件、通用软件、行业应用、安全保障”的大数据产品和服务体系初步形成。我国已成立 20 余家大数据交易所，上海、北京等地积极探索数据交易配套制度。但与国际上数据开放共享程度较高的国家相比，我国数据开放范围和渠道仍有不足，数据应用深度开发仍需加强。要建立健全国家公共数据资源体系，构建统一的国家公共数据开放平台和开发利用端口，推动人口、交通、通信等公共数据资源安全有序开放；支持构建农业、工业、商业、教育、医疗、安防等领域规范化数据开发利用场景；选取重点行业培育一批具有国际一流水平的行业大数据应用平台和应用市场开发主体，持续提升数据开发利用能力。

（三）以风险防护为重点强化数据安全保障

加强数据要素流通的风险防护，确保数据合规利用是释放数据价值的安全保障。我国在数据安全领域加速推进立法工作，2021 年出台《数据安全法》《个人信息保护法》，加强保护个人的合法权益和社会公共利益。“十四五”时期，数据资源总量将指数级持续增加，跨部门、跨领域的数据流通更加活跃，完善的数据安全机制、防范数据泄露等安全风险成为保障数据安全的重点方向。要加强数据收集、汇聚、存储、流通、应用等全生命周期的安全管理；建立数据分类分级管理制度和个人信息保护认证制度，加强对重要数据、企业商业秘密和个人信息的保护；强化平台企业数据安全保护责任；加强数据交易安全管理与监督保障；建立健全数据出境安全管理制度和安全评估机制。

三、加快数据要素市场培育

“十四五”时期，数据要素市场化进程将加速，需从市场制度、交易主体、技术人才支撑等多维度破除数据要素市场瓶颈，丰富数据要素供给，激活数据要素价值，加快培育更为完善的数据要素市场。

（一）深化理论研究建立数据要素市场制度

数据权属是构建数据要素市场的重要部分，涉及个人、企业、政府、中介等多类主体，包括所有权、使用权、最终控制权、商业交易权等多种权益，生成过程复杂多变，现有法律法规尚未作出明确规定。“十四五”期间亟需加强数据要素理论研究，建立兼顾发展与规范的数据要素市场新制度，在尚未形成广泛共识的数据产权、定价、交易等问题上，构建以促进产业发展为导向的数据产权框架，支持出台数据产权标准规范、共识合约、实施细则、操作指南等，建立健全数据有效流动制度体系，引导规范数据要素市场发展，为全国性、强制性立法提供路径参考。

（二）多方协同合作培育数据交易主体

当前阶段数据要素市场主体更加重视构建闭合生态，数据孤岛普遍存在，甚至出现了一定程度的数据垄断、交易黑市等不良现象。“十四五”时期，一方面要支持合规、创新的数据流通交易平台与运营体系建设。面向数据资产评估、登记结算、交易撮合、争议仲裁等需求，发挥政府、企业、数据中介、智库机构等各自作用，探索构建涵盖交易主体认证、资产评估、价格发现、交易分润、安全保障、争议解决的新型数据交易平台和市场运营体系。另一方面要充分调动行业商协会作用，建立健全数据产权交易和行业自律机制，强化数据交易平台的数据安全保护责任，不断提高对数据安全流通溯源的认识和能力。

（三）多措并举提升数据要素利用能力

提升数据要素的使用、交易效率和安全合规利用，需要以改革创新的思维多管齐下，充分利用技术工具，培育创新型人才，构建适应数据要素特征的产业支撑体系，不断催生数据要素市场新业态新模式，兼顾数据要素开发利用和数据安全。一是强化技术创新，推动区块链、安全多方计算、联邦学习等隐私计算技术应用，从技术层面实现数据交易流通中的可用不可见，保障数据安全与发展并重。二是加快知识型、技能型、创新型数据要素相关人才培养，推行大数据岗位专项技能培训和人才能力认证。三是完善数据要素利用支撑体系，开展面向大数据技术、产品、服务供给侧企业的能力评估，建立健全适应数据要素特点的税收征收管理制度和产业监测分析体系。（来源：网信中国）

➢ 新版《网络安全审查办法》筑牢网络安全和数据安全防线

《网络安全审查办法》自实施以来，在确保关键信息基础设施供应链安全、维护国家安

全方面起到了重要的保障作用。此次《网络安全审查办法》修订，依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《关键信息基础设施保护条例》，旨在确保关键信息基础设施供应链安全，保障网络安全和数据安全，维护国家安全。

一、《网络安全审查办法》修订的亮点

此次《网络安全审查办法》修订，增加了中国证券监督管理委员会作为国家网络安全审查工作机制成员。

同时，增加了审查申报对象：掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。这部分申报对象须提交材料包括：申报书、关于影响或者可能影响国家安全的分析报告，拟提交的首次公开募股（IPO）等上市申请文件，网络安全审查工作需要的其他材料。

网络安全审查重点评估的国家安全风险因素增加了两点内容：一是重点评估核心数据、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险；二是重点评估上市存在关键信息基础设施、核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险。

针对网络平台运营者赴国外上市申报网络安全审查的结论，从《网络安全审查办法》答记者问看审查结论共分三种情况：一是无需审查；二是启动审查后，经研判不影响国家安全的，可继续赴国外上市程序；三是启动审查后，经研判影响国家安全的，不允许赴国外上市。

二、各国为确保平台和数据安全纷纷出台监管措施

国际重点国家和地区为防范网络安全、数据安全等安全风险，纷纷出台网络平台的监管措施，如《美国选择与创新在线法案》《终止平台垄断法案》《平台竞争和机会法案》《并购

申报费现代化法案》《在线隐私法（草案）》等，《欧盟数字市场法（草案）》《数字服务法（草案）》《通用数据保护条例》，《俄罗斯联邦大众传媒法》《信息、信息技术和信息保护法》等等。

其中，美国为保障国家安全出台了《确保信息通信技术及服务供应链安全行政命令》及配套规则，明确提出其审查涉及的敏感数据包括企业数据和个人数据两类，具体包括：一是企业在 12 月内任何时间点保存、收集、维护超过 100 万个人数据的情况，以及为美国行政部门和军事部门的人员和承包商提供特定或专用产品服务的企业收集的信息情况；二是个人征信数据、消费数据、保险数据、健康状况数据、非公开电子通信数据、地理位置数据、生物识别数据、身份识别数据等，以及个人基因检测信息、疾病信息等遗传信息。

三、我国网络平台运营者赴国外上市风险加大

随着美国《外国公司问责法案》和最终配套规则的发布，美国公众公司会计监督委员会（PCAOB）6100 审计相关规则的发布，这些监管条款明显针对我国企业。如，要求在美上市企业提交关联公司的董事会成员中的中国共产党官员的姓名，明确发行人公司制度文件中是否包含中国共产党章程等。SEC 还专门针对我国赴国外上市企业发布了《致中国公司的信函范本》的声明，要求美国指定注册会计师事务所为发行人编制的审计报告，明确提出合同协议不等同于 VIE 业务的股权所有权。

如果我国企业连续三年被 SEC 认定为“发行人”，SEC 将会立即对其实施交易禁令。如果“发行人”希望终止交易禁令，必须证明 PCAOB 能够检查或调查的其使用的注册会计师事务所。但近日，PCAOB 又发布《〈外国公司问责法〉认定报告》，认定 60 余家在美注册中国会计师事务所“无法完成检查或调查”，国外的审计更加严格。

目前情况下，掌握关键信息基础设施、核心数据、重要数据或者大量个人信息的网络平台运营者赴国外上市存在着较大的安全风险。

四、企业应提高安全意识，积极主动申报审查

根据《中华人民共和国国家安全法》第十一条，中华人民共和国公民、一切国家机关和武装力量、各政党和各人民团体、企业事业组织和其他社会组织，都有维护国家安全的责任和义务。

我国网络平台运营者作为我国国家安全的责任主体的一部分，一是需加强国家安全的主体责任意识，防范上市给我国国家安全带来的风险；二是掌握关键信息基础设施、核心数据、重要数据或者大量个人信息的我国企业赴国外上市，存在被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险时，应积极主动申报网络安全审查，防范企业上市给国家安

全带来风险。（来源：中国网信网 作者：中国网络安全审查认证中心工程师 刘金芳）

➢ 2021 年国内网络安全相关立法回顾及思考

2021 年，网络领域重要立法密集出台，网络法治体系进一步充实完善，是网络立法繁荣发展的重要一年。广义来看，《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等相继出台实施，网络安全领域立法大为充实。同时，网络安全领域配套规则逐步明确清晰，为网络安全相关工作提供了确定的指引。

一、网络安全法律体系概述

2016 年，《网络安全法》正式出台，以网络安全法为基础和上位法依据，国家有关部门陆续出台配套法规、规章和规范性文件，逐步形成了系统的网络安全法律体系，主要覆盖网络运行安全、个人信息保护和网络内容管理等三个方面。

一是网络运行安全。《网络安全法》首要解决的就是网络作为对象的安全性问题，网络入侵、网络攻击等非法活动，对电信、能源、交通、金融等领域产生了严重威胁，云计算、大数据、物联网等新技术、新应用面临着更为复杂的网络安全环境。从体系上看，《网络安全法》对网络运行作出了一般性规定。在关键信息基础设施保护方面，出台了《关键信息基础设施安全保护条例》；在网络安全审查方面，出台了《网络安全审查办法》，并根据情况变

化正在进行修订；在网络漏洞管理方面，出台了《网络产品安全漏洞管理规定》。通过系列配套规则，明确和完善了《网络安全法》相关要求。

二是个人信息安全。《网络安全法》对个人信息安全作出了原则性、概括性规定。以《网络安全法》为依据，在国家网信办统筹指导下，工信部起草了《移动应用程序个人信息保护管理规定》。国家网信办出台了《儿童个人信息网络保护规定》，牵头制定出台了《常见类型移动互联网应用程序必要个人信息范围规定》等配套规定。在《个人信息保护法》颁布实施前，《网络安全法》及其配套规定，为个人信息保护工作提供了依据和保障。

三是网络内容管理。《网络安全法》为网络内容管理提供了充实的上位法依据。国家网信办以《网络安全法》为基础，基本形成了“2+N”的网信法律体系。“2”是指两部部门规章，国家网信办修订出台《互联网新闻信息服务管理规定》，规范了互联网新闻信息服务活动；制定了《网络信息内容生态治理规定》，从治理的高度对网络信息内容管理提出了新要求。“N”是指一系列规范性文件，覆盖了音视频、网络直播、公众账号、移动应用程序、即时通信工具、跟帖评论、微博客等领域，为全面依法治网提供了有力的法治基础。

随着技术发展和普及，《网络安全法》时代的形势和客观条件都发生了变化。今年，《数据安全法》和《个人信息保护法》相继出台实施，《网络安全法》所规范的有关活动和对象也出现了变化和调整。

二、网络安全法律体系调整及内涵外延变化

伴随《网络安全法》的深入推进实施，特别是普法宣传、执法培训相关活动丰富化、常态化，《网络安全法》的生命力和活力持续得以释放。同时，在《网络安全法》实施过程中，网络技术与应用继续深入发展和普及，进一步改变人们生产、生活的组织方式，网络安全法律体系的内涵和外延出现变化和调整。

从网络法治体系的整体结构看，党的十八届四中全会和中央全面依法治国工作会议对法治建设及依法治网提出了总体性、纲领性要求。党的十八大以来，尤其是党的十九大以来，网络法治建设快速推进。网络法具有跨领域性，普遍认为网络法属于领域法学。法律科学不属于纯粹理论，而是实践理论。网络活动日益普及和丰富，网络空间逐步成为社会生活的基本载体，网络法治研究持续深入，即将或者已经能够支撑网络法成为独立的法律部门。学科的繁荣势必伴随着细分化、专业化的过程。从今年来看，网络安全法律体系作为网络法的主要组成部分，也发生了调整和变化，呈现出精细化、聚焦化的特点，有些内容逐渐独立成体系，从网络安全框架中剥离并与之并行。

按照 2016 年出台的《网络安全法》架构，相关法律主要包括网络设施和运行安全（包

括关键信息基础设施）、网络信息安全等方面。其中，《网络安全法》以“网络信息安全”囊括了内容安全和个人信息安全，聚焦网络内容管理和个人信息权益。近年来，随着实践变化和理论研究深入，相应发生了一些变化，尤其表现为网络内容管理和个人信息保护逐步自成体系的趋势。

在网络内容管理方面，有关部门以《网络安全法》为上位法依据，出台了相关内容管理的部门规章和规范性文件，基本形成了完善的制度体系。党的十九大首次明确了“意识形态安全”的重要性，互联网和移动互联网技术发展，以及人工智能等新技术普及和应用，进一步拓展了网络空间的公共表达渠道和内容供给模式。2019 年底，国家互联网信息办公室出台《网络信息内容生态治理规定》，将管理思维转变为治理思维，体现多元主体共同参与，同时也将内容管理“二分法”（违法信息和合法信息）调整为“三分法”（违法信息、不良信息和合法信息）。在此基础上，网络内容管理立法体系相应进行了调整。今年以来，国家互联网信息办公室制定了《互联网用户公众账号信息服务管理规定》，启动了《互联网用户账号名称信息管理规定》修订工作。

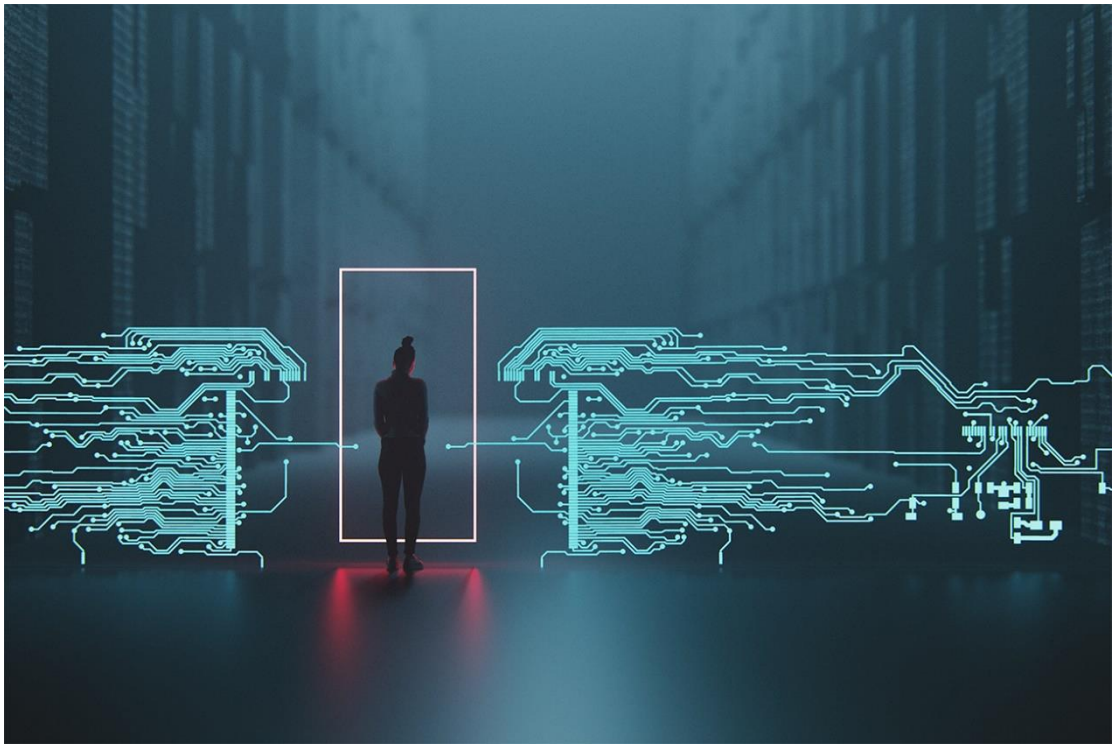
在个人信息保护方面，《网络安全法》对个人信息保护做出了原则性、概括性规定，以保护个人信息为主要目的。而近年来，个人信息保护实践日益普遍，主体多元、类型多样、场景丰富，大规模收集、使用个人信息的活动越来越成为常态，侵害个人信息权益的行为更为普遍，个人信息保护已经成为广大人民群众最关心最直接最现实的利益问题之一。同时，个人信息具有丰富的数据价值，对其合理利用也是数字经济发展的基础之一。个人信息保护统一立法的全球趋势也十分明显。结合国内外情况，有必要制定全面性、基础性的个人信息保护法律。今年 8 月，《个人信息保护法》正式通过，并于 11 月起实施。《个人信息保护法》作为个人信息领域的基础性法律，对个人信息保护进行了整体安排和制度重构，立法目的既包括对个人信息的保护，也包括个人信息合理利用。《个人信息保护法》对《网络安全法》中有关个人信息保护的内容进行了大幅拓展和一定程度调整，规定了个人信息处理的合法性基础、个人信息处理者的义务、个人在个人信息处理活动中的权利、个人信息保护监管体制等主要内容，基本覆盖了个人信息保护的各个方面，下一步将继续形成个人信息保护法律体系。

从网络安全法律体系自身来看，其组成架构也发生了变化和调整。一方面，传统的网络安全问题还是比较突出，传统网络攻击形式，如分布式拒绝服务（DDos）攻击仍然呈现持续上升趋势，2021 年 DDos 攻击的数量、规模较往年继续上升。《网络安全法》继续发挥应对传统网络安全的重要作用，今年以来，相关配套立法也相继出台，进一步规范网络安全相关

工作。另一方面，5G、物联网等技术发展普及，不断改变网络连接方式和连接对象，物理空间和网络空间的边界不断融合、模糊，内生式网络安全问题不断产生，其中明显以数据为主要对象。网络治理问题很大程度上已经凸显为数据治理问题，网络安全问题正在不断聚焦成为数据安全问题。围绕数据展开的一系列讨论越来越丰富，越来越深入。相关数据立法工作也在加速推进，逐步形成数据治理顶层法律体系。数据安全、数据权属等问题倍受关注，各方都期待数据领域能够广泛达成共识，建立起明确的数据活动规则，谋求安全与发展平衡之道。

三、网络安全配套法规体系持续完善

今年，《网络安全法》已经实施了四年。2016 年，习近平总书记在网络安全和信息化工作座谈会上做重要讲话指出，维护网络安全，要“聪者听于无声，明者见于未形”。如今，《网络安全法》制定之时的所听所见也都成为现实的迫切问题。《网络安全法》的制度潜力不断释放，依然是网络治理领域的重要法治依据。2021 年，以《网络安全法》为上位法的配套规定相继出台，有关具体要求得以确定。



一是关键信息基础设施安全保护法律制度最终明确。关键信息基础设施保护是网络安全的重要部分，主要思路是将为社会运转提供基础性、关键性服务的设施列为关键信息基础设施，并予以保护。美国、德国、日本、澳大利亚等都通过立法对关键基础设施进行保护。今年 7 月，《关键信息基础设施安全保护条例》（以下简称《条例》）正式出台。作为《网络安全法》的重要配套立法，《条例》积极应对国内外网络安全保护的主要问题和发展趋势，

为下一步加强关键信息基础设施安全保护工作提供了重要法治保障。《条例》界定了适用范围、监管主体、评估对象等关键信息基础设施安全保护相关基本要素，提出了安全保护要求及措施，确保对象具体、权责清晰、任务明确，为安全保护工作开展提供系统指引和工作遵循。

关键信息基础设施的范围一直是各方面关心的核心问题。《网络安全法》中有关三同步、供应链安全、跨境数据流动、风险评估等要求都仅适用关键信息基础设施运营者。确定关键信息基础设施运营者是开展关键信息基础设施安全保护工作的基础，有关主体十分关心自己是否以及如何被列入关键信息基础设施范围的问题。《条例》对此采取了主管部门认定和单独通知的流程，规定由负责关键信息基础设施安全保护工作的部门制定认定规则，组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并报国务院公安部门。

二是网络漏洞管理进一步完善。网络漏洞是网络安全中的主要隐患之一，需要有效的机制措施来防范和消除风险。《网络安全法》要求网络产品、服务提供者发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当采取补救措施并通知用户和报告主管部门；要求网络运营者及时处理系统漏洞等安全风险；规定“向社会发布系统漏洞……等网络安全信息，应当遵守国家有关规定”。今年 7 月，工业和信息化部、国家互联网信息办公室、公安部联合制定出台《网络产品安全漏洞管理规定》，推动网络产品安全漏洞管理工作的制度化、规范化、法治化，提高相关主体漏洞管理水平，引导建设规范有序、充满活力的漏洞收集和发布渠道，防范网络安全重大风险，保障国家网络安全。

三是供应链安全要求进一步深化。供应链安全是适应网络安全全周期、长链条等特点的子命题之一。《网络安全法》中对关键信息基础设施运营者采购产品和服务，规定了国家安全审查（即网络安全审查）的要求。2020 年，国家互联网信息办公室会同国家发展和改革委员会、工业和信息化部、公安部等十二部门联合制定出台了《网络安全审查办法》，加强关键信息基础设施供应链安全，确保国家安全。今年 7 月，国家互联网信息办公室修订了该办法，并就《网络安全审查办法（修订草案征求意见稿）》向社会公开征求意见。征求意见稿将供应链安全的主体进一步扩大到数据处理者，调整范围覆盖数据处理活动，体现了数据活动在供应链安全中的风险因素。

四是具体领域进一步细化配套规则。7 月 5 日，国家互联网信息办公室会同国家发展和改革委员会、工业和信息化部、公安部、交通运输部制定出台《汽车数据安全管理若干规定（试行）》，对汽车数据处理活动中的重要数据和个人信息予以保护，维护国家安全、数据安全和个人权益。9 月 13 日，工业和信息化部发布《关于加强车联网卡实名登记管理的通

知》，明确不同销售阶段车联网卡实名登记要求，防范车联网中的安全风险。9 月 15 日，工业和信息化部发布《关于加强车联网网络安全和数据安全工作的通知》，对车联网的网络安全和数据安全提出了基本要求。

五是反电信网络诈骗提上立法议程。今年 10 月，《反电信网络诈骗法（草案）》提交全国人大常委会首次审议，并向社会公开征求意见。草案的制定秉持了“小切入立法”以及“急用先行”的原则，对现实需求做出回应的同时，全面提升反电信网络诈骗工作的法治化、规范化水平。草案立足源头治理，打击“两卡”犯罪，强化实名制管理，突出新技术整治，完善救济措施，对内建立全链条整治工作机制，对外积极稳妥推进国际执法司法合作。

四、数据安全、个人信息保护、算法等立法快速推进

《网络安全法》在网络治理过程中发挥了重要的作用，也将持续提供制度供给。与此同时，数据安全、个人信息保护、算法等领域问题凸显，场景越来越丰富，活动越来越频繁，亟需立法规制。从历史意义和广义来看，这些法律法规也可以纳入网络安全法律体系的视角。

一是数据安全领域确立基础性法律。数据是数字经济的基础性战略资源，数据治理能力是国家竞争力的体现。2017 年，习近平总书记提出“要加强政策、监管、法律的统筹协调，加快法规制度建设。要制定数据资源确权、开放、流通、交易相关制度，完善数据产权保护制度。”《数据安全法》今年 6 月正式出台，数据治理制度实现从无到有的“突破”，成为我国数据安全领域基础性法律。《数据安全法》对数据分类分级、重要（核心）数据管理、数据安全审查等作出了明确规定，同时，在《网络安全法》的基础上，完善了跨境数据流动的管理要求，回应了关键信息基础设施以外的重要数据的跨境管理诉求。

二是跨境数据流动规则进一步构建完善。《数据安全法》《个人信息保护法》出台后，与《网络安全法》相衔接，完善了跨境数据管理制度。总体来看，跨境数据流动管理制度覆盖了关键信息基础设施运营者、重要数据处理者和个人信息处理者等主体，包括安全评估、认证、标准合同等具体手段。今年 10 月，国家互联网信息办公室对《数据出境安全评估办法（征求意见稿）》公开征求意见，该办法以《网络安全法》《数据安全法》《个人信息保护法》为上位法，细化和明确了我国跨境数据安全自由流动的具体规则，是我国数据治理框架性法律正式成型后，在数据出境安全管理系列规范中具有关键意义和地位的配套规则。

三是数据安全配套立法快速启动。今年 11 月，国家互联网信息办公室发布《网络数据安全管理条例（征求意见稿）》向社会公开征求意见，对网络数据处理活动中涉及的个人信息保护、重要数据安全管理、跨境数据流动规范等内容进行了全方位、多层次的细化规定。该条例将成为《数据安全法》的主要配套规则之一。

四是算法对经济和社会的影响逐步扩大，滋生了“大数据杀熟”“信息茧房”等损害公众利益，破坏正当竞争，扰乱社会秩序的行为。有关部门在高位阶立法对算法概括性要求的基础上，进一步深入推进，从内容安全、社会管理、市场秩序等多维度价值导向层面对算法推荐进行规范。

2021 年 8 月，国家互联网信息办公室发布了《互联网信息服务算法推荐管理规定（征求意见稿）》，对算法推荐技术作出专门管理规定。该规定以互联网信息服务为基础，从算法的公平公正及信息内容角度对算法推荐服务提出了各项具体细化的要求，明确了“算法推荐技术”的范围、算法推荐服务的监管原则与规则以及具体的分级分类、备案、安全评估等监管手段。9 月，国家互联网信息办公室、中宣部、教育部、科技部等九部委印发《关于加强互联网信息服务算法综合治理的指导意见》，提出要利用三年左右时间，逐步建立治理机制健全、监管体系完善、算法生态规范的算法安全综合治理格局。

五、下一步展望

网络安全是网络空间的基础性保障问题，网络空间越来越成为社会治理的主要载体，网络安全问题不仅是国家安全的主要内容，也可能成为社会安全的底层逻辑。今年，网络安全相关配套立法得以长足完善，同时网络法治精细化发展趋势，也使得部分领域从网络安全体系中抽离和分立，促进整体网络法治体系的结构化完善。

目前，《数据安全法》和《个人信息保护法》已经相继实施，但部分事项还需要配套规定予以明确。《网络数据安全管理条例》《数据出境安全评估办法》等正在加快制定之中，但数据安全、个人信息保护从功能和目标上来看，需要结构化的制度体系，中短期内仍然有大量的配套立法任务。从下一步来看，一方面，要持续补齐，尽快出台数据跨境管理、数据安全管理相关配套立法，确定有关法律制度的具体要求，为具体执法监督提供指引。另一方，面也要观察总结，适时结合新的发展变化，调整、形成思路和方法，修订或者制定相关网络安全法律规定，为我国网络安全工作持续提供法治保障。（来源:《中国信息安全》杂志 2021 年第 12 期）

四、政府之声

➢ 国家互联网信息办公室等十三部门修订发布《网络安全审查办法》

2022 年 1 月 4 日，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局等十三部门联合修订发布《网络安全审查办法》（以下简称《办法》），自 2022 年 2 月 15 日起施行。

国家互联网信息办公室有关负责人表示，网络安全审查是网络安全领域的重要法律制度，原《办法》自 2020 年 6 月 1 日施行以来，对于保障关键信息基础设施供应链安全，维护国家安全发挥了重要作用。为落实《数据安全法》等法律法规要求，国家互联网信息办公室联合相关部门修订了《办法》。

《办法》将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查，并明确掌握超过 100 万用户个人信息的网络平台运营者赴国外上市必须向网络安全审查办公室申报网络安全审查。根据审查实际需要，增加证监会作为网络安全审查工作机制成员单位，同时完善了国家安全风险评估因素等内容。国家互联网信息办公室有关负责人表示，《办法》修订对保障国家网络安全和数据安全具有重要意义。（来源：中国网信网）

- **《网络安全审查办法》全文：**
- http://www.cac.gov.cn/2022-01/04/c_1642894602182845.htm

➢ 证监会发布《证券期货业移动互联网应用程序安全检测规范》

2021 年 12 月 29 日，证监会发布《证券期货业移动互联网应用程序安全检测规范》金融行业标准，自公布之日起施行。

近年来，证券期货业移动应用体系建设快速发展，环境日臻完善，工具应用日益广泛，移动应用提供了快速便捷的证券业务服务，同时也存在一些安全隐患。《证券期货业移动互联网应用程序安全检测规范》规定了证券期货业移动互联网应用程序安全检测的总体要求及检测方法等，适用于信息安全检测服务、移动互联网应用程序的安全测试评估、自动化安全检测工具的设计与开发等。标准的制定实施，将统一行业对移动互联网应用程序的安全要求，提高移动互联网应用程序的安全性，增强行业机构移动业务信息安全能力，有效防范相关安全风险。

下一步，证监会将继续推进资本市场信息化建设，着力加强基础标准建设，完善技术安全监管制度，确保在技术进步的同时，实现安全管控水平稳步提升。（来源：中国证券监督管理委员会）

- **《证券期货业移动互联网应用程序安全检测规范》(JR/T 0240—2021)全文：**
- http://www.csrc.gov.cn/csrc/c101954/c1718681/content.shtml

➢ 中国银保监会发布《银行保险机构信息科技外包风险监管办法》

2021 年 12 月 30 日，为进一步加强银行保险机构信息科技外包风险监管，促进银行保险机构提升信息技外包风险管控能力，推动银行保险机构稳健开展数字化转型工作，中国银保监会近日印发了《银行保险机构信息科技外包风险监管办法》（以下简称《办法》）。


中国银行保险监督管理委员会
China Banking and Insurance Regulatory Commission
无障碍浏览 | 繁 | EN
请输入您要搜索的内容...
机构概况 | 新闻资讯 | 政务信息 | 在线服务 | 互动交流 | 统计数据 | 专题专栏
当前位置： 首页 > 新闻资讯 > 监管动态
发布时间：2022-01-26 来源：办公厅 文章类型：原创
打印 微博 微信 更多
中国银保监会发布《关于银行业保险业数字化转型的指导意见》
为深入贯彻落实以习近平同志为核心的党中央决策部署，加快数字经济建设，全面推进银行业和保险业数字化转型，推动金融高质量发展，更好服务实体经济和满足人民群众需要，近日中国银保监会印发了《关于银行业保险业数字化转型的指导意见》（以下简称《指导意见》），要求银行保险机构结合实际认真贯彻落实。
《指导意见》指出，要以习近平新时代中国特色社会主义思想为指导，全面贯彻《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》要求，立足新发展阶段，贯彻新发展理念，服务构建新发展格局，坚持以人民为中心的发展思想，深化金融供给侧结构性改革，以数字化转型推动银行业和保险业高质量发展，构建适应现代经济发展的数字金融新格局，不断提高金融服务实体经济的能力和水平，有效防范化解金融风险。

《办法》起草工作坚决贯彻落实中央精神，注重把握以下原则：一是坚持风险为本，在深入分析银行保险机构信息科技外包风险发展态势的基础上，提出针对性的监管要求；二是强化监管力度，在总结银行保险业信息科技监管实践经验的基础上，制定体系化的监管措施；三是对接国际标准，《办法》起草工作吸收借鉴了近年来国际组织、国外监管机构相关外包监管原则和良好实践。

《办法》共 7 章 46 条，对银行保险机构信息科技外包风险管理提出全面要求。一是在总则中明确信息科技外包风险管理的总体要求，即银行保险机构应当建立与本机构信息科技战略目标相适应的信息科技外包管理体系，将信息科技外包风险纳入全面风险管理体系，有效控制由于外包而引发的风险。二是在信息科技外包治理中对银行保险机构的组织和职责、外包战略、外包禁止、服务提供商管理策略、外包分类、外包分级管理、退出策略等提出明确要求。三是对信息科技外包准入提出监管要求，包括准入前评估、尽职调查、合同等进行了规定，并对非驻场集中式外包、跨境外包、同业和关联外包提出附加要求。四是明确信息科技外包监控评价要求，对外包过程监控、效能和质量监控、服务监控及评价、服务提供商经营监控、异常纠正、关联外包评价、外包终止做出规定。五是规范信息科技外包风险管理，

对外包风险识别与评估、业务连续性管理、信息安全管理、集中度风险管理、非驻场外包实地检查、年度风险评估和审计提出要求。六是对监管机构实施外包监督管理做出规定，包括事前报告要求、重大事件报告、监管评估和监督检查、风险监测、监管干预、实地核查、监管问责等内容。

下一步，银保监会将加强政策宣贯培训，将信息科技外包纳入对银行保险机构的日常风险监测和现场检查，推动银行保险机构建立有效的信息科技外包风险管理体系，促进《办法》有效落地实施。（来源：中国网信网）

- **《银行保险机构信息科技外包风险监管办法》全文：**
- http://www.cbirc.gov.cn/cn/view/pages/ItemDetail.html?docId=1029035&itemId=928&generaltype=0

➢ 国务院印发《“十四五”数字经济发展规划》

2021 年 12 月 12 日，国务院日前印发《“十四五”数字经济发展规划》（以下简称《规划》），明确了“十四五”时期推动数字经济健康发展的指导思想、基本原则、发展目标、重点任务和保障措施。

《规划》以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大和十九届

历次全会精神，立足新发展阶段，完整、准确、全面贯彻新发展理念，构建新发展格局，推动高质量发展，统筹发展和安全，统筹国内和国际，以数据为关键要素，以数字技术与实体经济深度融合为主线，加强数字基础设施建设，完善数字经济治理体系，协同推进数字产业化和产业数字化，赋能传统产业转型升级，培育新产业新业态新模式，不断做强做优做大我国数字经济，为构建数字中国提供有力支撑。

《规划》明确坚持“创新引领、融合发展，应用牵引、数据赋能，公平竞争、安全有序，系统推进、协同高效”的原则。到 2025 年，数字经济核心产业增加值占国内生产总值比重达到 10%，数据要素市场体系初步建立，产业数字化转型迈上新台阶，数字产业化水平显著提升，数字化公共服务更加普惠均等，数字经济治理体系更加完善。展望 2035 年，力争形成统一公平、竞争有序、成熟完备的数字经济现代市场体系，数字经济发展水平位居世界前列。

《规划》部署了八方面重点任务。一是优化升级数字基础设施。加快建设信息网络基础设施，推进云网协同和算网融合发展，有序推进基础设施智能升级。二是充分发挥数据要素作用。强化高质量数据要素供给，加快数据要素市场化流通，创新数据要素开发利用机制。三是大力推进产业数字化转型。加快企业数字化转型升级，全面深化重点行业、产业园区和集群数字化转型，培育转型支撑服务生态。四是加快推动数字产业化。增强关键技术创新能力，加快培育新业态新模式，营造繁荣有序的创新生态。五是持续提升公共服务数字化水平。提高“互联网+政务服务”效能，提升社会服务数字化普惠水平，推动数字城乡融合发展。六是健全完善数字经济治理体系。强化协同治理和监管机制，增强政府数字化治理能力，完善多元共治新格局。七是着力强化数字经济安全体系。增强网络安全防护能力，提升数据安全保障水平，有效防范各类风险。八是有效拓展数字经济国际合作。加快贸易数字化发展，推动“数字丝绸之路”深入发展，构建良好国际合作环境。围绕八大任务，《规划》明确了信息网络基础设施优化升级等十一个专项工程。

《规划》从加强统筹协调和组织实施、加大资金支持力度、提升全民数字素养和技能、实施试点示范、强化监测评估等方面保障实施，确保目标任务落到实处。（来源：中国政府网）

- **国务院关于印发“十四五”数字经济发展规划的通知全文：**
- http://www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm

五、本期重要漏洞实例

➢ Microsoft 发布 2022 年 1 月安全更新

发布日期：2022-1-11

更新日期：2022-1-11

描述：2022 年 1 月 11 日，微软发布了 2022 年 1 月份的月度例行安全公告，修复了多款产品存在的 127 个安全漏洞。受影响的产品包括：Windows 11（66 个）、Windows Server 2022（81 个）、Windows 10 21H1 & 21H2（79 个）、Windows 10 20H2 & Windows Server v20H2（81 个）、Windows 10 1909（77 个）、Windows 8.1 & Server 2012 R2（52 个）、Windows Server 2012（49 个）、Windows RT 8.1（48 个）和 Microsoft Office-related software（4 个）。利用上述漏洞，攻击者可进行欺骗，绕过安全功能限制，获取敏感信息，提升权限，执行远程代码，或发起拒绝服务攻击等。提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

CVE 编号	公告标题	最高严重等级和漏洞影响	受影响的软件
CVE-2022-21907	HTTP Protocol 栈远程代码执行漏洞	严重 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10
CVE-2022-21893	Remote Desktop Protocol 远程代码执行漏洞	重要 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2022-21849	Windows IKE Extension 远程代码执行漏洞	重要 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016
CVE-2022-21922	Remote Procedure Call Runtime 远程代码执行漏洞	重要 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012

			Windows 8.1
CVE-2022-21901	Windows Hyper-V 权限提升漏洞	重要 特权提升	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2 Windows 8.1
CVE-2022-21850	Remote Desktop Client 远程代码执行漏洞	重要 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1 Remote Desktop client Windows Desktop
CVE-2022-21920	Windows Kerberos 权限提升漏洞	重要 特权提升	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2022-21874	Windows Installer 权限提升漏洞	重要 特权提升	Windows 11 Server 2022 Server, version 20H2 Server, version 2004 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2022-21874	Windows Security Center API 远程代码执行漏洞	重要 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10

			Server 2016
CVE-2022-21857	Active Directory Domain Services 权限提升漏洞	严重 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2022-21836	Windows Certificate 欺骗漏洞	重要 欺骗	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2022-21919	Windows User Profile Service 权限提升漏洞	重要 特权提升	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2022-21840	Microsoft Office 远程代码执行漏洞	严重 远程代码执行	Excel 2013/2016 Office 2013/2016/2019 Office LTSC 2021 SharePoint Server — Subscription Edition SharePoint Server — Sub Edition Language Pack Office Web Apps Server 201 SharePoint Foundation 2013 SharePoint Server 2019 SharePoint Ent. Server 2016 SharePoint Ent. Server 2013 365 Apps Enterprise Office LTSC for Mac 2021 Office 2019 for Mac Office Online Server

CVE-2022-21837	Microsoft SharePoint Server 远程代码执行漏洞	重要 远程代码执行	SharePoint Server Subscription Edition SharePoint Foundation 2013 SharePoint Enterprise Server 2016 SharePoint Server 2019

来源：https://msrc.microsoft.com/update-guide/releaseNote/2022-Jan

➢ Adobe InDesign 资源管理错误漏洞

发布日期：2022-1-18
更新日期：2022-1-18
受影响系统：Adobe Adobe InDesign <=16.4
描述：

CVE(CAN) ID:CVE-2021-45059
Adobe InDesign 是美国奥多比（Adobe）公司的一套排版编辑应用程序。
Adobe InDesign 存在资源管理错误漏洞，攻击者可利用该漏洞绕过缓解措施，导致敏感内存泄露。
建议：

厂商已发布了漏洞修复程序，请及时关注更新：
https://helpx.adobe.com/security/products/indesign/apsb22-05.html

➢ Cisco Security Manager 跨站脚本漏洞

发布日期：2022-1-18
更新日期：2022-1-18
受影响系统：
Cisco Cisco Security Manager (CSM)
描述：

CVE(CAN) ID: CVE-2022-20643
Cisco Security Manager (CSM) 是美国思科 (Cisco) 公司的一套企业级的管理应用，它主要用于在 Cisco 网络和安全设备上配置防火墙、VPN 和入侵保护安全服务。
Cisco Security Manager 中存在跨站脚本漏洞，该漏洞源于产品基于 Web 的管理界面未对用户输入数据的特殊字符做有效处理。攻击者可通过该漏洞在接口上下文中执行任意脚本代码或访问敏感的、基于浏览器的信息。
建议：

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-mult-xss-7hmOKQTt

➢ IBM Spectrum Protect Plus 访问控制错误漏洞

发布日期：2022-1-19
更新日期：2022-1-19
受影响系统：
IBM Spectrum Protect Plus >=10.1.0.0，<=10.1.8.*
描述：

CVE(CAN) ID: CVE-2021-39063
IBM Spectrum Protect Plus 是美国 IBM 公司的一套数据保护平台。该平台为企业提供单一控制和管理点，并支持对所有规模的虚拟、物理和云环境进行备份和恢复。
IBM Spectrum Protect Plus 存在安全漏洞，该漏洞源于 IBM Spectrum Protect Plus 使用跨源资源共享(CORS)，但在访问控制头中存在错误配置，攻击者可利用该漏洞执行特权操作并检索敏感信息。
建议：

厂商补丁：
目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://www.ibm.com/support/pages/node/6525346

六、本期网络安全事件

➢ 美医疗系统 Broward Health 披露数据泄露事件 影响超 130 万人

2022 年 1 月 4 日，美国 Broward Health 公共卫生系统近日披露了一起大规模数据泄露事件，影响到 1357879 人。Broward Health 是一个位于佛罗里达州的医疗系统，有三十多个地点提供广泛的医疗服务，每年接收超过 60000 名入院病人。

该医疗系统在 2021 年 10 月 15 日披露了一起网络攻击事件，当时一名入侵者未经授权访问了医院的网络和病人数据。该组织在四天后，即 10 月 19 日发现了这次入侵事件，并立即通知了美国联邦调查局和美国司法部。

同时，所有员工被建议更改他们的用户密码，Broward Health 与第三方网络安全专家签约，帮助进行调查。调查显示，入侵网站的黑客获得了病人的个人医疗信息，其中可能包括以下内容：全名、出生日期、实际地址、电话号码、财务或银行信息、社会安全号码、保险信息和账户号码、医疗信息和历史、病情、治疗和诊断、驾照号码、电子邮件地址。

尽管 Broward Health 确认黑客已经泄露了上述数据，但它指出，没有证据表明他们滥用了这些数据。值得注意的是，入侵点被确定为一个第三方医疗机构，他们被允许进入系统以提供服务。

“为了应对这一事件，Broward Health 正在采取措施防止类似事件的再次发生，其中包括正在进行的调查，在整个企业中加强安全措施的密码重置，以及对其系统的所有用户实施

多因素认证，”Broward Health 在向受影响的病人和雇员数据泄露通知解释称。“我们还开始对不由 Broward Health 信息技术公司管理的访问我们网络的设备实施额外的最低安全要求，这些要求将于 2022 年 1 月生效。”由于暴露数据的关键性质，通知的接收者需要对所有形式的通信保持警惕。此外，该医疗系统正在通过 Experian 提供为期两年的身份盗窃检测和保护服务，信中还附有如何注册的详细信息。（来源：cnBeta）

➢ 公安部公布 2021 年侵犯个人信息十大典型案例

2022 年 1 月 8 日，公安部公布 2021 年侵犯公民个人信息犯罪十大典型案例。2021 年全国公安机关深入推进“净网 2021”专项行动，针对民众关注的个人信息保护问题，全力组织开展侦查打击工作，共破获侵犯公民个人信息案件 9800 余起，抓获犯罪嫌疑人 1.7 万余名，有力维护了网络空间秩序和人民群众合法权益。


中华人民共和国公安部
The Ministry of Public Security of the People's Republic of China
首 页 机构设置 警务信息 办事服务 警民互动 请输入关键字
当前位置：首页 > 工作动态 > 正文
“公安2021”年终盘点报道
打击侵犯公民个人信息犯罪这一年：公安部公布十大典型案例
时间：2022年01月08日 字体：大 中 小 分享到:
2021年，全国公安机关深入推进“净网2021”专项行动，针对人民群众关注的个人信息保护问题，全力组织开展侦查打击工作，共破获侵犯公民个人信息案件9800余起，抓获犯罪嫌疑人1.7万余名，有力维护了网络空间秩序和人民群众合法权益。公安部今日公布了2021年侵犯公民个人信息犯罪十大典型案例。
一、江苏公安机关破获何某非法获取公民个人信息案。江苏公安网安部门侦查查明，犯罪嫌疑人何某利用为相

后续，公安机关网安部门将会同有关部门，认真贯彻落实《刑法》和《个人信息保护法》《数据安全法》等法律法规，完善打击危害公民个人信息和数据安全违法犯罪长效机制，坚持打击和防范并重，做好源头防控，持续保持严打高压态势，不断提升民众的安全感。

一、江苏公安机关破获何某非法获取公民个人信息案。江苏公安网安部门侦查查明，犯罪嫌疑人何某利用为相关单位、企业建设信息系统之机，非法获取医疗、出行、快递等公民个人信息数十亿条，搭建对外提供非法查询服务的数据库，通过暗网发布广告招揽客户，出

售谋取不法利益。

二、湖北公安机关破获徐某等人利用外挂程序非法获取公民个人信息案。湖北公安网安部门侦查查明，武汉某公司工作人员徐某等人，利用李某编写的多款外挂程序，通过系统接口漏洞，窃取酒店、燃气、医疗健康等 33 个网站后台公民个人信息 3000 余万条用于债务催收等。

三、安徽公安机关破获吴某等人非法获取老年人个人信息推销虚假保健品案。安徽公安网安部门侦查查明，犯罪嫌疑人吴某成立多家健康咨询公司，通过网上购买、交换有保健品购买记录的老年人信息 200 余万条，通过制定话术、夸大效果推销虚假保健品，骗取 6 万余名老年人 1500 余万元。

四、江苏公安机关破获关某等人非法获取公民个人信息案。江苏公安网安部门侦查查明，犯罪嫌疑人关某利用多个空壳公司与多家电信运营商签订合同，非法获取电信用户手机上网标签数据 2 亿余条，按照地域、行业等分类后，向下游精准营销人员和电信网络诈骗犯罪人员贩卖牟利。

五、福建公安机关破获谢某等人利用木马窃取网民购物信息案。福建公安网安部门侦查查明，犯罪嫌疑人谢某诱骗某电商平台店铺客服点击木马链接，窃取 200 余家店铺的买家个人信息 1000 余万条，向林某等人层层贩卖，最终流向电信网络诈骗团伙。

六、辽宁公安机关破获石某等人非法获取公民信息注册游戏账号并向未成年人出售案。辽宁公安网安部门侦查查明，山东某网络科技公司从网上购买公民信息，在辽宁阜新石某团伙的技术支撑下，突破游戏公司验证机制，非法注册实名网络游戏账号 1.8 万余个，向未成年人出售，非法牟利 170 余万元。

七、广东公安机关破获某公司非法获取公民个人信息实施诈骗案。广东公安网安部门侦查查明，珠海某艺术品策划公司从某 APP 维护人员汪某处购买 APP 在运营过程中获取的古董持有人员个人信息 200 万余条，以协助拍卖古董为名，骗取客户服务费、托管费，非法牟利 1.9 亿余元。该公司员工邝某、黄某为谋取私利，将公司非法获取的个人信息向其他电信网络诈骗团伙贩卖。

八、江苏公安机关破获某公司非法获取公民个人信息案。江苏公安网安部门侦查查明，某公司非法搭建 5300 余个虚假网站，冒用其他公司资质在某自媒体平台发布免费领取男科用药、白酒、保健品等虚假信息，引流至其所建虚假网站，骗取网民的姓名、手机号、收货地址等公民个人信息 110 余万条并贩卖牟利。

九、浙江公安机关破获李某等人非法获取公民快递信息案。浙江公安网安部门侦查查明，

犯罪嫌疑人李某指使团伙成员应聘多家快递公司临聘人员，利用整理快递包裹之机，偷拍快递面单 2 万余张，汇总整理后在网上贩卖。

十、江苏公安机关破获张某等人非法获取公民个人信息案。江苏公安网安部门侦查查明，犯罪嫌疑人张某搭建服务器制作远程控制软件，出售给他人安装在受害人手机上，非法获取受害人手机的位置、通话记录等，涉及手机 1.1 万余台。（来源：公安部）

➢ 松下证实黑客在网络攻击中获取了求职者的个人资料

2022 年 1 月 11 日，据 TechCrunch 报道，日本科技巨头松下公司证实，黑客在 11 月的网络攻击中获取了属于求职者和实习生的个人信息。该公司在 11 月 26 日首次确认了数据泄露事件，当时该公司无法说明黑客是否获取了任何敏感信息。

然而，在 1 月 7 日发布的更新中，**松下公司表示：**与申请就业或在公司某些部门参加实习的候选人有关的一些个人信息在此次事件中被获取。松下公司表示，它正在通知受影响的人。当 TechCrunch 联系到松下发言人 Dannea DeLisser 时，她拒绝透露有多少人受到影响，以及被访问信息的性质。

松下公司的最新消息还证实，这次数据泄露事件始于 6 月 22 日，止于 11 月 3 日，于 11 月 11 日被发现--看到黑客获得了由商业伙伴提供的包含未指明的“业务相关信息”的文件，以及有关商业伙伴人员的信息。

该公司在外部安全顾问的帮助下进行的调查结果证实：第三方通过一家海外子公司的

服务器非法访问了日本的一台文件服务器。松下公司说，在发现非法访问后，它 “立即实施了额外的安全对策”，包括加强来自海外的访问控制，重新设置相关密码和加强服务器访问监控。松下公司表示，它正在加强安全措施，以防止再次发生攻击。

松下公司 11 月发生的数据泄露事件，是在该公司的印度子公司成为勒索软件攻击的受害者后几个月发生的，黑客泄露了 4GB 的数据，包括财务信息和电子邮件地址。 （来源：TechCrunch）

➢ 菲律宾两大银行遭黑客入侵 部分客户存款被盗

2022 年 1 月 20 日，中国人民银行南宁中心支行发布的一则行政处罚信息公示显示，中国农业银行崇左分行被罚 1142.5 万元。另外，该分行内 5 名相关责任人被罚，最高达 11 万元。处罚信息公示表显示，**因存在未落实个人银行账户实名制管理规定、违规使用个人金融信息、未严格落实银行账户风险监测要求、未按规定完整保存客户身份资料等违法行为，农业银行崇左分行被人民银行崇左市中心支行罚款 1142.5 万元**。

与此同时，相关责任人也领到罚单。时任农业银行崇左分行行长因对未严格落实银行账户风险监测要求、未按规定完整保存客户身份资料等违法行为负有责任，被处以警告并处 11 万元罚款;农业银行崇左分行副行长、个人金融部/个人信贷部/消费者权益保护办公室总经理被分别处以 5 万元罚款;时任农业银行崇左江州支行行长、时任农业银行崇左江州支行行长助理被分别处以 11 万元、5 万元罚款。

序号	当事人名称（姓名）	行政处罚决定书文号	违法行为类型	行政处罚内容	作出行政处罚决定机关名称	作出行政处罚决定日期	备注
1	中国农业银行股份有限公司崇左分行	崇左银罚字〔2022〕1 号	未落实个人银行账户实名制管理规定；违规使用个人金融信息；未严格落实银行账户风险监测要求；未按规定完整保存客户身份资料	处以警告并共处人民币 1,142.50 万元罚款	中国人民银行崇左市中心支行	2022 年 1 月 12 日	
2	梁晓军(时任中国农业银行股份有限公司崇左分行行长)	崇左银罚字〔2022〕2 号	对中国农业银行股份有限公司崇左分行以下违法违规行为负有责任：未按规定完整保存客户身份资料；未严格落实银行账户风险监测要求	处以警告，并处人民币 11 万元罚款	中国人民银行崇左市中心支行	2022 年 1 月 12 日	

3	高峰（中国农业银行股份有限公司崇左分行副行长）	崇左银罚字〔2022〕3 号	对中国农业银行股份有限公司崇左分行以下违法违规行为负有责任：未按规定完整保存客户身份资料	处人民币 5 万元罚款	中国人民银行崇左市中心支行	2022 年 1 月 12 日	
4	钟丽月(中国农业银行股份有限公司崇左分行个人金融部/个人信贷部/消费者权益保护办公室总经理)	崇左银罚字〔2022〕4 号	对中国农业银行股份有限公司崇左分行以下违法违规行为负有责任：未按规定完整保存客户身份资料	处人民币 5 万元罚款	中国人民银行崇左市中心支行	2022 年 1 月 12 日	
5	许亦猛（时任中国农业银行股份有限公司崇左江州支行行长）	崇左银罚字〔2022〕5 号	对中国农业银行股份有限公司崇左分行以下违法违规行为负有责任：未按规定完整保存客户身份资料；未严格落实银行账户风险监测要求	处以警告，并处人民币 11 万元罚款	中国人民银行崇左市中心支行	2022 年 1 月 12 日	
6	赖学芳（时任中国农业银行股份有限公司崇左江州支行行长助理）	崇左银罚字〔2022〕6 号	对中国农业银行股份有限公司崇左分行以下违法违规行为负有责任：未按规定完整保存客户身份资料	处人民币 5 万元罚款	中国人民银行崇左市中心支行	2022 年 1 月 12 日	

“莫名开户”事件引来的罚单

2021 年 12 月 10 日，广西崇左幼儿师范高等专科学校(下称“崇左幼专”)多名毕业生反映，自己名下莫名被开了银行电子账户，有人名下的账户多达 10 余个，这些账户的开户行均为中国农业银行崇左江州支行。崇左幼师学校发布声明称，没有通过任何渠道泄露学生的身份信息，没有代理学生开设银行账户或办理Ⅰ类、Ⅱ类、Ⅲ类卡账户的业务。该事件引发社会广泛关注。

农业银行广西区分行随后也作出通报：农业银行崇左江州支行因需完成银行账户开户增量指标任务，在未得到学生和学校同意、无相关开户文件的情况下，违规为广西崇左幼儿师范高等专科学校(以下简称“崇左幼师学校”)学生开立Ⅱ、Ⅲ类账户(未激活账户)。此事件系该行辖属崇左江州支行营业室违规操作所致，向学校师生诚恳认错、郑重道歉。

经查，2020 年 6 月 24 日，江州支行营业室批量开立 12536 户Ⅱ、Ⅲ类电子账户，涉

及 1457 名学生。开户所用信息为江州支行向学校提供代收学费服务时获得，江州支行营业室超范围使用，违规开立账户。崇左分行和江州支行存在严重违规、管理不力问题。已对涉及管理、经营、操作层面的 13 名责任人进行了免职、记过等追责。

人民银行崇左市中心支行相关负责人表示：人民银行崇左市中心支行对金融违法违规行为坚决依法严厉打击、严肃查处。此次处罚既体现了“严监管、强高压、长震慑”的监管态势，也为各金融机构敲响了合规经营的警钟。

下一步，人民银行崇左市中心支行将持续压实金融机构的主体责任，加大监管执法力度，全面开展警示教育，进一步提升金融行业合规意识和服务能力，切实保护金融消费者合法权益。（来源：安全学习那些事儿 ）

➢ 印尼央行遭勒索软件攻击 超 13GB 数据外泄

2022 年 1 月 20 日，印度尼西亚共和国中央银行——印度尼西亚银行(BANK INDONESIA)通信部执行主任 Erwin Haryono 证实，银行于上个月遭受了勒索软件攻击。中央银行有着管理货币部门、维持支付系统和金融系统稳定的重任，被攻击一事非同小可。据报道，**攻击发生在苏门答腊岛的印度尼西亚银行办事处，攻击者在银行系统上部署勒索软件，并窃取了印度尼西亚银行员工的“非关键数据”。**

印度尼西亚银行称，在采取措施后，事件没有造成太大影响，没有泄露任何重要数据，更重要的是银行的公共服务完全没有中断。

印度尼西亚银行没有将这次攻击归咎于特定的勒索软件团伙，但 Conti 组织表示对此负责，其威胁称若印度尼西亚银行不支付赎金，Conti 将泄露手中的 13.88GB 文件。

Conti 是世界上最危险的勒索软件团伙之一，其使用的恶意软件包括 Ryuk、TrickBot 和 BazarLoader，爱尔兰的卫生部(DoH)和卫生服务执行委员会(HSE)以及营销巨头 RR Donnelly 等都曾遭受过其攻击勒索。印度尼西亚银行还曾在 2016 年受到过一次网络攻击，那次印尼官方亦声称没有造成重大损失。据数据统计，印度尼西亚是近几年亚太地区最频繁受到恶意软件攻击的国家之一，在平均水平两倍以上。（来源：安全学习那些事儿）

➢ 黑客攻击欧洲港口石油设施，油轮无法靠港

2022 年 1 月 29 日，当地时间据央视新闻报道，因遭到勒索软件的攻击，位于荷兰阿姆斯特丹和鹿特丹、比利时安特卫普的几处港口的石油装卸和转运受阻。截至当地时间 2 月 4 日，至少有 7 艘油轮不得不在安特卫普港外等候，无法靠港。负责从这些港口经莱茵河向内陆城市转运石油的驳船也发生延误。**英国壳牌公司已经决定绕开这几处港口装运石油**。

这波网络袭击由何人发起目前还不清楚，受影响的公司正聘请网络安全专家进行调查。去年美国的几家石油公司也曾遭遇类似事件。

回溯来看：2021 年 5 月 7 日，美国最大燃油管道运营商科洛尼尔管道运输公司遭遇黑客攻击，被迫关闭整个管道系统。受管道关闭影响，美国多地出现燃油短缺和恐慌性购

买，导致燃油价格飙升。当地时间 2021 年 5 月 9 日，美国宣布进入国家紧急状态，原因是当地最大燃油管道运营商遭网络攻击下线。5 月 10 日，美国总统拜登称，攻击输油管道“是一种犯罪行为”。直到当地时间 5 月 13 日下午，科洛尼尔管道运输公司才宣布，重启了该公司的整个燃油运输系统并全面恢复运营。

国际油价创出逾 7 年新高

值得注意的是，此次欧洲几处主要油港遭遇黑客攻击，是在国际油价持续上涨的背景下进行的。数据显示，国际油价已连续上涨了 7 周，并创出逾 7 年新高。美东时间 2 月 4 日，国际油价大幅上涨，截至收盘，纽约 3 月原油期货收涨 2.04 美元，涨幅 2.26%，报 92.31 美元/桶，创 2014 年 9 月底以来新高;布伦特 4 月原油期货收涨 2.16 美元，涨幅 2.36%，报 93.27 美元/桶。（来源：央视新闻）