内部资料 免费交流

出版物准印证号：内资准印证 京内资准字 2124-L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯

特朗普2.0

网络安全迎来哪些巨变？ P15

第47期

2024 年 11 月

奇安信
新一代网络安全领军者

API安全卫士

曾获首届数据安全大赛金奖（产品能力评比）

检测、分析、防护闭环解决方案

守护API安全 数据安全

扫一扫 了解更多

特朗普网络安全政策的三个看点

以反复无常、难以预料而著称的特朗普，在其第二个任期会如何改变网络安全，这是全球的网络安全从业者都关心的问题。

显然，特朗普未来四年的科技政策领域面临众多的不确定性。但回顾其上一届的政策，仍然可以对其网络安全政策做出大概率的判断。

在笔者看来，至少有三个方向需要国内的网安行业关注。

首先，特朗普政府预计会持续推动网络安全现代化的政策。在其上一个任期中，特朗普提出了推动 IT 现代化的倡议，这在拜登政府得以延续。拜登政府发布了行政令与多项备忘录，推动零信任、供应链安全等技术在联邦政府机构的广泛部署。拜登在其离任前有望发布新的行政令，推动身份和访问管理技术的部署。网络攻防如同军事对抗，需要快速部署和利用前沿安全技术，这是其与追求稳定的 IT 系统所不同的方面。推进现代网络安全技术的广泛部署，目的在于打造主动防御体系，提升应对网络攻击的实战能力。我国主管部门与大型机构推动安全建设时显然需要参考和借鉴相关实践。

其次，特朗普政府可能采取更加大胆有力的网络反击政策，也就是“所有国家力量”对攻击活动做出更强硬的回应，包括美网络司令部将开展更频繁、更强有力的进攻行动。这超越防御态势的立场比 2018 年推出的“前置防御”战略更加激进。

最后，放松对人工智能的管制将占据主导地位，以释放行业创新潜力与中国在 AI 领域进行竞争。过去两年生成式人工智能快速兴起，业界在探讨创新应用的同时，主管机构尝试对 AI 开展严格监管、设置护栏，这不仅局限于美国。 事实上，对于事关未来的创新技术，是优先考虑监管还是押注创新，这是决定能否掌握竞争优势的关键。十多年前，欧盟和美国的经济规模几乎相同，现如今两者的 GDP 有 50% 的差距，这是选择监管和押注增长的不同结果。人工智能领域的竞赛显然需要更宽松的环境。

总编辑

李建平

2024 年 11 月 1 日

CONTENTS 目录

安全态势

月度专题

特朗普 2.0
网络安全迎来哪些巨变？

P15

从强化关基设施防护，采用比“前置防御”更加大胆的战略，到放松对人工智能的监管，特朗普 2.0 时代的网络安全政策将会非常值得关注。

攻防一线

安全之道

专　栏

奇安资讯

《网安 26 号院》编辑部
主办　奇安信集团

总　　编　　辑：李建平
安全态势主编：王　彪
月度专题主编：李建平
安全之道主编：张少波
奇安资讯主编：陈　冲
报告速递主编：刘川琦
专　　栏主编：任润波

奇安信集团　虎符智库　安全内参

索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557
出版物准印证号：内资准印证 京内资准 2124-L0058 号
编印单位：奇安信科技集团股份有限公司
发送对象：奇安信集团内部人员
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2024 年 11 月 26 日

政策篇

国内，行业数据安全政策标准不断推进。《反洗钱法》修订加强数据保护，《金融数据安全治理实施指南》等3项数据安全标准获批发布，工信部印发《工业和信息化领域数据安全事件应急预案（试行）》，国家数据局《可信数据空间发展行动计划（2024—2028年）》公开征求意见；

国际上，美国收紧敏感数据跨境流通规则，司法部、网络安全与基础设施安全局先后发布数据安全拟议新规，以防止外国获取敏感数据。美国联邦IT领导层还发布了《联邦零信任数据安全指南》，推动以数据为中心的保护理念。

国内

《反洗钱法》修订表决通过，更好地保护数据安全和公民个人信息

11月8日，十四届全国人大常委会第十二次会议表决通过了新修订的反洗钱法，自2025年1月1日起施行。为了更好地保护数据安全和公民个人信息，修订后的反洗钱法作了多方面规定。一是在保留现行反洗钱法关于严格规范反洗钱信息使用规定的同时，增加了规定对个人隐私的保护。二是明确要求提供反洗钱服务的机构及其工作人员对于因提供服务获得的数据、信息，应当依法妥善处理，确保数据、信息安全。三是增加规定金融机构在公司内部、集团成员之间共享反洗钱信息，也应当符合有关信息保护的法律规定。四是增加规定有关国家机关工作人员泄露反洗钱信息的法律责任。

《网络安全技术 终端计算机通用安全技术规范》等3项国家标准获批发布

11月5日，根据2024年10月26日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2024年第24号），全国网络安全标准化技术委员会归口的3项网络安全国家标准正式发布。具体包括《网络安全技术 终端计算机通用安全技术规范》《网络安全技术 存储介质数据恢复服务安全规范》《网络安全技术 网络弹性评价准则》。

住房城乡建设部印发《城市数字公共基础设施标准体系》

11月1日，住房城乡建设部组织编制了《城市数字公共基础设施标准体系》，为城市实现数字化转型发展提供统一数字底座，并对接底座一体化推进城市数字应用体系建设。该文件提出，城市数字公共基础设施标准体系框架分为九类，其中安全与保障类主要规范信息技术应用创新、安全与保障等方面的要求，包括网络安全、数据安全、密码应用安全和其他4个子类标准。

工信部印发《工业和信息化领域数据安全事件应急预案（试行）》

10月31日，工业和信息化部印发《工业和信息化领域数据安全事件应急预案（试行）》，以建立健全工业和信息化领域数据安全事件应急组织体系和工作机制，提高数据安全事件综合应对能力。该文件共八部分，包括总则、组织体系、监测与预警、事件响应、事后总结、预防措施、保障措施、附则。该文件将数据安全事件分为特别重大、重大、较大和一般四个级别。地方行业监管部门认为可能发生重大及以上数据安全事件的，应当立即上报工信部数据安全机制；工业和信息化领域数据处理者、数据安全应急支撑机构认为可能发生较大及以上数据安全事件的，应当立即向地方行业监管部门报告。

三部门印发《新材料大数据中心总体建设方案》

10 月 30 日，工业和信息化部、财政部、国家数据局联合印发《新材料大数据中心总体建设方案》，以充分发挥大数据、人工智能对新材料产业的技术支撑作用，培育材料研发与应用的全新发展模式。该文件提出，计划到 2027 年，搭建形成“1+N”（1 个中心主平台、N 个数据资源节点）的新材料大数据中心架构体系。该文件要求，完善数据安全管理技术标准规范，强化对新技术新应用的数据安全风险研究和评估，建立数据安全保障体系，研发安全可靠的关键技术和软件，并实施应用示范。

中国互联网金融协会发布《金融数据安全治理实施指南》等 3 项数据安全标准

10 月 25 日，中国互联网金融协会在京召开金融数据安全治理工作研讨会暨金融数据安全系列标准发布会，正式发布了《金融数据安全治理实施指南》《金融数据安全技术防护规范》《金融数据安全应急响应和处置指引》等 3 项标准，旨在从金融数据治理、金融数据安全技术防护、金融数据安全应急管理等不同角度，为做好新时代的金融数据安全治理工作提供相应指引和规范。

国家数据局《可信数据空间发展行动计划（2024—2028 年）》公开征求意见

10 月 18 日，国家数据局研究起草了《可信数据空间发展行动计划（2024—2028 年）》，现向社会公开征求意见。该文件指出，可信数据空间是基于共识规则，联接多方主体，实现数据资源共享共用的数据流通利用基础设施。该文件在安全保障方面提出加强两方面能力，一是安全防护能力，可信数据空间应针对数据流通的全生命周期，构建必要的防范和检测技术手段，防止数据泄露、窃取、篡改等危险行为发生，并建立相关的管理制度和应急处置措施；二是合规监管能力，可信数据空间应监测空间中违反相关法律法规的行为，并应在行为发生时，及时采取相应的处置措施。

国际

美国 NIST 发布后量子密码迁移路线图公开草案

11 月 12 日，美国国家标准与技术研究院（NIST）发布了《过渡到后量子密码学标准》初始公开草案，包含迁移的路线与时间表。根据草案，NIST 希望到 2035 年将政府机构的加密系统转变为后量子加密，该机构将在 2030 年前弃用 112 位及以下安全强度的加密算法，于 2035 年前禁用这些算法。NIST 指出，向后量子密码学迁移的初期可能会采用混合解决方案，这些方案在建立加密密钥或生成数字签名时结合了抗量子算法和易受量子攻击算法的使用，以确保至少一个算法安全时整体系统的安全性。

美国运输安全管理局发布拟议规则，要求管道和铁路公司必须建立网络风险管理计划

11 月 6 日，美国运输安全管理局发布《加强地面网络风险管理》拟议规则，要求部分铁路、轨道交通和管道等地面运输系统的所有者和运营者执行网络风险管理和事件报告要求。该文件沿袭了运输安全管理局 2021 年以来年度安全指令的基于绩效的网络安全要求，并基于 NIST 网络安全框架、CISA 跨部门网络安全绩效目标等成果，主要提出三方面要求，一是建立健全网络风险管理计划，二是向 CISA 报告网络安全事件，三是指定一名物理安全协调员专门向运输安全管理局报告重大物理安全问题。该文件将在 2025 年 2 月 5 日截止征求意见。

德国司法部发布计算机刑法修正草案，保护白帽黑客行为

11 月 4 日，德国联邦司法部发布计算机刑法修正草案公正征求意见，明确研究 IT 安全漏洞的法律责任。该文件主要提出了两方面修改，一是将发现安全漏洞行为排除犯罪，确

保发现并负责任报告安全漏洞的研究人员，不会有承担刑事责任的风险；二是加大对网络间谍活动的处罚，如刺探和拦截数据符合特别严重案件标准或导致德国关键基础设施、国家安全受到损害，可处以 3 个月到 5 年有期徒刑。德国联邦司法部长 Marco Buschmann 博士表示：“那些致力于弥补 IT 安全漏洞的人，应该得到的是表彰，而不是检察官的诉讼通知。”此前美国、欧洲比利时、马其他等国均有修订法律，对白帽黑客行为可豁免起诉。

美国政府发布《联邦零信任数据安全指南》

10 月 31 日，美国联邦首席数据官委员会、联邦首席信息安全官委员会等联邦政府 IT 领导层联合发布了《联邦零信任数据安全指南》，旨在强化数据安全实践。该文件共 42 页，重点强调了“保护数据本身，而非保护数据的边界”。官方认为这一理念是“有效实施零信任的基础支柱”之一。该文件提出了 5 个步骤的零信任安全路线图，概述了实践者可以采取的具体行动，包括发现、清点、分类、标记和映射数据流，进行风险分析，与零信任架构对齐，设计控制和监控，拥抱自动化和编排。

美国网络安全与基础设施安全局发布首部国际战略规划

10 月 29 日，美国网络安全与基础设施安全局（CISA）发布了《2025–2026 财年 CISA 国际战略规划》，旨在将加强国际伙伴关系作为全球竞争的“力量倍增器”，使美国能够在当前和未来竞争并战胜全球范围内的威胁和挑战，实现该机构为美国民众提供安全和有弹性的基础设施的愿景。该文件列出了 CISA 必须实现的三项目标，以应对美国及其国际伙伴面临的不断变化和动态的挑战。一是增强美国所依赖的外国基础设施的弹性；二是加强国际伙伴关系，促进美国关键基础设施的优先发展和海外利益；三是制定操作和技术全球标准、法规、政策、指南和最佳实践，以提高安全性。

美国财政部发布对外投资审查最终规则

10 月 28 日，美国财政部发布了一项最终规则，以实施拜登于 2023 年 8 月发布的第 14105 号行政命令（Reverse CFIUS 行政令）。根据该行政令的规定，最终规则禁止美国公民参与涉及特定技术和产品的某些交易，还要求美国公民通报涉及特定技术和产品的某些其他交易。涵盖的特定技术和产品分为三类：半导体和微电子、量子计算、人工智能。拜登政府认为这些技术是下一代军事、网络安全、监视和情报应用的核心。美国发布对外投资审查的新计划是对现有出口管制和投资审查工具的补充，试图阻止美国资本推动受关注国家敏感技术和产品的开发。最终规则将中华人民共和国、中国香港特别行政区及中国澳门特别行政区均列为受关注国家和地区。该规则将于 2025 年 1 月 2 日生效。

美澳网络安全监管机构发布软件安全部署指南

10 月 24 日，美国网络安全与基础设施安全局、联邦调查局及澳大利亚信号局旗下网络安全中心联合发布《安全软件部署：软件制造商如何确保对客户的可靠性》，以支持软件制造商实施具备健壮测试和测量组件的软件安全部署流程。该文件概述了软件安全部署的六个关键阶段，包括规划、开发和测试、内部推广、部署和小规模测试、受控推广、将反馈意见纳入规划。该文件强调创建和维护剧本（Playbook），为每个部署阶段提供明确的指导方针、最佳实践和应急计划。

美国政府发布首份关于人工智能的国家安全备忘录

10 月 24 日，美国白宫公开发布首份关于人工智能的国家安全备忘录，旨在确保美国在抓住人工智能机遇和管理人工智能风险方面发挥领军作用，鼓励联邦政府采用人工智能来推进国家安全使命，并寻求塑造围绕人工智能使用的国际规范。除了该备忘录，美国白宫还发布了《国家安全领域推进人工智能治理和风险管理框架》，对此前针对非国家安全任务的指南进行了补充。该框架提供了实施备忘录的进一步细节和指导，包括要求建立风险管理、评估、问责和透明度机制。

美国 CISA 发布数据安全拟议新规，防止外国获取敏感数据

10 月 21 日，根据美国总统拜登 2 月签署的第 14117 号行政命令《关于防止受关注国家获取美国人大量敏感个人数据和美国政府相关数据的行政命令》，美国网络安全与基础设施安全局（CISA）发布拟议实施文件公开征求意见。该文件主要针对参与受限交易领域的企业，特别是那些可能持有、处理大量美国政府和公民敏感数据，提出了多项安全措施。该文件提出了一系列组织级别与数据级别的具体要求，包括维护资产清单、漏洞修补、网络拓扑维护、多因素认证、数据加密与脱敏、限制未授权硬件连接等。

美国司法部发布拟议新规，防止外国获取敏感数据

10 月 21 日，美国司法部公布了《应对美国敏感数据面临的国家安全风险拟议规则》（NPRM），并再次征求公众意见。该项拟议规则以今年 2 月美国总统签署第 14117 号行政命令后司法部同日制定的拟议规则预通知（ANPRM）为基础。NPRM 在分析对 ANPRM 的相关公众反馈后再次对外发布，以解决美国人的敏感数据和政府相关数据，被包括中国在内的“关注国、地区、个人”获取的国家安全威胁。该文件定义了六类美国人敏感数据和两类美国政府敏感数据，将禁止数据经纪公司与关注国进行敏感数据交易、限制与敏感数据相关的投资和合作协议、实施数据交易记录和审查机制。

欧盟委员会通过 NIS2 指令首个实施条例

10 月 17 日，欧盟委员会根据《关于在欧盟实现高度统一网络安全措施的指令》（NIS2 指令），通过了有关关键实体和网络安全的首个实施条例。实施条例将适时在欧盟官方公报公布，并于 20 天后生效。该文件针对 DNS、TLD 域名注册、云服务、数据中心、CDN、托管服务、托管安全服务、在线市场、搜索引擎、社交网络服务、信托服务等提供商，提出了网络安全风险管理措施的技术和方法要求。该文件定义了构成重大事件的具体情形，并要求提供数字基础设施和服务的公司应履行向国家当局报告的义务。

新加坡网络安全局发布《AI 系统安全指南》

10 月 15 日，新加坡网络安全局发布了《AI 系统安全指南》《AI 系统安全配套指南》两份文件，以帮助 AI 系统所有者在全生命周期内保护 AI。这两份文件将有助于保护 AI 系统，免受供应链攻击等传统网络安全风险和对抗性机器学习等新风险的影响。其中，《AI 系统安全配套指南》是一份社区合作编写的参考文件，从工业和学术界精选了实用的措施、安全控制和最佳实践。这两份文件将动态更新，以反映该领域的最新发展。

美国防部发布网络安全成熟度模型认证计划最终规则

10 月 11 日，美国防部发布网络安全成熟度模型认证（CMMC）计划最终规则。该规则将评估级别从原来的 5 个减少至 3 个，并允许企业视情况对其合规性进行自我评估，以简化中小企业合规成本。联邦合同信息（FCI）的基本保护将需要 CMMC1 级的自我评估；受控非机密信息（CUI）的一般保护将需要第三方评估或 CMMC2 级的自我评估；部分需要更高级别保护，以防范 APT 风险的 CUI，需要由国防工业基础网络安全评估中心牵头进行 CMMC3 级评估。

欧盟理事会通过《网络弹性法案》

10 月 10 日，欧盟理事会宣布通过《网络弹性法案》，以保护欧盟的所有数字产品免受网络威胁。《网络弹性法案》是全球首个数字产品安全立法，它对所有硬件和软件设置了不同级别的强制性网络安全要求，制造商需要在产品生命周期内实施对应措施，并附带 CE 标志表明符合法律要求，才可以在欧盟销售。该法案已于 3 月 12 日经欧洲议会批准通过，下一步需欧盟理事会主席和欧洲议会主席签署发布才能成为法律。

事件篇

国内网络安全执法日益增多。大量个人信息数据遭境外访问窃取，上海某医疗科技企业被行政处罚；河南两公司泄露大量敏感数据被罚 10 万元；国家安全部披露，某境外企业“借壳”国内测绘企业非法窃取测绘地理信息被罚。

25 家跨国企业数据泄露，MOVEit 漏洞引发重大安全危机

11 月 11 日 Infostealers 消息，网络犯罪情报厂商 HudsonRock 发布报告称，一名昵称为“Nam3L3ss”的黑客 8 日在地下论坛发布了利用 MOVEit 漏洞（CVE-2023-34362）获取的大量企业员工数据，据称来自麦当劳、汇丰、亚马逊、联想、惠普等多家知名跨国企业，如涉及亚马逊超 286 万条记录、大都会人寿超 58 万条记录、汇丰银行超 28 万条记录等。此次被公开泄漏的被盗数据包括来自 25 家跨国企业的员工详细信息，如姓名、邮箱地址、电话号码、成本中心代码和组织结构等。这次泄密事件再次凸显了 MOVEit 漏洞的深远影响，以及未迅速应用安全补丁所带来的风险。

美国知名军工芯片厂商因勒索攻击损失超 1.5 亿元

11 月 6 日 SecurityWeek 消息，美国知名军工半导体厂商微芯科技（Microchip）5 日发布最新财报披露，因近期网络安全事件，公司已产生 2140 万美元（约合 1.53 亿元人民币）的相关费用。此次事件在 8 月首次曝光，当时微芯科技发现其网络系统中出现了可疑活动，并直接导致公司部分制造设施的生产中断。大约一周后，勒索软件团伙 Play 宣称对此次攻击负责。该团伙公布了一个 4GB 大小的压缩文件，声称其中包含微芯科技的内部数据。这些数据包括个人信息、客户文件及与预算、工资、会计、合同、税务和财务等相关的文件。9 月初，在恢复大部分运营后，微芯科技确认，威胁行为者确实从其系统中窃取了一些信息，其中包括员工的联系方式和密码哈希值。

国际石油巨头哈里伯顿因网络攻击损失超 2.5 亿元

11 月 8 日 Cybersecurity Dive 消息，美国石油巨头哈里伯顿（Halliburton）首席执行官 Jeff Miller 在季度财报电话会议上表示，8 月的网络攻击及墨西哥湾风暴导致收入损失或延迟，致使公司调整后每股收益减少了 2 美分。公司财报显示，此次网络攻击直接带来了约 3500 万美元（约合 2.51 亿元人民币）相关费用。公司表示，此次入侵迫使其推迟账单和收款，对当季现金流造成了影响，但不构成重大影响。这次攻击被怀疑与 RansomHub 威胁组织有关，该组织是今年全球最为活跃的黑客团体之一。

施耐德电气遭数据勒索：开发平台访问凭证暴露 40GB 数据失窃

11 月 4 日 BleepingComputer 消息，能源管理巨头施耐德电气确认，内部一个开发平台遭入侵。此前有威胁行为者声称，利用暴露的凭证从该公司 JIRA 服务器窃取了 40GB 数据，并威胁索要价值 12.5 万美元的赎金。施耐德电气表示：“公司正在调查一起网络安全事件，涉及未经授权访问我们内部的项目执行跟踪平台之一，该平台位于一个隔离的环境中。公司全球事件响应团队已立即动员应对此事件。施耐德电气的产品和服务未受到影响。”

德国大型药品批发商遭勒索攻击，欲扰乱超 6000 家药房供应

11 月 1 日 GovinfoSecurity 消息，德国药品批发商 AEP 在 10 月 28 日遭遇勒索软件攻击，部分 IT 系统被加密，通信系统也受到影响，无法处理订单，导致供应链中断，只能向药店提供有限范围的供货。AEP 负责向全德境内 6000 多家药房供应药品，据悉，目前尚未导致药品短缺。巴伐利亚药剂师协会表示，巴伐利亚州的药品供应不存在风险，药房通常会多家批发商合作。

墨西哥大型机场集团疑遭勒索攻击，旗下 13 个机场紧急切换备用系统

10 月 26 日 The Record 消息，墨西哥中北部机场集团（OMA）25 日披露，一起网络事件迫使其 IT 团队切换至备份系统，以维持墨西哥中部和北部 13 个机场的正常运营。24 日，RansomHub 勒索软件组织宣称对此次攻击负责，并威胁如果不支付赎金，他们将公开 3TB 的被盗数据。具体的赎金金额尚不清楚。此次网络攻击影响超 10 天，OMA 15 日在社交平台上首次承认了此次事件，表示旗下各机场的大屏已经关闭，目前仍只能通过备用系统和人工服务维持运营。

通过外网非法获取公民个人信息 1 亿余条，一安全公司员工获刑

10 月 28 日澎湃新闻消息，上海市杨浦区人民检察院召开新闻发布会，通报 2020 年以来侵犯公民个人信息隐私案件办理情况，并发布相关案例。其中一起通报案例显示，被告人吴某是某安全科技有限公司员工。2024 年 2 月，被告人吴某通过翻墙软件违规访问境外 Telegram 平台，并在该软件“ling 某”群的“资源共享”内下载含有公民个人信息的文件，储存在其持有的移动硬盘中，同时将上述下载渠道提供给他人。经鉴定，被告人吴某非法获取的公民个人信息共计 1 亿余条。经杨浦区检察院提起公诉，法院以侵犯公民个人信息罪判处吴某有期徒刑一年六个月，缓刑一年六个月，并处罚金 2000 元人民币。

近年最大规模！超 1 亿美国人医疗隐私数据被盗

10 月 24 日 BleepingComputer 消息，美国联合健康集团首次确认，由于旗下子公司 Change Healthcare 遭遇勒索软件攻击，超过 1 亿人的个人信息和医疗数据被盗。此次事件已成为近年来最大规模的医疗数据泄露事件。美国卫生与公共服务部民权办公室 24 日在其数据泄露门户网站上更新了受影响人数的统计，总人数为 1 亿人。这是联合健康集团首次为此次数据泄露事件提供官方数字。在民权办公室网站更新的常见问题解答中写道：“2024 年 10 月 22 日，Change Healthcare 向民权办公室报告，已向约 1 亿人发出了个人通知，告知他们此次数据泄露事件。”据悉，被窃取的数据包括健康保险信息、医疗诊断信息、账单索赔与支付信息、其他个人信息等。

河南两公司泄露大量敏感数据被罚 10 万元

10 月 23 日网信郑州消息，郑州市网信办工作中发现，该市两家公司未履行网络安全保护义务，未采取必要的安全防护，导致大量敏感数据被窃取。经调查核实，公司一在数据库中配置增加了远程登录空口令账户，导致黑客利用该空口令账户成功登录数据库，并窃取了数据库中的数据，被窃取的数据包括姓名、身份证号、手机号、邮箱地址等敏感信息。公司二缺乏网络安全意识，没有正确配置数据库，导致数据库存在未授权访问漏洞，攻击者通过漏洞登录数据库，查看、下载数据，导致敏感数据泄露。郑州市网信办依据《数据安全法》分别对两家公司作出责令改正，并给予警告，处以人民币 5 万元罚款的行政处罚。

国家网络安全通报中心：多个与某大国政府有关的境外黑客组织持续攻击国内单位企业

10 月 21 日国家网络安全通报中心消息，中国国家网络与信息安全信息通报中心发现一批境外恶意网址和恶意 IP，有多个具有某大国政府背景的境外黑客组织，利用这些网址和 IP 持续对中国和其他国家发起网络攻击。这些恶意网址和

IP 都与特定木马程序或木马程序控制端密切关联，网络攻击类型包括建立僵尸网络、网络钓鱼、勒索病毒等，以达到窃取商业秘密和知识产权、侵犯公民个人信息等目的，对中国国内联网单位和互联网用户构成重大威胁，部分活动已涉嫌刑事犯罪。相关恶意网址和恶意 IP 归属地主要涉及：美国、波兰、荷兰、保加利亚、土耳其、日本等。

卡西欧遭遇灾难式勒索攻击：系统瘫痪、交付延迟、财报推迟

10 月 21 日 The Record 消息，日本知名手表制造商卡西欧计算机株式会社宣布，由于 10 月 5 日发生的勒索软件攻击影响了公司的会计流程，原定于 11 月 6 日发布的第二季度财报将推迟至 11 月中旬。该公司官网声明称，此次攻击导致“交货日期严重推迟，并积压了大量维修请求。公司目前正全力应对这一情况，计划在 11 月底之前恢复系统的正常运行”。“Underground”勒索软件团伙声称对这次攻击负责。该组织称他们窃取了公司 204.9 GB 的数据，并发布了部分被盗数据作为证据。

上市公司科沃斯旗下扫地机器人被黑并发出骚扰声：用户受惊 官方回应

10 月 13 日 The Verge 消息，澳媒 ABC 新闻日前报道称，今年 5 月，黑客获取了科沃斯地宝 X2 Omni 扫地机器人在多个美国城市的控制权，利用这些机器人追赶宠物并向主人大喊种族歧视性言论，明尼苏达州、埃尔帕索、洛杉矶等多地均有用户反馈。科沃斯公司随后对此声明称，经调查，他们确认了一次“凭证填充攻击”事件，并已屏蔽了相关的 IP 地址。公司强调，目前“没有证据显示”攻击者获得了用户的用户名和密码。

国家安全部：某境外企业“借壳”国内测绘企业非法窃取测绘地理信息

10 月 16 日国家安全部公众号消息，国家安全部公众号发文称，国家安全机关工作发现，某境外企业 A 公司通过与我国具有测绘资质的 B 公司合作，以开展汽车智能驾驶研究为掩护，在我国内非法开展地理信息测绘活动。为尽可能直接获取原始测绘数据，A 公司越过项目转包的层层节点，全程主导测绘项目进展，直接指挥 B 公司人员在我国内多省份开展测绘，更是专门委派外籍技术专家对 B 公司的测绘人员开展实操指导，重点把控测绘数据的存储、处理和流转等环节。最后在 A 公司的操控指使下，B 公司将测绘所得数据转移出境。经鉴定，A 公司采集的数据多项属于国家秘密。在此事件中，B 公司开展测绘活动时忽视了测绘行业相关规定要求，任由境外企业把控数据流向，导致原始测绘数据失控外传。针对以上情况，国家安全机关会同有关部门开展了联合执法活动。涉事企业和有关责任人受到了法律追究。

大量个人信息数据遭境外访问窃取，上海某医疗科技企业被行政处罚

10 月 14 日网信上海公众号消息，上海市网信办接到线索，反映属地某医疗科技公司所属系统存在网络安全漏洞，致使系统大量个人信息数据发生泄漏被境外 IP 访问窃取。通过调查核实，涉事系统为该企业内部生产测试系统，部署于云服务平台，系统数据库内存储大量个人信息数据，包含姓名、单位名称、所属省市、所在乡镇 / 街道、手机号（已采取加密措施）等。该系统未采取有效网络安全防护措施，存在未授权访问漏洞，网络和数据安全管理制度不完善，网络日志留存不足 6 个月，造成数据泄漏被窃取，违反了《数据安全法》第二十七条规定。针对以上违法情况，上海市网信办依据《数据安全法》第四十五条规定对该医疗科技公司给予警告，并处以罚款的行政处罚。

伊朗政府部门和核设施遭受大规模网络攻击

10 月 12 日 Security Affairs 消息，伊朗遭受大规模网络攻击，导致伊朗政府服务中断、重要信息被窃取，尤其是核设施也受到了影响。伊朗最高网络安全委员会前秘书菲鲁扎巴迪表示，此次网络攻击影响了伊朗政府内部的关键部门，包括司法、立法和行政部门，大量重要信息也因此被窃取；伊朗的核设施及燃料分配、市政服务、交通和港口的关键网络也成为攻击目标。此次网络攻击被视为以色列对伊朗本月早些时候导弹袭击的可能报复，加剧了两国间持续的紧张局势，可能引爆更大范围的冲突。

漏洞篇

Web 控制面板开源项目 CyberPanel 曝出高危漏洞，可未授权远程执行任意命令。该漏洞技术细节和 EXP 均公开且可复现，测绘数据显示国内上万资产受影响，建议客户尽快做好自查及防护。

CyberPanel 远程命令执行漏洞安全风险通告

10月28日，奇安信CERT监测到官方修复CyberPanel upgrademysqlstatus 远程命令执行漏洞（QVD-2024-44346），该漏洞源于 upgrademysqlstatus 接口未做身份验证和参数过滤，未授权的攻击者可以通过此接口执行任意命令获取服务器权限，从而造成数据泄露、服务器被接管等严重的后果。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为12,289个，关联IP总数为4316个。目前该漏洞技术细节与 EXP 已在互联网上公开，奇安信威胁情报中心安全研究员已成功复现，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Fortinet FortiManager 身份认证绕过漏洞在野利用通告

10 月 24 日，奇安信 CERT 监测到官方修复 Fortinet FortiManager 身份认证绕过漏洞（CVE-2024-47575），未经身份验证的远程攻击者可以使用有效的 FortiGate 证书在 FortiManager 中注册未经授权的设备。成功利用漏洞后攻击者将能够查看和修改文件（如配置文件）以获取敏感信息，并能够管理其他设备执行任意代码或命令。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为 39,073 个，关联 IP 总数为 39,674 个。鉴于此漏洞已发现在野利用，建议客户尽快做好自查及防护。

Spring Framework 路径遍历漏洞安全风险通告

10 月 18 日，奇安信 CERT 监测到官方修复 Spring Framework 路径遍历漏洞（CVE-2024-38819），在 Spring Framework 受影响版本中，当应用程序使用 WebMvc.fn 或 WebFlux.fn 提供静态资源时，容易受到路径遍历攻击。攻击者可以编写恶意 HTTP 请求并获取目标系统上任何由 Spring 应用程序正在运行的进程访问的文件，从而导致信息泄露。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Apache Solr 身份认证绕过漏洞安全风险通告

10 月 16 日，奇安信 CERT 监测到官方修复 Apache Solr 身份认证绕过漏洞（CVE-2024-45216），该漏洞存在于 Apache Solr 的 PKIAuthenticationPlugin 中，该插件在启用 Solr 身份验证时默认启用。攻击者可以利用在任何 Solr API URL 路径末尾添加假结尾的方式，绕过身份验证访问任意路由，从而获取敏感数据或进行其他恶意操作。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

注：使用公司邮箱发送企业名称和需开通订阅的邮箱地址至 cert@qianxin.com，即可申请订阅最新漏洞通告。

对抗篇

国内攻防演习 8–10 月态势：哪些薄弱点最易被利用？

作者 | 奇安信安服团队

一、本期演习整体情况

2024 年 8 月至 10 月，奇安信 Z-TEAM 团队共承接攻防演习服务 46 场，国家级攻防演习 1 场，行业级攻防演习 2 场，省级攻防演习 5 场，省级行业攻防演习 2 场，地市级攻防演习 7 场。客户自主攻防演习 29 场。

10 月承接攻防演习数量较前两月的月均场次略有下降（见图 1）。

本月承接的攻防演习涉及金融、企业、政府行业较多，此情况较之前两月承接攻防演习涉及行业范围数据变化不大，但金融行业攻防演习数量明显增多，政府行业攻防演习数量明显减少（见图 2）。

8 月 –10 月攻防演习成果如表 1 所示：

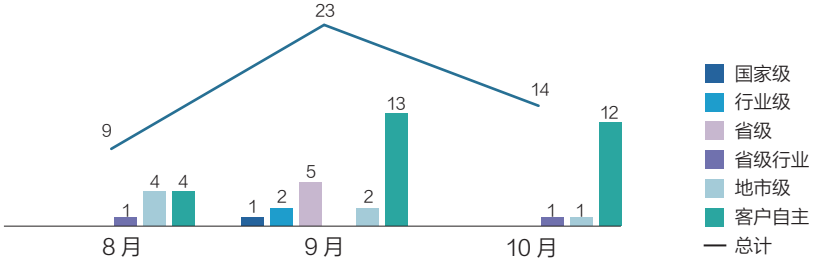


图 1 8–10 月 Z-TEAM 承接攻防演习数量统计

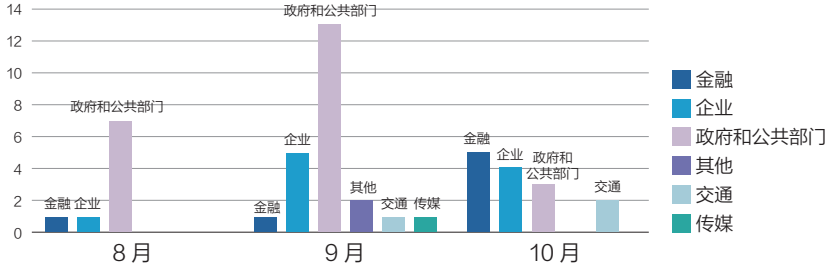


图 2 8–10 月攻防演习涉及行业统计

目标系统	靶标	强隔离内网	核心业务网	网站	堡垒机	安全设备	业务系统	服务器
数量	147	180	237	412	458	627	5032	32,780

表 1

二、任务目标特点

8 月 –10 月攻防演习和评估任务覆盖行业比较广泛，涉及目标包括金融、企业、央企、电力、交通、政府、教育、传媒、运营商等行业。随着互联网的快速发展和普及，网络信息安全问题日益引起人们的关注，教育行业作为社会结构的重要领域，与网络信息安全之间存在着紧密的联系和相互作用。网络信息安全问题给教育行业带来了诸多挑战，同时教育行业需要积极应对网络信息安全问题，履行保护学校和社会成员信息安全的责任。8 月 –10 月的攻防演习中教育行业占比为 4%（见图 3）。

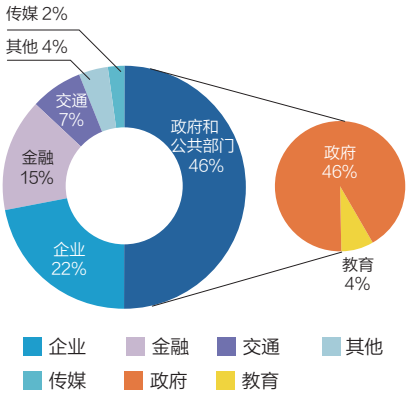


图 3 8–10 月攻防演习分布

三、主要攻击手段分析

基于 8 月 –10 月的奇安信 Z–TEAM 团队实战成果，对多个行业的网络目标进行了攻击分析，对不同的行业目标使用不同攻击手段，如政府部委、运营商、教育行业外网突破的主要手段包括 VPN 仿冒接入和漏洞扫描利用等；交通、企业、其他行业主要是口令爆破和供应链攻击等；传媒、电力行业主要是漏洞扫描利用和口令爆破等；金融和央企行业外网突破的主要手段包括漏洞利用、钓鱼攻击和隐秘隧道外联等。因此，我们建议各个行业加强外网安全管理，定期检测和修复漏洞，加强口令策略，增强员工安全意识，以防止攻击者利用外网攻击内网。各个行业使用的主要技术手段分布如下（见图 4）。

8 月 –10 月攻防演习服务中，攻击队使用的攻击手段主要有：漏洞扫描利用、钓鱼攻击、口令爆破、隐秘隧道外联、VPN 仿冒接入、供应链攻击技术等。

整体攻击手段与 5 月对比，漏洞扫描利用手段利用率基本趋同，口令爆破和隐秘隧道外联手段有明显下降趋势，钓鱼攻击和 VPN 仿冒接入、供应链攻击有明显上升趋势。

在教育行业的攻防演习任务结束后，通过分析演习数据，我们发现收集开源情报，包括学校的域名、IP 地址范围、联系方式、产品代码等关键信息，对于后续攻击行动具有重要价值。这些情报能够为攻击行动提供必要支持，使攻击队可以利用弱密码、历史漏洞等攻击手段，针对系统的薄弱点完成突破。一旦找到突破点，攻击者便能在内网中横向移动，扩大影响范围。在攻防演练中，攻击手段的运用通常是相互交织和协同的。一个渗透扩展步骤的成功，往往依赖两种或多种攻击手段的共同配合。

四、典型攻击手段实现案例

随着互联网及信息技术的迅猛发展，教育领域正逐步向数字化转型迈进。在现代教育体系中，互联网为学生、教师和学校管理人员提供了诸多便利，然而，它也伴随着很多潜在的安全风险。这些风险源于大量敏感数据的存储与处理，涵盖了学生及教职工的个人信息，以及各类教育资源和财务数据等。因此，网络安全在教育领域中显得尤为关键。

案例：借助敏感信息泄露，成功渗透某校园核心业务网络

在对某高校进行的攻防演练过程中，攻击队基于多年实战经验总结与分析，认识到只有深入理解目标的业务流程，才能明确下一步的攻击策略设计。那如何实现攻击队在外网的突破与内网的横向移动，形成连贯的攻击流程，从而彻底摧毁目标单位的纵深防御体系，并造成更严重的破坏呢？攻击队制定了如下的技战术策略。

获取外部突破口主要有两种途径：一种方法是通过多种手段搜集目标网络的敏感信息，包括登录口令、安全认证及网络安全配置等；另一种方法则是漏洞利用，通过攻击目标网络的外部接口，如 Web 网站、邮件系统、防火墙网关及外部应用的后台命令执行，来实现对目标网络的突破。

攻击队首先通过各种渠道收集与校园网络相关的信息，包括学校的域

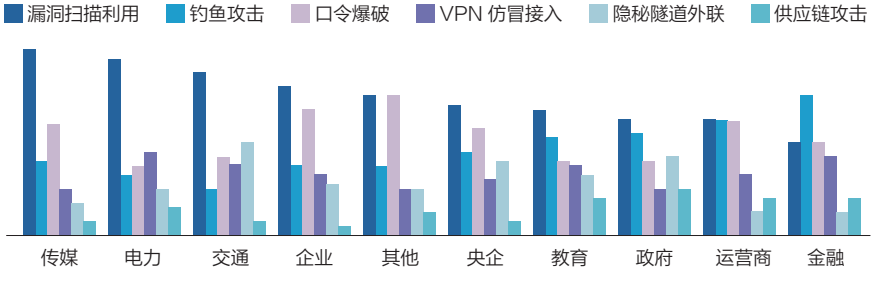


图 4 行业攻击手段分布

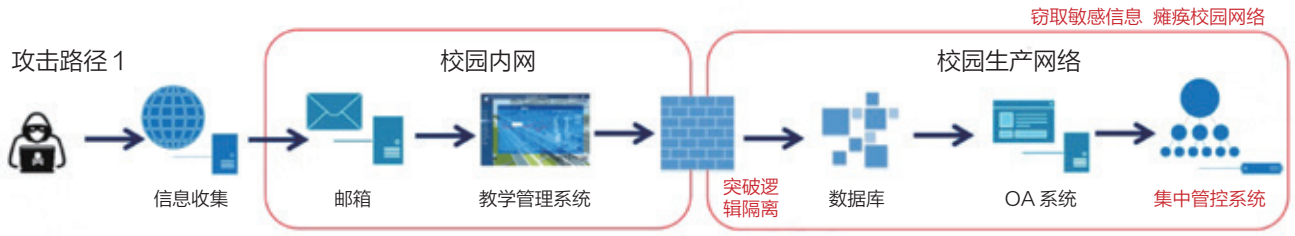


图 6 案例攻击路线图

名、IP 地址范围、使用的软件和服务等。使用网络扫描工具、搜索引擎等手段进行全面的、细致的信息收集与分析。通过搜索引擎查找学校网站上公开的信息，了解学校的业务范围及可能存在的敏感信息。攻击队通过敏感信息泄露成功获取了一位教职工的邮箱账号和密码，利用获取的邮箱账号和密码登录邮箱，审阅邮件内容后，发现了一些与学校业务紧密相关的关键信息和链接。在获得初步访问权限之后，攻击队尝试提升自己的权限，以期获取更多的敏感信息和对系统的更高控制权。攻击队发现学校教学管理系统中存在一个权限提升漏洞，通过精心构造的请求，成功将自身的权限从普通用户提升为管理员权限。此外，通过“敏感信息泄露漏洞”，攻击队突破了目标网络外围防线，悄无声息地潜入目标内网系统。

在进入目标内网后，通过教学管理系统进行内网扫描，从而定位到某高校培训系统。利用弱密码及未授权漏洞，获取了 8 台数据库权限。接着，攻击队利用 MySQL 的弱密码漏洞进行提权，漏洞获取了内网 OA 系统服务器权限，通过弱密码登录数据库，检索数据库用户表，进而登录了成绩查询系统。此外，攻击队还通过未授权访问漏洞，获取了多台业务系统的源代码。通过未授权访问查阅配置文件，找到了账号和密码，使攻击队能够登录 GitLab 平台，发现平台上管理着多套业务系统的源代码。

“擒贼擒王”，在成功打通目标网络的访问通道后，选择“最直接”“最有效”的攻击策略，针对目标网络中的域控服务器、vCenter 和堡垒机等集中管控系统、终端管理系统开展攻击渗透，以达到目标核心业务系统的快速、高效和全面控制。

五、安全加固建议

1. 案例剖析

教育行业特别是高等教育体系在过去二十年经历了大规模扩大招生并建设与之配套的基础设施的阶段，在 IT 基础设施建设过程中，校园网的安全建设工作也在同步进行，重点在于学校外网侧，如官网、报名系统的安全建设，在内部对众多教师及学生的个人信息也做了针对性的防护。

然而，因学校人员的流动性较大，技控之外的安全培训及安全管理等手段无法有效覆盖全员，存在因人员安全意识不强泄露个人信息导致被攻击人员利用的风险。另外，作为校园管理的安全管理部门，往往对外网系统更加关注，对校园网内部的管理往往强度较低，一旦集权设备被侵入，可能造成的横向攻击范围极大，会造成内网瘫痪或者数据窃取等安全事件的发生。

案例暴露问题：账号 / 密码等重要信息泄露，数据库安全防护薄弱，多套系统源代码集中存放且鉴权机制差。

2. 防护策略

（1）在教师及学生个人账号信息无法全面防止泄露的前提下，建议邮件 /OA 系统增加二次认证机制，增加攻击者社工攻击的难度；

（2）针对存放重要学生、教师相关数据的数据库，避免部署与普通办公网及宿舍网等处于同一安全域，并进行强化鉴权管理，对管理账号重点监控、定期行为审计；

（3）学校自建及第三方开发系统的源代码严令禁止上传至外网，如 GitHub，并采购敏感信息泄露服务定期在互联网侧发现可能泄露的信息；源代码不建议在内网集中存放，如 GitLab 平台可部署多套，将源代码分布存储，并避免多 GitLab 平台使用相同账号密码；

（4）加强对集权设备如域控、堡垒机等设备的异常访问行为管理（异常时间段、非常规 IP 等），并重点关注集权设备高危漏洞、0day 漏洞等信息发布，做到及时升级；

（5）学生入学、教师入职等节点加强安全意识教育，并将安全事件责任人惩罚措施写入学生手册或教师年度测评中，以表警示。

校园网因受众面广、流动性大等因素，安全防护无法做到面面俱到，工作重点应遵循抓大放小的原则，重点在防护重要信息泄露、防止外围系统被撞库、集权设备防护上，通过以上技术手段保障校园网不发生严重的数据安全事件，避免造成更大的舆情损失。安

特朗普 2.0
网络安全迎来哪些巨变？

从强化关基设施防护，采用比“前置防御”更加大胆的战略，到放松对人工智能的监管，特朗普 2.0 时代的网络安全政策将会非常值得关注。

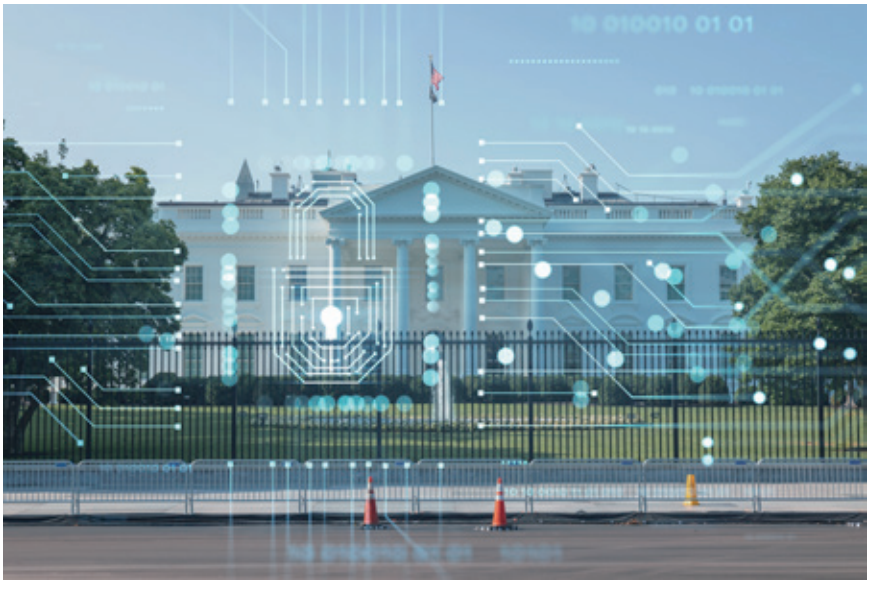
特朗普第二任期网安政策迎来五大变化

特朗普和拜登的执政理念大相径庭，重返白宫的特朗普在网络安全政策方面会有哪些变化？是否会接受拜登的“网络安全遗产”？这是全球网络安全行业当下最为关心的话题之一。

网络安全是少数几个得到美国共和与民主两党支持的领域。穆迪评级承认美国两党的网络政策在很多方面是相同的，但同时也认为，关键的政策差异可能会导致发生重大变化。

安全专家预测，特朗普可能会对现有的网络安全政策进行调整，以突出其一贯的“灵活响应、减少监管”策略。

- 保留和强化对关键基础设施和联邦网络防护措施，但减少对私营企业的过多监管。
- 继续加大防御投入，推进网络现代化进程，部署“所有工具”保护关基安全。
- 放松监管：减少“安全设计”相关强制措施、放松人工智能监管，让企业有更多的自主权，释放创新活力。
- 重新聚焦短期网络威胁，减少对后量子密码学等前沿技术的长远部署，转而专注于目前的实际网络威胁。
- 减少国际合作力度，采取更为独立的国家安全策略。



特朗普再次当选后，可能会重新审视拜登政府在网络安全领域的政策和行政命令，鉴于二位在网络安全、经济、国际关系等关键政策上的理念差异，有理由推测特朗普可能会对拜登的网络安全行政令做出调整或重新定义。

1、总体政策方向：全面防护 vs. 重点防御

拜登政府的网络安全政策以广泛覆盖为主，致力于巩固美国的网络安全基础，涉及零信任架构、供应链安全、后量子密码学、人工智能和身份管理等多个领域。

2021 年拜登发布的网络安全行政令（EO 14028）推动部署多种安全措施，尤其是在联邦政府和关键基础设施中的防护措施。

相比之下，特朗普在其首个任期内（EO 13800）则更注重保护联邦网络和关键基础设施的网络安全，但整体策略更加聚焦于具体威胁，特别是防范国家级对手的网络攻击。政策上侧重于快速行动和减少监管，以提高政府机构和企业的灵活性和应变能力。

安全人士分析，如果特朗普在新任期内选择对拜登的网络安全行政令进行调整，他可能会减少对全面网络安全政策的关注，将更多资源集中于特定的国家安全威胁，并简化部分监管，以鼓励私营部门的快速响应。

特朗普时期设立的网络安全和基础设施安全局（CISA）在拜登政府时期不断发展壮大， 持续加强政府和关键基础设施的网络防护措施。在拜登政府的推动下，CISA 的预算从 2021 财年的约 20 亿美元扩大到 2025 年的 30 亿美元。2021 年，CISA 成立了联合网络防御协作组织，旨在改善网络安全公司、联邦政府和关键基础设施提供商共享信息的方式。

曾在特朗普上届政府的国土安全部任职的布莱恩 · 哈雷尔 (Brian Harrell) 表示，特朗普政府可能会为 CISA 提供资金，以开发更强大的威胁检测和响应威胁的能力，以及与各州和地方政府在网络安全方面进行更好的协调。

特朗普政府可能会为 CISA 提供资金，
以开发更强大的威胁检测和响应威胁的能力，
以及与各州和地方政府在网络安全方面
进行更好的协调。

2、加大防御投入，推进网络现代化

尽管有业内人士预计，由埃隆 · 马斯克牵头、旨在削减 2 万亿美元联邦预算的计划可能会削弱美国的网络安全工作，但众多安全人士认为，为网络安全提供足够资金支持仍是特朗普政府的优先事项。布莱恩 · 哈雷尔表示，特朗普上任后不太可能立即开始削减网络和国家安全预算。一位业内高管甚至预测，特朗普政府将选择在网络领域投入更多资金。美国商会在选举前预测，无论哪位候选人获胜，将继续实施当前的网络安全政策。

实际上，网络安全是少数得到美国共和与民主两党共同支持的领域。国家网络安全联盟执行董事丽莎 · 普拉格米尔（Lisa Plaggemier）强调，网络安全是“特朗普政府和现任政府之间的两党议题，”“将网络安全建设作为优先事项的策略依然坚定、超越党派界限。”

一位接近过渡团队的人士表示，预计新一届特朗普政府将继续实施 2020 年未执行的网络政策。这意味着，要了解未来特朗普政府的网络安全政策，可以回顾一下他的首个任期。

2017 年，特朗普颁布行政令，强调 “关键基础设施保护”，呼吁联邦政府 IT 现代化”。次年，特朗普政府公布了该国 15 年来首个国家网络安全战略，放宽允许情报机构通过网络攻击“反击”对手的规则。同年，特朗普签署了《网络安全和基础设施安全局法案》，成立了同名机构，负责领导保护关键基础设施免受网络攻击的工作。

在网络威胁日益严重的时代，网络安全不仅是优先事项，而且势在必行。从交通运输到电网等关键基础设施暴露的漏洞越来越多，遭受的网络攻击也日益增多，网络威胁达到了前所未有的高度。网络安全基础设施需要进行前所未有的投资，也意味着未来的特朗普政府在网络防御将会强化其积极应对的策略。

在其首个任期，特朗普加快了信息保护法规的制定。其核心是网络安全成熟度模型认证（CMMC）计划规则。这项始于特朗普首个任期的标准，在拜登的任期内得以延续，并即将发布最终的计划规则。

共和党全国委员会 2024 年 7 月发布的《政策路线图》，将保护关键基础设施免受黑客攻击列为 “国家优先事项”，这是整个文件中唯一提到网络相关的内容。《政策路线图》承诺，将“提高关键系统和网络的安全标准”“动

用一切国家力量工具”来保护美国关键基础设施和国家工业基础“免受恶意网络攻击”。

特朗普政府承诺部署“所有工具”来保护重要资产，这表明其将继续致力于加强国家防御，优先防止国家级对手窃取政府、联邦承包商及其供应链所掌握的关键信息。这一做法可能意味着特朗普政府将加大对尖端网络防御的投资，同时与私营科技公司加强合作，打造坚固弹性的系统，以抵御未来的网络威胁，尤其是来自敌对国家的威胁。

“我们将以国家安全为重点，重点保护关键基础设施、政府网络和关键行业免受网络威胁。”在特朗普第一任期内担任网络安全和基础设施安全局基础设施安全助理主任的布莱恩·哈雷尔说。

3、放松监管，实现全面逆转

美国律师事务所 Hunton Andrews Kurth 的合伙人丽莎·索托 (Lisa Sotto) 认为，放松监管将成为特朗普政府的首要主题。哈雷尔也认为：“特朗普 2.0 时代的网络安全政策可能会侧重于消除多余的监管，增加安全能力，减轻来自中国、人工智能和量子计算的威胁。”

近四年来，拜登政府一直试图让美国科技公司和基础设施运营商对国家的网络安全态势承担更多责任，并限制间谍软件的传播，对人工智能设置护栏，并打击网上虚假信息。但当特朗普上任后，几乎肯定会取消或大幅缩减这些限制，转而支持有利于商业的网络战略，并强调对敌对国家的网络军队发动积极攻势。

因此，预计未来的特朗普政府可能会放弃拜登雄心勃勃的计划，即对目前缺乏安全保障的美国基础设施实施网络监管。这一努力在铁路、输油管道和航空领域取得了成果，但在水利和医疗卫生等领域却遭遇挫折。

尽管针对重要系统的网络攻击日益增多，共和党的政纲承诺“提高关键系统和网络的安全标准”，特朗普政府不太可能支持对基础设施运营商实施新的监管要求。

美国战略与国际研究中心高级副总裁兼战略技术项目主任詹姆斯·刘易斯认为，“（将来）未经国会明确授权，将不再进行监管”。哈雷尔则表示，拜登任期内充斥着新的网络监管，有时会让行业感到困惑和负担过重。“未来白宫将寻求简化合规流程，降低监管负担。”

但一位美国网络官员表示，这种做法可能不会持久。“最终特朗普政府会认识到，网络监管对于确保关键基础设施的安全是必要的。”民主防御基金会网络与技术创新中心高级主任马克·蒙哥马利（Mark Montgomery）则预测，为保护脆弱的行业，特朗普政府将在安

特朗普政府承诺部署“所有工具”来保护重要资产，这表明其将继续致力于加强国家防御，优先防止国家级对手窃取政府、联邦承包商及其供应链所掌握的关键信息。

全防护措施中强调合作和激励手段。

削减“安全设计”合规监管。拜登的网络安全政策强调，软件和设备制造商在产品安全性上承担更大责任，强调“安全设计”（Secure by Design）原则，即在产品设计阶段即嵌入安全防护，防范潜在的供应链漏洞。为此，拜登政府在联邦政府层面推进了多项强制性网络安全标准； CISA 则在过去几年发起一场宣传活动，鼓励企业“从设计上保证产品安全”，希望在企业中形成自上而下的安全责任文化，要求企业在防护设计、数据管理和威胁检测方面承担更多的合规责任。

民主党政府利用“安全设计”推动新的监管，但未来特朗普执政期间，安全设计最多可能是一个口号。”预计，特朗普可能会削减此类合规监管，不过多地推行“安全设计”原则，给予企业更多的自由，鼓励企业自行采取安全防护措施，以灵活、快速地应对安全威胁，而不是通过强制性标准实施。然而，鉴于供应链安全问题在过去几年屡次引发重大事件（如太阳风安全事件），特朗普或会在某些高风险领域保留拜登的供应链安全策略。

废除人工智能行政令。特朗普的竞选团队已经暗示，计划审查并可能废除拜登政府实施的有关人工智能发展指南的行政令。特朗普团队认为，放松监管限制可以释放创新活力——这对于在与中国日益激烈的人工智能竞赛中竞争至关重要。拜登任期内成立的人工智能安全研究所旨在平衡创新与严格的监管保障。特朗普的政策将强调人工智能的快速发展，同时探索在监管阻碍进展的领域放松管制。特朗普团队表示，加强国家的人工智能基础设施和营造有利于创新的环境对于国家安全和经济主导地位至关重要。

蒙哥马利也认为，
特朗普可能对国家网络防御“采取更积极的方式”，
包括让国民警卫队在保护国内基础设施方面
“发挥更重要的作用“。

4、比“前置防御”更加大胆的战略

特朗普从拜登政府手中接过接力棒的一个领域是政府使用军事手段对黑客攻击，以及对外国对手的网络行动作出反应。

在拜登的领导下，美国军方网络司令部扩大了与盟友在海外追捕黑客的行动。但共和党敦促拜登对国家级的黑客攻击活动做出更强硬的回应，特朗普很可能会采取这种做法——尤其是在他选择众议员迈克 · 沃尔兹（Mike Waltz）担任国家安全顾问之后，沃尔兹主张对攻击组织实施网络攻击。

蒙哥马利也认为，特朗普可能对国家网络防御“采取更积极的方式”，包括让国民警卫队在保护国内基础设施方面“发挥更重要的作用”。

蒙哥马利还预计，美军网络司令部将开展更频繁、更强有力的进攻行动。在其第一任期内，特朗普将网络司令部提升为完整的作战司令部。他预测，特朗普政府将“更赞成”成立单独的军事网络部门。

2024 年 9 月，奥本大学麦克拉里网络与关键基础设施研究所和网络空间日光浴室委员会 2.0 的 40 名网络安全专家发布了 39 项建议，为下一届政府提供了网络安全政策建议路线图。

专项工作组认为，现在是采取大胆、果断行动的时候。特别工作组特别强调，需要“超越纯粹的防御态势，让那些在网络空间对美国造成伤害的组织承担真正的代价”。 对此，Gartner 高级副总裁分析师卡黛儿 · 蒂勒曼表示，这一立场比国防部 2018 年为网络安全推出的“前置防御”战略更加大胆。

网络安全政策建议路线图建议新政府使用“所有国家力量——外交、经济，必要时还有军事”来应对网络攻击。地缘政治和技术顾问凯文 · 艾利森 (Kevin Allison) 表示：“特朗普政府在决定如何在网络空间反击对手时，将考虑全套

随着对监管的关注度逐渐降低，
特朗普的第二任期可能会继续打击网络攻击活动，
并采取更积极的方式来解决勒索软件问题，
包括更多地使用攻击反击手段。

政策手段。

5、减少国际合作，推行更独立的防御策略

拜登政府的网络安全政策更强调国际合作，与盟国在网络威胁和网络政策方面紧密协作。为此，拜登政府加强了与欧洲、亚太等地区的网络安全伙伴关系，以共同应对各种国家级网络攻击。

鉴于特朗普在外交政策上倾向于“美国优先”，未来的政府可能会减少在网络安全上的国际协作，更专注于独立的国家防御战略。特朗普倾向于通过对外施压来达成网络安全目标，而非通过跨国协作来推动整体安全框架的建立。然而，由于全球网络安全形势复杂，特朗普可能会在特定领域保持有限的国际协作。

此外，拜登政府提出加速向后量子密码学的迁移，旨在为可能出现的量子计算威胁做准备。拜登的网络安全行政令鼓励联邦政府和私营部门协作，提前应对量子技术对传统加密技术的潜在威胁。

特朗普政府在量子计算领域支持技术创新，但可能不会如拜登政府般密集推行后量子密码学的标准。特朗普的网络安全政策或许会更多地聚焦于短期威胁，可能放缓后量子密码学的推广步伐。

6、总结

随着对监管的关注度逐渐降低，特朗普的第二任期可能会继续打击网络攻击活动，并采取更积极的方式来解决勒索软件问题。 众包安全平台 Bugcrowd 创始人凯西 · 埃利斯 (Casey Ellis) 预计，美国的网络攻击能力将会增强，包括更多地使用攻击反击手段。

- 特朗普和拜登在总统任期颁布过的网络安全总统行政令，虽然在具体政策细节上有所不同，但都聚焦于提升联邦网络和关键基础设施的安全性。拜登的网络安全策略侧重于全面的系统防护，注重“安全设计”和供应链安全，而特朗普则更加偏向简化监管，灵活应对实际威胁。特朗普新政府可能会保留部分拜登的网络安全政策基石，同时进行调整以使政策更具灵活性，并减少对企业的监管，以符合其一贯的“减少政府干预”理念。
- 特朗普可能对拜登的网络安全监管政策进行部分削弱，但在面对国家级威胁和关键基础设施保护方面，特朗普或将延续强化防护措施，以维护美国的网络安全根基。此外，特朗普也会使用“所有国家力量——外交、经济，必要时还有军事，来应对网络攻击”。

巩固网络安全遗产：拜登的最后一项网安行政令

特朗普胜选后，业界普遍预测“跛脚鸭总统”拜登很可能在 2024 年年底前颁布第二项网络安全总统行政令，以在卸任前完成更多网络安全政策的布局。

据消息人士透露，这项总统令预计将在国会“跛鸭期”内发布，重点关注联邦网络标准和新兴技术威胁，覆盖从“安全设计”倡议到供应链责任、IT 和运营技术安全、互联网路由、密码管理、身份管理、人工智能，以及网络安全人才培养等一系列主题。

奥巴马时代国家安全委员会网络安全协调员、现任非营利性网络威胁联盟负责人的迈克尔·丹尼尔 (Michael Daniel) 表示，特朗普重新入主白宫，拜登政府公布行政措施是合乎逻辑的。

新的总统行政令重点包括如下内容。

1、通过行政令巩固网络安全政策

消息人士表示，拟议中的行政令将解决拜登政府 2021 年网络安全行政令未曾涉及或未完全涉及的领域。一位消息人士将这项新命令描述为一项“彻底的”法令，将解决美国网络安全政策领域中未完成的工作。

其中，推进向后量子密码的迁移，预计也将成为即将出台行政令的一个主要内容。这一标准旨在应对未来量子计算机可能突破传统加密的威胁，确保政府和企业网络环境的安全性。

即使在拜登任期的最后数月，白宫也在努力完成大量网络安全和技术政策议程。2024 年 10 月下旬，白宫与财政部发布了一项最终规则，禁止在人工智能、半导体和量子计算等先进技术领域开展对外投资，以保护美国的国家安全态势。

2024 年 10 月底，拜登政府宣布禁止在 AI、半导体、量子计算等高科技领域进行对外投资，以防关键技术

外流，削弱美国的技术主导地位，影响美国国家安全。

作为拜登政府 2024 财政年度结束前，在系统中实施零信任架构期限的一部分，整个联邦生态系统的各机构一直在加快其内部安全态势提升工作。

拜登政府意图通过该项行政令巩固其在科技和网络安全领域的遗产。迈克尔 · 丹尼尔（Michael Daniel）表示：“拜登政府在 12 月份颁布这一行政令是合理的选择。”丹尼尔认为，颁布这一行政令不仅是为应对特朗普上台后可能出现的政策调整，也为确保网络安全政策的连贯性打下基础。

2、聚焦政府身份管理，促进零信任架构迁移

据另一位熟悉行政令草案内容的人士称，预计该行政令将部分侧重解决政府部门的身份和访问管理，以确保在网络威胁日益复杂的环境下关键政府数据的安全，而非期待已久的覆盖每个美国人的数字身份行政令。

2024 年 3 月，白宫曾表示，在制定针对公共福利计划身份盗窃的行政令，以减少福利计划欺诈行为。根据该计划的草案，任何公共福利计划都必须向用户提供公共运营的数字身份服务，作为访问服务的一种方式。此前有报道称，在疫情期间启动或扩大的救济计划中存在大量身份盗窃行为。

在政府层面，联邦机构已在加速改进内部网络安全态势，以在 2024 财年结束前，实现零信任架构的全面实施。

2022 年 1 月 26 日，拜登总统办公室向联邦政府行政部门和机构负责人发布了一份行政备忘录，为零信任架构 (ZTA) 战略提供指导和方向。备忘录“提出了一项联邦零信任架构 (ZTA) 战略，要求各机构在 2024 财年结束前达到特定的网络安全标准和目标，以加强政府对日益复杂和持续的威胁活动的防御能力。”

在政府层面，
联邦机构已在加速改进内部网络安全态势，
以在 2024 财年结束前
实现零信任架构的全面实施。

根据白宫管理和预算办公室（OMB）的备忘录，各机构必须在 2024 年 9 月 30 日之前放弃基于边界的防御。因此相关机构必须在 2024 年 11 月提交更新的零信任架构实施计划，概述将如何实现关键的安全目标，包括消除隐性信任、保护关键资产及持续实时验证用户和设备。

CISA 零信任计划负责人布兰迪 · 桑切斯 (Brandy Sanchez) 表示，“随着各机构准备提交更新的零信任实施计划，网络安全和基础设施安全局正在与 OMB 和利益相关者进行协调，以确保对即将发布的定性数据进行彻底审查。”

桑切斯表示，“CISA 和 OMB 将加强对整个联邦政府采用零信任的技术援助。”CISA 还将评估各机构如何“测试其零信任框架的有效性”，例如，在模拟攻击场景中使用渗透测试和 MITRE ATT&CK 评估，以衡量对已知网络攻击技术的防御能力。

2024 年 6 月，美国国防部首席信息官发布了一份近 400 页的“零信任覆盖”文件，旨在作为路线图和指南，帮助该部门实现拜登政府行政令中提出的目标。零信任尚未在国防部整个部门实施，但到 2027 财年，预计将达到“目标水平”实施。这意味着美国国防部已实施了其《零信任战略和路线图》中确定的 152 项目标中的 91 项。

联邦首席信息官克莱尔 · 马托拉纳 (Clare Martorana) 在 2024 年 9 月表示，一些主要联邦机构在 9 月 30 日的最后期限前已在其网络上建立并采用一定程度的零信任架构。24 个联

邦监管机构“全部处于 90% 的高位”。但她早些时候曾承认，对于零信任的持续推进和确保各机构能在预算优先事项和资源不断变化的情况下有力推进零信任架构而言，持续的资金投入是一项关键挑战。

3、推进“安全设计”，鼓励内置安全

此外，这项行政命令还将涉及“安全设计”的原则。CISA 一直在推动安全的产品设计，鼓励企业在产品设计初期内置安全特性，以应对近年来多起高调的网络安全事件。

2023 年 3 月，拜登政府设立的网络安全办公室（ONCD）在发布了一项全面的政府网络安全战略，以推行安全设计原则，敦促开发人员采用内置防护功能的内存安全编程语言，以防止黑客造成的未经授权的访问、数据破坏或系统崩溃。白宫网络办公室还在努力提高边界网关协议（BGP，一种骨干数据传输算法）的安全性。

美国网络安全和基础设施安全局 (CISA) 局长珍 · 伊斯特利 (Jen Easterly) 表示，在推进“安全设计”计划时，CISA 是基于对长期趋势的认识。她表示，“在过去四十年中，从互联网的诞生到软件的大规模采用，我们见证了一场技术革命，迫使安全和保障退居次要地位，技术制造商和软件生产商优先考虑上市速度和功能，而不是安全性。”

自 CISA 于 2023 年启动“安全设计”倡议以来，已有近 170 个机构签署了承诺。据悉，签署承诺者将会采取一系列措施来减少产品的漏洞，包括建立默认的多因素身份验证和其他形式的防网络钓鱼身份验证保护，并减少使用默认或硬编码密码。这些企业还承诺通过官方渠道更加透明地披露安全漏洞，做出专门努力减少常见漏洞，并帮助客户快速安装安全补丁。

> “安全设计”的思维转变可能需要较长时间才能扎根，就像汽车安全带和安全气囊花了几十年才被广泛接受一样。

但她指出，这种“安全设计”的思维转变可能需要较长时间才能扎根，就像汽车安全带和安全气囊花了几十年才被广泛接受一样。

4、为下一阶段的网络安全工作奠基

丹尼尔指出，新的网络安全行政令不仅是在收尾现有政策，更是为未来进一步强化网络安全奠定基础。“从整体上看，美国的网络安全防护已得到提升，但离理想状态还有距离。”

特朗普的当选为拜登政府推进这一政策增添了紧迫性。拜登第二道总统行政令的核心目的是确保拜登的网络安全遗产得以延续，也为下届政府预留了继续推进网络安全政策的空间。

分析：特朗普网安政策影响与应对

作者　虎符智库

2024 年美国大选，特朗普最终获得 312 张选举人票，取得压倒性胜利。共和党也同时拿下参众两院，这意味着特朗普将拥有超级执政权力，推行他的激进主张。

尽管特朗普与哈里斯之间的选举竞争，更多围绕生育权、移民、经济等国内政策。两者都未提出处理关键网络问题的政策与计划，但从相关分析与报道中，两者在网络安全政策差异及潜在影响仍可看出端倪。

分析显示，与代表民主党的哈里斯相比，特朗普将在网络安全方面更加激进，包括对我国采取更主动的攻击行动、鼓励人工智能领域的竞赛，以及加大针对我国的信息战投入等方面。

一、网安问题超越两党界限，对华强硬是主流

分析人士认为，网络安全是美国民主、共和两党共同关心的问题，其背后的驱动因素来自国家威胁而非社会或经济问题。通常的党派界限在这里并不总是适用。这意味着无论特朗普还是哈里斯谁能胜出，在利用网络安全话题攻击和妖魔化中国方面，两党将会有着共同的诉求和主张。

拜登政府的相关网络政策足以说明这一点。拜登政府保留了特朗普第一个任期内的很多国家安全和网络安全政策。例如，特朗普政府期间成立的美国网络安全和基础设施安全局（CISA）；以及特朗普任期内启动的“总统杯网络安全大赛”等大型联邦活动。第六届年度总统杯网络安全竞赛将于 2024 年 12 月启动。

近年来，美国持续以网络安全问题对中国进行打压。美国相关智库机构甚至指责，中国成为美国的主要网络威胁，称“中国已经做好准备并计划通过制造混乱和不和来破坏美国社会”。

2023 年 5 月，“五眼联盟”国家（美国、英国、加拿大、澳大利亚、新西兰）的网络安全主管部门联合发布预警通报称，名为“伏特台风”的中国黑客组织，针对美国关键基础设施单位实施了网络间谍活动。2024 年 1 月，美国联邦调查局局长克里斯托弗·雷向众议院中国竞争特别委员会表示，与中国政府有关的黑客正瞄准美国关键基础设施，准备对美国人造

分析人士认为，网络安全是美国民主、共和两党共同关心的问题。
在利用网络攻击攻击和妖魔化中国方面，两党将会有着共同的诉求和主张。

成“现实世界的伤害”。他称，美国水处理厂、电网、石油和天然气管道及交通枢纽，都是中国国家支持的黑客行动的目标。

在网空领域，利用网络攻击事件对华施压已成为两党共识，特朗普将会持续利用这一问题对华施压。

二、未来特朗普政府对华网络攻击将会更主动

目前，特朗普这位共和党总统候选人，尚未提出处理关键网络问题的详细政策与计划。今年早些时候，美国传统基金会发布的《2025 项目》报告，被视为特朗普第二届政府的政策蓝图，其中，提出大幅削弱网络安全和基础设施安全局 (CISA) 职能及其他网络安全政策的构想，可能未必全部实施。但相关人士仍然可以从中拼凑出特朗普第二任期的网络安全政策方向。

1、鼓励军方实施“进攻”，而不是专注于阻止网络威胁。

据媒体对五位前特朗普政府高级官员的采访，大多数受访者认为，特朗普政府的国家安全方针将会比现任政府更强硬、行动更快。他们都表示，特朗普本人在网络安全政策上投入了大量心思和时间。

在特朗普第一个任期内，美国政府将网络威慑作为其网络安全战略的核心支柱，提出了以“前置防御”和“持续交手”为核心的进攻性威慑策略，对外开展低烈度的网络攻击。

预计，美国讨论已久的网络部队将会组建，以进一步提升所谓的网络进攻能力。此外，美国可能还会以互惠对等为由，限制中国等国对美国互联网和关键基础设施对访问；同时持续推动对 TikTok 等中国互联网应用等监管限制与打击。

2、进攻网络行动重点转移到中国和伊朗。

据受采访的前政府官员透露，特朗普可能会将进攻性网络安全工作重点从俄罗斯和朝鲜转移到中国和伊朗。据路透社发布的消息，在特朗普第一个任期内，就授权中央情报局对发动攻击性网络行动：即在中国社交媒体实施秘密活动，引导中国公众舆论反对中国政府。三名前官员透露，中情局为此组建了小型特工团队，使用虚假网络身份传播中国政府的负面言论，同时向海外新闻媒体泄露诋毁性情报。这一行动始于 2019 年，此前从未被报道过。

3、放松监管增加投入，加码中美人工智能竞赛。

特朗普本人关注人工智能的应用，重视确保美国在中国和其他对手的竞争中保持领先地位。因此预计，特朗普将支持放松对人工智能和其他新兴技术的监管，制定更有利于商业的网络安全政策。

前 CISA 助理部长哈雷尔（Brian Harrell）表示：“特朗普第二任期的网络安全政策可能会侧重于消除多余的监管。此外，特朗普政府可能会再次增加人工智能和量子信息科学等科

技的经费；在人工智能芯片等技术出口限制上持续加码，同时推动联邦机构的人工智能部署和采用。作为在人工智能、量子等领域与中国竞争的重要措施。

4、加强关基设施安全监管，多手段保护美国利益。

针对未来新政府可能加强网络防护的举措，前任网安官员预计，（特朗普政府）将可能会提高关键基础设施提供商和业主的标准，为 CISA 提供资金，以开发更强大的威胁检测和响应能力，加强与州和地方政府的协调，加大对保护工业控制系统 (ICS) 举措的支持。

保守派智库 R 街研究所 (R Street Institute) 网络和新兴威胁团队政策主管布兰登 · 普格 (Brandon Pugh) 也认为，尽管共和党政府不愿实施严格的监管，但特朗普仍有可能以国家安全的名义对关键部门实施基本的网络要求。

此外，未来特朗普政府将会采取从网络攻击、制裁到外交等多个层面的手段，加强对关基设施的防护。 前能源部前高级网络官员肖恩 · 普兰基 (Sean Plankey) 表示：“我们会从战略和战术角度利用网络空间行动，来实现美国的国家安全目标。”

三、美网络安全政策影响与应对建议

根据初步披露的提名信息，特朗普政府的组成由多个对华强硬的人士组成，除了在贸易政策上对我国施压，一定会利用其网络安全政策对我进行打压。

建议研究可能的风险与问题，从多个角度进行防范：

1、持续增加我国应对网络攻击，尤其是国家级网络攻击的能力。

正如美国的网络攻击与防护，充分发挥了公私机构和民间人士的作用，我国也应该建立起公私能力协作、信息共享的常态化机制，确保我国保持应对美西方的进攻性网络攻击的能力。

2、充分利用人工智能技术，加强对社交媒体的监测，消除内容风险。

美西方的信息战会充分利用各国的社交媒体，发布虚假的信息，抹黑丑化我国政府与领导人，放大社会事件的负面影响，我国应尽快依靠先进的人工智能技术，建立识别发现和快速阻止此类信息传播的能力 。

3、为中美博弈中的科技企业提供必要法律与资金支持。

为实现打压和阻碍中国科技发展的目标，美西方会利用政策和技术等多种手段，对我国人工智能、网络安全及社会化媒体等科技企业实施打压和封锁，需要我国政府部门成立专门组织因应，提供包括政策、法律和资金方面的支持。

4、将推动网络安全能力与体系现代化落到实处。

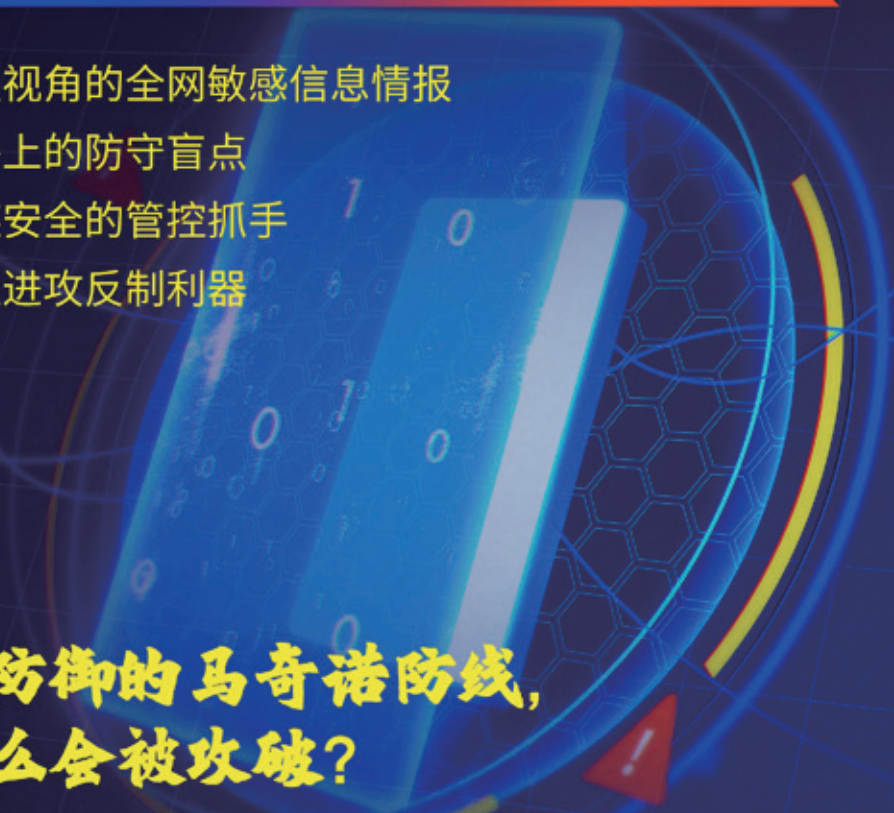
目前美国、欧盟都在推动旨在提升网络防护能力的现代化，尤其是明确要求政府机构和关基部门采用零信任、供应链等先进技术，且规定了达标时间。我国主管部门也在推动安全能力与体系现代化，但在推进方面相对笼统，缺乏可实施、具有约束力的要求，建议网安全主管部门针对美国的措施，制定出技术要求明确、效果可验证的实施计划。安

> 建议网安全主管部门针对美国政府的
> 网络现代化措施，
> 制定出技术要求明确、效果可验证的实施计划。

奇安信

敏感信息泄露情报服务

- 攻击队视角的全网敏感信息情报
- 急需补上的防守盲点
- 供应链安全的管控抓手
- 预防性进攻反制利器



纵深防御的马奇诺防线，为什么会被攻破？

- 完整的防御体系，既要考虑正面防御，侧翼的情报收集和对抗也必不可少！
- 忽视全网视角的情报，是防守的重大盲点！

服务定位 SERVICE POSITIONING

- **攻击队视角**：使用渗透专家交付，不是简单的信息收集。
- **全网视角**：核心功能是从外部探测全互联网第三方应用中的敏感泄露数据；而非只关心自己的网络和应用。
- **情报级**：专家梳理的情报级信息，而不是简单数据抓取：给出利用思路和可能的攻击链，更有详细的整改建议。

奇安信安服团队

中外安全事件处罚对比：重锤还是搔痒，网安事件应罚多少？

作者 裴智勇

罚款，是世界各国对系统运营者网络安全违法责任的明确标价。只不过标价的方式和价位有所不同，对运营者的“震慑”程度也有所不同。相比于某些国家动辄数百万，上亿元的“重锤式”罚款，中国监管机构仅给出10万元以下的罚款，可以用“挠痒痒”来形容了。

各国的国情不同，监管目标也不同，我们不能用简单的、一刀切的判断方式判断谁对谁错。但是，一个显而易见的事实是，当罚款金额显著高于建设成本时，运营者就会自然而然的选择投入资金进行必要的网络安全建设；反之，如果罚款金额远远小于建设成本，那么，在自身尚未产生明确的经济损失之前，运营者也会自然而然的选择“碰碰运气”，放弃网络安全建设与投入。

笔者就曾经历过这样一件事：有一所高校，因为发生重大数据泄露事件，被判罚 80 万元。于是这家高校就向很多安全公司咨询了数据安全的建设方案。结果发现，就这所高校的实际情况而言，各家安全公司给出的最低报价都是接近于 200 万元。最后这家高校咬了咬牙，还是放弃了数据安全建设项目。毕竟，建设了就是要投入 200 万，不建设也未必一定会被处罚，而且一次性建设投入，足够被罚两次半了。

本文将为大家总结一下 2024 年以来，媒体公开报道的国内外网络安全处罚事件，并对国内外的罚款金额进行对比分析。如果某些处罚案件的公开信息中，没有明确具体的处罚金额，本文将不进行收录和分析。

> 一个显而易见的事实是，
> 当罚款金额显著高于建设成本时，
> 运营者就会自然而然的选择投入资金
> 进行必要的网络安全建设。

1、2024 年国内网络安全处罚事件与罚金分析

下表给出了 2024 年媒体报道的10件国内机构网络安全责任处罚事件，部分处罚事件实际发生在 2023 年，但直到 2024 年才被集中报道出来。其中，涉及数据泄露的处罚事件 7 件，

时间	被罚机构	处罚机构	主要处罚原因	罚金（RMB）
2023.6	某生物技术公司	公安	19.1GB 个人信息泄露	5 万元
2023.7	某教育公司	公安	12 万 + 条个人信息泄露	5 万元
2023.8	某教育公司	公安	70 多万订单信息泄露	5 万元
2024.1	某科技公司	网信办	大量个人信息泄露	10 万元
2024.2	某超市	网信办	多台服务器、终端被木马控制	5 万元
2024.5	某集团	网信办	服务器被入侵，大量数据泄露	10 万元
2024.7	某培训学校	网信办	网页被篡改加挂涉黄违法链接	1 万元
2024.10	某 IT 公司	网信办	未落实等保，存在大量漏洞	5 万元
2024.10	某科技公司	网信办	大量敏感数据泄露	2 万元
2024.10	某两家公司	网信办	大量敏感数据泄露	10 万元

系统遭入侵 / 篡改等处罚事件 2 件，未履行网络安全义务处罚事件 1 件。总体而言，数据泄露事件，是国内机构被处罚的主要原因。

从处罚金额来看，绝大多数事件都是 5 万元或 10 万元。下面就对这些事件进行简要的介绍。

（1）泄露 19.1GB 数据，北京一生物技术公司被罚 5 万元

安全内参 2024 年 1 月消息，昌平网安部门在 2023 年 6 月的一次检查中发现，昌平某生物技术有限公司存在数据泄露的情况：其委托的另一软件公司研发的“基因外显子数据分析系统”中，包含大量公民个人信息、技术机密信息等需要加密保护的数据，但该软件公司在开发系统互联网测试阶段，未对相关数据进行加密，未落实安全保护措施，导致 19.1GB 的敏感数据被泄露。北京市公安局昌平分局依据《中华人民共和国数据安全法》（以下简称《数据安全法》）相关规定，给予该公司警告并处罚款 5 万元的行政处罚。

（2）泄露 12 万 + 条个人信息，北京某教育公司被罚 5 万元

安全内参 2024 年 1 月消息，北京朝阳网安部门 2023 年 7 月检查发现，朝阳某教育公司数据被泄露到境外非法网站上，该公司的一个客户关系管理系统内存储的该公司员工账号及对应客户姓名、手机、下单时间、成交金额等 12 余万条信息被泄露。造成这一泄露事件的原因是，该公司技术人员在对系统测试过程中，将有权限的测试账号设为弱口令，且系统正式使用后未将测试账号进行清空删除处理，进而导致系统被黑客入侵。北京市公安局朝阳分局依据《数据安全法》相关规定，给予该公司罚款 5 万元的行政处罚。

（3）泄露 70 多万订单信息，北京某教育公司被罚 5 万元

安全内参 2024 年 1 月消息，某境外黑产论坛于 2023 年 8 月，发布题为“某教育站点教 70 多万订单信息”的帖文。针对此情况，海淀网安部门立即开展核查处置工作。经查，该公司教务排课系统在账号密码传输前未进行加密，存在账号密码被爆破的可能。黑客可通过爆破手段获取账号密码，通过访问导出大批量后台数据，造成数据泄露。北京市公安局海淀分局《数据安全法》相关规定，给予该公司罚款 5 万元的行政处罚，给予直接负责的主管人员罚款 1 万元的行政处罚。

总体而言，依照目前的国内相关法律法规对政企机构做出的行政处罚，尚无法对涉事机构起到震慑作用，涉事机构的违法成本相对较低。

（4）泄露个人信息，北京某科技公司被罚 10 万元

2024 年 1 月，衡阳市网信办检查发现，某个在衡阳从事做软件开发业务的北京科技公司，其开发应用的网站数据库存在未授权访问漏洞，造成了公民个人信息泄露。经查，该科技公司主要为教育类单位提供互联网软件应用与开发服务。2023 年 1 月，该公司开发了一家网站用于教学，同时也存储了包含用户姓名、手机号、电子邮箱在内的大量个人信息。但由于该公司在开展数据处理活动时并未加强风险监测，系统存在安全漏洞，造成个人信息泄露等问题。衡阳市网信办依据《 数据安全法 》相关规定，给予该公司罚款 10 万元的行政处罚。

（5）计算机遭黑客远程控制，南昌一超市被罚 5 万元

2024 年 2 月，南昌市网信办在日常的网络安全监测中发现，属地某连锁超市所属 IP 疑似被黑客远控，频繁对外发起网络爆破攻击。经调查发现：该连锁超市未对运营的网络及信息系统开展网络安全等级保护测评等相关工作，所属的服务器和多台终端感染木马病毒，且未能及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险，导致被控终端与服务器持续对内、对外发起大规模网络攻击，严重危害网络安全。南昌市网信办依据《 中华人民共和国网络安全法 》（ 以下简称《 网络安全法 》）相关规定，给予该连锁超市罚款 5 万元的行政处罚，给予直接负责的主管人员罚款 1 万元的行政处罚。

（6）大量数据遭境外窃取，南昌某公司被罚 10 万元

2024 年 5 月，南昌市网信办在日常的网络安全监测中发现，南昌某集团有限公司所属 IP 疑似被黑客远程控制，频繁与境外通联，向境外传输大量数据。经调查发现：该公司未采取相应的技术措施和其他必要措施保障数据安全，所属的服务器遭境外黑客攻击并植入可获取服务器文件管理权限和命令执行权限的木马程序，大量数据疑似遭泄露或被窃取。南昌市网信办依据《 数据安全法 》相关规定，给予该公司罚款 10 万元的行政处罚，基于直接负责的主管人员罚款 2 万元的行政处罚。

（7）网站被篡改，长沙一培训学校被罚 1 万元

2024 年 7 月，长沙市望城区网信办调查发现，长沙某职业技术培训学校所属多个网站多次被不法分子篡改加挂涉黄违法有害链接信息，在多次收到网信部门下达的整改通知后，仍未按照网络安全等级保护制度的要求，履行网络安全保护义务。长沙市望城区网信办根据《 网络安全法 》相关规定，

给予该培训学校罚款 1 万元人民币的行政处罚。

（8）存在安全漏洞，湖南一 IT 公司被罚款 5 万元

2024 年 10 月，湖南省互联网信息办公室在工作中发现，湖南某信息技术有限公司未落实网络安全等级保护制度，未采取相应的技术措施和其他必要措施保障数据安全，系统存在未授权访问漏洞，网络安全日志大量缺失，严重损害数据安全。湖南省互联网信息办公室依据《数据安全法》和《湖南省网络安全和信息化条例》相关规定，给予该公司警告并责令改正，作出罚款 5 万元的行政处罚，并对该公司主管人员和直接责任人员作出罚款、2 万元和 1 万元的行政处罚。

（9）大量数据泄露，四川一科技公司负责人被罚 2 万元

2024 年 10 月，南充市互联网信息办公室在检查中发现，高坪区轩某科技有限公司自营业以来，相关责任人网络安全、数据安全意识淡薄，未建立网络安全、数据安全相关管理制度，数据安全保障技术手段不足，未履行网络安全防护和数据安全保护义务，并导致数据泄露。南充市互联网信息办公室依据《网络安全法》《数据安全法》相关规定，给予该公司责令改正，并对该公司负责人处以罚款 2 万元的行政处罚。

（10）大量敏感数据被窃取，河南两公司被罚 10 万元

2024 年 10 月，郑州市网信办在工作中发现，郑州市两家公司未履行网络安全保护义务，未采取必要的安全防护，导致大量敏感数据被窃取。郑州市网信办依据《数据安全法》相关规定，作出责令改正，给予警告并分别处以罚款 5 万元人民币的行政处罚。

经调查核实，郑州市某互联网信息服务有限公司在数据库中配置增加了远程登录空口令账户，导致黑客利用该空口令账户成功登录数据库，并窃取了数据库中的数据，被窃取的数据包括姓名、身份证号、手机号、邮箱地址等敏感信息。

另一起案件也非常相似。郑州市某科技有限公司缺乏网络安全意识，没有正确配置数据库，导致数据库存在未授权访问漏洞。攻击者通过漏洞登录数据库，查看、下载数据，导致敏感数据泄露。该公司系统访问日志功能未开启、重要的通联日志留存不足六个月，数据库系统配置不当，存在未授权访问漏洞。

小结

总体来看，国内的网络安全事件处罚主要呈现以下几个特点：

1、 事后处罚。绝大多数处罚事件都是在实际损失已经发生后，在检查相关企业时发现存在安全问题，再进行相应的处罚。

2、 处罚金额普遍较低，一般在 10 万元以下，甚至是 5 万元以下。

3、 部分处罚会涉及主要责任人，但处罚金额一般也不会超过 2 万元。

总体而言，依照目前的国内相关法律法规对政企机构作出的行政处罚，尚无法对涉事机构起到震慑作用，涉事机构的违法成本相对较低。

2、2024 年国外网络安全处罚事件与罚金分析

下表给出了 2024 年媒体报道的 18 件国外主管机构网络安全责任处罚。其中，涉及数据泄露的处罚事件 10 件，涉及违规跨境数据传输的处罚事件 2 件，违规分享数据处罚事件 4 件，其他原因遭处罚的事件 2 件。

从处罚金额来看，仅就本文收录的处罚事件而言，国外的机构受到的罚款，动辄数百万，甚至上亿美元，最少的一个处罚也有 99 万美元，约合人民币 715.5 万元。

从处罚金额来看，仅就本文收录的处罚事件而言，国外的机构受到的罚款，动辄数百万，甚至上亿美元，最少的一个处罚也有 99 万美元，约合人民币 715.5 万元。

时间	被罚机构	处罚机构	主要处罚原因	罚金
2024.7	阿里巴巴（电子商务）	韩国个人信息保护委员会	违规跨境传输个人信息	20 亿韩元
2024.4	Verizon（运营商）	美国联邦通信委员会	未经同意向其他机构分享用户数据	4690 万美元
2024.4	AT&T（运营商）	美国联邦通信委员会	未经同意向其他机构分享用户数据	5730 万美元
2024.4	T-Mobile（运营商）	美国联邦通信委员会	未经同意向其他机构分享用户数据	8010 万美元
2024.4	Sprint（运营商）	美国联邦通信委员会	未经同意向其他机构分享用户数据	1220 万美元
2024.5	Kakao（即时通信）	韩国个人信息保护委员会	泄露超 6 万用户个人信息	151 亿韩元
2024.5	必胜客（餐饮业）	澳大利亚通信与媒体管理局	违法发送垃圾邮件广告	250 万澳元
2024.6	Guidehouse（咨询公司）	美国司法部	APP 未经充分安全测试即上线，泄露大量个人信息	760 万美元
2024.6	NMA（咨询公司）	美国司法部	APP 未经充分安全测试即上线，泄露大量个人信息	370 万美元
2024.8	T-Mobile（运营商）	美国外国投资委员会	未能防止和报告敏感数据泄露事件	6000 万美元
2024.8	Uber（交通出行）	荷兰数据保护局	违反 GDPR 进行跨境数据传输	2.9 亿欧元
2024.9	AT&T（运营商）	美国联邦通信委员会	泄露超过 890 万名移动客户数据	1300 万美元
2024.9	Meta 公司（Facebook 母公司）	爱尔兰数据保护委员会	以明文形式存储数亿用户密码，并允许内部员工广泛访问这些密码	1.01 亿美元
2024.10	万豪（连锁酒店）	49 个州总检察长组成的联盟、美国联邦贸易委员会	泄露全球 3.44 亿用户个人信息	5200 万美元
2024.10	Check Point（网络安全）	美国证券交易委员会	在数据泄露事件中做出误导性披露	99.5 万美元
2024.10	Mimecast（网络安全）	美国证券交易委员会	在数据泄露事件中做出误导性披露	99 万美元
2024.10	Unisys（IT 集成商）	美国证券交易委员会	在数据泄露事件中做出误导性披露	400 万美元
2024.10	Avaya（通信服务商）	美国证券交易委员会	在数据泄露事件中做出误导性披露	100 万美元

罚款，动辄数百万，甚至上亿美元元，最少的一个处罚也有 99 万美元，约合人民币 715.5 万元。不得不承认，这是重拳出击。下面就对这些事件进行简要的介绍。

（1）未经同意，分享用户数据，美国四大运营商被罚近 2 亿美元

2024 年 4 月，美国联邦通信委员会（Federal Communications Commission，FCC）宣布，经过调查发现，电信运营商 Verizon、AT&T、T-Mobile 和 Sprint 在未经用户同意的情况下，将用户位置数据访问权限出售给数据聚合商，后者又将数据转售给第三方，并且这四家运营商即使在得知数据未经授权就被访问后仍继续出售给数据聚合商，并未采取任何措施确保第三方在被允许访问前取得用户同意。

FCC 表示，除非运营商获得用户的明确同意，否则必须对用户数据保密，因此决定对这四家运营商处以近 2 亿美元罚款。其中，Verizon 被罚款 4690 万美元，AT&T 被罚款 5730 万美元，T-Mobile 被罚款 8010 万美元，

Sprint 被罚款 1220 万美元（Sprint 和 T-Mobile 于 2020 年合并）。

（2）内部 VPN 遭漏洞攻击未向监管报告，这家金融巨头被罚超 7000 万元

2024 年 5 月，美国洲际交易所（ICE）因未能确保其子公司及时报告 2021 年 4 月出现的 VPN 安全漏洞，遭美国证券交易委员会（SEC）指控，需支付 1000 万美元罚款。

洲际交易所是一家位列《财富》500 强榜单的美国公司，在全球范围内拥有并经营多家金融交易所和结算所，包括纽约证券交易所。2023 年，该公司雇佣了超过 1.3 万名员工，报告总收入为 99.03 亿美元。

SEC 的调查显示：2021 年 4 月，有国家级攻击者，利用一个 VPN 安全漏洞，在一台 VPN 设备上安装了 Webshell 代码，试图窃取该设备处理的信息，包括员工姓名、密码和多因素认证代码。利用这些数据，威胁行为者或能访问内部企业网络。

美国《监管系统合规性和完整性》（Regulation SCI）法规要求，如公司发现入侵等安全事件，必须立即通知 SEC，并在 24 小时内提供更新，除非他们确定事件对其业务或市场参与者的影响微乎其微。而洲际交易所却足足花了四天时间评估事件影响，因此被判定违规。

（3）泄露超 6 万用户个人信息，韩国即时通讯巨头被罚 151 亿韩元

2024 年 5 月，因通信服务公司 Kakao 泄露超 6 万用户的个人信息，韩国个人信息保护委员会（PIPC）在全体会议上批准了对该公司 151 亿韩元的罚款，约合 7822 万元人民币。

此前有报道称 KakaoTalk 开放式聊天用户的个人信息被非法交易。一个交易在线营销计划的网站上出现了提供提取开放式聊天室参与者真实姓名和电话号码的广告。2023 年 3 月，PIPC 对此展开调查。

PIPC 调查发现，黑客在开放的聊天室中找到用户的临时用户名，然后使用 KakaoTalk 的“添加好友”功能和非法黑客程序，获取用户的会员序列号及其他信息。这些数据被组合起来创建个人信息文件，然后在 Telegram 等平台上出售。一位 PIPC 官员表示，“我们确认 696 名开放聊天室用户的信息被发布在特定网站上，而黑客访问了至少 65719 条个人信息记录。”

PIPC 得出的结论是，Kakao 没有对开放式聊天服务参与者的临时 ID 进行加密，因此很容易识别会员序列号，而临时 ID 中包含常规聊天会员序列号，被指出是数据泄露的重要原因。

（4）违规发送垃圾邮件，必胜客被罚 250 万澳元

2024 年 5 月，澳大利亚通信与媒体管理局（Australian Communications and Media Authority，ACMA）宣布，在接到消费者投诉后，判定 Pizza Pan Group Pty Ltd（必胜客）违反《2003 年垃圾邮件法》（Spam Act 2003，以下简称《垃圾邮件法》），向未经同意或已取消订阅的顾客发送 590 万条营销信息。被判处 250 万澳元（约合 167 万美元）的罚款。

ACMA 表示，其收到投诉，称连锁餐厅必胜客向已撤回接收营销信息同意的消费者发送营销信息。此外，投诉人称这些信息没有有效的取消订阅功能。

（5）上线前未做安全测试，美国两家知名企业被罚 1130 万美元

2024 年 06 月，美国知名咨询公司 Guidehouse 和 Nan McKay and Associates（NMA）在新冠（COVID-19）援助部署过程中存在

2024 年 08 月，GDPR 罚款“单王”诞生。荷兰数据保护局（DPA）对全球出行巨头优步（Uber）开出了一张创纪录的罚单，罚款金额高达 2.9 亿欧元（约合 3.24 亿美元）。

网络安全缺陷，被控违规。这两家公司已同意支付总计 1130 万美元的罚款。

具体来说，Guidehouse（前身为普华永道美国公共部门，总部位于弗吉尼亚州麦克莱恩）支付 760 万美元，NMA（总部位于加利福尼亚州埃尔卡洪）支付 370 万美元。根据和解协议，揭发此事的前 Guidehouse 员工将获得 194.925 万美元（约合 1414 万元人民币）的奖励。对于去年收入高达 55 亿美元的 Guidehouse 来说，这笔罚金微不足道。相比之下，NMA 的年收入大约为 1.9 亿美元。

美国司法部上月发布的和解协议披露了事件详情。两家公司被纽约州选中管理该州的紧急租赁援助计划（ERAP）。ERAP 由美国国会在 2021 年年初建立，覆盖美国全境，是联邦政府新冠疫情救济资金计划的一部分。在疫情封锁期间，这些安全网计划为低收入人群提供财政援助，帮助他们支付租金、水电费和其他与住房相关的费用。

在纽约州，临时和残障援助办公室负责该任务，并在 2021 年 5 月与 Guidehouse 签订了一份 3.1 亿美元的合同，指定其为主要承包商，负责向纽约居民提供 ERAP 技术和服务。NMA 作为 Guidehouse 的分包商，负责向纽约州居民提供提交租赁援助在线申请的 ERAP 系统。

两家咨询公司本应确保该 ERAP 应用程序在部署前经过适当的网络安全测试。但根据和解协议，NMA 和 Guidehouse 在测试工具未能发挥作用的情况下，依然批准应用程序上线。自 2021 年 6 月 1 日上线后，个人敏感信息的泄露几乎立即开始。在 ERAP 应用程序上线约 12 小时后，临时和残障援助办公室通知两家咨询公司，申请者的某些数据已经泄露到互联网上。

（6）违规跨境传输用户信息，阿里被罚约 20 亿韩元

2024 年 7 月，韩国个人信息保护委员会（以下简称“PIPC”）在第 13 次全体会议上，决定对违反个人信息保护法规跨境传输用户个人信息的 Alibaba.com Singapore E-Commerce Private Limited（以下简称“阿里”）处以 19 亿 7800 万韩元（约合 1025 万元人民币）的罚款和 780 万韩元（约合 4 万元人民币）的滞纳金，以及责令整改并提出改进建议。

PIPC 指出，当用户在阿里的某个平台上购买商品时，卖家会配送商品，并在此过程中将消费者的个人信息跨境传输给发货工厂，经查实，已有超过 18 万韩国用户的个人信息被提供给了中国卖家。

以该种方式跨境传输个人信息。很难根据法律规定的采取适当保护措施。韩国《个人信息保护法》要求企业必须在信息主体明确知晓的情况下获得其同意，并在与用户的合同内容中反映安全性保障措施、个人信息侵犯的投诉处理，以及纠纷解决等相关措施。

然而，阿里并未向用户告知“个人信息转移的国家”“接收个人信息的个人或法人的姓名（公司名称）及联系方式”等根据个人信息保护法规

定的应告知事项，也未在卖家须知中反映保护个人信息所需的措施。

（7）敏感数据泄露，T-Mobile 被罚 6000 万美元

2024 年 08 月，电信运营商 T-Mobile 因未能防止和报告敏感数据泄露事件，被美国外国投资委员会（the Committee on Foreign Investment in the U.S.，以下简称 CFIUS）处以 6000 万美元罚款，这也是该委员会有史以来开出的最大罚单。罚款金额之大，以及 CFIUS 前所未有地决定公开此事，显示该委员会正在采取更强硬的执法方式，以阻止未来可能发生的违规行为。

CFIUS 实施的处罚与 T-Mobile 违反了在 2020 年以 230 亿美元收购美国 Sprint 公司时与该委员会签订的缓解协议有关。美官员透露，T-Mobile 的敏感数据泄露事件发生在 2020 年和 2021 年，该公司未能及时报告这些事件，延误了 CFIUSS 实施调查和缓解任何潜在危害美国国家安全的努力。

T-Mobile 在一份声明中表示，公司在与 Sprint 合并后的整合过程中遇到了技术问题，影响了“少量执法信息请求中共享的信息”。该公司强调，这些数据从未离开执法部门，并且已“及时报告”和“迅速解决”。

（8）2024 年最高罚单！ Uber 因违反 GDPR 被罚 2.9 亿欧元

2024 年 08 月，GDPR 罚款“单王”诞生。荷兰数据保护局（DPA）对全球出行巨头优步（Uber）开出了一张创纪录的罚单，罚款金额高达 2.9 亿欧元（约合 3.24 亿美元）。罚款原因是优步在将欧洲出租车司机的个人数据传输至美国时，涉嫌未能遵守欧盟严格的数据保护标准。

> 综合来看，某些比较发达的国家对于企业违规的罚款金额是相当惊人的。某些国家开出的千万美元、上亿美元的罚单，的确可谓“天价罚单”。

荷兰 DPA 表示，优步在数据传输过程中未能适当保护司机的敏感信息，严重违反了《通用数据保护条例》（GDPR）的规定，同时也暴露了优步在数据保护方面的重大疏漏。据悉，优步在美国的服务器上存储了司机的敏感信息超过两年，包括账户详情、出租车执照、位置信息、照片、支付详情和身份文件。在某些情况下，这些数据甚至包含司机的犯罪记录和医疗信息。

（9）供应商泄露用户信息，AT&T 被罚近 1 亿元

2024 年 09 月，美国联邦通信委员会（FCC）与 AT&T 就 2023 年 1 月发生的重大数据泄露事件达成了一项 1300 万美元的和解协议。该事件源自 AT&T 的一家第三方云服务供应商。FCC 调查认为，该供应商未能按时删除数据并泄露，FCC 要求 AT&T 严格落实审查责任。

此次数据泄露导致 AT&T 超过 890 万名移动客户的信息被窃取。根据和解协议，一家未具名的公司，负责为 AT&T 提供用于营销、账单处理和生成个性化视频内容的服务，是此次事件的罪魁祸首。协议中提到，AT&T 为了使用这家供应商的服务，与其共享了包括用户数据在内的大量客户信息。

AT&T 与该供应商之间签署的合同中，明确规定了对这些数据进行保护和处理的要求。2016 年至 2020 年间，经过多次审查和评估，表明该供应商遵循了数据删除政策。然而，在 2023 年 1 月的泄露事件中，本应在 2017 年或 2018 年删除的数据被盗。FCC 最终认定，AT&T 对这一失误负有不可推卸的最终责任。

（10）明文存储用户密码，美国互联网巨头被罚超 7 亿元

2024 年 9 月，爱尔兰监管机构对 Meta 公司（Facebook 母公司）处以 1.01 亿美元（约合 7.08 亿元人民币）的罚款，原因是 Meta 以明文形式存储了数亿用户密码，并允许公司内部员工广泛访问这些密码。

Meta 早在 2019 年年初就披露了这一疏漏。该公司表示，旗下多个社交网络应用程序在记录用户密码时，

集体维权，在国内非常少见，
但在国外，特别是在欧美国家则时有发生。
网络安全事件也不例外。

使用了明文存储的方式，并将这些密码存储在了一个数据库中。该数据库被大约 2000 名公司工程师查询过，查询次数累计超过 900 万次。

爱尔兰数据保护委员会副专员 Graham Doyle 说：“鉴于访问这些数据的人可能会滥用数据，大家普遍认为用户密码不应以明文形式存储。我们必须考虑到，在这个案件中被讨论的密码尤为敏感，因为它们可以用于访问用户的社交媒体账号。

（11）泄露全球数亿人信息，国际酒店巨头万豪被罚超 3.6 亿元

由于 2014 年至 2020 年期间发生的多起重大数据泄露事件，影响了全球超过 3.44 亿人，2024 年 10 月 9 日，万豪宣布同意支付 5200 万美元（约合 3.67 亿元人民币）罚款，并制定一项全面的信息安全计划。

这是当日宣布的两项和解协议之一。第一项是万豪与美国 49 个州总检察长及华盛顿特区组成的联盟之间达成的和解协议。这一联盟在网络入侵者窃取了包括部分财务信息在内的敏感客户信息后发起调查。该笔 5200 万美元赔偿将分配给所有 50 位联盟成员。

第二项是万豪与美国联邦贸易委员会（FTC）达成的和解协议，要求万豪国际及其子公司喜达屋酒店及度假酒店国际集团（以下简称“喜达屋”）在未来 20 年内实施更严格的网络安全措施，并向 FTC 证明其合规情况。此外，万豪还需为客户提供便捷的方式，允许他们请求删除酒店已收集的个人信息。

（12）四家上市公司因网络安全信披违规被罚 5000 万元

2024 年 10 月，美国证券交易委员会（SEC）宣布，因四家公司在 2019 年“太阳风”（SolarWinds）数据泄露事件中做出误导性披露，决定对其处以民事罚款。被处罚的四家公司分别是网络安全公司 Check Point（罚款 99.5 万美元）、Mimecast（罚款 99 万美元），科技公司 Unisys（罚款 400 万美元）和 Avaya（罚款 100 万美元）。

这些公司均为“太阳风”黑客攻击的受害者，该攻击影响了多个使用“太阳风”软件的公司和政府机构。根据 SEC 的说法，四家公司都存在不同程度的违规行为，它们“敷衍了事”地淡化了这些攻击带来的损害。

SEC 执法部门代理主管 Sanjay Wadhwa 表示：“虽然上市公司可能成为网络攻击的目标，但它们有责任通过准确披露网络安全事件，保护股东和公众投资者的利益，而非提供误

导性信息。在这起案例中，SEC 认定这些公司在相关事件上提供了误导性披露，导致投资者无法了解事件的真实范围。”

SEC 指出，四家公司各自存在不同的违规之处。Avaya 宣称黑客仅访问了“有限数量”的公司电子邮件，却未提及黑客还访问了“其云文件共享环境中的至少 145 个文件”。Check Point 在明知漏洞存在的情况下，仅以“泛泛之辞”描述了网络入侵和潜在风险。Mimecast“拒绝披露”被盗代码及公司加密凭证的数量，“企图淡化攻击的严重性”。Unisys 则将其“网络安全事件的风险描述为假设性的”，尽管该公司遭遇了与“太阳风”相关的两次攻击。

小结

综合来看，境外某些比较发达的国家对于企业违规的罚款金额是相当惊人的。和国内一般只有 5~10 万元人民币的罚款金额相比，某些国家开出的千万美元、上亿美元的罚单，的确可谓“天价罚单”。不过，从本文收录的案例来看，事后追责式罚款，并不是“天价罚单”产生的主要原因，反而是违反 GDPR，违规跨境传数据，以及安全事件处置不及时等具体的违规行为，更容易遭到“天价罚单”，而且越是知名的大公司，越容易遭到“天价罚单”。

3、罚单之外，还有集体诉讼和民事赔偿

集体维权，在国内非常少见，但在国外，特别是在欧美国家则时有发生，网络安全事件也不例外。比如，2024 年 9 月，因勒索攻击泄露患者敏感数据，美国医疗巨头 LVHN 就被起诉赔偿了 6500 万美元。

利哈伊谷健康网络（Lehigh Valley Health Network，简称 LVHN）是美国宾夕法尼亚州最大的初级医疗集团之一。该机构于 2023 年 2 月 6 日发现其 IT 系统遭受入侵，随后确认臭名昭著的 ALPHV（又称 BlackCat）勒索团伙是这次攻击的幕后黑手。

勒索者共窃取了 13.4 万名患者和员工的相关数据，数据量达数 GB。这些被窃取的数据包括姓名、地址、社会安全号码、州 ID 信息，以及医疗记录和手术照片。勒索者要求 LVHN 支付赎金，否则将这些信息泄露到网上。

根据随后对 LVHN 提起的诉讼，该医院长期以来拍摄癌症患者的裸照。在某些情况下，甚至未经患者知晓。由于 LVHN 拒绝向 BlackCat 支付赎金，犯罪分子将部分资料发布到了网上，引发了客户的极大愤怒。

起诉书中指出：“虽然 LVHN 公开宣称他们勇敢地对抗了这些黑客，拒绝支付赎金，但实际上，他们忽视了真正的受害者。LVHN 并未优先考虑患者的利益，而是将自身的经济利益置于首位。”

3 月 4 日，ALPHV 团伙在其网站上发布了警告，威胁如果 LVHN 不支付赎金，他们将在线发布被盗的照片。LVHN 拒绝了这一要求，犯罪分子遂将部分窃取的资料上传至其暗网门户，其中包括带有个人身份信息的照片。

法庭文件显示，一名未具名的原告于 3 月 6 日接到医院合规副总裁的电话，得知她的裸照已被上传到网上。随后，这位副总裁“笑呵呵”地提供了两年的信用监控服务。这位匿名原告表示，她并不知情医院在她接受乳腺癌治疗时拍摄了她的裸照，更不清楚这些照片被存储在医院的企业服务器上。

尽管 LVHN 已通知客户和员工有关隐私泄露的情况，但 ALPHV 团伙继续加大压力，3 月 10 日再次泄露了 132GB 的数据，并威胁将每周继续泄露，直到赎金支付为止。

原告律师指出，医院未能履行其保护信息的责任，其行为还涉嫌违反了美国《健康保险可携性与责任法案》（HIPAA）。尽管 LVHN 同意了和解条款，但他们否认有任何不当行为。

2023 年 3 月，原告们正式对 LVHN 提起集体诉讼，指控这家医疗机构未能妥善保护患者数据。2024 年 9 月 11 日，原告代理律师事务所 Saltz Mongeluzzi Bendesky 宣布，已与 LVHN 就此集体诉讼达成 6500 万美元的和解。这家律所指出，“如果按每位患者计算，和解金额是医疗数据泄露勒索软件案件中最高的。”

那些数据被公开发布到网上的患者被分为四个等级。如果和解获得批准，最低等级的患者将获得每人 50 美元的赔偿。而最高等级（那些裸照被泄露的患者）在扣除律师费后，将获得 7 万至 8 万美元不等的赔偿。凡是收到 LVHN 通知的个人都将被视为集体诉讼的一部分，并自动获得赔偿，无需采取任何额外行动。安

奇安信
新一代网络安全领军者

聚焦安全运营，构建智能平台

奇安信网神态势感知与安全运营平台（简称NGSOC）以大数据平台为基础，通过收集多元、异构的海量日志，利用关联分析、机器学习、威胁情报等技术，帮助政企客户持续监测网络安全态势，为安全管理者提供风险评估和应急响应的决策支撑，为安全运营人员提供威胁发现、调查分析及响应处置的安全运营工具。

国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

首款分布式关联分析引擎 - Sabre

国内首款具备分布式关联分析能力的安全运营平台，提供多元异构数据关联分析、灵活威胁建模、丰富的告警上下文信息展示及分布式横向扩展能力，已获得数十个相关专利。

将平战结合进行落地

演练态势监测攻防演练中防守方管理信息、系统建设、威胁运营等信息的总体状况，平战结合，全面提升安全防御能力。

重大安全事件的威胁预警

当出现重大网络安全事件时，帮助用户第一时间掌握是否遭受到攻击？首个被攻击的资产？影响部门？影响面趋势？事件处置情况？

专业的安全运营服务

奇安信集团具有专职产品运营服务团队，可提供原厂一线驻场、二线分析、运营方案咨询及培训服务，帮助客户解决无人运营困难。

市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证
态势感知解决方案市场领导者——IDC认证
态势感知技术创新力和市场执行力双第一——数世咨询认证

治理、技术、运营三管齐下，解读华南某市政数局数据安全建设“三部曲”

作者　研究员 张少波

近年来，全球政府行业重大数据泄露事件频发。2024 年 10 月，联合国终止暴力侵害妇女信托基金数据库在互联网上公开暴露，超过 11.5 万份敏感文件被泄露；2024 年 9 月，美国某州计划生育协会遭入侵，近 100GB 敏感数据被泄露；2024 年 8 月，马来西亚国家基建遭勒索攻击，疑泄露超 300GB 数据……这些事件都凸显了加强政府机构数据安全防御的紧迫性。

早在 2022 年，国务院印发的《关于加强数字政府建设的指导意见》就明确指出，构建数字政府全方位安全保障体系，强化安全管理责任，落实安全制度要求，提升安全保障能力，提高自主可控水平，筑牢数字政府建设安全防线。

华南某市是珠三角中心城市之一，粤港澳大湾区重要节点城市，国家历史文化名城之一。近年来，该市政数局大数据中心积极开展政务信息资源共享工作，随着各委办局数字化业务不断扩大，政务大数据中心数据治理与共享业务不断增多，一期原有的单数仓技术架构主件难以满足实际的数据共享需求，中心随即启动二期“一湖双仓”新技术架构设计工作，基于新技术架构的数据安全保障亟待完善。

经过多方比较，该市政数局最终选择和奇安信合作，后者依托数据安全治理、数据安全技术、数据安全运营三大体系，基于对业务的深入分析，本着治理先行、循序渐进的原则，形成贴合实际需求的整体解决方案，树立了政务数据安全“三同步”建设的样板间。

现状篇：三大场景亟待补齐安全短板

该市大数据中心在数据安全二期内容建设中，严格遵循了《数据安全法》《个人信息保护法》《网络安全法》等三大上位法，以及《XX市政务数据管理办法》《XX市政务数据管理规范（试行）安全类》等相关规范条例，确保在合法合规前提下开展相关工作。

在建设要求方面，围绕“一湖双仓”业务开展全方面数据安全保护，并适配业务特色数据环境，保障安全策略有效性，同时基于本市政务云环境设计定制方案，确保落地，目标是提供持续运营价值，树立政务数据安全新标杆。在建设过程中，该市大数据中心意识到，必须兼顾以下三方面的典型场景：

首先是政务数据价值高、覆盖面广，亟需进行分级保护。

本市“一网共享”平台承载各委办局的敏感业务数据，一旦泄漏可能对当地的经济运行、社会秩序、公共利益，组织、个人权益等产生影响。同时其数据中包含人口、法人、信用、证照、地图、视频等400多种类别的数据内容。考虑到业务的复杂性，一刀切的保护方式严重影响业务，因此需要对政务数据进行分类分级并形成分级保护。

其次是存在跨边界数据传输需求，需要对数据调用全面监控。

该大数据中心承载的业务数据，需从本市各委办局进行采集，经过申请后会产生数据回流、省级上传、其他地市同级传输等多种使用场景，但对于这些接口中传输的数据类型、数量等缺乏监测手段，存在超范围超量传输的风险。

最后是对于接触数据的相关方需要严格管理。

数据在采集、流转过程中链条越长、接触的对象越多，潜在的安全风

图：数据安全治理工作

险也就越大。因此，需要采用管理与技术相结合的方式，保障非业务数据操作的安全性。

该市政数局和奇安信紧密合作，双方以“零事故”为目标构建大数据中心数据安全体系，遵循“零事故”三大原则：合规不踩线、数据不出事、业务不中断，按照治理先行、防范泄露、持续运营的路线节奏，稳步推进。在建设思路方面，采用完整的数据安全治理、数据安全技术、数据安全运营三大体系，形成贴合实际需求的整体方案。

治理篇：安全有道，治理先行

没有规矩，难成方圆，“合规不踩线”是“零事故”的首要原则，数据安全建设的首要工作，就是“安全有道，治理先行”，在合规指导之下，开展数据安全治理服务。

该阶段工作具体分为四个阶段：

第一是调查数据安全现状，评估服务内容。

该市政数局和奇安信一起，对现状进行了全面调研，包括通过政策解读，明确数据安全合规遵从需求；调研业务和数据现状，识别关键业务场景及关键数据，数据流转情况等；同时梳理现有管理、技术防护措施与执行情况。基于充分的调研基础，就能开展科学的安全评估，识别数据安全关键风险，并给出风险缓解措施和整改建议。

第二是建立组织框架，编制制度

和规范。

该部分核心工作是管理体系设计，包括建立数据安全管理组织框架及明确各级职责；设计数据安全制度体系；编制数据安全相关管理制度、规范及流程、表单等。

第三是推动数据安全分类分级，绘制敏感数据流转视图。

该部分具体包括开展自身的数据资产梳理和盘点，制定分类分级标准，实施分类分级工作，形成数据分类分级清单等。根据数据类型、重要级别、敏感程度等，制定敏感数据资产目录、形成核心数据、重要数据、个人数据等目录或清单。结合这些材料，绘制敏感数据流转视图，洞察敏感数据风险。在这个基础上，开展分级管控和防护策略设计，以确保相关产品能力落地。

第四是数据安全防护体系设计服务。

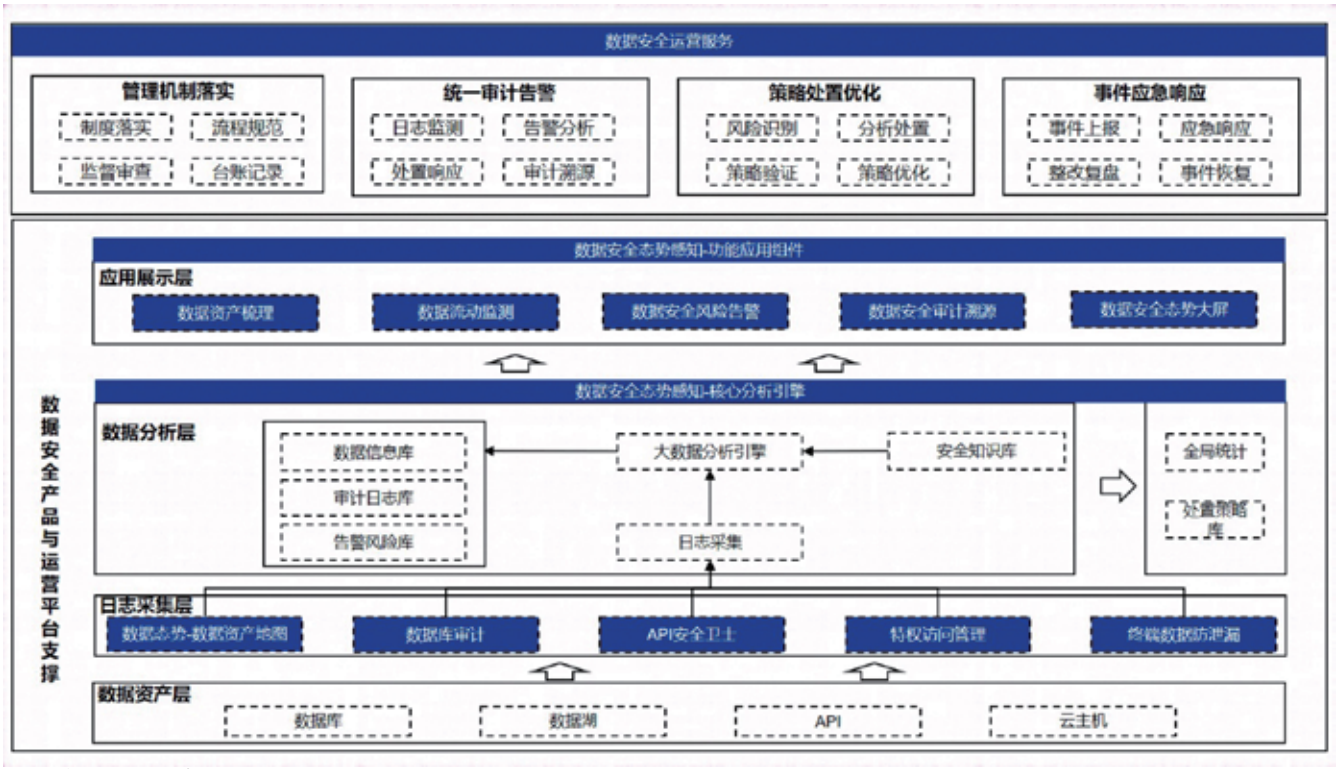
该部分根据现状调研结果，结合业务战略、合规、治理和风险容忍度制定数据安全总体目标、方针和策略，结合现状评估结果，设计数据安全防护体系及演进路线。

技术篇：防范泄露，杜绝勒索

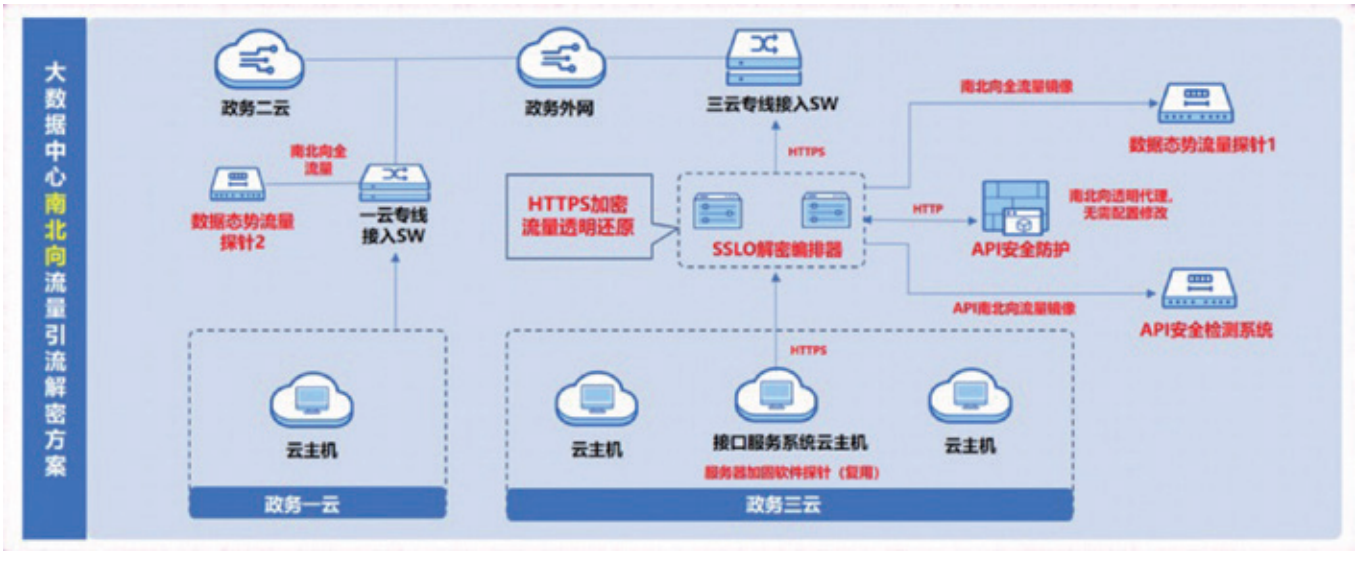
IBM 不久前发布的 2024 年《数据泄露成本报告》显示，全球数据泄露事件的平均成本在今年达到 488 万美元，未来还将进一步提升。因此，该市政数局高度重视数据泄露带来的危害，通过技术手段强化安全能力，抵御数据泄露、勒索攻击等各种内外部威胁。

针对这些风险，奇安信通过防泄露方案设计，实现数据资产可视、数据风险可知、泄密行为可管、安全事件可溯源四个目标。

第一是数据资产可视。通过数据态势 – 数据资产地图能力，结合数据安全治理资产梳理服务，形成安全视角下的一湖双仓数据资产可视化。



图：某市大数据中心防泄露方案



图：大数据中心南北向流量引流解密方案

第二是数据风险可知。通过专业产品能力和定制化安全策略，检测数据库访问、API 访问、特权访问三大重点应用场景下安全风险，同时通过数据安全态势感知汇集安全日志关联分析，构建风险检测模型。

第三是泄密行为可管。通过特权会话控制、API 安全防护，实现数据风险行为阻断，通过终端数据防泄漏模块，管理终端数据操作行为，防止通过终端路径泄露。

第四是安全事件可溯源。通过数据安全态势感知汇集多源安全日志，利用泄露线索还原分析安全事件。

针对日渐肆虐的勒索攻击，奇安信围绕四种攻击入口，构建勒索病毒识别及防护，包括网站挂马入口、软件供应链入口、系统本身漏洞入口、运维人员终端入口等，通过部署 WAF、防火墙、代码检测、虚拟主机安全软件、终端天擎杀毒等措施，将勒索病毒拒之门外。

同时，奇安信还提供了数据备份机制，确保即便出现极端情况，也能第一时间修复重要数据，将损失降至最低。

运营篇：技术落地，持续运营

安全建设只有起点，没有终点。如果没有持续的运营，安全能力就无法持续，最终依然会被攻破。因此，该市政数局建立了“专家 + 流程 + 平台”的运营机制，根据业务数据及风险情况，实时调整安全策略，依托多源数据汇聚、数据流动监测、监测与分析、安全事件及时发现、审计溯源等做整体态势感知。具体包括以下内容：

第一步，完成特色数据库、国产化适配方案设计。

数据安全产品的有效应用必须适配客户的实际应用环境，通用的产品能力极易出现产品无法使用，成为“摆设”。通过对大数据二期项目范围有可能涉及的特色数据库和国产化环境进行详细调研，评估安全产品在实际应用环境的支撑情况，协同后端产品研发线，设计了完整的适配计划，以保障项目落地的有效性。

第二步，聚焦南北向场景，部署SSLO“引流 + 解密”及 API 安全卫士，解决云外到云内的安全威胁。

数据安全的重点是要发现和管控异常访问行为，因此需要对流量进行引流和解密，为保障在该市政数局环境中的多云互访场景下落地，通过长时间的环境及需求调研，以奇安信特有的 SSLO 解密编排器为核心，设计出适配该市政务云环境的南北向“引流 + 解密”解决方案，有效解决云间访问 HTTPS 流量加密问题、API 访问控制透明部署问题、多副本流量分发问题、关键链路可靠性保障问题。

第三步，聚焦东西向场景，解决政务云内云主机之间的风险。

针对政务云内云主机之间的东西向流量，通过复用现有主机安全组件，设计出适配该市政务云环境的东西向引流 + 解密解决方案，有效解决主机侧多副本流量网卡占用问题、主机云原生封装流量加密问题，多副本流量分发问题。针对政务大数据中心对外 API 接口服务，以奇安信特有的 SSLO 解密编排器为核心，设计出适配该市政务云环境的东西向引流 + 解密解决方案，有效解决 API HTTPS 流量加密问题、代理部署应用改动大等问题。

第四步，建立常态化数据安全运营体系及应急响应体系，确保管理得到有效执行、技术得到有效使用。

奇安信帮助该市政数局建设了数据安全运营中心，承担了全局感知、集中运营、风险闭环、合规保障等职责。在运营体系中，分为日常运营和场景化运营两大部分。其中日常运营包括数据资产运营、安全策略运营、安全风险运营、安全事件运营、运营监控等，场景运营包括数据安全风险评估、系统上线评估、应急响应、重大保障、赋能培训等。

效果篇：三大成效，打造政务数据安全实践标杆

经过一年的建设，该市政数局在数据安全建设方面，取得了三大成效：

首先是全过程数据的分类分级得到有效执行。

截至目前，对于委办局上报的数据自带分类分级标签，通过检查及指导机制确保采集数据分类分级的正确性，对于治理、分析过程中产生的衍生数据进行分类分级核验机制，确保平台中的全部数据均得到相应的保护。

其次是实现了平战结合，持续运营，让数据安全保障贯穿始终。

其中在常态化运营方面，重点围绕数据的合规使用，动态优化策略，主抓数据安全风险及事件。

在实战化运营方面，一方面，在重保和实战攻防演习期间加强防护，在上级监督检查时有备无患；另一方面，显著增强数据安全应急能力，包括周期性应急演练，强化全员协同，同时通过应急响应支撑，即便事件发生时，也能最大程度减少影响。

最后是完善资产识别和脆弱性管理，将威胁防患于未然。

其中包括完成 API 资产识别 4300 多个，API 接口用途及分类梳理 2600+，数据库资产识别 34 个，完成分类分级 1.6W 字段；接口脆弱性及未授权访问 30 条，明文账密 +URL 路径超过 20 条，这些均完成整改。落实 30+ 场景化监测规则，主要围绕数据采集、数据请求、数据传输等实际业务场景，完成 44 次安全通告。

结束语

2025 年 1 月 1 日起，《网络数据安全管理条例》将正式施行，这使得各级政府构筑数据安全防线更加迫切。通过该市政数局的建设实践，充分验证了奇安信数据安全的“三步走”方法论的可行性和良好效果，最终通过治理、技术、运营的闭环形成，让安全能力与日俱增，让政府数据处于持续安全的状态，从而保障数字政府建设行稳致远。安

奇安信
新一代网络安全领军者

「零事故」安服团队重磅力作

900余次实战攻防演练的经验总结
从红队、蓝队、紫队视角全面解读攻防演练

扫码购买

大事记

华为首批安全伙伴！奇安信获鸿蒙 HarmonyOS NEXT 技术认证

11 月 14 日，华为“企业工作必备应用鸿蒙化论坛”在京举行，论坛汇聚了众多行业精英和合作伙伴，共同探讨原生鸿蒙系统在企业应用中的广阔前景。会上，奇安信集团作为华为首批安全伙伴，“奇安信网神 TrustSpace 移动安全管理系统 V3.0 版本”获得鸿蒙 HarmonyOS NEXT 技术认证书。未来，双方将继续共同推动国产应用软件在相关业务领域的深入应用。

郑州大学党委书记别荣海一行到访奇安信集团

11 月 13 日，郑州大学党委书记别荣海带队赴奇安信科技集团股份有限公司开展访企拓岗座谈交流。奇安信集团董事长齐向东，奇安信集团党委副书记、副总裁蒋虎，副总裁尹智清等集团领导，郑州大学副校长刘春太，以及双方相关单位负责同志参加座谈。

内蒙古呼和浩特城市网络安全运营中心正式启动

11 月 10 日，呼和浩特市公共数据资源开发利用启动大会召开，标志着呼和浩特市数字化发展踏上了转型升级新路径，开启了数据赋能经济社会发展的全新征程。在会上，由呼和浩特市大数据管理局与奇安信集团共同组建的呼和浩特城市网络安全运营中心宣布正式启动。

奇安信集团相关负责人介绍，在做好归集数据安全保障体系搭建的基础上，呼和浩特城市网络安全运营中心逐步向算力算网枢纽节点、终端安全、人工智能安全等领域拓展延伸，积极营造数据开发利用的良好生态，促进数字经济创新发展，更好地支撑首府经济社会高质量发展。

Windows 10 停服或致数亿计算机“裸奔” 奇安信提供多重应对方案

近日，微软公司正式宣布将于 2025 年 10 月 14 日终止对 Windows 10 系统的支持服务。对此，国内领先的网络安全公司奇安信第一时间宣布，将依托旗下天擎终端安全管理系统、天狗漏洞攻击防护系统等产品与体系化服务，为所有 Windows 10 用户，以及希望向信创平台迁移的用户，提供切换、升级、过渡等多场景的终端安全解决方案和安全运营

长效机制，妥善解决微软停服导致的安全问题。

揭示七大安全风险、提供治理路径，奇安信发布首个《政务大模型安全治理框架》

近日，奇安信集团发布《政务大模型安全治理框架》（以下简称《框架》）。该安全治理框架从政务大模型的应用趋势、安全风险、治理框架及管控措施四个方面，详细阐述了政务大模型安全治理方法。《框架》指出，训练合法、应用合规、运行可靠是政务大模型安全治理的三大目标。

《框架》指出，当前政务大模型主要面临七个主要安全风险，即数据安全风险、训练语料安全风险、使用安全风险、应用安全风险、软件供应链安全风险、生成内容风险、大模型自身风险。政府部门、大模型开发商、网络安全工作者，应该如何共同应对这种潜在的安全风险，正是《框架》提出的主要目的。

北京市政协副主席张家明带队走访调研奇安信集团

10月29日，北京市政协党组副书记、副主席张家明带队，赴奇安信集团走访调研，详细了解奇安信的生产经营状况、未来发展规划，听取企业诉求，协调推进“服务包”事项落实。

张家明指出，按照市委部署要求，今年再次走访奇安信集团，主要是了解“服务包”落实情况和企业的新需求。近年来，面对经济下行压力，奇安信集团积极作为、有效应对，展现了生机活力，为全市重大活动提供了网络安全保障。市有关部门和西城区、经开区要增强责任感和使命感，竭尽所能帮助企业解决实际困难。公司要加强与政府部门的沟通联系，立足北京加快发展，为新时代首都高质量发展多做贡献。

荣誉墙

AI 化大提速！奇安信多领域获权威机构“AI+ 安全”报告推荐

近日，全球领先的 IT 市场研究和咨询公司 IDC 正式发布了《生成式 AI 推动下的中国网络安全软件市场现状和技术发展趋势，2024》报告（Doc# CHC51928724，2024 年 11 月）（以下简称《IDC 报告》）。奇安信凭借在终端安全、网络检测与响应（NDR）、威胁情报、API 安全、零信任网络访问、态势感知等全系列产品 AI 化的突出表现，成为本次《IDC 报告》的代表厂商之一。

唯一网安企业！奇安信入选 Wind 中国上市公司“ESG 最佳实践 100 强”榜单

近日，知名金融信息服务商万得（Wind）发布“2024

年度 Wind 中国上市公司 ESG 最佳实践 100 强”榜单。凭借在环境、社会和治理方面的卓越表现，奇安信集团以信息技术行业最优的 AA 评级入选，并成为唯一登榜的网络安全企业。

奇安信入围 SASE 领域“青龙 · 综合领先型企业”

11 月 15 日，由云安全联盟大中华区（CSA GCR）主办的第八届云安全联盟大中华区大会在北京盛大开幕。奇安信作为 SASE 领域的重要贡献单位应邀出席本次大会，凭借在 SASE 领域的技术、产品、实践成果等多方面领先优势和市场影响力，被评为“SASE 神兽方阵 – 青龙 – 综合领先型企业”。该评估结果肯定了奇安信在 SASE 领域的专注投入，并在研发能力、产品成熟度、市场营收及知名度等方面为综合实力强的头部企业。

权威报告：奇安信安全咨询服务、托管安全服务稳居市场第一

全球领先的 IT 市场研究和咨询公司 IDC 近日发布了《2024 上半年中国安全服务市场跟踪报告》（简称《IDC 报告》）。奇安信在安全咨询服务、托管安全服务两大子市场均位居第一，进一步彰显了集团安全服务方面领先综合实力和市场地位。

奇安信入选 Gartner®《中国特权访问管理创新洞察》代表供应商

近日，国际市场研究与咨询机构 Gartner® 发布了

《中国特权访问管理创新洞察》（《Innovation Insight for Privileged Access Management in China》），剖析了特权访问管理工具的关键作用、技术演进并给出了实践建议。奇安信凭借特权账号管理系统（PAM）及配套解决方案，被评为国内特权访问管理领域的代表性供应商(Representative Providers)。

奇安信霸榜三甲，蝉联终端、数据、分析情报市场冠军

近日，全球领先的 IT 市场研究和咨询公司 IDC 发布《中国 IT 安全软件市场跟踪报告，2024H1》，深入分析了 2024 年上半年在数据安全软件、终端安全软件、身份和访问管理软件、软件安全网关、安全分析和情报、响应和编排软件等多个细分市场的表现情况。奇安信在终端安全、数据安全、安全分析与情报三大关键领域进一步强化了市场领导地位。

产品动态

奇安信中标某大型能源基础设施运营商工控网络安全项目

近日，奇安信集团中标某大型能源基础设施运营商地方公司工控网络安全项目，中标产品涵盖工业防火墙、工业网闸、工业安全监测与审计系统、工业主机安全防护系统等核心工业安全防护产品，是继不久前全系列工业安全产品中标特大型国有能源企业之后的又一显著成就，展现了奇安信保障能源关键信息基础设施行业网络安全的卓越实力。

奇安信中标某股份制银行 2024 网络安全实战防守项目

日前，奇安信集团中标某股份制银行 2024 网络安全实战防守项目。奇安信结合今年持续时间长、攻击强度大等实战攻防演习特点，为该银行提供涵盖前、中、后期的整体安

全防护体系，产品包括零信任、天眼、椒图等，全面提升其实战攻防水平。今年攻防演习期间，奇安信防守团队帮助客户多次检测到攻击队的网络钓鱼、口令破解以及漏洞利用等渗透行为，取得了优异的成绩，获得客户的高度认可。

首批、唯一网安企业！奇安信 QAX-GPT 安全机器人获公安部三所大模型安全认证

11 月 6 日，公安部网络安全等级保护评估中心对外发布了首批大模型系统安全能力验证结果。奇安信 QAX-GPT 安全机器人系统和浪潮、百度、腾讯等四家大模型系统率先通过测评，成为首批获得安全测评报告及“大模型系统安全能力评价证书”的企业，同时也是唯一一家通过此项测评的网络安全企业。


大模型系统安全能力评价证书

（证书编号：CSPEC-MHY24002）

委托单位名称：
奇安信科技集团股份有限公司

委托单位地址：
北京市西城区新街口外大街28号102号楼3层332号

任务号：
CSPEC-A24118

大模型系统名称：
奇安信QAX-GPT安全机器人系统

版本号：
V1.0

类别：
通用类☐ 行业类☑

评价依据：
T/ISEAA 005-2024《大模型系统安全保护要求》
T/ISEAA 006-2024《大模型系统安全测评要求》

评价结果：
奇安信QAX-GPT安全机器人系统安全能力达到 领先级☐ 成熟级☑ 基本级☐

备注：大模型系统安全能力评价结果详见编号为CSPEC-24118-Z001的测评报告。

颁证日期：2024年10月29日
有效期至：2025年10月28日

8624 万！奇安信中标中海油网络安全服务框架

奇安信集团中标中海油能源发展股份有限公司 2024—2027 年网络安全测试检查及系统保障服务框架，项目总额为 8624 万。该项目的中标，进一步凸显了奇安信在能源等关基行业网络安全服务的领先实力。2024 年以来，奇安信安全服务标杆项目不断，IDC 报告显示，奇安信在安全咨询服务、托管安全服务两大子市场均位居第一。

党政信创替代政策下沉，奇安信接连中标市镇信创网络准入项目

奇安信信创网络安全准入系统相继中标山东、广东等地地级市、乡 / 镇人民政府的网络安全建设项目，助力地方政府部门信创体系构建。在当前党政信创替代政策下沉的大背景下，展现了奇安信推动乡镇党政机关信创安全能力建设的巨大潜力。

近千万 奇安信中标中国联通 IT 域网络维护及安全服务项目

日前，奇安信成功中标 2024—2026 年中国联通软件研究院 IT 域网络维护及安全服务项目，凭借出色的技术实力和全面的服务体系，成为独家供应商，项目总价值接近千万元。除集团项目外，奇安信还广泛参与到各地联通公司的网络安全项目建设中，赢得了中国联通各级运营单位的高度认可与信赖。

奇安信发布上网行为管理系统 V10.2 显著提升合规监管能力

近期，奇安信对外正式发布了上网行为管理系统 10.2 版本，该产品继承原有产品近 20 年来的技术积累优势，尤其强化了 AI 能力，实现了从文本类文件的识别，转向音频、视频等富媒体内容信息识别及审计的跃迁，从而显著提升了合规监管能力，适应未来技术发展的方向。新版本提炼专属

功能，更加贴近客户的业务场景和细分需求，推出金融和教育等行业特定场景功能。

奇安信 QAX-GPT 安全机器人系统获评 2024 年大模型安全实践优秀案例

10 月 24 日，在中国电子信息产业发展研究院、中国软件评测中心（工业和信息化部软件与集成电路促进中心）主办的 2024 年数据安全关键技术研究及产业应用成果评价大会上，奇安信集团的“QAX-GPT 安全机器人系统”荣获“2024 年大模型安全实践优秀案例”，再次体现了业界对奇安信在大模型安全技术创新和应用实践成效方面的高度认可。

奇安信椒图云锁服务器安全管理系统升级新版本引入多项优势功能

日前，奇安信椒图云锁服务器安全管理系统发布 V8.0.8 新版本，引入了病毒修复、用户登录控制、防火墙进程规则、Bybass 等多项优势功能，并对主机管理功能设置、应用防护能力、Agent 资源管控、检测规则等 150 个功能点进行优化。此次升级，全面提升了产品整体的防护能力、管理能力，以及易用性、兼容性、竞测能力。

社会责任

奇安信集团获评“责任 100|CSR 中国教育榜”最佳责任企业品牌

近日，“责任 100|2024 年第八届 CSR 中国教育榜”获奖名单正式发布，奇安信集团凭借“补天漏洞响应平台校园活动”项目，获评最佳责任企业品牌，也是唯一上榜的网络安全企业。

通过旗下的补天漏洞响应平台，奇安信集团与全国多所高校展开深度合作，推出了“补天漏洞响应平台校园活动”。该项目旨在通过一系列校园活动，提升学生的网络安全意识和技术能力，培养一批具备高度专业素养的网络安全人才，为维护国家网络安全、促进经济社会稳定发展贡献力量。截至目前，“补天漏洞响应平台校园活动”已走进了全国近百所院校，组织了 122 场校园活动，覆盖校园白帽黑客 15000 余人。

| 精彩图集 |

奇安信
闪耀 2024 世界互联网大会，载誉而归

11 月 20 日 ~22 日，2024 世界互联网大会乌镇峰会隆重举行。奇安信集团载誉而归。

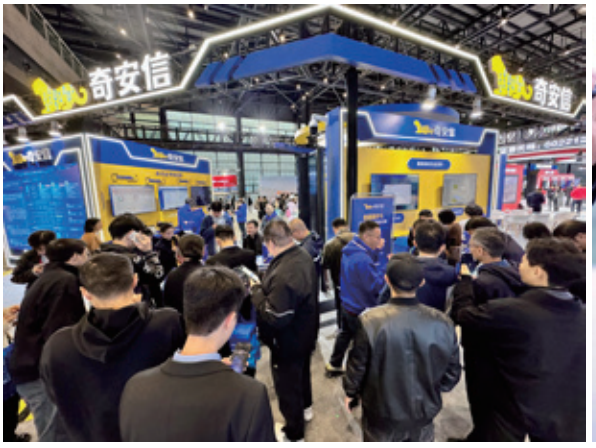
- 奇安信集团获世界互联网大会杰出贡献奖，全球仅有 14 家企业获此殊荣，这是对奇安信的高度认可！
- 奇安信 AISOC 获“新光产品奖”，在颁奖现场见证荣耀时刻。
- 奇安信集团董事长齐向东在网络安全技术发展与国际合作论坛、粤港澳大湾区国家发展论坛、智能交通论坛等分论坛作主题演讲。
- 在乌镇峰会期间，奇安信集团董事长齐向东接受了 50 余家媒体采访，展现了奇安信的风采。
- 世界互联网大会人工智能专业委员会成立，奇安信集团副总裁、人工智能研究院院长张勇获聘世界互联网大会人工智能专业委员会副主任委员。
- 乌镇峰会专业观展团参观奇安信展区、央视新闻报道奇安信乌镇峰会展台，奇安信展区成为焦点。


聘 书
LETTER OF APPOINTMENT

兹聘请 张 勇 先生担任世界互联网大会人工智能专业委员会副主任委员，聘期自 2024 年 11 月至 2027 年 11 月。

This letter is hereby granted to Mr. Zhang Yong for the appointment as Vice-Chair of the World Internet Conference Specialized Committee on Artificial Intelligence from November 2024 to November 2027.

世界互联网大会
WORLD INTERNET CONFERENCE
2024.11



分析：美国推进零信任建设的举措与启示

作者　虎符智库研究员 刘安

作为当前最受关注的新型网络安全防御理念，零信任强调“永不信任，始终验证”，是一种更加主动、预防性更强和更精细化的网络安全方法，能够更好地应对当前复杂和不断演变的网络威胁环境。

美国在推进零信任安全架构方面采取了一系列重要举措，这些措施涵盖了战略规划、技术实施和组织架构调整等多个方面。

一、战略规划

美零信任发展涉及多个层面的战略规划，是一个由概念提出到国家层面、政府部门、军方机构逐步采纳和推进的过程，其发展历程体现了对网络安全的高度重视和对现代化防御需求的响应。通过这些举措，美国旨在提升其网络安全防护能力，以应对日益复杂的网络威胁环境。

美零信任发展涉及多个层面的战略规划，是一个由概念提出到国家层面、政府部门、军方机构逐步采纳和推进的过程，其发展历程体现了对网络安全的高度重视和对现代化防御需求的响应。

（一）国家层面：拜登政府首次正式提出实施零信任

2021 年 5 月，拜登政府发布第 14028 号《改善国家网络安全》的行政命令，指示联邦政府各机构实施零信任方法，这是美政府首次正式提出实施零信任。该行政令是拜登政府上台以来签发的为数不多的网络安全总统令之一，反映了该届政府在网络安全管理领域的基本基调。

拜登政府认为渐进式改进难以满足保护国家和政府机构网络安全的需求，需要做出根本性的改变，因此，提出在联邦政府各机构实施零信任，要求联邦政府机构迁移到零信任架构，并实现基于云的基础设施安全优势，以降低相关网络风险。

该行政命令的核心在于推动联邦政府网络安全的现代化，特别是在关键基础设施和国家安全系统的保护上，推广基于零信任架构的云技术使用，鼓励联邦各机构负责人为云技术的部署和使用划拨资源，并给出完成系统向云端迁移的时间表；要求各机构尽可能采用零信任架构向云环境迁移原有系统，并在迁移过程中遵循相关的安全原则和指南。

OMB 发布《联邦零信任战略》，指导联邦各机构着手实施零信任。为响应并落实 2021 年拜登政府发布的《国家网络安全行政命令》，白宫管理和预算办公室（OMB）2022 年 1 月发布《联

邦零信任战略》，旨在推动联邦机构采用安全架构适应零信任原则。本战略以备忘录的方式发布，要求联邦各机构在2024年前实现相应的网络安全标准和目标，以加强美政府抵御日益复杂和持续的网络威胁的能力。

（二）部门层面：各部门分头行动，加速战略布局

美政府提出实施零信任以来，美国土安全部、商务部、白宫管理和预算办公室等紧随其后，陆续出台了指导和实施零信任的基本原则、战略规划、体系架构、模型指南等，加速完善美零信任战略布局。

NIST高频发布零信任架构相关文件，推动美网络安全防御方式加速向零信任过渡。2019年起，美商务部国家标准与技术研究院（NIST）先后发布《零信任架构第一版》草案、《零信任架构第二版》草案、《零信任架构》、《零信任架构实施规划指南》、《实施零信任架构》等多份规划指导文件，明确了零信任的核心原则、逻辑组件、部署模型和用例，强调了基于身份而非仅仅基于网络位置来实施安全控制的重要性，并提出了一套全面的零信任原则和参考架构，以实现动态的访问控制和资源保护，为美联邦机构和私营部门提供了一套全面的框架和指导，以实现更安全、更适应现代信息技术环境的网络安全策略。与国防部《零信任战略》相比，NIST发布的零信任相关文件更加强调技术，且更细化、更具体，是执行层面的指导文件。

国家安全局发布《拥抱零信任安全模型》，旨在提升国家和国防安全系统网络安全。2021年2月，国家安全局（NSA）发布零信任框架指南《拥抱零信任安全模型》，旨在识别国家安全系统、国防部及国防工业基础领域信息系统威胁，制定和发布相应的网络安全规范和缓解措施。作为美重要的情报机构，NSA在美网络空间安全领域扮演着极其重要的角色，负责保护国家安全系统，即敏感度较高的网络和系统，包括涉密信息系统。《拥抱零信任安全模型》是国家安全局对在国防网络及国家关键网络和系统实施零信任的明确表态，对建议在高敏感网络中应用零信任方面，具有很强的权威性。

（三）美军：零信任能力建设稳步推进

国防部发布《零信任战略》，制定长期战略目标，明确实施计划。2022年11月，国防部发布《零信任战略》，提出了全面实施零信任架构的计划和目标。早在2020年，国防信息系统局局长提出将发布初始零信任架构，并于2021年5月和2022年7月，先后发布《国防部零信任参考架构》的两个版本。经历近两年的完善与迭代，国防部最终发布的《零信任战略》战略围绕7个支柱，设定了45项独立能力，旨在构建可扩展、弹性、可审计和可防御的网络环境，其核心是为国防部的数据、应用程序、资产和服务（DAAS）提供安全保护。

《战略》计划于2027年前将国防部及各机构的所有信息系统全面过渡到零信任架构，确保国防部的信息企业在联合信息环境内，特别是国防部信息网络中的安全性和弹性。自《战略》发布以来，美军零信任能力建设稳步推进。

二、部署实施：多维推动

在部署实施层面，美从政策指南、预算投入、技术研发等多个维度推动零信任技术加速部署落地，全力推动实现国防部零信任战略目标。

（一）发布政策实施指南

2024年6月4日，美国防部首席信息官发布了《美国防部零信任覆盖》（Department of Defense Zero Trust Overlays）文件，作为零信任战略的路线图和实施指南，帮助国防部实现拜登总统签署的2021年网络安全行政命令中设定的目标。该文件是美国防部实现零信任战略的指南，旨在将整个美国防部实施零信任的方式标准化，同时指导系统架构师和授权官员开展零信任差距分析。

（二）稳步增加零信任国防预算

美国防部及各军种高度重视零信任技术发展，大幅投入预算资金，支持相关技术研发，推动网络安全防御过渡到零信任架构。2022年起，美在国防预算开始单列“零信任”预算，2022—2025财年，国防部为零信任投入的预算分别为：8.59亿美元、10.06亿美元、11.56亿美元、12.77亿美元，主要用于身份、认证和访问管理（ICAM）、合规性连接（C2C）、零信任架构迁移等。此外，美陆军在2024财年预算中，投入4.39亿美元，用于加速推进零信任网络安全建设。

（三）攻关核心技术

零信任架构的研发与部署涉及身份认证与访问管理（ICAM）、微隔离和软件定义边界（SDP）、自动化编排、数据安全、可视化和分析等关键技术，这些技术作为零信任架构的重点技术，受到美政府、国防部及军方的高度重

视。

一是 ICAM 技术作为零信任的基石，是美国实施零信任架构的重要组成。美国防部在 2022 财年投资了 2.44 亿美元用于发展 ICAM 相关技术，以实现对“任意时间、任意位置、任意人员”的最低权限管理控制，是向零信任架构迈进的重要举措之一。

二是微隔离技术，在零信任的 7 大支柱中，“网络与环境”支柱特别强调使用细粒度访问和策略限制对内外部网络 / 环境进行物理或逻辑分段、隔离和控制，直接涉及微隔离技术的实施。此外，微隔离技术遵循零信任的核心原则，即“最低权限”，不再划分网络边界，默认所有行动均不可信，限制未经用户在网络内部横向移动，有效保护数据安全。

三是零信任原型系统“雷霆穹顶”投入生产。“雷霆穹顶”项目是美军零信任安全试点项目，由美国防信息系统局（DISA）牵头。该项目通过构建零信任原型积累系统迁移经验，为零信任推广树立示范应用。

三、机构设置

美国在推进零信任架构的过程中，成立了多个专门机构负责相关的战略规划、实施和监督工作，统筹推进零信任部署和迁移。一是成立零信任行动小组。2020 年，美国土安全部成立零信任行动小组，主要任务是推行零信任工作计划，以提升联邦政府的网络安全水平。零信任行动小组的成立是为了落实一系列战略举措，包括培育零信任防御理念，加速零信任技术发展，赋能零信任工作。此外，零信任行动小组还负责协调资源分配的优先顺序，并通过多个行动方案加快零信任理念的落地。

二是成立零信任投资组合管理办公室。2022 年 1 月，美国防部成立零信任投资组合办公室，负责协调和加速整个国防部范围内零信任的采用和执行，还负责制定战略指导、协调工作，并优先分配资源以推动零信任的实施。该办公室的成立对国防部实施《零信任战略》具有重要意义，一方面，确保零信任原则在整个国防部得到统一实施，并确保所有相关工作与零信任战略保持一致；另一方面，确保零信任能力和活动在战略目标期限内顺利部署落实，并统筹零信任技术和解决方案集成，以构建以数据为中心的安全防护架构。

美国在推进零信任架构的过程中，
成立了多个专门机构负责相关的战略规划、
实施和监督工作，
统筹推进零信任部署和迁移。

四、影响与启示

美统筹谋划、加紧布局零信任战略规划和落地，此举深刻地颠覆了传统的网络安全防御理念，引领了新一代网络安全防御范式的新潮，其经验和做法值得借鉴和关注。

一是引入下一代网络安全防御架构，彻底转变传统防御方式，我应积极布局，紧跟变化。我应紧跟形势变化，积极布局零信任技术发展与实践推广，积极谋划战略布局，培育新型人才，加快技术创新，更好地应对日益复杂的网络安全挑战，保护关键信息基础设施，促进数字经济健康发展。

二是促进技术发展跨部门管理相结合，有效推动零信任架构落地实施，我应探索特色发展模式，提高参与意识。我应探索适合我国的零信任发展模式，加强顶层规划，转变防御理念，鼓励企业和研究机构加大对零信任核心技术的研发投入，推动零信任产品和解决方案的创新。在关键行业和领域开展零信任试点项目，通过实践验证零信任的有效性，并逐步推广到更广泛的应用场景中。

三是实施零信任是美实现国防数字战略现代化的需求，是美基于顶层设计的网络安全宏观布局，我应加强自主可控网络安全体系建设，应对大国竞争压力。美零信任建设的推进也启示我需要加强自主可控的网络安全体系建设，在数字化转型的浪潮下，解决企业传统安全架构面临的挑战，有效应对企业数字化转型过程中的安全痛点，提升企业 IT 架构的安全性，筑牢整体安全防御底线，以应对日益复杂的网络威胁和潜在的大国竞争压力。

多因素认证不再万能，如何守护网安第一道防线?

作者 邱燕娜

今年 2 月，香港一名金融工作人员被使用深度伪造技术冒充公司首席财务官的诈骗者支付了 2500 万美金，尽管这个工作人员还通过视频通话做了“确认”……

随着网络威胁的日益复杂，类似这样的身份伪造案例越来越多，曾经被认为万能的 MFA（多因素认证）已经难再应对。供应商和政府机构都在警告公司，当前很多情况下，MFA 系统是无效且容易受到攻击的。英国国家网络安全中心近日就建议企业要改变对 MFA 的看法，不应将 MFA 视为一劳永逸的安全措施，因为攻击者能像拦截密码一样拦截 MFA 密钥。

如果 MFA 的魔法失灵了，那我们该怎么处理身份认证呢?

MFA 不可承受之重

身份认证被认为是网络安全的第一道防线，确保只有授权的用户能够访问敏感数据和资源，从而防止未经授权的访问和数据泄露。

近年来，网络攻击日益烦杂，传统的身份认证方法如密码已难以提供足够的保护。Verizon 的一项研究发现，80% 的数据泄露事件涉及弱密码或被盗凭证，凸显了强化身份认证的重要性。为应对这一挑战，多因素认证开始广泛应用于企业和关键基础设施。美国网络安全与基础设施安全局 (CISA) 将 MFA 列为基本网络安全防护措施之一。

多因素认证通过结合两种或多种独立凭证来验证用户身份，为身份认证提供额外的安全层，旨在防止未经授权的访问。微软 2020 年的数据显示，启用 MFA 可以阻止 99.9% 的账户入侵尝试。缺乏 MFA 保护已经成为很多网络攻击的目标。

然而，MFA 并非万无一失。攻击者一直在寻找新的方法来破坏 MFA。英国国家网络安全中心（NCSC）指出，社会工程技术已被用来破坏 MFA，并观察到针对启用 MFA 账户的攻击在过去几年中呈上升趋势。

Uber 在 2022 年遭遇了一起针对 MFA 的严重网络安全事件。攻击者通过向员工发送虚假的 MFA 通知，结合社会工程学手段，诱骗其点击恶意链接并输入凭证，最终获得了内部系统的访问权限。可见，即使启用了 MFA，员工的安全意识薄弱也可能导致身份认证被破坏。

除了社会工程攻击，MFA 还面临其他局限性。传统的基于短信的 MFA 容易受到 SIM 卡交换攻击和 SS7 漏洞的影响。推送通知也可能被用户误认为是垃圾信息而忽略。此外，MFA 的实施与管理可能带来额外的复杂性和成本，特别是对于拥有众多用户和遗留系统的大型企业而言。

正如 NCSC 所建议的那样，企业需要重新审视其 MFA 策略；不能将 MFA 视为一劳永逸的解决方案，而应

根据组织的特点和风险状况，选择合适的身份认证方式。

总而言之，随着网络威胁的不断演进，MFA 等传统身份认证方法已经难以应对日益复杂的网络威胁，企业需要采用更先进、多层次的认证手段。

可验证凭证网络（VCN）有望重塑数字身份管理的格局

未来，身份认证技术将朝着更加智能、无缝、安全的方向发展。

零信任安全模型的兴起预示着身份认证的重要性将进一步提升。与传统的基于边界的安全模型不同，零信任要求对每个用户和设备进行持续的身份验证和授权，确保只有受信任的实体才能访问网络资源。在零信任架构下，身份认证不再是一次性的行为，而是贯穿整个访问生命周期的动态过程。

同时，身份认证也将变得更加无缝和透明。随着人工智能和生物识别技术的进步，未来的身份认证将能够在不影响用户体验的情况下提供更高的安全性。连续身份认证和隐形认证等新兴技术可以持续监测用户行为和环境因素，实现实时风险评估和动态访问控制。用户无需频繁输入密码或进行显式认证，系统会根据用户的行为模式和上下文信息，自动判断其身份的可信度。

此外，身份认证的互操作性和标准化也将成为重要趋势。随着企业 IT 环境日益烦杂，不同的身份认证系统需要实现无缝集成和互通，一方面可以最大限度地降低与跨各种平台存储多个凭证相关的风险，另一方面还可以减少数据泄露和身份盗用的漏洞。身份联盟和联合身份管理可以允许用户使用一个身份凭证访问多个应用程序和服务，简化身份管理流程。跨域身份认证和单点登录技术则可以实现跨组织、跨平台的身份共享与协作。

然而，构建未来的身份认证生态也面临诸多挑战。隐私保护和数据安全始终是备受关注的问题。用户的生物识别数据和行为信息属于高度敏感的个人数据，一旦泄露或滥用，后果不堪设想。因此，在采用新的身份认证技术时，必须严格遵守隐私法规，并采取强有力的数据保护措施。

值得一提的是，可验证凭证网络（Verifiable Credentials Networks，VCN）可能会在这种背景下兴起。VCN 是一种去中心化的系统，通过提供去中心化的凭证发行、存储和验证框架，增强用户控制、隐私和安全性，同时降低欺诈风险。其中，可验证凭证（VC）是一种标准化的方式，用于数字化表示和共享身份信息，旨在安全、防篡改并易于验证。VC 使用加密方法确保其中包含的信息可以被信任，并且第三方无需直接联系发行者即可进行验证。VCN 代表了一种变革性的数字身份管理方法，使个人能够安全、私密地控制和分享自己的个人信息。这种方法符合日益增长的隐私问题和法规要求。

有观点认为，VCN 有望重塑数字身份管理的格局，使其更加高效、安全和以用户为中心。当前，Badge 和 Cisco Duo 等合作伙伴专注于通过可验证凭证实现无密码注册，让用户能够通过生物识别进行身份验证，无需传统的 MFA 方法，如令牌或重复的身份验证。

与此同时，多因素认证（MFA）与可验证凭证（VC）网络的融合正在成为增强数字安全的重要趋势。这种融合利用了两种技术的优势，提供强大的身份验证和访问控制机制，不但能够显著降低未授权访问的风险，比如说，用户可能需要提供一个 VC 并完成一 个 MFA 验证才能访问敏感信息或服务；还能简化用户体验：一旦用户的身份通过 VC 验证，他们可选择干扰较小的 MFA 方法进行身份验证，如生物识别验证或推送通知。

在网络威胁不断演变的背景下，企业需要与时俱进，积极拥抱创新技术，构建多层次、动态适应的身份认证体系。同时，身份认证的未来也离不开各方的通力合作。产业界、学术界、政府等不同主体应通力合作，携手推动身份认证相关标准和规范的建立，加强跨域互信与协作。

关于作者

邱燕娜

安全牛安全研究员，安全牛是中国网络安全领域的专业媒体和旗舰智库，精确定位并服务于 CISO/CSO/CTO/CIO 决策者人群，向国内企业的决策管理者及 IT 专业人士提供独立客观、高品质、有价值的战略性网络安全内容。

以人为本的网络安全：将人的因素融入网络安全设计

作者　罗伯特 · 莱莫斯

如何推动“以人为本的网络安全”，以提高安全产品和服务的可用性和有效性。

许多安全团队往往将非安全领域的同事视为安全计划中的潜在薄弱环节，认为他们难免决策不当。安全团队会引入技术手段，减轻不当决策带来的影响。这种观点不难理解：Verizon 发布的《数据泄露调查报告》显示，2023 年有 68% 的安全漏洞与“人为因素”有关，而在 2022 年这一比例高达 74%。

然而，“单纯依靠技术补救不当决策”的方法，正在让那些期望提升网络安全的公司感到失望。在美国国家标准与技术研究院（NIST）发布的名为《用户并不愚蠢》的手册中，NIST 提醒组织，糟糕的可用性设计、过度叠加的安全措施以及忽视用户反馈反而会制造出内部威胁。

相反，组织应采取以人为本的网络安全（HCC）方法，重点关注基于用户需求和动机的流程与产品设计，并通过激励机制引导用户实施安全行为。HCC 项目通常包括安全意识培训、反网络钓鱼课程、为安全产品增加用户反馈渠道，并力求减少普通员工在安全方面承担的责任。HCC 方法中至关重要的工具包括安全监控及用户 / 实体行为分析（UEBA）。

NIST 信息技术实验室 HCC 项目负责人 Julie Haney 强调，HCC 不仅仅是寻求以用户为中心或友好的安全产品。Haney 表示：“在设计和实施安全措施时，真正重要的是将人放在首位。如果网络安全方案没有以人为中心，忽视了用户的实际需求，最终得到的安全解决方案将无法使用——这样反而更容易让人犯错或做出冒险决策，甚至为了应付任务而选择不那么安全的替代方案。”

2024 年 10 月，NIST 推出了“以人为中心的网络安全利益社区”（COI），旨在汇集从业者、学者和政策制定者，共同探讨如何使安全更高效、更贴近用户需求。

网络安全应赋能于人

关注人性化安全设计的并不止是政府机构，越来越多的企业安全团队也开始重视 HCC。根据研究机构 Gartner 的预测，到 2027 年，半数大型企业的首席信息安全官（CISO）将采用以人为本的实践和设计来提升网络安全。实际上，Gartner 在 2023 年将以人为本的安全设计列为顶级网络安全趋势之

> 网络安全方案在设计和实施时，
> 真正重要的是将人放在首位。
> 如果没有以人为中心，忽视用户实际需求，
> 最终得到的安全解决方案将无法使用。

一。该公司在今年略微调整了命名，但仍然将“安全行为与文化项目”（SBCP）视为 2024 年顶级网络安全趋势之一。

Gartner 高级首席分析师 Victoria Cason 指出，安全团队需要停止对员工说教，而是与之建立对话，共同创造以网络安全为核心的文化。

她表示：“采用以人为本的方法意味着我们面对的不是冰冷的机器，而是拥有不同行为、需求和动机的个体。我们需要努力解决他们在最佳安全实践上的需求、愿望和行为，而不仅仅是告诉他们该做什么。”

Gartner 认为，SBCP 的实施步骤包括威胁模拟、自动化与数据分析的引入，以帮助用户做出安全决策，鼓励员工报告潜在安全事件，以及通过跟踪指标展示 SBCP 的效果。根据 Gartner 的数据，近一半实施 SBCP 的公司已经采取了所有这些步骤。

减少网络安全中的摩擦不仅可以改善公司的安全状况，还能减轻传统对抗性工作模式带来的压力。Gartner 预测，2023 年至 2025 年间，半数网络安全领导者将更换工作，其中四分之一将完全离开这个行业，原因是过大的工作压力。

HCC：相关工作正在持续推进

目前，HCC 还没有一个标准化的定义，这也是 NIST 推动进一步研究的原因之一，目的是帮助企业更好地支持员工的安全意识和成长。HCC 的核心包括员工对网络安全的态度、他们接受的培训、安全产品的易用性及政策的制定。

2023 年 12 月，拜登政府发布了最新的《联邦网络安全研究与发展计划》，将 HCC 确定为国家安全保护的重点任务之一。该计划强调的一个研究方向是开发模型，以评估数字技术的影响并验证其安全属性。

计划指出：“有必要减少网络安全要求对个人、组织、社区和社会造成的负担，并改善数字技术和系统的可用性与用户体验。以人为本的计算研究表明，若在设计和开发的早期阶段融入终端用户的需求，能创造出更加可用的系统，提升用户体验。”

Gartner 提出了实施 SBCP 的独特方法，称之为 PIPE 框架，四个字母分别代表实践、影响、平台和推动因素。

Victoria Cason 表示：“大多数传统的安全意识项目只依赖于年度或季度的培训，但这并不能触及行为背后的根本原因。因此，我们需要超越传统的计算机培训和网络钓鱼模拟，利用现有的工具与能力，如身份与访问管理（IAM）和安全监控，甚至是 AI 等新兴工具，以提升用户的参与度与效率。”

根据商业情报公司 Forrester 的说法，HCC 的一个关键发展方向可能是“人类风险管理”，这是一种安全意识与培训市场的演进模式，加入了自适应的人类保护机制。Forrester 在 2 月份发布的一份报告中指出，与那些流于形式的安全培训项目不同，人类风险管理专注于积极教育员工，并有效减少其行为带来的安全风险。

员工确实关心网络安全

大多数员工都意识到自己在保护业务安全中的重要作用。他们担心自己可能成为下一次泄露的突破口。根据安永咨询公司对 1000 名员工的调查，约三分之一（34%）的员工担心自己可能会因某些行为而将组织置于风险之中。

Julie Haney 表示，公司应与这些员工合作，找到将担忧转化为积极行动的方式，而不是在出现问题时对他们进行指责。

她说：“如果有人点击了网络钓鱼链接，组织往往将所有责任推给员工，但并没有真正回顾公司内部之前可能存在的程序、流程或人员问题。这不仅仅是最终执行操作的那个人犯的错——往往在此之前已经有很多环节出现了问题。”

网络安全专业人员应努力培养一种文化，摒弃将用户视为敌人或薄弱环节的心态。与用户对话可以发现安全措施中的漏洞，而赋予用户报告问题的权利，则能加速问题的早期检测。

最后，随着类似于人类风险分析服务的产品出现，公司在采用这些工具时应持谨慎态度，并设定合理的期望。Julie Haney 指出，虽然追踪经常犯错的用户可能有用，但不应带有惩罚性；相反，这种方法应为安全团队提供程序问题的信息，并为额外培训提供可能性。

她总结道：“数据确实很有价值，但你必须谨慎，避免给人贴上‘坏员工’的标签，不要轻易断定某人不擅长安全，而另一个人擅长安全。这是一条需要小心走好的平衡线。”安

关于作者

罗伯特 · 莱莫斯

资深科技记者，从业超过 20 年，前研究工程师，为二十多家出版物撰稿。

网安26号院

SECURITY INSIDER

征稿启事

当下，网络空间态势日趋严峻，关基设施成为重要攻击目标，因网络攻击导致的系统瘫痪、数据泄露现象频发。网络安全建设和运营需时刻因应形势变化进行创新。分享行业趋势、交流建设与运营之道成为提升安全防护水平的重要途径。

为此，奇安信《网安 26 号院》联合虎符智库、安全内参联合征稿。具体要求如下：

一、征稿对象：

投稿人为政企网络安全负责人、从业者，以及研究人员。

二、征稿时间：

本次活动活动长期有效。

三、征稿要求：

投稿论文应为投稿人原创，且尚未被任何期刊接受或发表。投稿人应对所投稿件的著作权及其他法律责任负责。

四、稿件说明：

来稿主题包括但不限于网络安全合规解读、网络攻防态势分析、网络安全建设经验、安全运营最佳实践，创新安全技术及应用等网络安全领域相关的议题。

稿件字数（含注释）原则上应控制在 4000 ~ 8000 字。

五、评选及奖励：

来稿经专家组评审入选刊登后，即获得相应的稿费（不低于 2000 元人民币）。

优秀获奖作者将有机会受邀参加 “BCS 北京网络安全大会”，发表主题演讲并分享研究心得。

六、其他荣誉：

长期供稿作者可以获聘“虎符智库”专家，授予聘书和徽章。

七、投稿方式：

投稿以附件形式通过电子邮件
发送至 lijianping@qianxin.com;
或者微信添加 security4 咨询联系。

扫码咨询

奇安信连续四年位居“中国网安产业竞争力50强”第一名

9月6日，中国网络安全产业联盟（CCIA）
公布“2024年中国网安产业竞争力50强”榜单，
凭借扎实的技术实力和领先的市场表现，
奇安信连续四年高居榜单第一名。

“2024年中国网安产业竞争力50强”榜单

TOP15	公司名称
1	**奇安信科技集团股份有限公司**
2	启明星辰信息技术集团股份有限公司
3	深信服科技股份有限公司
4	华为技术有限公司
5	天融信科技集团股份有限公司
6	新华三信息安全技术有限公司
7	杭州安恒信息技术股份有限公司
8	亚信安全科技股份有限公司
9	绿盟科技集团股份有限公司
10	三六零安全科技股份有限公司
11	天翼安全科技有限公司
12	中电科网络安全科技股份有限公司
13	杭州迪普科技股份有限公司
14	北京山石网科信息技术有限公司
15	中孚信息股份有限公司