2023
网信自主创新调研报告

网信自主创新调研报告编委会

2024年4月

2023 网信自主创新调研报告

网信自主创新调研报告编委会

2024 年 4 月

版权声明

免责声明

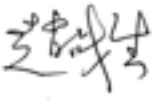
排　　版：伊敏娜
校　　对：李　雪
开　　本：720 X 980　1/16
版　　次：2024 年 4 月第 1 版
印　　次：2024 年 4 月第 1 次印刷
本报告咨询联系方式：cii_zgc@163.com

刊首语

《2023 网信自主调研报告》是在我们十四五规划的关键一年出台的。这一年我们终于走出了三年抗疫斗争的环境，克服了各方面的困难，为取得更大的进步努力奋斗！今年的调研报告，更多的反映了自主创新成果应用推广面临的现状和桃战，可以说更加注重脚踏实地，稳步推进。我希望大家认真体会我们网信创新一线同行们的心声，从中找到对各自有益的信息、数据和思考。预祝 2023 网信自主创新调研报告发布成功！

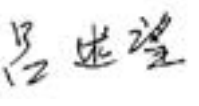
——中国计算机学会计算机安全专委会主任　严明

信息技术研发打牢的基础，促成了信息化的蓬勃发展，催生出五彩缤纷的新质生产力的丰硕硕果和预期遐想。信息系统和网络生态构成了承载新质生产力的重要基础平台。信息安全是保障新质生产力效率效益，国家主权不受制于人的战略要务。习主席在发展新质生产力的学习会上，再次提出了“自主可控，安全可靠”的明确要求。每年的网信自主创新调研报告反映了我们的新进步。《2023 网信自主创新调研报告》又给我们带来了可喜的发展，可以看到，我们从“缺芯少魂”发展到了“强芯壮魂”。但魂要附体，芯要归位才能发挥“自主可控，安全可靠”的最高使命。让我们继续努力，用我们的智慧，把自主的系统，自主的网路为新质生产力的需求应用搭建起来，运作起来。为新百年强国梦的早日实现建新功，创新业。



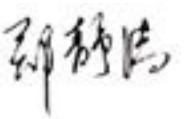
——中国科学院大学教授　赵战生

落实网空主权和不受制于人的原则，深化网信自主创新工作，机遇和风险挑战并存。《2023 网信自主创新调研报告》比较全面系统地分析了当前各个产业节点的现状、问题，并提出了对策。相信对于网信工作者聚焦新质生产力、扎实推进高质量发展有所帮助。



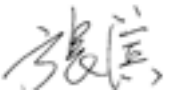
——中科院信息安全国家重点实验室教授　吕述望

2023年是深化自主创新成果拓展应用领域，攻关爬坡取得重要进展的一年。《2023网信自主创新调研报告》站在所涉及的各个产业节点和创新成果推广应用的视角，研究分析了当前网信产业的现状和面临的问题，并提出了相应的对策和建议。对进一步深化自主创新成果的应用推广、推动我国网信事业的高质量发展，极具参考价值。



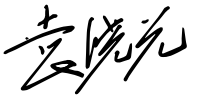
——公安部网络安全保卫局原副巡视员　郑静清

新质生产力是当前和今后一个时期的重要话题，自主创新水平直接反映出新质生产力的质效。《2023网信自主创新调研报告》从应用出发，用案例和数据，展示了自主创新在推动产业升级、提升国际竞争力等方面的积极作用，针对性提出了加强政策引导、优化创新环境等多项推进建议，有利于激发创新活力，促进网信产业繁荣发展。



——中国移动通信有限公司研究院党委书记　张滨

《2023网信自主创新调研报告》系统性地对国内网信产业链进行了总结和分析，在肯定成绩的同时，直面存在的问题。面向未来，加快发展网信领域的新质生产力，扎实推进网信产业的高质量发展，把握科技创新这一要素，构建正向产业生态，依然面临巨大挑战！



——航天科工集团二院网信产业总指挥　袁晓光

《2023网信自主创新调研报告》客观、真实地展现了几年来网信自主创新的成果，分析了当前面临的痛点、难点问题及其成因，并提出了破解困局的建议和路径，为营造自主创新的产业链和生态圈提供了极具价值的参考资料，对新质生产力的形成具有重要的现实意义。

——北京航天情报与信息研究所党委书记　吴锋

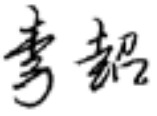
网信创新是实现网络强国，数字经济战略的基础，调研报告六年持续跟踪，据实调查，科学分析，这为网信领域的各专题创新提供了有益的指导，同时为相关部门对网信创新的管理决策提供了有力支持。

——中国网络安全审查认证和市场监管大数据中心原首席专家　张剑

《2023 网信自主创新调研报告》充分反映了近年来我国信创产业取得的成果：产品技术取得不断突破，产业生态实现日趋完善，行业应用得到良好发展。祝愿在产学研用各界的共同努力下，在市场参与主体的通力合作下，信创将迎来更加广阔的未来。

——国家信息技术安全研究中心原副主任　李冰

《2023 网信自主创新调研报告》较全面地梳理了产业界在网信自主创新以及成果落地过程中遇到的问题，积极思索了问题的原因和对策措施，可以作为有关主管部门和产业界从各自层面深入推进网信自主创新工作的重要参考，尤其是产业界加强协作协同标准化和生态建设的呼吁应得到大家的积极响应。



——北京计算机技术及应用研究所技术总监　李超

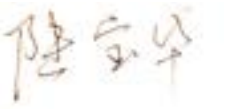
网信自主创新调研报告的编写工作持续开展了六年，取得了大量来自产业一线的数据，对于不断深化自主创新有很好的支撑作用。2023 年的报告从行业应用的角度展示了新进展、分析了新问题，对于供给侧和需求侧都有参考价值。

——贵州大数据安全工程研究中心主任　杜跃进

《2023 网信自主创新调研报告》如约而至。2024 年，国家将从顶层设计思路，统筹工作方向，安全合规管理等方面，进一步强化数据安全体系。过去的一年中，我们在信息技术创新上取得了长足的进步。实现了关键核心技术与产品的自主可控，积累了丰富的经验。阅读本报告可以给大家带来有益的借鉴和参考！

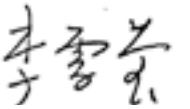
——中国智能终端操作系统产业联盟秘书长　曹冬

网信自主创新是国之大事，网信也是新质生产力的重要组成部分。核心技术、关键产品，买是买不来的，必须立足于我们自己的力量。报告多年以来一直在强力推动，并且取得了可喜的成绩，是这个领域中不可多得的精品荟萃。



——青海省委科技顾问　陆宝华

《2023 网信自主创新调研报告》以“进一步深化自主创新”为主题，聚焦国产化软硬件、安全产业创新等领域，从产品侧、用户侧、行业应用等多角度挖掘分析，客观、清晰、准确的反映各企业所在领域的创新活动以及遇到的问题。报告对产业发展提供了十分重要的参考价值。为推进我国网信自主创新贡献了力量，进一步赋能数字经济安全发展。

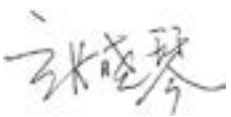


——天融信科技集团董事长兼 CEO　李雪莹

《2023 网信自主创新调研报告》积极探索自主创新发展新模式，申威有幸与之并肩六年，深刻认识到自主创新的重要性与必要性，报告作为极具参考价值的资料为行业发展启明方向，引领伙伴们携手将网信自主创新之路进行到底。

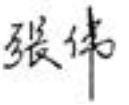
——中电科申泰信息科技有限公司总经理　周昱

在数字化浪潮席卷全球的大背景下，《2023 网信自主创新调研报告》应运而生。这次的报告紧扣“进一步深化自主创新”主题，以行业应用为切入点，深入剖析了我国网信自主创新的现状、成因及应对策略，内容丰富、数据翔实、分析透彻，充分展示了我们对国家网信自主创新能力的坚定信念。报告对网信自主创新产品规划与设计具有较高参考价值，也为我们指明了前进的方向和路径。



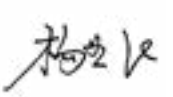
——重庆市信息通信咨询设计院党委书记、总经理　张晓琴

《2023 网信自主创新调研报告》作为业内具有卓越影响力和口碑的报告，一如既往立足信创事业根本，以务实的风格，从信创产业的芯、魂着手，关注芯片、操作系统、数据库、部件、整机、应用、安全、供应链等元素，紧抓当前信创热点、难点及客户侧、产业侧诉求，客观反映从业者关切的问题，以发现问题、分析问题、解决问题的逻辑思路，为阅读者提供高质量的参考和指导。相信报告会为信创产业发展提供助力。



——同方计算机信创业务集团总经理　张伟

《2023 网信自主创新调研报告》深入分析了网信行业创新发展的前景，汇聚了丰富的前沿产业信息，并基于这些数据提出了极具价值的见解和建议，为推动网信核心技术领域的自主创新提供了重要的指导和参考。对于致力于推动网信产业发展和技术革新的参与者和行业引领者而言，这份报告是一份不可多得、极富价值的文献。



——深圳大普微电子股份有限公司 CEO　杨亚飞

《2023 网信自主创新调研报告》是一份具有里程碑意义的研究成果，深入剖析了自主创新领域的现状和面临的挑战。通过对行业发展趋势和政策环境的深入分析，报告准确把握了当前自主创新的关键问题，并提出了一系列切实可行的对策建议。这份报告的发布将有力推动自主创新领域的持续发展，为行业发展注入新的活力和动力。

——江苏云涌电子科技股份有限公司董事长　高南

《2023 网信自主创新调研报告》从技术创新、产品创新、工程创新、应用创新等不同角度集中展示了基础软硬件、应用软件和网络安全等方面的创新成果，尤其是对国产芯片、数据存储、信息安全等领域的产品需求、技术研发、产业生态高质量发展具有重要借鉴意义和引领作用。

——英韧科技股份有限公司总经理　刘刚

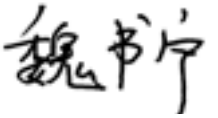
自主创新是企业的生命，是企业发展壮大的根本，是国家新质生产力的发展基石。《2023 网信自主创新调研报告》作为网信领域的权威报告，集中反映了我国当前网信技术的自主创新情况，为企业自主技术创新规划提供参照，为政策制定者在产业体系谋篇布局提供参考。

——第五空间信息科技研究院院长　谈剑锋

《2023 网信自主创新调研报告》编委会连续 6 年组织开展脚踏实地的调研工作，取得了大量来自产业一线的数据，形成了非常有价值的观点和建议。我们东方通也一路见证和陪伴了报告的成长。报告站在不同的产业节点，内容丰富、观点明确，记录了中间件等基础软硬件多年的创新成果、产业难点、对策与期许，对基础软件的创新发展有较高的参考价值。

——北京东方通科技股份有限公司董事、副总经理　李利军

《2023 网信自主创新调研报告》如约而至，本次报告以“进一步深化自主创新”为主题，全面解读网信领域在技术、产品、应用等各方面的现状、特点、趋势，内容丰富，视角前瞻。其中，基础软件是信息社会的核心基础设施，国产基础软件的发展则是实现网信领域自主创新的战略基石，对于确保国家信息安全、增强国家战略竞争力、推动产业升级和技术进步等方面具有深远的意义和价值。因此，各行业企业都应该进一步提升对软件质量及安全的关注和要求，《2023 网信自主创新调研报告》具有重要的参考价值。

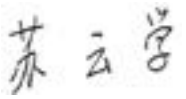


——湖南泛联新安信息科技有限公司董事长　魏书宁

新质生产力在我们信息产业领域，意味着要构筑一个自主可控的坚实基础，涵盖CPU、GPU、操作系统等核心技术的自主化。这既是一项艰巨的任务，也是一次意义深远的机遇。《2023网信自主创新调研报告》以“进一步深化自主创新”为主题，对发展新质生产力有较高的参考价值。

——龙芯中科技术股份有限公司副总裁　张戈

《2023网信自主创新调研报告》围绕“进一步深化自主创新”的主题，对产业各个领域均做了深入调研，展现了自主创新成就，增强了科技自信，分析了当前的机遇与挑战并提出了建设性的建议。“调查就是解决问题”，本报告对行业发展具有很强的指导性，对从业者具有很高的参考价值。



——山东华翼微电子技术股份有限公司副总经理　苏云学

主要编写单位（按拼音排序）

安天科技集团股份有限公司
安芯网盾（北京）科技有限公司
百信信息技术有限公司
北京安普诺信息技术有限公司
北京安御道合科技有限公司
北京安天网络安全技术有限公司
北京长擎软件有限公司
北京辰光融信技术有限公司
北京东方通科技股份有限公司
北京得意音通技术有限责任公司
北京海泰方圆科技股份有限公司
北京惠而特科技有限公司
北京计算机技术及应用研究所
北京金山办公软件股份有限公司
北京久安世纪科技有限公司
北京凯思昊鹏软件工程技术有限公司
北京可信华泰信息技术有限公司
北京炼石网络技术有限公司
北京珞安科技有限责任公司
北京启明星辰信息安全技术有限公司
北京人大金仓信息技术股份有限公司
北京赛博云帆教育科技有限公司
北京山石网科信息技术有限公司
北京神州绿盟科技有限公司
北京时代亿信科技股份有限公司
北京数盾信息科技有限公司
北京天融信网络安全技术有限公司
北京万里开源软件有限公司
北京网迅科技有限公司
北京网御星云信息技术有限公司
北京小佑网络科技有限公司
北京信安世纪科技股份有限公司
北京亦心科技有限公司
北京优炫软件股份有限公司
北京云起无垠科技有限公司
北京中关村通力科技服务有限责任公司
北京众人数安科技有限公司
长扬科技（北京）股份有限公司
成都储迅科技有限公司
重庆市信息通信咨询设计院有限公司
广东中科实数科技有限公司
哈尔滨安澜科技有限公司
杭州安恒信息技术股份有限公司
杭州孝道科技有限公司
杭州亿格云科技有限公司
湖南泛联新安信息科技有限公司
湖南麒麟信安科技股份有限公司
江南信安（北京）科技有限公司
江苏云涌电子科技股份有限公司
精壹致远（武汉）信息技术有限公司

科来网络技术股份有限公司
凯云联创（北京）科技有限公司
昆仑太科（北京）技术股份有限公司
龙芯中科技术股份有限公司
南京南瑞信息通信科技有限公司
普华基础软件股份有限公司
麒麟软件有限公司
三六零数字安全科技集团有限公司
三未信安科技股份有限公司
山东华翼微电子技术股份有限公司
山石网科通信技术股份有限公司
上海上讯信息技术股份有限公司
上海碳泽信息科技有限公司
上海众人智能科技有限公司
深圳大普微电子股份有限公司
深圳市金蝶天燕云计算股份有限公司
四川航天七零六信息科技有限公司
腾讯云计算（北京）有限责任公司
天津神舟通用数据技术有限公司
同方计算机有限公司
武汉赛博网络安全人才研究中心
武汉万数科技有限公司
无锡沐创集成电路设计有限公司
厦门服云信息科技有限公司
兴唐通信科技有限公司
英韧科技股份有限公司
永中软件股份有限公司
友虹（北京）科技有限公司
渔翁信息技术股份有限公司
元心信息科技集团有限公司
浙江华途信息安全技术股份有限公司
中电长城网际系统应用有限公司
中电科申泰信息科技有限公司
中电智能科技有限公司
中航鸿电（北京）信息科技有限公司
中国长城科技集团股份有限公司
中国航天科工集团第二研究院七〇六所
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）
中国移动通信集团有限公司
中国移动通信有限公司研究院
中联安翔（北京）信息技术有限公司

序一

数字产业化、产业数字化，是推动我国经济高质量发展的必征之路。数字经济既是新兴技术和先进生产力的代表，同时也对网络安全提出了新的挑战。我国《“十四五”数字经济发展规划的通知》提出，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。我国网络安全法律、战略和制度明确要求“推广安全可信的网络产品和服务”。

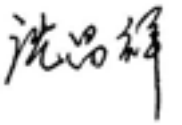
导致网络安全问题的根本性原因在于计算科学少安全理念、体系结构缺防护部件、计算工程应用无安全服务。由于设计IT系统不能穷尽所有逻辑，利用必定存在的逻辑缺陷挖掘漏洞、进行攻击的风险始终存在，网络安全是永远的命题。

因此，解决网络安全问题需要从两个方面着手，一是建立安全可信的基础软硬件产业新生态，降低逻辑缺陷的风险以及供应链安全风险；二是构建网络安全主动免疫保障体系，达到“六不”的防护效果：攻击者进不去；非授权者重要信息拿不到；窃取保密信息看不懂；系统和信息改不了；系统工作瘫不成；攻击行为赖不掉。

近年来，随着信创工作的不断深入，我国在互联网核心技术自主创新方面持续取得突破，自主可信的产业体系日益完善，网络安全和信息化设备的产业生态已经基本构成。芯片、操作系统、数据库、中间件等基础软硬件的自主研发能力不断提升，终端、服务器、交换机、路由器以及各种网络安全设备的性价比接近或已经达到了国际先进水平，安全可信程度不断加强，在政务、金融、能源等各个重点行业逐步应用推广，在保障国家安全方面发挥了重要作用。

在肯定成绩的同时，我们需要清醒地认识到，自主并不等于安全。信息技术应用创新可以在一定程度上解决后门和供应链风险，但不可避免地会产生很多新的漏洞。进一步做好重点行业领域的信创工作，需要构建主动免

疫安全可信的防御体系，有效抵御已知和未知的各种攻击。尤其是推广使用安全可信的网络产品和服务，使得网络空间所有的产品设备都应具备基本主动免疫能力，并通过服务治理得到进一步提高，从而筑牢网络强国、数字中国的安全底座。



2024 年 3 月 1 日

序二

《2023 网信自主创新调研报告》和大家见面了，这是我们开展网信自主创新技术和产业调研工作的第 6 个年头。6 年来，直接参与这项工作的企业和个人越来越多，已经从最初的 30 多家企业、不到 50 人，发展到超过 200 家企业、将近 300 人。如此高的参与度与各界的关注和认可充分说明了这项工作的价值和意义。

在本年度报告发布之际，我首先向坚持参与组织和编写这个报告的编委会成员表示敬意和祝贺！

去年的报告以“深化自主创新”为主题，重点从供给侧分析如何将自主创新的网信产品和解决方案应用于重点行业。今年的报告则侧重于从自主创新成果的应用推广视角，研究分析当前网信产业的现状和面临的问题。从报告的字里行间我们可以看出，编写者普遍认为目前推动创新成果在各个行业的应用落地尚有不少问题需要解决。

去年，我在《2023 网信自主创新调研报告》的序言中提出，深化自主创新的成功，至少应该得到两个方面的响应：一是在需求侧，创新成果要开始向数字化、信息化的核心应用领域推进；二是在供给侧，要实实在在地解决好核心技术问题，进一步提高产品的性能，进一步完善产业链。从《2023 网信自主创新调研报告》收集的信息看，需求侧和供给侧都有不少问题需要解决，如怎样处理合规要求和实际需求的关系、如何在开源和商业版本之间做选择、如何应对供应链新出现的安全风险、如何搞好产品和服务的结合、如何提高解决方案的可推广性等。

对这些现象和问题，《2023 网信自主创新调研报告》从所涉及的各个产业节点的视角进行了分析，提出了相应的对策建议。其中有一部分建议是有共性的，比如继续加大核心技术的攻关力度，切实提高产品的性能、稳定性和可靠性；通过标准化缩减供需双方之间的认识和要求的不对称；如何加强开源社区建设以促进产业生态健康发展等。还有一些话题，在报告里涉及尚不够深。比如技术路线的收敛、国产化产品的真替真用、管理上的合规和实际上的可控等问题等。这看来需要供需双方在政策指引下为“解决受制于

人的问题”共同努力，“双向奔赴”以最终解决好。

今年是中华人民共和国成立75周年，是实现“十四五”规划目标任务的关键一年。我坚信，只要我们坚持脚踏实地、坚持实事求是、坚持集思广益，网络安全和信息化工作就会一步一个脚印地稳步推进。

让我们坚持自主创新，努力构筑网信自主创新的新格局，着力推动我国网信事业的高质量发展，为实现中华民族伟大复兴不断贡献力量！

2024年3月1日

目录

前 言

在业界专家的大力支持和企业广泛参与下，《网信自主创新调研报告》已经连续编写 6 年了。6 年来，参与到报告编写工作的企业从 30 多家发展到 200 多家，人员从 40 多人发展到 300 多人。这从一个侧面反应了产业界对网信自主创新工作的重视程度越来越高。

回顾 6 年来《网信自主创新调研报告》的编写历程，编委会始终将“坚持脚踏实地、坚持实事求是、坚持集思广益”作为一以贯之的工作原则，全体参编人员不以系统性、完整性为目标，不去追求教科书式的表述方式，而是站在产业一线的视角将取得的成绩和遇到的问题呈现出来，并尝试着对具有代表性的问题提出对策建议。从专家和用户的反馈看，报告所力求的一个“实”字得到了充分的认可。

自 2023 年以来，深化自主创新工作从党政领导向关键信息基础设施行业拓展，产业界普遍感觉遇到了一定的困难。这一方面有技术、产品与更复杂的应用场景结合时必然会面临的客观因素，另一方面也有用户的观念、意识等主观因素。因此，深化自主创新不仅仅需要供给侧发力，还需要需求侧的推动和监管侧的引导。

本年度的报告尝试着站在产业的视角分析行业应用的现状和问题，共涉及 21 个领域：

1、服务器 CPU 和网络控制器芯片

随着国内芯片设计能力和生产工艺的不断提高，部分国产芯片在性能方面已经接近国际水平，并在党政办公领域发挥重要作用。未来一个时期，国产芯片向党政办公以外的重点行业进军，在持续技术创新的前提下，要注重解决生态建设问题。

2、固件

国产固件在党政等行业领域得到规模化应用，无论是功能还是性能都达到了“可用”的程度，但产业化水平与国外相比还有相当大的差距。

3、操作系统

国产操作系统得到了快速发展，在服务器、桌面、移动、云、嵌入式、物联网领域占据一定市场地位，但在用户体验度、系统功能等方面都有不足，距离“好用、易用”还有一定差距。同时，操作系统的生态建设还存在明显短板，配套软件体系建设还有较长的路要走。

4、存储

国内存储产业得到长足发展，整体形势向好。自主创新的存储产业也存在一些问题，比如 HDD 产业缺失、RAID 卡刚刚起步、安全问题未解决、NAND flash 厂商单一且产能受限、主流技术及标准受制于国外等。

5、数据库

截止到 2023 年，国产数据库引擎的性能、可扩展性和安全性等方面均有显著提升并获得了市场认可，但在兼容、迁移、智能运维等方面还需加强。

6、中间件

国产商用中间件在行业市场的覆盖率偏低。行业侧系统建设模式发生变化、建设放缓；用户习惯于使用免费开源中间件；供给侧创新能力及技术标准自主能力有待加强等是主要原因。

7、整机

信创整机产业已经形成一定规模的生态体系，对标国际成熟的技术生态体系，仍然面临技术选型难、适配验证工作繁重、应用系统不稳定、行业场景化方案不足，以及缺乏统一权威标准参考等挑战。

8、办公软件

办公软件正经历数字化、智能化的变革期。多重趋势叠加的大背景下，办公软件产业迎来巨大发展机遇，同时也面临着“真替真用”、适配负担、盗版软件、标准体系等问题和挑战。

9、打印设备

国产打印设备在党政和金融等行业得到了相对广泛的应用，由于产品化成熟度待提升、高端产品仍需持续投入、产品成本优势仍不明显等原因，在其他领域的应用推广还存在挑战。

10、软件测试工具

国产软件测试工具产品覆盖较全，但总体水平相对落后。当前，自主软件测试行业已经进入加速发展阶段，相关产品陆续投入市场，但总的来看市场占有率还有待提高。

11、商用密码应用

商用密码产业规模整体呈上升趋势，在部分领域初步实现了与应用场景的融合。由于行业的特殊性、专业性和复杂性，商用密码产品和服务在与行业应用相融合的过程中面临着较大的挑战。

12、终端安全

终端安全越来越受到各企事业单位的重视。成熟的国产化终端安全产品获得相对广泛的应用，为用户终端资产、系统环境和业务应用提供综合安全管控能力，但存在对国产化环境的响应相对滞后等问题。

13、云计算安全

云安全成为用户重点关注的问题，云计算安全市场潜力巨大。信任风险由人员向云计算基础设施转变，安全左移导致责任划分不清晰等问题影响云

计算安全落地。

14、数据安全

数据安全产业得到了快速发展。产品门类从传统的数据加密、数据库审计，拓展到了包括数据资产管理、数据监测、数据共享、隐私保护、追踪溯源等在内的数据全生命周期。深化数据安全应用、有效保障行业用户的数据安全，面临意识、技术和生态等方面的问题需要解决。

15、高级威胁检测

高级威胁攻击和防御具有强烈的技术驱动属性，攻防两端的技术演进共同推动了高级威胁防御市场发展，为了应对高级威胁，组织需要采用多种安全产品与服务构建纵深防御体系。

16、漏洞管理

随着信创产业的发展，安全漏洞问题也日益凸显。漏洞管理成为信创的重要议题：一方面漏洞管理的重要性和必要性越来越被业界认可；另一方面漏洞管理也面临着生态和技术双重挑战。

17、反恶意代码引擎

随着威胁数量与复杂度的持续增加、攻击的场景不断泛化，信息系统复杂性、资产规模和网络带宽不断加大，给反恶意代码引擎的检测能力、检测效率、算力成本和精准分类命名提出了新的要求。

18、安全管控

安全管控作为政企网络安全管理和运营的综合型平台，所带来的价值和作用逐步得到认可，已成为政企构建网络安全体系的核心，但在精细化实战方面表现差强人意。

19、工控安全

工控安全国产化进入加速期，主动防御技术不断涌现并开始落地，但国产化覆盖不足，同时新型工业化要求融合新技术、新应用构建新业态，从而产生新的安全挑战。

20、电子取证

电子数据取证是国内安全领域的一个重要方向，但在推广进程中还存在一些难点和挑战，制约了电子数据取证产业的国产化发展。

21、软件供应链安全

软件供应链高度依赖开源组件或国外技术，针对软件供应链的攻击越来越多，相关的安全保障问题逐渐被业界关注，但尚未得到足够重视。

编委会深知由于参与编写单位的覆盖面有限等原因，报告在深度和广度上还有很大的上升空间，例如对人工智能等热点问题的分析有所欠缺，相关话题将在《2024 网信自主高新调研报告》有所加强。

基础篇 »

1、服务器 CPU 和网络控制器芯片

2、固件

3、操作系统

4、存储

5、数据库

6、中间件

7、整机

8、办公软件

9、打印设备

10、软件测试工具

第 1 章 服务器 CPU 和网络控制器芯片

随着国内芯片设计能力和生产工艺的不断提高，部分国产芯片在性能方面已经接近国际水平，并在党政办公领域发挥重要作用。未来一个时期，国产芯片将向党政办公以外的重点行业进军，在持续技术创新的前提下，要注重解决生态建设问题。本章选取服务器 CPU 和网络控制器芯片两个维度对相关问题进行初步分析。

1.1 芯片技术取得长足进步，仍需坚持自主创新

1.1.1 CPU 是信息技术体系的重要支点

从技术依赖的角度，信息技术体系可以分为四个层次。第四层是应用层，如电商、办公系统、智慧城市等。第三层是整机层，如 PC、服务器、手机、打印机、防火墙、交换机等。第二层是以 CPU 为代表的芯片及以操作系统为代表的基础软件层。第一层是 CPU 和操作系统的关键核心技术，包括指令系统、核心 IP（如 CPU、GPU、内存接口、高速 IO 接口等）及 EDA 工具、生产工艺等。

1.1.2 自主指令系统取得突破

指令系统是信息产业的根技术，CPU 和操作系统都依赖于指令系统，但指令系统不再依赖其他技术。龙芯推出了自主指令系统龙架构（LoongArch），已经得到国际开源软件界广泛认可与支持，成为与 X86、ARM 并列的顶层生态系统，国内统信、麒麟、欧拉、龙蜥、鸿蒙等操作系统以及 WPS、微信、QQ、钉钉、腾讯会议等基础应用均推出龙架构版本。申威基于自主指令系统 SW64 持续进行基础软件迭代升级，充分发挥双线程等核心新特性，性能得到进一步释放。同时，申威研发的适配迁移工具和二进制翻译工具为申威平台的软件迁移提供了便利。

1.1.3 材料、设备和封装基板问题需要攻关

测试工艺比较简单。国内封装工艺已经处于世界先进行列。硅片的生产方面，14nm 已经量产，7nm 也已研制成功，可以满足绝大多数应用需求。芯片工艺线中的材料和设备以及封装基板问题需要攻关解决。

1.2 国产芯片深入行业市场要解决生态问题

1.2.1 芯片设计完成技术“补课”，性能不再是瓶颈

构建信息产业新发展格局，要从基于自主 IP 核的芯片研发、基于自主指令系统的软件生态和基于自主工艺的芯片生产三个环节提高自主可控度。经过多年的努力，国产芯片设计企业在指令集、IP 核和芯片性能方面均取得可喜的进展。

龙芯在自主指令系统龙架构（LoongArch）的基础上，通用处理性能已经逼近市场主流 X86 CPU 的水平。龙芯 3A6000 芯片 SPEC CPU 2006 Base 单线程定 / 浮点分值达到 43.1/54.6 分，SPEC CPU 2006 Base 多线程定 / 浮点分值达到 155/140 分，Unixbench 实测分值超 7400 分，性能达到 Intel 酷睿十代四核处理器水平。

申威基于自主指令系统 SW64 完成了第四代处理器微架构 Core4 的研发工作，实现了多线程的支持；并在此基础上完成了申威新一代服务器处理器的研发，SPEC CPU 2006 Base 多线程定 / 浮点分值均超过 1000 分。

网讯网络控制器芯片现已支持 802.3ab-1G、802.3ae-10G 及 802.3ba-100G 的系列标准，100G 以上高端网络芯片处于样机测试阶段，100G 以下网络控制器芯片已实现自主研制和量产，1G/10G 芯片在 PC 服务器领域实现批量替代，25G/100G 高速智能网络控制器芯片正在向 SMART NIC\DPU 演进。

1.2.2 应用生态成为自主 CPU 发展的短板

现有的信息产业基本上都建立在 Wintel（Intel+ 微软）体系和 AA（Arm+Android）体系基础之上。在信创工作推进过程中，各行业的业务系统存量的应用软件都需要与国产 CPU 及相应版本的操作系统、数据库重新适配。相对于指令系统差异（如从 X86 到龙架构），操作系统差异（如从 Windows 到 Linux）对应用的影响更大。在自主 CPU 性能不断提高、操作系统趋于成熟的情况下，应用软件生态成为自主 CPU 的发展瓶颈。另外，国产 CPU 配套芯片（IO 桥片、BMC、GPU、AI 等）国产化水平和性能不高，这也是芯片厂商面临的生态问题之一。

1.2.3 定制需求多、适配周期长，影响网络芯片应用推广

国产网络高速智能芯片目前主要用于专用领域，在消费级别的互联网平台等领域应用数量没有形成规模，DPU/SmartNIC 25G ~ 100G 以上的网络高速智能芯片也没有成体系的国产化替代。国家重要领域的基础设施中，数据中心、高性能计算、AI 加速运算等场景的服务器国产化推进还处于起步阶段，技术难度大且专用化程度高，高速智能网卡的调优进展缓慢，导致网络芯片厂商投入高、回报慢。

国产主流 1G/10G 网络控制器和网卡产品适配工作量大，产品导入进程缓慢，影响主流网络控制器的全面推广进度。在商用领域，国产网络芯片软件适配在驱动能力、兼容性和安全性等方面的问题比较突出，硬件适配在功能、性能、接口和专用定制等方面困难较多，因此定制化需求较多，导致网络控制器和网卡的适配迁移、测试、生产上线周期长。在工业领域，由于驱动和接口等技术体制复杂，硬件设计技术不规范，客户定制需求多，导致适配任务繁重。另外，由于国产 CPU、OS、BMC/BIOS、光模块和路由器品牌和技术路线众多，国产网络芯片为了匹配上下游厂商，开展了大量的适配工作。

1.3 在坚持自主创新的基础上加强生态建设

1.3.1 基于自主指令系统构建信息技术体系

引进国外技术做不出新的技术体系，反而会造成依赖国外信息产业生态的惰性，强化国外垄断企业已经形成的垄断态势。就像我们可以基于英文写文章，但不可能基于英文构建中华民族文化一样，我们可以基于国外指令系统做产品，但不可能基于国外指令系统构建自主信息技术体系。因此，建议出台政策鼓励整机厂商和应用开发商加强针对自主指令系统 CPU 的产品开发和应用适配，鼓励信创应用单位采购基于自主指令系统的信创产品。

1.3.2 加强自主指令系统生态建设

芯片设计企业要持续关注自主指令集架构的生态建设，采用兼容性迭代发展策略，使新一代处理器核心的指令集保持对上一代核心的兼容，并基于自主研发和设计能力及二进制翻译、浏览器定制化、外设定制化等成熟技术，通过产业适配中心、创新实验室、ODM/OEM 联合研制中心等方式，加强与整机厂商、基础软件厂商和应用开发商的合作，在资源共享、技术创新、平台适配、应用推广、人才培养等方面全面规划、统筹推进，缩短一体化 ODM 产业链和降低成本，构建软硬件定制化的解决方案，形成示范带动作用，不断完善自主指令系统的生态体系。

另外，在条件具备的情况下，应积极推动基础软件版本及迭代研发规则的规范化，推动制定统一编程框架，更好地实现指令集架构和跨平台应用兼容。通过研制应用迁移评估工具，为应用提供标准的开发适配环境，减少应用厂商的迁移成本，促进自主指令系统生态建设。

同时，积极建立自主生态开源社区，建立健全评价体系，优化包括平台基础软件在内的重点开源软件，激发国内软硬件厂商的参与度和贡献度，提

升国内 CPU 系列芯片产品配套应用的系统软件和应用软件供给能力。

1.3.3 加大研发投入，细化国产网络芯片标准规范

网络芯片厂商应加大与 CPU、GPU 和存储等产业生态伙伴的协作，加大 100G 以上的 SmartNIC/DPU 智能网卡关键技术研究，尽快形成标准并推广应用，以摆脱依赖，突破封锁。以行业应用为抓手，以消费市场数据中心为拓展平台，细化算法、协议、数据及内容卸载等标准和规范，推动产业再循环、可复制的良性发展。

加强主流 1G/10G 的芯片在商业领域和工业领域适配工作，加强国产化技术攻关能力。针对国产网络芯片在商业领域的软件适配，加强与操作系统厂商的配合力度，积极维护开源社区，降低软件适配的难度和成本；主动进行 DPDK 等网络加速或自研加速协议测试，加强网卡安全协议的支持和特殊定制服务，积极植入国密算法，积极对接定制协议需求。针对国产网络芯片在商业领域的硬件适配，尽快建立标准规范体系和检测机制，加大监督力度，面对国内平台完善和优化硬件接口功能；加大对新总线协议等前沿技术的研究力度，完成国产化产品，增强适用性适配；增加开放性和普适性服务规范，发布详细的开发手册及 demo 案例，降低国产网络芯片的使用难度。针对国产网络芯片在工业领域的适配，联合上下游厂商共同开展适配测试，加大 TSN 等工业以太网先进技术的研究；同时不断改造软硬件设计，提升产品的耐用性和稳定性，加强对工控环境的模拟测试，保证过硬的产品质量。

本章编写人员：

龙芯中科技术股份有限公司 靳国杰、柳军

北京网迅科技有限公司 胡金山 、钱利国、史绍程

中电科申泰信息科技有限公司 桂江华

无锡沐创集成电路设计有限公司 王孟元

北京安御道合科技有限公司 谢依夫

第 2 章 固件

固件是计算机系统中的核心部件，主要包括基本输入输出系统（Basic Input Output System，BIOS）和基板管理控制器（Baseboard Management Controller，BMC）。固件的自主可控和安全可靠是提升国产计算设备安全水平、增强关键信息基础设施自主保障能力的重要环节。目前，国产固件在党政等行业领域得到规模化应用，无论是功能还是性能都达到了“可用”的程度，但产业化水平与国外相比还有相当大的差距。

2.1 国内固件产业呈现“小而散”的特点

BIOS 固件和 BMC 固件的市场与 PC、服务器等计算设备的出货量直接相关。经推算，国内 PC 的 BIOS 固件产品市场规模在 4.85 亿元至 7.28 亿元之间，服务器固件产品市场规模在 8.96 亿元至 13.43 亿元之间。

目前，国产固件在信创市场得到了广泛应用，但由于信创市场空间相对有限，固件在信创计算机产业链中的定位一直不明确，固件技术和产业发展未得到充分重视。在成熟的计算机产业生态中，独立固件供应商是重要参与者。独立固件供应商立足于固件本身，独立于处理器、板卡、操作系统和整机厂商，面向整个计算机产业提供全面的、多样化的、高水平的固件技术和产品服务，是计算机产业专业化发展、市场化选择自然形成的主体。反观国内固件产业，呈现出“小而散”的现状。从全局来看，没有独立的固件厂商开发普适、高效、可靠、安全的固件产品，导致计算机产业链整体成本上升，制约全自主可控计算机产品的研发速度，影响计算机产业链的健康发展。

2.2 产业问题在人才、标准、安全方面的投影

2.2.1 人才队伍规模小且分散

美国 AMI 是一家独立固件厂商，该公司拥有近两千人的研发团队。反

观中国，全国从事固件专业的总人数在一千五百人左右，其中大部分分布于两个独立固件厂商（昆仑太科和南京百敖），小部分人员就职于整机厂商和小型嵌入式软件公司。除部分大厂外，多数整机和嵌入式软件公司的技术团队不具备独立的固件研发能力。

2.2.2 固件标准体系空白

计算机固件标准的现状与国产固件的核心位置不匹配，固件标准体系研究仍属空白。工信部联合其他部委已推出了国产计算机整机、数据库、操作系统系列标准，但是国产固件的相关标准还是空白。与固件相关的标准内容多分布在整机标准或安全可信相关标准中，不成体系且不完整，不能对国产固件的研制、生产和测评起到指导作用。

2.2.3 固件安全不受重视

由于固件在计算机体系架构中的特殊位置，其安全性十分重要，且具有以下特点：一是一旦植入恶意代码就难以发现和清除；二是有可能对硬件进行严重破坏。美国国家标准与技术研究所制定了固件安全防护系列规范，包括 NIST SP 800-147、147B、155、193 等。这些标准旨在确保固件的安全性能并防范潜在的威胁。目前，国内缺乏相应的固件安全标准规范和配套的安全检测软件。

2.3 加快固件技术突破创新实现合作共赢

2.3.1 标准先行，促进产业走专业化、集约化道路

专业化、集约化是固件产业发展的必由之路，要聚合优势力量把产业做强做精。这也是由 AMI、Phoenix、Insyde 三家国际固件厂商证明过的正确道路。

由于固件承上启下的特殊地位，同时由于国产固件产业生态的特殊性，要走专业化、集约化道路离不开政策因素的大力支持。建议国家产业主管部门进一步明确固件在产业中的定位和作用，组织制定国产固件的高标准细化要求，并纳入计算设备采购要求，促进国产固件技术革新和产品升级，制定包括固件兼容适配、安全可信、测试验证等标准；将固件作为安全评估关键项，健全和细化固件国产自主、可控可靠的评估标准。

2.3.2 提升创新能力，以信创固件赋能产业链下游

首先，固件厂商要与处理器、板卡、操作系统厂商进行紧密的合作，深度参与新产品的设计、研发、生产、测试和调优的流程，实现整机功能性能优化和稳定可靠的运行效果。

其次，基于固件层的安全策略保护终端和服务器，确保硬件设备持续可见并处于受控状态，面对网络攻击和威胁时能够快速应对。例如通过安全启动、可信计算等方式增强 BIOS、BMC 的安全性，提高其整体可靠性和可用性。

第 3，进一步挖掘固件在云计算、大数据、人工智能、算力网络等计算模式下的新需求，加强固件在终端集中安全管控、服务器集群智能运维、数据中心节能降耗、算力优化调度等方面的应用。通过联合研究项目、共享技术资源，实现跨技术、跨领域的多维度集成应用创新，发挥固件在信息系统中的基础作用。

本章编写人员：

昆仑太科（北京）技术股份有限公司 陈小春、孙亮

第 3 章 操作系统

近年来，国产操作系统得到了快速发展，在服务器、桌面、移动、云、嵌入式、物联网领域占据一定市场地位。以银河麒麟为代表的国产操作系统，已能满足党政领域的办公需求，同时向重点行业拓展。不可否认，国产操作系统在用户体验度和系统功能方面，距离“好用、易用”还有一定差距。同时，操作系统的生态建设还存在明显短板，真正具备核心生态的操作系统很少，和微软等国外成熟的操作系统相比，配套软件体系建设还有较长的路要走。

3.1 国产操作系统面临工程化、碎片化和多样化问题

3.1.1 操作系统整体效能有差距

现代的操作系统功能复杂，软件特别庞大，由于软件工程化能力相对欠缺，使得国产操作系统的整体性、功能的一致性、资源调度的有效性，与国外产品有一定的差距。从技术的角度看，主流操作系统厂商都具备了 Linux 内核之外代码开发能力，但是二次开发的模式导致创新水平存在天花板，面临系统架构、内核、网络、图形等方面能力的技术挑战，特别是操作系统内在的原理、资源的调度方式、应用软件广泛的兼容性方面核心技术积累不足。从投入的角度看，操作系统研发需要持续投入大量资金支持。微软公司在研发 Windows 操作系统新产品时，投入 4000 多名工程师，历经 2 年，才公布了 Windows 3.0，但 Windows 3.0-3.2 并没有形成市场收入，之后又高强度的投入，到 Windows 95 才逐渐形成市场规模。根据欧盟执委会发布的《2023 年欧盟工业研发投资记分牌》（The 2023 EU Industrial R&D Investment Scoreboard）显示，2022 年全球投入研发金额最高的企业是 Google 母公司 Alphabet，达到了 370.34 亿欧元；Meta 以 315.20 亿欧元排名第二；微软以 254.97 亿欧元名列第三；苹果以 246.12 亿欧元排名第四。这些大型科技公司在研发资金投入方面都呈逐年增长趋势，而国内操作系统厂商投入上亿元研

发经费的少之又少，且盈利见效周期长，这是国产操作系统发展的短板。

3.1.2 生态适配规模显著增长但碎片化明显

国内操作系统生态发展大致经历 3 个阶段，分别是单品起步阶段、单机阶段（1.0 阶段）和创新生态建设阶段（2.0 阶段）。单品起步阶段操作系统的功能性能得到提升，但在与 CPU、整机、数据库等软硬件组合后，暴露出较多兼容性、功能和性能问题。单机阶段对于发现的缺陷、短板进行了补齐，推动了产品进一步升级完善。当前正处于创新生态建设阶段，适配和测试规模快速增长，从通用场景转向行业场景。

目前，国内主流操作系统厂商生态合作伙伴数量已超 7000 家，软硬件生态适配数量已超 400 万款。主要的国产 CPU 技术路线包括 X86、ARM、LoongArch、MIPS、Alpha、RISC-V 等。然而，多技术路线加剧了适配复杂度，生态建设呈现碎片化趋势。参照国外主流操作系统，Windows 10 月活设备数超过 7 亿台，适配应用程序超过 3500 万个，软件版本超过 1.75 亿个，硬件 / 驱动组合 1600 万件。反观国产操作系统，工具软件、管理软件等应用软件生态尚没有建立，专门为国产操作系统开发的应用软件十分缺乏，适配的软硬件数量与主流操作系统相比存在数量级的悬殊差距。

3.1.3 行业需求多样性与产品通用性的矛盾日趋显现

操作系统作为一种基础软件，通常具备跨行业的通用性特点，一般体现在上层应用和下层硬件两个方面：对于上层应用，操作系统遵循国际标准规范，实现应用互操作和数据共享的目标；对于下层硬件，操作系统需要兼容各种硬件设备，满足不同行业的需求。另外，虽然操作系统具有通用性，但在某些特定场景中针对具体需求进行定制和优化也是必须的。

例如，金融行业对通用操作系统的需求体现在安全性和稳定性；另外在

柜面运营场景（如高拍仪、身份证识别、智能终端柜员机等）需要满足多形态的交互需求；大型金融机构的自研场景，对操作系统的配套工具和组件环境方面有修改化需求。能源行业对操作系统的需求体现在实时性和高性能计算，比如石油勘探和生产过程中对数据分析和处理的实时性要求。交通运输行业对操作系统的需求主要体现在稳定性、安全性和实时性，部分场景下要求操作系统在设备利旧适配和资源配置较低的环境下可以稳定运行。电信行业对操作系统的需求体现在可扩展性和灵活性，以适应不断变化的业务需求和市场环境。

3.2 国产操作系统产业存在技术、生态和应用方面的问题

3.2.1 技术体系缺乏长期积累

（1）内核技术水平不足

操作系统的内核是其核心部分，影响整个系统的性能和稳定性。国产操作系统相对缺乏在内核技术上的深度积累，导致系统性能和稳定性不及国际先进水平。

（2）设备驱动支持不足

对各种硬件设备的充分支持是操作系统的基本要求。缺乏对广泛硬件设备的成熟驱动支持可能导致用户在使用过程中遇到兼容性问题，或者无法充分发挥硬件性能。

（3）多核处理器优化不足

随着计算机硬件的发展，多核处理器已经成为常见的硬件架构。操作系统需要充分利用多核处理器的优势，提高系统性能。缺乏在多核处理器上的深度优化可能导致系统在多任务处理和并发性能上的不足。

（4）实时性能不足

越来越多的应用场景对操作系统的实时性能提出较高要求，如果操作系统缺乏对实时性能的充分优化，可能导致在这些领域的应用受限。

（5）社区支持不足

与国际先进水平相比，国产操作系统的开源社区相对较小，缺乏足够的社区支持和贡献。这可能导致问题难以及时发现和修复，影响系统的稳定性和安全性。

3.2.2 产业生态没有形成持续迭代机制

国产操作系统的生态规模与国外主流操作系统存在百万到千万的数量级差距。与 Wintel 体系的应用功能 / 性能相比，国产操作系统也存在较大差距，多数应用厂商没有在国产操作系统上建立持续迭代机制。在原生开发方面，国产原生认证刚刚起步，开发者数量少，开发工具、环境和标准有待完善。基于国产操作系统原生开发的软件数量少，缺少版本升级机制。在适配标准方面，厂商独立维护验证标准规范，不同平台之间的测试方法和评估指标有所差异，应用适配验证标准规范不统一。

3.2.3 需求多样化迟滞了产业快速发展

应用多样性的挑战主要表现在两个方面，一是各行业所采用的技术路线存在较大差异；二是由行业属性导致的业务复杂度高。技术路线差异的问题集中体现在国产操作系统与行业应用产业链上的芯片、硬件设备、基础软件、应用软件等各环节的配合衔接困难，无法确保产品和解决方案的兼容和高效。业务复杂度高导致的问题体现在两个方面: 一是国产操作系统厂商服务能力跟不上，缺乏应用程序和开发工具支持，在用户文档、培训材料、技术支持渠道等方面有欠缺，用户在遇到问题时无法及时获得帮助和解决方案；二是由于技术栈、

业务逻辑、接口标准等方面的原因，行业应用开发经验难以跨平台复用。

3.3 多方协同、共同突破，实现操作系统高质量发展

3.3.1 健全技术创新体系

国产操作系统厂商应针对重点行业进行核心技术的提升，聚焦于操作系统内核、性能优化、安全性等核心技术领域，加强操作系统的安全性，提升用户界面的友好性。通过积累关键技术，提升核心竞争力，吸引更多的用户和开发者，共同推动技术创新和产业发展。同时，积极参与开源社区，加速技术共享与迭代，借鉴外部创新成果，以达到健全技术创新体系的目标。具体举措包括：（1）设立技术创新基金，支持国产操作系统相关的研发项目，资助开源社区。（2）提高知识产权保护水平，鼓励创新机构对操作系统的核心技术进行专利保护，增强创新机构的创新动力和经济效益。（3）建立技术交流平台，促进不同机构之间的技术合作和经验分享。（4）建立开放创新生态系统，鼓励开源社区、产业界、科研机构共同参与操作系统的开放创新。

3.3.2 打造操作系统生态新时代

以通用生态、行业生态需求为牵引，通过培育开发者生态、共建专业生态联盟、生态软件提质三项行动，开启生态发展的新时代，力争在未来 3 到 5 年生态适配数量突破千万，促进生态建设自主创新和高质量发展。具体举措包括：（1）建设和持续丰富生态体系，推动操作系统与软硬件厂商、集成商建立长期合作伙伴关系，建设完整的自主创新生态链。（2）以国家战略需求为导向，面向重点行业和关键基础设施，加强供应链上下游的原生开发、适配和迁移协作。（3）统筹兼顾自主创新能力与推动软硬件生态构建，增强产业链供应链自主可控能力。（4）加强适配标准和开发者平台建设，积极探索服务模式创新，打通卡点堵点，通过在更多生产场景的大规模应用，

加快操作系统在功能、性能、稳定性方面走向成熟。

3.3.3 加强操作系统在行业中的示范应用

操作系统厂商、行业应用开发商、用户以及其他利益相关方要共同参与和协作，共同推进操作系统与行业应用的融合发展。通过用户调研、用户测试、用户反馈等方式与用户紧密互动，确保产品的发展方向与用户需求保持一致。组织技术团队对操作系统与行业应用进行攻关适配，包括技术方案的制定、代码的修改和优化、测试和验证等工作，解决操作系统与行业应用的兼容性和互操作性问题。通过联合共建，汇聚各方的优势和资源，共同解决技术发展和市场推广中的难题，加速操作系统与行业应用的融合。从重点行业中选择一些具有代表性的行业应用场景，率先部署和实施操作系统与行业应用的融合方案，树立成功的先例和标杆。在树立标杆的基础上，通过行业会议、展览、宣传等多种方式，将成功的解决方案和经验向整个行业进行推广。鼓励更多的企业和行业采用创新解决方案，提升整个行业的竞争力和创新力。

本章编写人员：

麒麟软件有限公司 杨汇成、朱天旭、张楠、朱文玉

北京长擎软件有限公司 徐宁、代向东、王鑫

湖南麒麟信安科技股份有限公司 石勇、高洪鹤

普华基础软件股份有限公司 王江涛

元心信息科技集团有限公司 李何佳

北京凯思昊鹏软件工程技术有限公司 陈鹏、李云翔、闫苗

第 4 章 存储

在有关政策的推动下，国内存储产业得到长足发展，整体形势向好。截止 2022 年，我国存储能力总规模超过 1000EB[1]，NAND 闪存介质技术达到全球一流水平、SSD 主控整体份额占据四分之一、存储系统占据绝大部分份额。同时，自主创新的存储产业也存在一些问题，比如 HDD 产业缺失、RAID 卡刚刚起步、安全问题未解决、NAND flash 厂商单一且产能受限、主流技术及标准受制于国外等。

4.1 存储领域的自主创新形势不乐观

4.1.1 自主可控的存储技术体系尚未形成

由于技术专利壁垒，机械硬盘领域短期内难以形成良性（投入产出比）的产业生态。在闪存领域，部署全闪存储成为产业共识，虽然围绕 eSSD 主控芯片已有政策文件出台，但依然存在驱动力不足的问题。此外，数据安全问题没有得到足够重视，如在加密存储方面，国外使用 TCG-opal 作为加密 SSD 标准，国内由于缺少加密 SSD 与上层传输的标准规范，服务器与加密 SSD 模组无法沟通，安全功能难以落实。要实现数据加密的存储产品，只能通过自定义标准实现互通，这就造成加密存储模组难以标准化和推广。

4.1.2 国产存储产业生态不健全

据统计[2]，中国 IT 基础设施先进存力的占比（全闪存部署率）为 24.7%，远低于发达国家的 52.8%。目前，国内机械硬盘产业链布局基本上处于空白状态，HDD 机械硬盘市场被希捷、西数和东芝三家外企占据。另外，国内仅有长江存储一家企业能与国际厂商同台竞技大容量 3D NAND Flash，

[1] 中国信息通信研究院《中国综合算力评价白皮书 (2023)》

[2] Gartner 2020 对“美国 / 西欧 / 中国全闪存收入以及占比”

仅华为一家可以提供 SAS SSD，消费级 SSD 市场“披马甲”、以次充好、恶性竞争的问题也较为严重。同时，企业级 SSD 也存在低价竞争的情况，影响可持续发展。

在存储设备及存储系统中，生态不健全问题依然存在。在存储设备领域，RAID 卡市场份额被外资占据，前三的国外品牌占据了超过 75% 的市场份额（如下图）。在分布式存储系统领域，多数厂商以开源软件为基础开发自主产品；在高性能集中式存储领域中，还存在贴牌的现象。

	2018	2019	2020	2021	2022	2023
Broadcom	60.74%	61.13%	60.89%	60.82%	61.74%	61.09%
Microchip (Adaptec)	14.80%	14.26%	13.91%	14.15%	13.86%	13.76%
HighPoint	3.08%	3.45%	3.46%	3.26%	3.38%	3.46%	
Intal	2.88%	3.13%	3.00%	3.27%	3.25%	3.40%
Dell	3.30%	3.15%	3.35%	3.19%	3.08%	3.14%
郑州云芯智联信息技术有限公司	0.00%	0.00%	0.00%	0.00%	1.40%	3.50%
Hewleit Packard	0.90%	0.80%	0.78%	0.83%	0.79%	0.84%
Lenovo	1.04%	1.00%	1.10%	1.01%	1.07%	1.13%
Areca Technology	1.23%	1.37%	1.38%	1.27%	1.20%	1.17%
华澜微	0.00%	0.09%	0.34%	0.36%	0.40%	0.54%
其他	12.04%	11.61%	11.79%	11.83%	9.83%	7.97%
总量	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%

图 4-1：2018-2023 年中国 RAID 卡主要厂商的市场份额 [3]

4.1.3 关键技术的突破面临较大困难

由于存储技术门槛高，企业创新代价高，且受国外技术壁垒影响，国内厂商面临着技术滞后、供应链薄弱和国际竞争压力的挑战，国内自主可控存储技术布局尚未实现“连线成网”，还存在诸多问题。

存储介质面临起步晚、研发周期长、专利限制和产业链上游受制于人，

[3] 贝哲斯咨询《中国 RAID 控制卡行业市场调研报告 2023-2029》

以及芯片人才缺乏等客观问题，需要持续投入。

由于 HDD 技术被国外垄断，作为唯一有替代机会的闪存介质 QLC 还需要进一步降低成本。中国在 HDD 技术标准、制造工艺上的布局基本空白，在读写磁头、磁头控制芯片、盘片和磁粉技术上与国外还存在较大差距，并且也受专利限制。当前国内基于 SSD 的闪存存储产业已具备了技术创新性和领先性，闪存替代 HDD 成为大型存储的主导技术正逐步成为共识，但仍存在一次性成本较 HDD 大，需要从存储系统层面进一步降低成本的问题。

RAID 卡及其主控芯片技术门槛高，国内企业尚未达到国际主流技术水平，且未经过市场充分检验。另外需要关注的是，由于 RAID 技术出现早，产品可支持 SATA/SAS/PCIe 三模形态，但未能满足主流 NVMe SSD 的性能，因此不仅无法充分发挥闪存的性能优势，也存在知识产权风险。

4.2 政策引导、市场监管和标准化工作需要加强

4.2.1 政策法规的引导作用需要加强

（1）全闪存替代方面

HDD 受到技术和市场的多重制约，要打自主创新的翻身仗十分困难，全闪存替代是可能存在的一条路径。然而，国内用户普遍存在重视初次投入、忽视总体拥有成本和绿色节能综合效益的现象。这导致全闪存替代面临一定的市场阻力，需要全行业推动以闪存为介质的先进存储系统的部署。另外，在闪存存储产业，SAS SSD 来源受限导致的高性能集中式存储设备的关键部件国产化进程落后问题，还需要更为先进的 NVMe SSD 来弥补国产化替代空缺。单纯依靠企业的市场行为去推动这一转变难度很大（基本不现实），因此需要政策的引导。目前，相关机构暂未针对全闪存替代机械硬盘出台专项政策。

（2）数据安全方面

在信息加密与认证方面，相关要求重点关注了数据的可靠性，在数据存储、流转和使用中的安全保密和授权认证方面没有细化。这导致企业级存储产品大多按照国际标准设计安全机制，有些设计仅支持国际密码算法，有些虽兼容国密算法的硬件逻辑，但多数停留在盘内的数据自加密，对数据与上层传输及文件级别的加密和认证的体系化设计关注不够。

4.2.2 市场需要体系化监管

行业市场缺乏对自主产品的认定标准及完整生态链；消费市场则陷入价格战，存在容量虚标、品质不稳等情况。这些现象不仅导致产业界持续投入的动力不足，同时也影响到用户的消费预期，限制整个产业的技术创新和研发能力，不利于行业的健康发展。

4.2.3 标准体系需要健全

国内厂商在起步阶段面临技术滞后、供应链薄弱和国际竞争压力等诸多挑战，出现了由标准不统一引起的兼容性问题、技术验证问题、沿用机械硬盘时代的旧架构导致的可靠性问题，以及核心算法沿用 HDD 设计的 RAID 或衍生技术、存储系统中使用 SBB（存储桥接坞）架构导致的闪存性能不被发挥和侵权风险等问题。为解决这些问题，健全相关技术标准是当务之急。

4.3 筑牢自主可控的安全存储基座

4.3.1 加快推进全闪存化和安全标准化

以双碳应用加快推进数据中心全面闪存化。使用国产闪存替代传统

HDD，有效减少数据处理产生的能源消耗。在加快以全闪技术为核心的新型数据中心建设的同时，对使用传统存储技术的提出升级计划表，逐步完成自主可控产品的应用。

制定存储架构、模组和系统的国产化替代标准细则，使国产 SSD 按照标准规范在外部接口层面和内部传输通道上增加支持国密 SM 算法的软硬件逻辑，或在 SSD 与主板之间增加支持国密 SM 算法的存储通道加密模组，体系化地实现数据加解密和安全认证等功能。

4.3.2 培育自主的企业级市场和规范的消费级市场

加强构建自主可控的核心技术体系的同时，要统一技术标准和检测规范，并从研发驱动力、产品质量及供应可持续性入手，切实提高存储产业的自主可控水平，打击伪国产。在存储产业链上游培育龙头企业，推动产业链协调配套，确保国产存储介质市场的稳定运行。同时，行业监管部门营造公平的市场环境，企业级市场要推动厂商对供应商进行统一管控，寻求建立有韧性的供应链生态系统，促进产业良性发展；消费级市场要加强规范化，打击虚假宣传，鼓励企业遵守规范，推动整个行业向更加可持续和健康的方向发展。

4.3.3 厂商持续投入解决关键技术问题

在国产替代 HDD 介质的大背景下，厂商应积极应对，加大对全闪存替代及 NVMe 替代 SAS SSD 的支持力度。不仅要通过 RAID 卡架构的创新，还要加大替代技术研究，使得国产存储控制卡能够支持各类 SSD 并充分发挥性能优势。还应加大加密等存储安全功能的开发投入，以满足用户对数据安全性的需求，从而提高产品的差异化优势，打造安全自主可控的国产生态链。

本章编写人员：

深圳大普微电子股份有限公司 杨亚飞、黄运新、陈祥

成都储迅科技有限公司 李根岱、胡金山、宫新伟

北京众人数安科技有限公司 石建兵、黄磊、朱易翔

第 5 章 数据库

截止到 2023 年，国产数据库引擎的性能、可扩展性和安全性等方面均有显著提升，完整的国产数据库产品生态已经初步建立，自主数据库解决方案开始与国际巨头竞争，并获得了市场认可。

5.1 国产数据库需要解决兼容、迁移和智能运维问题

5.1.1 兼容问题

我国数据库技术来源复杂，主要有自主研发、基于国外开源数据库二次开发、购买国外商业数据库授权包装成国产三条技术路线。发挥国产数据库安全性和自主可控的优势，首要问题是数据库的兼容性。

国外数据库（Oracle、DB2、SQLServer 等）发展较早，特别是 Oracle 在国内市场占领了一定先机。因此，兼容性问题主要存在于两个方面：一是 Oracle 经过多年的发展，在 SQL 语言、性能、实例形态、容灾方案等方面有很多积累扩展。若要实现 Oracle 数据库的国产化替代，首先要解决的就是如何兼容 Oracle 的大量 SQL 方言问题，尤其是 Oracle 的 PL/SQL 这一独特的广受欢迎的语法体系。二是用户经过信息化的长期积累，基于 Oracle 开发了大量的业务系统。为了适配新的国产数据库，必须对这些业务系统的代码进行修改，各数据表的数据类型、函数、语法规则需要进行系统、全面的改造，这就要求国产数据库对原有数据库能够兼容，降低代码改造成本。

5.1.2 迁移问题

国产数据库以“存量替换”的场景为主，因此数据库迁移是一项重要工作。目前，在迁移方面取得的进展主要表现在以下三个方面：一是提升了迁移成功率。通过不断的技术迭代，国产数据库针对中国市场的特性，提升了

异构数据库迁移的成功率，减少了数据库国产化的工作量。二是提升了迁移效率。通过数据库本身的优化和高效的迁移工具，国产数据库大幅度缩短了迁移时间，使得用户能够在较短时间内完成迁移工作，减少了对业务的影响。三是降低了迁移风险。通过完善的迁移方案和技术手段，确保在迁移过程中业务不中断，数据不丢失，降低了迁移风险。

然而，数据库迁移是一个十分复杂的过程，国产数据库在对各类应用场景的适应能力、功能全面性、自动化处理等方面，还需要进一步完善和提高。目前的挑战主要包括：一是迁移评估效果不理想。多数数据库厂商的迁移工具提供一定功能的异构数据库对象及数据迁移评估，但评估的结果与实际情况往往有较大出入。二是高级对象迁移能力不强。目前多数数据库厂商的迁移工具只能迁移部分高级对象，且成功率不高，对不能迁移的高级对象往往也不能准确定位问题。三是应用系统迁移能力弱。不同应用系统涉及到的编程语言和数据库接口方式各异，在技术、架构、处理模式、运维管理等方面有较大的差异性，这些都是应用系统迁移要考虑的因素。目前，多数数据库迁移工具并不提供对应用系统迁移的评估，部分国产数据库提供的应用系统迁移工具功能简单，应用系统迁移工作主要依靠人工完成。

5.1.3 智能运维问题

随着业务的快速发展和技术架构的不断演变，数据库的运维和管理面临着越来越多的挑战。随着数据量的爆炸式增长和数据库类型的多样化，提供从安装部署到运行维护的生命周期管理能力，降低数据库管控门槛，是一项重要课题。目前国产数据库的运维管理还没有形成统一的规范和标准，这会导致运维管理的效率低下，且容易出现人为错误。一方面，国产数据库类型繁多，不同类型的国产数据库在安装部署、配置管理、备份恢复、性能优化等方面存在差异。由于缺少专业知识和经验，普通用户很难进行有效的运维

管理。另一方面，传统的运维管理方式效率低下，虽然有一些智能化运维工具，但复杂问题仍然需要人工干预，导致运维成本上升，同时也存在一定的盲目性和随意性。

5.2 提高兼容性能在很大程度上解决问题

5.2.1 对 Oracle 的兼容是主要问题

兼容性问题源于异构数据库的差异性，存在于很多方面，如：字符集和时区差异，数据类型差异，数据库索引、序列号、自增字段、物化视图、触发器、全局临时表、系统包、事务隔离级别和 MVCC 等特殊功能差异，SQL 语法的差异，hint、sql profile 等优化 SQL 执行计划能力差异，PL/SQL 差异和多元化应用系统和多种国产化软硬件平台兼容性等。在上述兼容性问题中，国产数据库对 Oracle 的兼容最为突出。由于国内大部分关系型数据库产品基于 MySQL 和 PostgreSQL 二次开发，因此这些产品对 MySQL、PostgreSQL 兼容性较好，但没有体系化地兼容 Oracle（尤其是在 PL/SQL 方面）。

5.2.2 迁移工具的成熟度是主要问题

如前文所述，数据库迁移问题主要体现在迁移评估、高级对象迁移和应用系统迁移三个方面。迁移评估包括数据库迁移评估和应用迁移评估两方面，评估的内容包括实际迁移时会遇到哪些问题、要花费多长时间等，评估的目的是事先对迁移过程有一个较为全面、相对准确的了解，以便做好相关准备工作，提高迁移成功率、降低迁移风险，从而提升用户对数据库国产化替换的信心。目前迁移评估效果不理想的主要原因在于国产数据库与已广泛使用的国际主流数据库存在较多不兼容性，以及应用系统的千差万别。数据库高级对象是指除表、视图、序列之外的自定义存储过程、函数、触发器、程序包等对象。数据库高级对象迁移涉及到源数据库、目标数据库的多个层

面（如自定义存储过程、函数、触发器、程序包等）及多个方面（如数据类型、SQL 语法等）的差异性，与数据库的兼容性有直接关系。数据库的兼容性越好，高级对象的迁移工作量越小、相对越容易。因此，解决兼容性问题是解决高级对象迁移问题的本源。在此基础上，尽量提升高级对象自动化迁移比例，不能自动化迁移的也要准确定位问题，减小工作难度，减轻工作量。应用系统迁移工作一般由用户或用户的应用供应商完成，有时候也需要国产数据库厂商的参与。因此，相关人员不了解国产数据库与原数据库的差异，而数据库厂商又不了解用户的应用系统，这是问题的根源。实际上，这又回到了数据库的兼容性问题。但国产数据库做到 100% 兼容国外主流数据库也是不现实的，因此需要提高迁移工具的成熟度，尽可能提升自动化迁移比例，不能自动迁移的部分也能准确定位问题。

5.2.3 智能运维面对多方面困难

国产数据库运维问题的原因主要包括技术复杂性、人才短缺、运维管理模式落后、缺乏行业标准和规范等。

（1）技术复杂

国产数据库产品种类繁多，不同的数据库技术路线和实现原理各不相同，这使得运维人员需要具备多种技能。每种国产数据库都有其独特的管理、配置和优化方法，运维人员很难掌握所有技术。同时，国产数据库在性能优化、高可用性等方面的支持相对较弱，这给运维带来了更多挑战。

（2）人才短缺

数据库运维领域的人才储备不足，尤其在国产数据库领域。运维人员需要具备专业的知识和实践经验，但目前国内相关的培训和教育资源有限，无法满足市场需求。这导致运维人才供给不足，给企业的运维工作带来困难。

（3）运维管理模式落后

传统的运维管理模式主要是人工操作，效率低下且容易出错。随着数据量的增长，传统方式越来越难以应对日益繁重的运维任务。

（4）缺乏行业标准和规范

国产数据库运维管理尚未形成统一的行业标准和规范，导致用户在运维过程中难以形成统一的管理体系。缺乏标准规范还会影响到运维人员的技能提升和经验分享。

5.3 加强适配迁移能力，引入人工智能技术

5.3.1 加强多系统、多平台、多款数据库无缝兼容适配

针对异构数据库适配主要是高度兼容 Oracle 语法与 PL/SQL，支持 VARCHAR2/NVARCHAR2、NUMBER 等全部常用数据类型。在 PL/SQL 语法上，支持控制语句、集合、动态 SQL、子程序、预定义包、错误处理等全部 PL/SQL 语法，通过自主原创 PL/SQL 编译器，支持复杂 PL/SQL 程序，解决 Oracle 业务迁移到国产化数据库的核心痛点问题，并为完善其他兼容性问题提供基础。在 Oracle 数据库对象、DML、函数、系统视图、内置包、驱动等方面，做到常用功能的兼容，满足大部分业务的迁移需求。

5.3.2 通过技术创新和标准化提高迁移能力

在增强迁移评估能力方面，一是建立完善的数据库迁移评估体系，包括全面评估现有数据库系统、预测迁移过程中可能遇到的问题并制定解决方案等。二是加强技术研发和创新，通过加强技术创新，结合人工智能等新型技术，不断改进迁移工具，提高迁移评估的适应能力和准确性。三是提高数据库管理员的技能和水平。

在提升数据库高级对象的迁移能力方面，一是理解源数据库及目标数据库架构的各个方面，以便在迁移过程中能够更好地处理这些对象。二是理解源数据库及目标数据库之间的数据模型转换方法，了解如何将一个数据库系统的对象转换为另一个数据库系统的对象。三是借助其他项目累积的迁移经验和最佳实践，利用人工智能算法以适应新的环境，尽可能提高自动迁移比例和迁移成功率。

在应用系统迁移方面，主要工作在 SQL 语句的改写上。因此，需要迁移工具遍历应用程序的所有源文件，自动识别出所有访问数据库的 SQL 语句，智能分析 SQL 语句，查找出所有需要改写之处，并进行智能改写，对于不能改写的要标记出来，最后生成 SQL 语句改写的报告，以便相关人员检查及对需要人工处理的作进一步处理。

5.3.3 基于人工智能实现国产数据库的智能运维和自治

（1）架构设计

构建一个具备智能化和自治能力的国产数据库系统，需要在架构设计时就考虑引入人工智能和机器学习技术，通过设计层次化的系统架构，将数据处理、存储、查询等模块与智能运维模块相互独立，便于后期进行智能化的运维和优化。

（2）自动化运维

实现国产数据库自治的关键在于提高运维效率，降低人工干预。可以通过自动化运维工具，对国产数据库的安装、配置、备份、恢复、性能监控等日常工作进行自动化处理。同时，结合故障预测和诊断技术，实现国产数据库的自我故障排查和修复，从而降低故障发生率和人工干预次数。

（3）性能优化

借助大数据分析和机器学习技术，对国产数据库的性能数据进行实时监控和长期积累，通过分析国产数据库的运行状态和负载情况，自动调整国产数据库参数、索引、分区等，实现性能的优化。同时，结合人工智能技术，对国产数据库的性能进行动态评估和预测，提前发现性能瓶颈，为运维决策提供支持。

（4）智能诊断与预测

利用人工智能和机器学习技术，对国产数据库的运行日志、性能数据等进行深度分析，实现故障的智能诊断和预测。通过构建故障诊断模型，自动识别和定位故障原因，为运维人员提供精准的故障排查和处理方案。此外，还可以利用预测模型对国产数据库的未来运行状态进行预测，提前采取措施防止潜在问题。

（5）知识图谱与专家系统

构建一个涵盖国产数据库运维知识图谱，将各类运维知识和经验进行结构化存储和关联分析。结合专家系统，实现国产数据库运维知识的自动推理和决策，为运维人员提供智能化的决策支持。同时，知识图谱还可以不断学习和优化，提高运维知识的准确性和实用性。

（6）运维人员赋能

实现国产数据库自治还需要培养一支具备智能化运维能力的团队。通过培训和实战演练，提高运维人员对人工智能、大数据、机器学习等技术的掌握程度，使其具备运用先进技术进行国产数据库运维的能力。同时，鼓励运维人员积极参与国产数据库智能化技术的研究和开发，不断推动国产数据库自治技术的创新和进步。

本章编写人员：

天津神舟通用数据技术有限公司 王天访、耿志鹏

北京万里开源软件有限公司 彭蔚刚、徐爽

北京人大金仓信息技术股份有限公司 刘俊、尹强、李楠

北京优炫软件股份有限公司 王国军、王军、梁星

第 6 章 中间件

目前，国产商用中间件在行业市场的覆盖率偏低。2023 年，国产中间件市场并没有如预期实现快速发展，原因有多方面：第一，政策导向有待加强，未将基础软件“三驾马车”中的中间件与操作系统、数据库一并考虑，《安全可靠测评工作指南》未纳入中间件；第二，行业侧系统建设模式发生变化，同时由于资金紧张，建设放缓；第三，基于市场以及开源获取的便捷性，用户习惯于使用免费开源中间件；第四，供给侧创新能力及技术标准的自主能力有待加强，国内中间件企业规模普遍偏小，抵抗风险能力较低。

6.1 国产中间件在各行业的应用不均衡

6.1.1 党政用户国产中间件应用放缓

当前，国产应用服务器中间件在党政领域的替代取得阶段性成果，但采购进度放缓。消息中间件、分布式数据缓存中间件、交易中间件、负载均衡中间件、ESB 中间件、文件传输中间件等产品的替代还处于探索期。

6.1.2 金融电信系统逐步采用国产中间件

在金融行业，国产应用服务器中间件支撑了部分银行的核心业务。一些整体解决方案在银行的重要业务场景开展了技术验证，事实证明国产中间件能满足银行的业务要求。在保险行业，国产中间件在部分核心业务系统进行了应用，并在多家头部保险机构落地实施。证券、基金、期货机构更加活跃，应用服务器中间件、消息中间件、缓存中间件、负载均衡中间件等多款产品都在一定范围内得到了应用。尽管如此，国产中间件在金融行业各细分领域的核心业务应用方面，无论是品类还是数量都没有放开。这些领域仍以采用国外商业中间件或开源中间件为主，且开源中间件的使用比例有明显的上升趋势。

在电信行业，国产应用服务器中间件、消息中间件已通过各大运营商的测试，在天翼云、移动云、联通云等公有云平台，以及运营商内部的私有云平台皆已上架，但下载量不多。为适配运营商行业的云原生架构，应用服务器中间件、交易中间件、消息中间件等多款中间件已推出云原生版。应用服务器中间件已在计费、客服等核心系统大规模应用，各省分公司也在积极探索应用其他品类中间件。

6.1.3 部分行业应用国产中间件的意愿不强

其他行业用户应用国产中间件的意愿不强，原因主要包括以下几方面：

（1）用户普遍接受开源中间件

目前，开源中间件在各行业大规模应用，其中不乏行业头部企业。由于中间件开源社区主要集中在国外，我国参与开源社区的人数有限，且能贡献核心技术的软件非常少，因此我们对开源中间件的掌控程度明显不足，面临知识产权、断供、停服等各种风险。

（2）用户开展国产中间件替代缺乏政策依据

各行业对于中间件的替代没有提出明确要求，所以用户普遍认为中间件属于可替可不替范畴。应用系统直接应用开源组件，或使用云平台提供的开源中间件，也被认定符合要求。虽然多数央国企在国产中间件替代方面已经有了初步计划，但仍有部分单位对于国产中间件替代持观望态度。加上目前行业解决方案针对性弱，用户认为没有围绕实际业务场景需求进行兼容适配验证，普遍缺乏信心。

（3）用户对业务系统的升级改造持谨慎态度

以医疗行业为例，医院信息系统包括 HIS、LIS、PACS、EMER 等多个

子系统，业务量庞大，涉及的开发厂商较多、采用的技术路线各异，系统之间关联关系复杂、数据类型复杂。因此，应用系统的升级改造牵一发而动全身，对用户和开发商都是极大的挑战，所以较少采购国产中间件。

6.2 中间件厂商面临市场模式和标准规范问题

6.2.1 中间件厂商接触最终用户的机会少

随着行业用户数字化转型不断深入，对数字化建设基础技术能力提出更高要求，需要打破系统模块“烟囱”模式的边界，有效实现能力复用，实现数据、流程的拉通，以适应数字化时代对业务敏捷性、弹性及动态组合能力的要求。单一的中间件产品已无法满足上述需求，中间件的个性化、多样化需求愈发明显，品类也在逐步扩充。行业用户正在积极寻求能够灵活支持其实现业务，以及面向未来的完整解决方案，这就需要多种中间件产品组合的一体化平台来适应其特定需求。

云计算引发了软件开发部署模式的创新，云平台成为承载各类应用的关键基础设施，行业应用上云进程持续加深。中间件在云平台中扮演着核心角色，它连接了底层基础设施和上层应用，是云平台的重要组成部分，以服务形态呈现。

由于中间件服务化，用户对于中间件的采购模式从面向中间件厂商转向面向云平台厂商。目前，国内政务云、信创云、行业云等通常由头部集成商或云厂商统筹建设，中间件的选型一般由云平台建设厂商决定。这些厂商在平台建设初期，出于成本考虑，通常选择开源中间件或基于开源组件自研。常年积累下来，云平台技术架构体系已固化，技术人员已习惯使用这些组件，把云平台中的开源中间件替代成国产商用中间件的意愿不强。另外，由于中间件只属于云平台的一小部分，用户基本不关注，中间件厂商直接面对用户的机会变少。

6.2.2 中间件厂商很难参与优化性适配

随着应用场景的不断拓展，用户对中间件的需求也呈现多样化、定制化、智能化的趋势，对产品的性能、安全、稳定等指标提出了更高要求。用户越来越关注中间件对已建系统、新建系统、待建系统的兼容能力。

目前，中间件厂商与产业链上下游企业开展的适配，大部分属于兼容性适配，解决了中间件和其他软硬件产品之间的兼容性问题。但是，国产中间件要深入行业，不能把适配目标停留在简单调通，而是要真正用起来。这也就意味着要从兼容性适配转向优化性适配，基于实际业务场景实现整体调优。

然而，大部分行业客户并不直接面对中间件厂商，用户通常委托系统开发商组织开展应用系统的优化性适配，中间件厂商按照系统开发商要求，提供产品安装包及技术支持，处于被动地位。由于中间件在应用系统中比重小，影响力有限，厂商很难牵头开展围绕业务场景的优化性适配。实际上，中间件作为基础软件的三驾马车之一，处于操作系统和应用程序之间，是信息建设中的一个“连结器”，需要不断的保持技术更新以匹配上下层技术的发展，中间件的效率和性能将直接影响应用系统的效率与可靠性，在优化性适配环节至关重要。

6.2.3 中间件标准规范体系不健全

中间件技术标准主要由国外主导。应用服务器中间件一直遵循 Oracle 公司主导的 Java EE 规范，以及 Eclipse 基金会主导的 Jakarta EE 规范。国内厂商如果采用该技术研发应用服务器中间件，按照知识产权规定，每年必须缴纳不菲的技术使用许可费和认证测试费，且随时存在新技术许可被拒绝授权使用的可能性。

我国中间件标准规范体系不健全，存在技术标准老化及缺位的情况。如2011年发布的《基于J2EE的应用服务器技术规范》（GB/T 26232-2010）至今未做修订，已经不适应当前的技术体系框架。虽然供给侧为实现中间件研发、使用、维护的规范化在努力推动标准规范体系的建设，发布了一些团体标准，与用户单位合作编制中间件产品叠加应用场景的技术规范，但这些标准规范的影响范围有限。另外，我国尚未建立与自主技术路线相匹配的中间件技术标准和测评标准体系。随着中间件在信创领域应用的不断深入，面向此领域的中间件技术图谱已逐步形成，但是具有信创特点的中间件技术标准不多，与自主技术路线相匹配的标准体系尚未建立。

6.3 多措并举，促进国产中间件的行业应用

6.3.1 规范市场秩序，引导中间件产业做大做强

统筹规划包含中间件在内的基础软件全面发展，在相关政策文件中将中间件与操作系统、数据库一并考虑，引导各行业积极使用、应用尽用国产中间件。在国产商用中间件无法满足业务需求的情况下，依次可选择根技术在国内的开源中间件、国外开源中间件。

鼓励中间件厂商与国内开源基金会合作，积极参与我国中间件开源技术体系和开放产业体系的发展。参考操作系统领域openEuler、openKylin开源社区的先进经验，组织建设我国主导的中间件开源社区。同时，保护开源生态下的新型盈利模式，引导用户为中间件软件的专业版、定制化、版权授权等付费，助力企业营收增长。

通过抑制低价竞争、统筹建设行业信创生态实验室等手段，引导扶持国内中间件企业进一步向规模化方向发展，培育和打造一批具有国际竞争力的中间件企业，带动中间件产业竞争力整体提升。

6.3.2 围绕行业需求，加速技术攻关和生态建设

（1）满足行业用户高性能高并发高可用需求

中间件厂商充分利用国家政策和资金支持，开展产学研联合攻关，全面对标国外产品，找差距、补短板，加强中间件核心基础技术研究，持续提升各类中间件的整体性能，以及适配云计算环境的云化能力；紧跟新技术发展，在云原生中间件、物联网中间件、大模型中间件等新兴中间件领域提前布局，尽快实现研究成果转化，推出新产品。另外，还应深入了解重点行业、重点用户的应用需求，加强针对国内软硬件设备整体架构、整体性能优化的核心技术研究，满足行业用户高性能、高并发、高可用需求，树立用户对国产中间件的信心。

（2）尽快补齐新兴中间件领域的短板弱项

中间件的发展历经支撑中间件、SOA 集成中间件、数据中间件、云原生中间件时代，伴随人工智能迅速发展，即将迈入智能化中间件时代。在支撑中间件、SOA 集成中间件等传统中间件领域，我国已有深厚积累，国产商用中间件产品成熟稳定，具备替代国外同类产品的实力；在云原生中间件、智能化中间件等新兴中间件领域，成熟的国产商用中间件产品暂时较少，仍以国外开源中间件为主。中间件厂商应尽快加紧新技术研究，克服云原生技术栈复杂、技术迭代快等困难，尽快推出能替代开源组件的成熟商用中间件产品。

（3）围绕应用场景开展适配，不断完善生态体系

行业信创已逐渐进入落地实施阶段，围绕应用场景开展产品适配，建立完善的生态体系尤为关键。中间件厂商应积极与各相关方开展广泛合作，围绕应用场景开展产品适配，将生态适配发展成为产品的核心竞争力；积极探

索与云平台厂商的合作方式，实现优势互补、合作共赢；建立全面优质高效的技术服务体系、培训体系，提高整个生态系统的凝聚力和向心力；提供开放的技术平台，吸引更多的开发者和合作伙伴参与技术创新；同时，加强市场推广和品牌建设，提高自身知名度和影响力。

6.3.3 供需双方合力，加强中间件开源治理工作

（1）梳理开源中间件清单，评估潜在风险

由相关部门牵头，组织厂商全面梳理中间件开源技术，形成开源中间件清单。准确评估每一款开源中间件的潜在风险，包括技术风险、安全风险、法律风险等，如：审查开源中间件的历史和社区，了解质量和安全性的线索；对代码进行审查，发现其中的潜在问题；检查开源中间件的依赖项；检查开源中间件的文档和日志，发现任何潜在的问题或错误。

（2）建立开源组件治理体系，确保软件供应链安全

厂商应建立开源中间件治理体系，组建团队负责开源组件的统一管理；建立管理流程，明确开源组件选型测评、使用管理、运维管理、定期健康评估等方面的工作内容和步骤；建立开源组件黑白名单机制，规范开源组件使用；采用开源治理工具，定期开展开源组成分析和安全性分析，识别开源组件漏洞、许可证和隐私安全方面的安全，保证安全合规使用开源组件；针对开源组件潜在风险落实应对措施，例如进行代码审查、加密通信、授权许可等。

（3）统筹建设行业开源中间件治理体系

行业主管部门加强对开源中间件的防范意识，统筹本行业开源中间件治理体系建设。首先，对业内单位使用开源中间件的情况进行摸查，梳理业内使用开源中间件清单；其次，行业主管部门参考供给侧形成的开源组件风险

评估结果，充分考虑业内单位实际情况，围绕开源中间件引入、使用、清退各阶段，制定开源中间件治理体系框架；最终，业务单位根据本行业开源中间件治理体系框架要求逐步落实。

6.3.4 统一推进我国中间件技术标准体系建设

（1）标准组织统筹中间件标准规范建设

中间件软件产品形态越来越多，建议由国内相关标准组织牵头，成立中间件标准体系建设小组，专门负责中间件标准规范体系的规划、建设和推广工作。由建设小组统筹现有中间件标准规范的更新、修订和补充，制定标准规范编制计划，为国内中间件研发、使用、维护提供更好的指导和参考。

（2）测评标准体系与技术标准体系并重

将中间件测评标准体系与技术标准体系放到同等重要的地位，通过标准化推动解决中间件在信创建设中的问题。中间件测评标准的建立应该紧密围绕产业发展实际，建立多维度能力评估体系。由单一以性能评价为主，转向场景化测评、安全性评估、自主可控度评估等多维度能力评价。

（3）将标准规范宣贯统一纳入中间件标准规范体系

鼓励中间件厂商组织开展中间件标准规范培训，推动从业人员、行业用户掌握标准、理解标准。

本章编写人员：

北京东方通科技股份有限公司 于滨峰、俞立平、曾鹏冰

深圳市金蝶天燕云计算股份有限公司 成勇斌、邝敏越、刘志杰

第 7 章 整机

从现阶段国内实际情况看，虽然信创产业已经形成一定规模的生态体系，但对标国际成熟的技术生态体系，仍然面临技术选型难、适配验证工作繁重、应用系统不稳定、行业场景化方案不足以及缺乏统一权威标准参考等挑战。

7.1 市场取得一定成绩，规模不及预期

7.1.1 在部分行业实现增量发展，但整体市场规模不足

在信创产业中，整机是用户首要关注的产品，无论是商业用户还是消费用户都离不开高性能、高稳定性的整机设备。在国家、地方和行业多重推动下，行业用户对信创的了解越来越多，这无疑是对信创产业发展的一种肯定，但是业内期盼的 2023 年信创市场爆发局势并未出现。与普遍的预期相反，2023 年整机市场数据呈下滑趋势，主要原因在于：一方面，在整机市场占比最高的党政领域采购量下降；另一方面，行业的采购虽稳步推进，但规模有限，无法弥补党政市场销量降低造成的缺口。

7.1.2 产品不断丰富，稳定性和可靠性相对不足

整机企业与产业链上游企业同步，加大解决方案、生态建设力度，持续丰富产品种类并进行迭代，不断提升产品竞争力。在通用计算服务器方面，新的型号和配置不断推出，以满足不同用户的需求。在 AI 服务器领域，整机企业基于昇腾、海光 DCU 等新产品发布了新品，以满足高性能 AI 计算需求。台式机和电脑更关注使用体验，向小型化方向发展，基于信创软硬件的云终端产品也在不断丰富。在解决方案方面，结合数字化转型的目标，可以为用户提供定制化服务。

但是不可否认，部分信创产品在稳定性和可靠性方面还有差距，这在客

观上影响了行业用户采购信创整机产品的决心。

7.1.3 信创整机在使用和开发方面可能面临困难

尽管信创整机在部分行业的市场占有率有不错的表现，随着产业链上下游企业的互认证数量快速增长，产业生态也在逐步完善，但由于生态问题导致的使用和开发困境仍然存在。这个问题如不能得到很好地解决，会对信创整机产业造成比较大的负面影响。用户在实际应用中可能会遇到兼容性和适配性的问题，信创整机在真替真用方面效果并不理想。例如，一些软件只能在特定的操作系统上运行，而部分信创产品无法完全兼容该操作系统。通过对用户的回访发现，“采而不用”或者在信创产品上通过虚拟化技术继续使用 Windows 操作系统及其生态下的各类应用软件的情况并不罕见。另外，由于开发者社区和支持体系还不够完善，导致开发者在使用信创产品时面临缺乏开发文档、示例代码和技术支持等困难。

7.2 市场表现受政策标准和生态建设的影响较大

7.2.1 空间有限，产业内卷，用户观望

造成整机市场这一情况的主要原因有市场和政策两方面因素。一方面，整机市场过分依赖于党政等几个行业，市场基本面小，导致厂商不得已采取低价策略抢占市场份额。另外，用户因经费紧张暂缓采购也是影响市场规模的因素之一。

另一方面，用户的采购行为受政策影响较大。2022 年以来，为促进整机市场发展，引入更多企业参与其中，相关机构发布了一系列产品标准规范，引导企业生产符合标准要求的产品。随着相关采购标准进入实质阶段，新企业可以更容易地进入市场，并与现有企业进行竞争，有助于提高市场活力，推动行业创新和发展。但这一变化客观上导致用户在没有明确政策依据的情

况下，普遍持观望态度。此外，整机厂商在过渡阶段缺少符合标准规范要求的产品，客观上也造成了市场推广的困难。

第三，部分用户对信创整机产品“采而不用”的现象并不少见。尽管主要原因是使用习惯问题（这一问题随着政策的逐步落实必将有所解决），但在现阶段的确导致部分潜在用户采购意愿不强。

7.2.2 上游技术路线分散

整机产品上游技术路线过于分散，全面适配基础软硬件技术路线的工作量十分巨大，进而导致驱动程序、基础环境软件和应用软件的开发难度陡增。因此，基于信创整机的软件多为轻量级或基于 WEB 架构开发的应用，缺少重量级业务系统软件。这也是导致信创整机产品无法深入行业的原因之一。

构成信创整机的元器件种类繁多，元器件的质量稳定性直接影响整机的质量和稳定性。元器件之间的兼容适配性，也是影响整机稳定性的主要因素。由于需适配的元器件多，不同厂家、型号的器件都要适配，工作量大，需要整机企业协调元器件企业、固件企业和操作系统企业合作，共同努力完成兼容性适配工作，这是影响整机稳定性最大的难题。

7.2.3 行业应用场景适配量不足

当前整机与生态伙伴的适配认证多集中于设备与软、硬件产品的单点认证，针对行业应用场景的集成化、系统化解决方案相对欠缺。从需求侧分析，整机应用是与行业、客户、应用场景的业务强相关的，行业应用需求是整机市场规模提升的根本。如能提升“真替真用”力度，对于行业应用本身和整机行业来说将会产生相互促进的良性循环。一方面，信创环境下的行业应用在落地过程中会对整机及其生态伙伴产品给予正反馈，刺激整机产品逐步丰富；另一方面，整机产品的丰富又降低为行业应用适配的难度。反之，应用

和整机之间会相互制约。同理，缺乏行业应用也会制约开源社区的发展。

7.3 标准化和解决方案拉动整机真替真用和市场发展

7.3.1 政策牵引和标准规范并行，提高行业信创产品占比

信创产业本身具有一定的政策属性，因此推动和解决行业的信创整机问题，也需要加强政策引导并通过标准规范市场行为。一方面，主管部门应继续强化信创政策的落地，加大监督考核和激励力度，提高信创产品在行业信息化、数字化、智能化过程中的应用比例，从而使行业用户在政策指导下，进一步坚定决心和信心，加大投入、加快替代升级的步伐。另一方面，相关机构要加快推进信创整机产品的技术标准和采购标准制定，以及采购预算与采购配置的分级分档等工作，帮助行业用户对整机产品的成熟度、性能、稳定性做出有效判断。

7.3.2 通过供应链成熟度检测和质量监控提高产品质量

整机企业作为生态链的中间环节，需要做好衔接，向上对接基础软硬件供应商，协同解决芯片、系统、应用等各环节的问题，提升产品的质量、性能和用户体验；向下对接用户需求，营造生态合力，加速推进产业化进程。针对供应链元器件质量与兼容性问题，整机厂商需建立正确评估供应商元器件质量的能力，量化供应商的生产能力数据，以确保供应链的可靠性。针对下游厂家的生产制造问题，需要依据企业的产品范围和特性进行定制规范，引导工厂向智能化发展，建立有效信息传递机制，提高信息拉通与内部信息的传递效率。

7.3.3 以生态建设和培训拉动 " 真替真用 "

整机企业要充当生态引领者角色，发挥产业链资源优势，联合上下游企

业加强合作、协同创新，加快推进生态建设，重点聚焦面向行业的场景化解决方案，不断丰富生态体系，满足行业信创建设需求。针对用户在使用过程中出现的各种困难，建议从两方面着手：一是加大终端用户培训频次力度，提高使用者对整机产品的了解、提升他们对自主创新的信心，提高他们的操作能力，逐步改变使用习惯。二是对运维人员进行信创运维方面的培训和认证工作，储备相关运维人员，使其能够在需求侧及时响应并解决使用过程中出现的问题，提高服务效率。

本章编写人员：

同方计算机有限公司 张伟、邓忠良、李亚军

中国长城科技集团股份有限公司 阮开利、徐庆荣、刘美、陈睿博

中国航天科工集团第二研究院七〇六所 王晓光、田斌峰

中航鸿电（北京）信息科技有限公司 严华锦

百信信息技术有限公司 侯飞、李正中

武汉万数科技有限公司 杨倩

第 8 章 办公软件

当前，信创产业进入以行业信创为主的深水区，办公软件正经历数字化、智能化的变革期。多重趋势叠加的大背景下，办公软件产业迎来巨大发展机遇，同时也面临着诸多问题和挑战，如“真替真用”比例还有待提升、行业用户替代需求不足、厂商适配负担过重、盗版软件挤占市场空间、用户对信创产品的认知较浅、信创标准体系尚不完善等。

8.1 用户“裹足不前”，厂商“负重难行”，行业“荆棘丛生”

目前，国产办公软件在党政和金融领域渗透较高，已步入常态化应用阶段。2022 年行业信创政策相继出台，电力、电信、石油、交通、教育、医疗、航空航天等行业的信创逐步启动，企业成为行业信创的主力。据海比研究院调研数据显示，民营企业是最大的信创用户群体，占比 62.4%[4]，存在巨大的市场潜力。但整体来看，行业用户由于种种原因多持观望态度，替代动作较为缓慢，信创采购量相对于现有市场的设备存量，比例依然很低；同时，厂商面临巨大的产品适配、服务保障等方面的成本和负担；盗版软件影响市场公平竞争、健康发展的因素依然存在。

8.1.1 用户使用量稳步增长，“真替真用”仍有提升空间

随着国产办公软件在党政、金融领域的推广应用，用户使用量稳步增长，并且由于成熟度高、稳定性好、独立性强，功能和性能上已完全能够支撑用户的日常办公需求，获得了良好的替代进展和积极的使用反馈。然而，由于使用习惯固化、双系统并行等原因，党政机关和行业机构中活跃用户的比例依然较低，“替而不用”的现象仍然存在，“真替真用”仍有提升空间。这

[4] 《2022 中国信创生态市场研究及选型评估报告》

影响信创企业产品技术的快速迭代和服务能力的不断提升，不利于信创产业的可持续发展。

8.1.2 行业信创存在“重硬件轻软件”的倾向

随着行业信创的启动，办公软件看似将迎来比党政信创更大的市场。然而在实际的采购中发现，行业用户普遍存在“重硬件轻软件”的倾向，用户采购的重点大多在于服务器、计算机等硬件设备。以教育行业为例，很多教育行业用户将采购的预算更多放在电子黑板等硬件设施，软件则继续沿用之前的国外软件。据东吴证券测算，行业信创 PC 存量为 6000 万台，行业信创服务器存量为 800 万台[5]，与之相比，办公软件的采购数量明显少于硬件。究其原因，可能在于硬件产品较能产生直观的视觉和性能体验，而软件产品的价值体现则相对较为间接。

8.1.3 部分办公软件未赶上名录，等不来标准

在过去的党政信创阶段，信创名录是地方政府、企事业投入信创改造的重要标准依据。名录最后的更新时间是 2021 年，此前未能加入名录的企业，相当于错过了名录的“末班车”。当前，虽有使用行业标准来替代名录的说法，但不同产品品类标准出台的时间不尽相同。这导致仍有一些信创概念的产品既没有录入名录，也没有对应的标准支撑，处于政策“空窗期”，在市场推广中，缺乏说服用户采购使用的强有力依据。

8.1.4 低价恶性竞争存在，适配成本过重

根据目前的办公软件市场来看，恶性的低价竞争和高昂的适配成本，成为制约企业发展的两个重要因素。首先，信创市场缺乏对企业资质、产品技

[5] 东吴证券相关数据

术和服务质量等方面的规范要求，造成一定程度的恶性竞争，阻碍信创产业良性发展；其次，信创采购中软件定价机制不完善，无最低限价等限制措施，造成部分企业通过低价竞争策略扰乱市场秩序。此外，在软件和信息技术服务行业，不同的软件产品之间需要进行适配和集成才能实现更好的功能和性能，但是由于不同的软件产品来自不同的厂商，其接口标准、数据格式、技术架构等方面都可能各不相同，因此需要进行适配和集成，这难免会增加企业的成本和技术难度。由于需要适配的软件产品数量较多，相互组合的可能性更多，使得企业的成本呈指数级增长。

8.1.5 盗版软件扰乱市场，阻碍自主产品普及

虽然相关部门加大执法力度，对盗版软件行为进行了严厉打击，但目前用户使用盗版办公软件的情况仍然存在。一些盗版软件通过在线销售平台以低廉的价格销售，对用户声称是正版软件。用户可以方便地以异常低的价格购买盗版软件，自然不会支付更高的价格购买正版软件。在此情形下，自主产品不能以价格优势来争夺市场，难以普及。

8.1.6 用户对软件存在使用惯性，制约自主软件推广

UOF、OFD 作为国家自主知识产权的电子文件格式标准，在支撑行业深度应用、探索前沿技术创新等方面具有强大的自主性和灵活性，在关键技术产业链中也具有显著的技术价值和经济价值。随着国产化替代的推行，UOF、OFD 逐步进入到普通大众的视野，能够满足人们日常办公的基本使用需求。但是 docx、pptx、xlsx、pdf 等国外标准的文档格式已经为用户所习惯，用户先入为主的使用惯性仍旧很大，加上用户对于国产自主文档格式的认知较浅，缺乏使用积极性，严重影响了自主知识产权文件格式的推广应用速度，阻碍了国产自主软件生态的构建进程。

8.2 技术要提升，标准待加强，市场需优化

8.2.1 重要短板技术还需持续攻关

目前，在与 AI 和云计算等新兴技术融合应用方面，国内办公软件厂商与国外巨头还存在差距，在信创环境下这种差距尤为明显。国内办公软件厂商和生态伙伴仍须加大技术攻关投入，不断提升产品好用、易用程度，推动产品和服务为更广阔的市场所认可，减少对政策扶持的依赖。

流式办公软件、版式办公软件在关键核心技术上有了很大提升，但在重要短板技术上还需持续攻关。一是在线办公软件功能不够完善。目前在线办公软件深度功能略显薄弱，一些复杂的内容格式设置无法在网页端和移动端解决。例如，在线表格对 Excel 公式、函数和图表的支持不如桌面端完善，数据处理效率不高。二是二次扩展能力有待增强。随着企业端用户业务需求的多样化和复杂化，在线办公软件需进一步增强定制化开发和二次扩展的能力，针对不同的业务场景提供个性化、智能化、可扩展的协同办公工具，目前这方面能力有待加强。

就图像处理类办公软件而言，国内图像处理软件已覆盖 Photoshop 90% 的功能，在技术成熟度上虽然完成了超大像素图片处理的突破，实现了较丰富的特效和 AI 处理能力，但在细节处理、性能方面还存在差距。在 PSD 的兼容上还不能做到 100% 的兼容。这些产品、技术成熟度的差距也是国产软件在专业图像处理方面滞后于国外软件的主要原因。

8.2.2 产品还需与国际产品兼容适配、做到平滑过渡

长期以来，国内办公软件市场一直为微软、Adobe、Google 等国际 IT 软件巨头所占据，从用户习惯到功能接口均形成了国际惯例和标准规范，用户对国外品牌体系形成了很强的认知和使用惯性，日常办公所使用的软硬件

设备、内外部沟通互动所使用的界面等都与国外产品深度绑定。虽然国内的流式软件和版式软件在功能界面和使用性能方面都越来越接近甚至超越了国外软件，但用户由于长期形成的品牌认知和使用惯性，缺乏自主转换的动力，在短时间内难以转换。为了满足用户跨国、跨地区的文件交互需求，国产办公软件需要具备与国际产品相似的功能和性能，以确保用户可以平滑迁移、无感过渡。

8.2.3 下层系统数量多，技术能力参差不齐，标准不统一

在信创产业链上，办公软件处于最末端，因此也受下层技术路线众多的影响最大。所有的技术路线组合都要求应用软件产品能完美运行，这就要对每种组合做适配测试，而目前这些系统的技术能力参差不齐，也没有统一的标准。各操作系统的底层支撑库也不一致，产生若干种适配组合，同时，适配过程中还可能存在缺失或者版本不统一的情况，经常出现各种问题。有时应用软件代码一个简单的功能，要设置多个开关、分支来适应不同的组合。以上种种情况造成适配工作量巨大，服务成本高。

8.2.4 自主知识产权文件格式政策力度不足

自主知识产权文件格式的发展与应用虽小有成果，总体上仍旧处于起步期，国家政策的扶持与引导至关重要，但目前来看政策力度稍显不足，主要体现在：一是政策标准宣传力度不足。导致用户对自主文件格式标准应用的定位、意义和作用认识不到位，没有认识到自主标准的技术特点与应用优势；二是行业标准支持力度不足。在行业应用系统中对自主文档格式标准的应用不够重视，在技术选型中对国外标准与国家标准不加区分，支持国家自主标准的意愿导向含糊不清，进而难以扭转国家标准在实际应用中的劣势局面。三是行业场景应用力度不足。目前除了电子公文、电子证照等少数领域

构建了基于自主文档格式标准的应用场景，在更多的行业场景中，用户单位技术决策相对保守，导致自主文档格式缺少杀手级应用场景，应用生态构建缓慢。

8.2.5“应替”“能替”的范围不够明确

在推广和应用国产办公软件的过程中，对于能够替代哪些国际办公软件，以及在什么情况下应该选择国产办公软件，各领域缺乏明确的认识和界定。要做到“应替尽替”“能替尽替”，但用户并不明确什么是“应替”或“能替”的范畴，导致在采购时犹豫不决，产生“多一事不如少一事”的心态，偏向于“不明确指出需要替代的就先等着不替”的思想，导致一些信创办公软件推广进度缓慢。

8.2.6 用户版权意识有待提升，盗版软件打击力度不足

在国产办公软件行业中，盗版软件在市场上仍然存在。一方面，用户对版权保护的重要性缺乏足够的认识，可能出于节省成本、方便获取、版权意识淡薄等原因，抱有“不出事就使用盗版”的观念，选择使用盗版软件。另一方面，有关部门对盗版软件的打击力度不足，导致用户在网络上能轻易搜索获取盗版软件。甚至有些网站还以平台的方式提供大量的、低廉的盗版软件。

8.2.7 信创软件定价体系不完善

当前，软件价格仍然是用户选择软件的主要考虑因素之一。因此，一些信创软件厂商为了争夺市场份额，会采取低价策略，进行激烈的价格竞争。为了降低成本，一些信创软件厂商甚至会在产品质量上做出妥协。这可能导致软件产品存在漏洞、功能不完善、性能不稳定等问题，从而影响用户的使

用体验和满意度。这暴露出信创软件定价体系不完善的问题，也造成用户对软件价值的低估。

同时，由于用户对信创软件的价格存在刻板印象，认为信创软件就应该价格低廉，对于价格较高的软件产品往往会产生抵触情绪，使得信创软件厂商陷入产品质量不断提升、服务保障不断优化、成本节节攀升，但价格很难提高的困境，导致厂商利润微薄，难以支撑长期的技术研发成本和服务成本，难以形成规模效应，最终限制企业的发展和壮大。

8.3 以投入增实力，从底层推适配，用标准促发展，借正版化推国产化

8.3.1 加大研发投入，增强技术实力

产业的长远发展离不开过硬的技术研发能力，办公软件厂商还需持续坚持自主创新、加大研发投入、提升技术实力。流式软件在保障主流办公功能的基础上，还需针对在线流式软件的 AI、云计算等技术短板持续攻关，加快在线流式软件与云计算、存储等融合技术的研发，加强在线流式软件与信创云的兼容适配，加大服务端信创应用技术研发力度。针对在线版式软件的图像渲染处理、行业融合应用等技术短板，还需加快精确渲染、自然语言处理、行业融合应用等技术研发，进一步提升在线 OFD 产品技术水平，推动自主产权的在线版式创新技术成果的落地应用。

国产图像处理软件虽然种类较多，但绝大多数都属于非专业类的图像处理软件，更多的是偏向于娱乐、消费类的 C 端产品，也有一些是偏向于某个细分行业的专用产品。对标 Photoshop 的专业软件需要加速研发，在功能覆盖度上更上层楼，在性能上力求达到和超过国外同类产品。这样才能打下替代的基础，解决替代问题。当前，国内图像处理类办公软件还需加强 AI 在图片处理的能力、加大 AI 在图片处理的应用范围。在图像底层的算法上加

大投入，优化图片处理性能，争取早日实现弯道超车。

8.3.2 推动底层系统厂商带头整合生态适配

应用软件直接面向用户，但底层架构还是构建在芯片、操作系统上。应用软件能否向用户提供稳定、可靠、优质的服务，一定程度上取决于芯片、操作系统的支撑能力。相应地，国产芯片、国产操作系统能否得到用户认可，也和构建在其基础上的应用软件多少、优劣有很大的关系。这是一个相互依存、共同发展的生态体系。办公软件厂商还需持续优化完善办公软件产品，加强与国产 CPU 和操作系统的适配性，加强与信创云、第三方中间件和数据库等的兼容适配，创新智能云办公等产品的服务形式，提高产品吸引力和用户黏性。加快在线办公软件平台化发展，为用户提供定制化平台服务。

同时，针对目前各种产品出现的适配问题，建议由底层系统厂商牵头，成立信创适配“专委会”，带头整合生态适配，收集、分析问题，提出整体解决方案，促进技术路线收敛，从而降低各应用软件厂商的适配成本，加速产品推出和完善。

8.3.3 完善标准体系、推动标准落地，促进国际接轨

目前，我国关于办公软件的标准有了一定的发展，特别是流式办公软件的标准，无论是团标、行标还是国标都在修订中，版式办公软件的标准相对较少。因此，完善办公软件标准体系，加快标准落地，促进标准与国际接轨，成为办公软件行业发展的重要任务。未来，办公软件行业还需从完善体系、深化使用、拓展行业三方面着手发力。一是以信创技术标准建立为核心，完善在线办公软件标准体系。研究制定用户从微软生态向信创生态无感过渡的评估指标，促进信创产品的易用性，拓展信创产品应用。二是加快办公软件二次开发标准、OFD 软件功能标准等重要技术标准的迭代更新，推进服务端

的文档协作、安全防护等服务接口的标准化，促进上下游厂商协同发展。三是推动办公软件厂商在 UOF、OFD 等自主版式标准上加速布局，加快推出 UOF3.0、OFD2.0 标准，推动电子票据、电子健康档案、电子法律文书等细分领域中 OFD 标准子集的编制。基于 OFD 标准的技术特点和产业优势，推动 OFD 标准在国际相关领域进行深化应用，提升 OFD 标准的国际化水平。通过标准推动不同产品的互通性，并加强反垄断监管。四是探索面向 AI 机器学习、自然语言处理方向的文档技术标准，推动技术标准逐步从面向文档生成、阅读的简单场景向文档流转管控、分析处理、智能办公等复杂场景进行深入扩展，充分发挥自主标准、自主软件在行业应用下的创新能力。五是加速推进基于 UOF、OFD 的技术应用方案在财政票据、金融凭证、医疗卫生、公安司法等行业的落地推广。六是要让国产办公软件产品与国际产品兼容适配、做到平滑过渡，需要建立兼容标准、加强技术研发、适配国际标准、推进生态建设、加强用户培训和教育以及政府支持等多方面的努力和支持。

8.3.4 出台办公软件信创采购标准

相关部门已出台软硬件信创采购标准，但有关办公软件的信创采购标准尚未出台，针对信创名录不再更新，行业标准尚未推出的“空窗”期现象，还需加快出台办公软件信创采购标准，新出台的标准应包含进更多品类的办公软件。或者在标准出台前发布一个过渡阶段的解决办法。同时，为提高“真替真用”比例，还需明确“真替真用”使用要求、加大对用户使用情况的动态监测、出台“真替真用”评估检查标准、建立定期评估检查工作机制等。

8.3.5 正版化和国产化协同推进

软件正版化和国产化是推进各产业高质量发展的重要保障。加大办公软件正版化工作力度，加速办公软件国产化进程，是实现中国式现代化的必由

之路。在宣传上，还需持续提倡尊重知识产权，提倡软件正版化，对用户做正向的引导。在打击盗版上，还需清除盗版软件的源头，特别是要严格监管网络上的各种应用软件下载网站，严厉打击以低价出售盗版软件的平台。让用户不能轻易获取到盗版软件，也避免用户上当受骗。同时，加大对使用盗版软件的企事业单位的处罚。只有正反两面双向合力，才能促进国产软件产业的健康快速发展，才能促进信创工作的高质高效推进。

本章编写人员：

北京金山办公软件股份有限公司 刘彬、马静

北京亦心科技有限公司 韦祖兴

永中软件股份有限公司 梁勇

友虹（北京）科技有限公司 黄岩、宋涵

第 9 章 打印设备

在政策驱动下，国产打印设备在党政和金融行业得到了广泛应用，但在其他领域的应用推广还存在挑战。在政策红利逐步结束、产品化成熟度待提升、高端产品仍需持续投入、产品成本优势仍不明显的情况下，打印设备发展进入了一个缓慢发展时期。

9.1 打印设备深入行业市场面临阻力

9.1.1 全行业推广任重道远

打印设备在党政办公系统中的应用趋于成熟，其采购工作基本告一段落。金融行业是全面推广信创的第二大行业，五大行及部分商行在 2023 年逐步完成了集采招标。电力行业也组织了集采工作，目前尚未实现大量采购。在交通、电力、能源、教育、电信等行业，国产打印设备的推广仍处于起步阶段。在医疗、工业等领域，虽然国产中低端打印设备已满足日常办公的市场低端需求，但在涉及业务系统和生产环境的专业领域和高端市场，打印设备的应用推广依然任重道远。

9.1.2 技术标准明显滞后

2023 年，中国电子技术标准化研究院组织完成了对 GB/T 29244-2012《信息安全技术 办公设备基本安全要求》的修改，合并了 GB/T 38558-2020《信息安全技术 办公设备安全测试方法》主要内容，标准名称修改为《信息安全技术 办公设备安全规范》。该标准已于年底完成了征求意见稿的确认。尽管标准中增加了基于可信计算的相关安全要求，但是打印设备核心技术，如打印文件格式支持、网络打印协议、耗材标准规范等具有信创生态技术特色的标准依然缺失。

以对 OFD(Open Fixed-layout Document) 版式文件直打为例，目前 OFD 作为中国自主的文档格式，在政府机关和关键行业得到了广泛应用，对电子公文 / 业务凭证的格式统一、共享交流、安全保证等具有重要意义。由于相关标准的缺失，打印设备对 OFD 打印的支持能力缺乏，导致目前对 OFD 文档的打印都需要转化为 PDF 文档格式。受 PDF 文档规范的制约，在打印过程中，OFD 文档打印内容解析错误、输出不稳定、传输安全性等问题比较突出。

网络打印协议等底层自主协议仍旧空白。网络打印协议是打印系统的核心规范。当前，国内打印系统仍旧全部采用国外的网络打印协议。一方面，现有的网络打印协议不能完全适应国内的应用环境，无法满足国内应用需求，不仅影响打印应用的深入开发，还存在打印安全隐患。另一方面，自主打印网络协议的缺乏，制约了国内自主打印技术的底层创新和国内打印技术链、产业链的完整构建，影响了国内打印设备竞争力的进一步提升和整个行业的深入发展。

9.1.3 核心技术实现攻关后面临新的挑战

龙芯于 2023 年 11 月完成了打印主控芯片 2P500 的发布，实现了打印机主控芯片的技术突破。北京辰光融信、汉光、汉图、长城等打印机厂商完成了基于 2P500 的打印机研发及发布，奔图也基于自研芯片完成了高速黑白激光打印机的研发。自主打印主控芯片的成功研发，解决了打印主控方面的“卡脖子”问题。此外，打印机用高速马达及马达驱动芯片、打印机用二极管驱动芯片均实现了技术上的突破，实现了在国产打印机上的成功应用。但是，产品要完全满足市场化的需求，仍面临新的挑战。定型量产、降低成本、完善生态等问题，都是面对市场需要解决的问题。

9.2 打印设备厂商面对开放市场的考验

9.2.1 政策驱动对行业市场影响力微

目前，打印设备已逐步进入市场化阶段，通过政策护航国产化打印设备的优势正在逐步减弱。随着党政办公场景下的国产化替代接近尾声，打印设备的后续重点目标市场是行业用户。与党政领域不同，行业用户更关注产品的性价比，采购成本及耗材成本对其采购有直接的影响。国内打印设备厂商的全自主产品刚刚陆续完成研发及小批量生产，无论从产品稳定性还是从产品整体成本控制方面，还不具备与国外成熟产品直接竞争的能力。

9.2.2 标准滞后源于技术积累不足

标准是技术发展和积累的体现。自主技术积累的不足是制约打印设备行业标准制定的重要因素。当前，国内打印设备大部分企业仍旧没有完整掌握相关的底层核心技术。以打印系统为例，从底层数据处理引擎到网络打印协议，从打印应用到驱动程序，从打印服务框架到打印安全体系，相关技术的研究和积累仍旧不足。

除此之外，企业制定标准的动力也不足，缺乏抢占标准制高点的意愿。一方面，与生产和营销相比，制定标准的效益显现时间较长；另一方面，面对国外成熟的标准和规范体系，国内企业对制定自主标准的影响力也似乎信心不足。

9.2.3 投入产出失衡对供应链产生影响

经过近两年的技术积累，具有自研能力的打印设备厂商联合上下游供应链企业，已逐步实现了打印机核心技术及核心零部件的技术攻关，实现了国内打印设备供应链体系的建设。由于尚未实现量产且研发成本较高，新产品的价格与国外成熟产品相比没有竞争优势。另外，由于产品尚未接受市场考

验，无论是对打印机厂商，还是对核心技术攻关联合厂商而言，在产品未定型量产、生态尚未完善的情况下，均面临未来新的挑战。

9.3 多管齐下推动打印设备突破困境

9.3.1 主动适应行业需求

一方面要以用户为中心，打造“好用”“易用”且“用得起”的精品。相关厂商要始终以行业应用为抓手，以产品好用为目标，以应用需求牵引技术攻关、倒逼技术创新，引导优势技术和资源整合。在功能、性能、兼容性、易用性、可靠性、维护性、可移植性方面更多地深入了解各行业的需求和痛点，提供真正解决需求痛点的行业定制化产品、解决方案和增值服务，如骑缝章打印、溯源打印、保密打印、红头专色输出、移动打印、静音打印、铜版纸打印、不干胶打印、长纸打印等。

另一方面要主动适应行业需求，提升行业用户打印安全的防范意识，培养用户使用习惯。相关企业应充分发挥国产化打印机的安全特性，通过加强对用户的培训，提升用户对国产打印设备的了解和使用水平，提升行业用户对打印设备的安全意识，促进自主可控安全打印设备的应用和推广。针对开放市场，要加强品牌建设、驱动平台支持和售后维护的力度，切实提升用户对产品的认知度和忠诚度。

另外，要加强产业协作和生态链建设，解决产品兼容性难题。兼容性认证和适配工作非常重要且非常繁琐。打印厂商要针对行业的使用场景，解决技术协同和产品适配问题，从底层解决不同产品之间的兼容性和互操作性问题，在应用层建立统一应用编程框架，统一规范 API 接口。

9.3.2 尽快完成标准化

建议标准化管理机构对发布于十年前的办公设备安全要求和测评规范进

行充分修订，以满足当前外部设备的安全需要。同时，还应当制定一批标准和规范，如网络打印协议、文印服务数据安全要求、OFD 打印语言规范等，以推动外部设备底层技术链条构建、推动行业的持续和深入发展。

技术积累是标准发展的根基。因此，打印设备厂商需要不断加强技术研发工作，加大对核心技术、前瞻性技术的研究投入（如数据处理引擎、可信嵌入式体系、高效网络打印通信机制、对自主版式文件的底层支持，以及打印安全体系、无驱打印框架体系等），为标准制定提供技术验证和底层支撑。

9.3.3 产业联合提升核心竞争力

从大局来看，如果要把多年的研发成果实现经济转化，国内打印设备厂商需由竞争转向合作，在核心技术、专利授权、供应链体系建设、制定相关规范标准等方面，共同推动国内打印设备核心技术及生态的发展。

本章编写人员：

北京辰光融信技术有限公司 侯海波、杨香玉、陈占福

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）刘翔宇、马世民

第 10 章 软件测试工具

软件测试工具所包含的类别众多，在软件开发过程中扮演着至关重要的角色。当前，自主软件测试行业已经进入加速发展阶段，相关产品陆续投入市场，但总的来看市场占有率还有待提高。

10.1 自主软件测试工具在市场侧面临挑战

10.1.1 自主软件测试工具本身存在差距

如同其他基础软件一样，自主软件测试工具用户少，这就必然导致使用反馈少，进而在产品易用性、可靠性、稳定性等方面更新迭代缓慢，导致国产软件测试工具的成熟度普遍不高。另外，国产化的软件测试工具对国内市场的针对性不够强，虽然适配了大量国产化环境，但真正在国产化环境下开发，针对国内市场需求的产品并不多。最后，国内厂商重软件主体轻配套资料，导致软件使用手册、在线帮助、学习资料、二次开发接口等方面有较大差距。

10.1.2 自主软件测试工具没有形成市场规模

首先，功能、性能和稳定性等方面的差距是导致市场认可度低的根本原因。其次，以 B/S 架构为主的行业普遍重软件使用质量，轻软件内部质量。软件使用质量更依赖于黑盒动态测试，造成软件代码分析工具的重要性被人为降低。另外，由于标准不统一，市场上的自主软件测试工具存在数据格式差异，工具间难以打通、数据难以兼容，这进一步导致整个行业难以形成规模效应。最后，国外开源软件测试工具在软件测试从业者中影响较大，也对自主软件测试工具造成了一定程度的冲击。

10.1.3 行业对软件测试的认知有较大差异

代码静态分析工具、单元 / 集成测试工具、功能自动化测试工具、接口测试工具、性能测试工具的使用在全行业都已经得到了基本的共识，在软件工程过程中也都得到了不同程度的应用。全数字仿真测试系统、半实物仿真测试系统、FPGA 测试工具仅在部分行业有所应用。

部分行业对国产软件测试工具的重视程度有所提高，但全行业仍缺乏认识。在政府、金融、互联网、电信等领域，用户对软件质量的认识还停留在软件的使用质量方面，缺少行业共识的高质量软件编码规范、软件单元测试 / 集成测试、第三方测评制度，采用的软件测试工具主要是国外产品或开源工具，国产软件测试工具厂商在这些行业中的市场占有率几乎为零。

10.2 自主软件测试工具需要资源投入和多维度支持

10.2.1 在国外工具的基础上进行仿制或改进

软件测试工具有典型的工业软件属性，其具有体量小、集中度高、开发难度大、开发周期长、资金需求量大和见效慢等特点。由于这些因素，真正专注于开发这些工具的厂家数量较少。同时，国内软件测试工具市场碎片化，研发思路相对保守，研发资源有限，导致国内测试工具多是在国外工具的基础上进行仿制或改进，缺乏原创性。另外，由于缺乏统一标准规范，使得不同品牌和型号的软件测试工具在性能、功能和可靠性等方面存在较大差异。

10.2.2 缺少政策牵引和标准支撑

国产自主软件测试工具在当前的市场环境中面临着行业支持不够和引导不足的现实情况。首先，行业内的认证认可机构在进行推进工作时，尚未广泛采用国产自主软件测试工具，导致国产工具在起源阶段就缺乏必要的认可

度，无法发挥其应有的牵引作用。其次，国产软件测试工具的测评标准目前尚不健全，缺乏权威性的评估体系，使得国产软件测试工具在面临国际竞争时，难以凭借自身实力赢得用户的信赖。最后，国外软件测试工具在行业内的标杆性地位过于强大，同等条件下，用户倾向于选择国外工具。

由于市场竞争激烈，许多厂家为了争夺市场份额，采用了一些不正当的竞争手段，如包壳、超低价竞争等。这些行为无疑扰乱了市场秩序，进一步导致很多国产品牌在竞争中处于劣势地位。

10.2.3 没有和信创体系有效协同

信创产业的发展不能依赖于国外工具，而应积极推动国产自主软件测试工具的应用和发展。然而，受自身的成熟度和适配能力所限，自主软件测试工具对于信创产品的质量和安全保障力度不足，主要表现在：一是技术不成熟，导致测试工具的性能不稳定、功能不完善；二是标准化程度不高，导致数据交换困难。三是生态环境不成熟，导致自主软件测试工具没有与信创体系有效融合，没有针对信创体系的需求做研发，进而不能高效地解决信创体系中软件的质量问题。

10.3 建立高效权威的软件测试工具生态

10.3.1 提高产品的先进性和成熟度

提升技术创新能力，加强关键基础技术研究，推动自主软件测试工具的技术创新。通过引入新技术、新方法，提高测试工具的自动化、智能化水平，降低人工干预，提高测试效率。一方面在软件测试工具的核心算法上加大研发投入，尽快突破各类软件测试关键技术，不断降低代码缺陷检测工具的漏报率和误报率，加强与集成开发环境、软件工程工具、产品数据管理系统等平台的融合力度，全方位提升国产工具的性能、可靠性、易用性、标准符合

性和运维能力；另一方面，提升与国产基础软硬件环境的适配能力，不断适应国内各行业软件工程过程的特点，将国产软件测试工具有机融合进各行业软件研发与生成过程中，通过方案、产品、技术服务相结合的多种方式，更好地为各行业用户提供多场景的使用方式。

同时要加强知识产权保护工作，保护创新成果，鼓励技术研发和创新。

10.3.2 推动标准建设与认证检测工作

参考国际标准和行业最佳实践，制定适合国情的软件测试工具评测标准。这些标准应涵盖功能性能、易用性、稳定性、安全性等多个方面，以确保全面客观地评价软件测试工具的优劣。同时，注重制定和完善自主软件测试工具和信创体系的标准体系，加强产品的认证和检测工作，提高产品的质量和可靠性，增强市场竞争力。

10.3.3 强化产业链整合，服务信创产业

强化产业链整合，加强产业链上下游企业的合作交流，形成产业生态链。通过整合产业链资源，提高产品的市场占有率和竞争力，实现信创体系与自主软件测试工具的协同发展，共同推动产业升级。具体举措可包括：一是树立标杆。选择具有代表性的信创企业和项目，作为自主软件测试工具的应用标杆。二是逐步推广。加强与信创企业和项目之间的交流与合作，扩大自主软件测试工具的知名度和影响力。三是加强协同。自主软件测试工具厂商要深入了解信创产业的需求和趋势，与信创企业建立紧密的合作关系，共同推动自主软件测试工具在信创产业中的应用和普及。

10.3.4 加强人才队伍培养工作

为了推动国产自主软件测试工具的发展和应用，需要加强人才培养和引

进,提高人才的复合型能力,促进人才聚集和流动。一是与高校建立合作关系,共同推动国产软件测试工具在教学中的普及和应用。二是针对国产软件测试工具开发专门的教程,供学生和从业者学习实践。三是与高校共建实验室,提供国产软件测试工具的设备和环境,供学生进行实践活动,提高他们的实践能力。四是举办软件测试大赛,通过比赛提升学生的软件测试技能,同时增加对国产工具的认识和信任。五是提供技术支持和培训,帮助从业者更好地理解和使用这些工具。六是与高校和研究院所开展研究合作,共同探索新的测试技术和方法,推动软件测试领域的发展。

本章编写人员:

湖南泛联新安信息科技有限公司 田昊、毛伟、韩葆

凯云联创(北京)科技有限公司 陈策 、钱光磊

北京云起无垠科技有限公司 沈凯文、王书辉、夏营

安全篇 »

11、商用密码

12、终端安全

13、云计算安全

14、数据安全

15、高级威胁防御

16、漏洞管理

17、反恶意代码引擎

18、安全管控

19、工控安全

20、电子数据取证

21、软件供应链安全

第 11 章 商用密码

商用密码产业规模整体呈上升趋势。数据显示[6]，2021 年我国商用密码行业市场规模 585 亿元，2017-2021 年复合增长率为 25.08%，增速高于全球水平。预计 2023 年市场规模将达到 985.85 亿元，同比增长 39.32%。在有关政策的带动下，国家鼓励密码技术与云计算、大数据、物联网、车联网等新兴技术融合，并发挥安全的基础支撑作用。目前，商用密码在部分领域初步实现了与应用场景的融合。然而，由于行业的特殊性、专业性和复杂性，商用密码产品和服务在与行业应用相融合的过程中面临着较大的挑战。

11.1 商用密码产品在行业应用推广中面临挑战

11.1.1 政策法规不完全适应行业发展需求

商用密码产业和应用具有明显的政策导向性。我国在多部法律法规中明确规定了商用密码应用要求，形成了一套全面的商用密码应用政策法规体系。

现行的政策法规标准在指导商用密码在行业的应用上，仍存在针对性和有效性不足的问题。如各行业商用密码应用相关标准体系暂未构建，针对具体细分行业属性制定的密码应用标准尚不健全，尤其是关键信息基础设施密码应用标准编研工作进程需加快。其中主要问题聚焦在政策针对性低、管理机制弱、标准规划不完善、组织环境变化等方面，导致行业用户在缺乏指引的情况下，采用模板化的解决方案，或照搬其他单位的经验或方法。

另外，政策标准在规划制定阶段没有深入考虑企业经营情况和周边环境问题，由于政策施行不到位导致的管理机制不完善，以及组织环境的快速变

[6] 赛迪智库

化导致政策法规标准更新滞后等情况，也是影响商用密码在重点行业应用的现实问题。

11.1.2 复杂化应用场景对商密技术提出更高要求

商用密码的应用主要集中在对信息安全具有较高要求的行业领域。近年来随着高新技术的发展，各行业领域均引入了全新的技术手段来提升其行业竞争力，行业应用场景的复杂性和安全性要求快速增长，对商用密码的应用需求呈现出常态化、多样化的特点。5G、云计算、大数据等技术衍生出海量数据存储、传输、处理的需求，目前在这些场景下缺乏商用密码高效的解决方案。在物联网领域，各类不同设备的密码应用上，存在接口、协议不通用的问题，同时，设备在控制改造成本的前提下如何方便快捷地融合密码技术也是迫切需要解决的问题。人工智能技术的发展，同样也包含了大数据等技术的应用，想要计算机达到类人的处理能力，需要在极短时间内对环境因素等进行大量运算，在处理的同时保护数据需要同态加密等隐私计算技术进一步发展。目前，针对这些场景的商用密码应用还远远不足，如何紧跟快速发展的信息技术推出符合行业应用场景需求的商用密码技术和产品，实现商密产品的进一步创新是密码行业发展中急需解决的问题。

11.1.3 密码人才队伍有缺口

密码技术的应用推广离不开密码人才队伍的支撑。在商用密码产业快速发展的大背景下，培育一支规模和质量相匹配的密码人才队伍十分必要。然而，我国密码人才队伍的现状还远远不能满足信息化和数字经济发展的迫切需要。供给侧，密码企业的扩张、传统安全厂商的转型，都需要密码专业人才的支撑，而现实的情况是密码专业人才的培养跟不上产业的快速发展。需求侧，绝大多数从业人员对密码的认知还处于相对较浅的阶段，不可避免地

导致了密码建设不规范、不完善，资源浪费、工作效率低等情况。这从客观上对商用密码的应用推广造成了一定的阻力。

11.2 商用密码发展需要全方位思考

11.2.1 行业标准中需要明确商用密码的定位

当前的商用密码标准规范主要聚焦于商用密码技术维度，包括商用密码基础类标准、基础设施类标准、产品类标准、应用支撑类标准、应用类标准和检测类标准。相对于技术标准，商用密码在行业应用维度的标准化工作有所滞后，导致商用密码应用工作缺乏指引。

不同行业的应用存在差异，商用密码的应用需要贴合场景，与场景中的具体业务相结合才能发挥密码的保护作用。因此，需要持续关注商用密码的应用问题，明确商用密码应用在行业标准中的定位；推广可参考的标准规范，为商用密码应用提供指导；通过广泛地试验、验证、修订和完善标准形成行业共识，推进商用密码在各个重点行业的应用工作。

一些行业已经注意到这一问题。2023 年 1 月，中国通信标准化协会成立了通信网商用密码应用特色任务组（ST10），旨在统筹通信网商用密码应用技术标准发展，引导和促进商用密码技术在通信网的有序应用，提升我国通信网商用密码应用保障能力和水平。

11.2.2 供给侧需要服务思维，在融合创新上下功夫

当前，商用密码产业的供给模式仍以产品为主，通过“外挂式”、“打补丁”的方式给信息系统提供密码支持。由于密码产品只是提供基础的密码服务，如何与信息系统相结合，与数据安全真正互动起来，需要大量软件和中间件的研发工作，这是密码服务的核心内容。缺乏服务思维在客观上造成

了两方面的后果：一是厂商同质化竞争，低水平重复；二是一体化、服务化密码能力供给不足。在物联网、大数据、人工智能等应用场景中，密码技术和产品缺乏与行业深度融合，导致通用产品无法满足实际业务需求，带来安全问题和大量密码产品的闲置。因此，供给侧亟需“破局”式转型升级，从产品思维向服务思维转变，从粗放发展到精细耕作升级。

11.2.3 密码人才培养需要实现体系化

在密码人才培养方面，现有的培养体系尚不完善。高校的密码人才培养侧重理论研究，在工程和应用方面相对不足，导致基础研究人员多、工程技术人员少，研发人员多、应用人员少，这与国内密码产业发展的局面形成反差。因此，必须加强顶层设计，从基础理论、技术研发、工程应用、评测管理等方面培养一大批密码专门人才，才能满足商用密码推广应用的迫切需要。

在培养密码学历人才的同时，为尽快解决密码应用快速推进面临的人才紧缺问题，在职人员密码培训和评价也尤为重要。当前我国大多数商用密码从业人员都是因工作需要才从事密码工作，接受过密码专业全日制教育的人员不足 20%。密码从业人员专业性不足、知识深度不够、系统性不强，高端技术人才和管理人才紧缺。因此，需要结合实际工作需求，研究建立相应的在职密码人才培训课程体系，建立不同层次密码人才的评价标准，在必要的岗位对人员资质提出准入要求。

11.3 体系化保障措施助力建设商用密码发展快车道

11.3.1 完善行业标准，推动密码应用快速普及

加强商用密码标准化工作总体研究和规划布局，不断完善商用密码标准体系。坚持急用先行，紧扣国家新技术新业态新应用的重大战略部署，开展配套商用密码标准研制，提升商用密码标准对国家重大战略实施的服务保障

能力。加大商用密码检测和监管部门对密码技术创新和应用创新提供政策上的支持，缩短商业化应用周期，降低企业成本。加大商用密码标准宣贯力度，组织开展应用培训，引导企业知标准、懂标准、用标准。推动“产学研用测”优势资源开展供需对接，鼓励在商用密码活动中采用商用密码推荐性国家标准、行业标准，提升商用密码产品和服务的安全防护能力。建立商用密码标准实施信息反馈和评估机制，遴选优秀试点企业和示范项目，提升标准应用价值与实施效果，形成一批可复制、可推广的行业应用解决方案。

11.3.2 密码与新技术融合，为行业安全护航

坚持应用导向，坚持需求拉动与技术驱动相结合，加强密码前瞻性、基础性、通用性技术研究攻关，大力推进行业应用场景中的商用密码深度应用。目前，我国在密码算法、产品认证、应用推广和检测规范等方面均取得了显著成果，在新型密码算法上已经达到国际先进水平。在基础密码应用领域，应进一步提升密码产品的通用性、好用性，通用性保证密码产品互联互通以及平滑升级换代问题，好用性保证密码体系建设完成后，能够在不影响业务正常流转的前提下提高系统的安全性。在大数据领域，应聚焦密码相关软硬件的性能提升问题，以密码卡等硬件为基础、密码应用等软件为支撑，切实提高密码使用效率，以适应海量数据场景下的安全需求。在物联网领域，应先解构场景需求，再对技术和产品进行有关联性的迭代，提高密码和设备的兼容性，对不同场景做针对性设计，避免为了创新而创新。

11.3.3 多元化培养模式为产业和行业输送密码人才

一是加强产教融合，建立密码人才实践能力培养体系。密码深度融入信息系统设计、开发、建设、运维、管理、评测的各个环节，需要大量具有工程实践能力的专业人才。商用密码企业在生产运营中直接面对应用需求，对人才能力的需求有着最直接的了解。因此，在密码人才培养过程中应当充分

发挥密码企业的优势，通过构建实验系统、提供实习岗位等方式使人才培养更加贴近产业和行业需求。

二是加强科研机构和行业协会在培养密码人才中的纽带作用。通过举办密码应用和技术创新比赛等方式，加大密码产学研用各方交流力度，发掘和储备行业密码应用人才。同时，在兼顾创新性与实用性的基础上，瞄准某个行业痛点做深入研究，有助于促进密码的创新应用与推广。

本章编写人员：

北京计算机技术及应用研究所 石波、许睿、印哲然

北京炼石网络技术有限公司 白小勇、魏婷

湖南麒麟信安科技股份有限公司 孙玉峰、高洪鹤

杭州安恒信息技术股份有限公司 陈佳豪

北京信安世纪科技股份有限公司 汪宗斌、李秀兰

无锡沐创集成电路设计有限公司 王孟元

北京安御道合科技有限公司 陈普贵

渔翁信息技术股份有限公司 岳鹤涛

北京久安世纪科技有限公司 刘博文

北京众人数安科技有限公司 钱金金、朱易翔

江南信安（北京）科技有限公司 王鸿志

江苏云涌电子科技股份有限公司 高渊

北京时代亿信科技股份有限公司 沙勇

中国移动通信有限公司研究院 马爱良、张杨、张艳

北京海泰方圆科技股份有限公司 王学进 冯子祥

兴唐通信科技有限公司 梁广颖、胡睿、申苏浩

北京天融信网络安全技术有限公司 刘治平、李振楠

北京数盾信息科技有限公司 钟博、何济尘、杜一鸣

三未信安科技股份有限公司 鹿淑煜

第 12 章 终端安全

终端作为用户与信息系统交互的主要接口，承载着业务运行和数据处理、传输、存储等重要职能，其安全也越来越受到各企事业单位的重视。经过几年的技术演进，现已有成熟的国产化终端安全产品获得相对广泛的应用，为用户终端资产、系统环境和业务应用提供综合安全管控能力。

12.1 国产化终端安全产品总体向好，但也存在问题

12.1.1 终端安全产品对国产化环境的响应相对滞后

近年来，国内安全厂商和科研机构大力开展终端安全技术研究，并开始参与国产化生态适配等工作。在技术体系上，终端安全产品的基础能力（包括资产清点、威胁检测、准入控制、违规外联、响应处置、身份鉴别、打印刻录和主机审计等）已经非常成熟，零信任、EDR 等新产品发展迅速并逐步落地应用。在合规要求上，终端安全产品落实网络安全法、等保、关保、个人信息保护法等相关要求，建立健全终端管理制度，约束操作行为，同时规范特征库升级、漏洞补丁修复、安全策略调整等管理流程，进一步完善终端管控措施。在国产化场景上，终端安全产品基本完成了与国产化终端的底层硬件、操作系统、数据库和中间件等基础设施的兼容性适配。

但是，终端安全产品在国产化整体产业中还面临一些挑战。由于国产整机、国产操作系统和硬件平台快速迭代演进，终端底层硬件、操作系统等已构成一套生态体系，但因终端安全产品与终端基础设施产业生态的融入度不高，加之国产处理器架构复杂、基础软件版本杂、行业应用差异大，导致适配成本高和单次适配产出低，终端安全产品对基础软硬件的适配响应滞后。这在一定程度上影响了需求侧的终端部署实施和推广应用进程。

12.1.2 应用场景对终端安全产品的需求多样化

因政策法规要求、终端设备差异、系统环境繁杂和各行业的安全管理需求等因素，导致终端安全产品的需求越来越多样化。目前，各行业的办公机、服务器、虚拟机、移动终端等逐步进行国产化替换，移动终端和专用终端也越来越多地作为网络中的“节点”出现，终端安全产品已经能够基本覆盖上述各类终端设备，为各场景提供安全防护能力。在终端安全产品应用中，常见的终端安全能力需求主要包括：

一是恶意代码检测与防护能力。目前的恶意代码程序不仅在入侵、传播、破坏和隐藏等方面的技术水平显著提升，而且攻击技术和手段愈发复杂多变。针对恶意攻击的检测和防护技术，依旧是终端安全产品最基础的能力。

二是终端数据采集和细粒度识别能力。终端数据采集的覆盖度和识别的颗粒度，是终端安全防护能力的基础。需要在考虑设备类型、硬件配置、操作系统版本和 CPU 架构的差异性，设备承载业务的差异性，设备部署位置和防护等级的差异性等因素的基础上，建立专属数据采集机制，既满足应用场景防护需求，又不影响业务稳定运行。

三是终端防护和加固能力。因终端设备存在暴露面和脆弱性，需要通过终端安全产品来防止攻击者利用各类型漏洞和配置缺陷实现攻击入侵；防止因 U 盘、移动硬盘等不受控制的使用，导致攻击者利用这些移动介质向隔离网络投放攻击载荷进行摆渡攻击；防止因访问外网和随意安装软件带来的病毒攻击。

四是终端入网管控能力。当前存在越来越多的“云化”IT 架构和远程办公工作场景，以及某些行业运维需求，也存在厂商自带设备办公（BYOD）入场工作的情况。为满足终端安全可控，此类终端在接入企业网络时需进行

合法性审查，并通过身份认证、安全认证和资产权限控制等终端准入控制措施，避免内网资源受到非法设备、非授权访问的威胁。

12.1.3 终端安全产品在部署实施上存在兼容性和性能消耗问题

响应政策法规、行业需求、国产化迭代发展和终端环境多样化等因素，终端安全产品为行业用户提供了良好的安全管控和防护价值。同时，为了支持纵深防御体系，终端安全产品与其他安全设备实现了联动，提供了日志上报和响应处置等能力。但是，同一终端上部署多款安全产品的情况经常出现，值得关注。出现这一现象的原因包括两个方面：一是面对众多终端产品，用户出于满足合规要求的目的重复部署安全产品；二是用户的信息化和网络安全建设是逐步递进的过程，阶段、人员和目标的不同都可能导致一定程度上的重复建设。这一情况造成了安全产品之间的兼容性冲突和性能消耗问题。另外，安全厂商为了增加终端安全能力的覆盖面，也会主动实现产品能力的叠加，进而造成实施和运营难度的提升。

12.2 国产化终端安全产品在应用推广中面临挑战

12.2.1 国产化环境适配难度大，响应滞后

目前基础软硬件和终端的现状是品牌多、架构多、型号多。鉴于基础软硬件在信息化建设过程中发挥的关键作用，对于终端安全产品厂商来说，兼容性适配是必须开展的工作。面对几十种组合的基础环境，适配工作量就变得非常巨大。另外，由于行业需求不同，基础设施和基础软件经常以定制化版本的形态出现，在配置、组件、版本上有较大的差异性，这对安全团队的专业技术背景和研发水平提出了更高要求。

由于终端安全产品与终端产品是伴生关系，终端安全产品与国产化环境的适配工作必然是在基础软硬件更新发布之后才具备条件。因此，终端安全

产品与信创环境的适配天然具有一定的滞后性。加之目前产业生态相对不够健全，终端安全厂商没有渠道快速了解基础软硬件厂商发布的新版本信息，导致终端安全产品的迭代滞后于国产终端的迭代，在项目实施中终端环境与终端安全产品经常出现兼容性问题，需要终端设备厂商、操作系统厂商、软件厂商和终端安全厂商联合分析和定位问题才能解决。这在客观上造成了项目实施交付周期长、产品稳定性风险和解决问题成本高的现状。

12.2.2 行业属性和应用场景决定了终端安全产品的防护能力必须快速演进

由于行业属性不同，各行业安全能力建设的侧重点会有所不同。即便是同一行业，不同单位之间由于网络环境、业务系统、应用场景不同，终端设备的安全防护需求也有较大差异。另外，随着数字化投入的不断加大，终端类型变得越来越多、应用软件越来越复杂、接入方式越来越多源、网络边界越来越模糊、安全暴露面不断增加，也要求终端安全产品的防护能力随场景变化而快速演进。

12.2.3 终端安全产品的实施和运营难以实现集约化

终端安全产品在部署上面临系统环境杂、数量多且分散的问题。通常，终端安全产品的部署范围以百、千或万台为数量级。虽然技术上可以通过远程方式实现在线部署和升级，但实际业务场景中往往需要人力进行现场实施。这对安全厂商来说是极大的人力成本、时间成本和资源消耗。终端场景有办公机、服务器、虚拟机、移动智能终端和工控终端等多种架构，相应地终端安全产品的品类和版本也很多，加上不同厂商产品的技术架构又不统一，运维人员在没有高效的自动化管理工具的前提下，很难实现安全能力的集约化。

从安全运营的角度看，终端安全产品品类多、厂商多、逻辑复杂，同时

终端安全往往又需要进行个性化的配置和针对性的优化，以适应各行业的不同业务场景需求，需要安全运维人员有较高的技术能力和丰富的安全处置经验。当安全运维人员配备不足且专业能力有限时，安全运营的效果自然无法达到预期。

因此，如何整合终端的安全需求，优化产品或能力组件之间的交互逻辑，简化产品的操作，降低运维使用难度是终端安全防护集约化要重点考虑的问题。

12.3 创新提升产品价值，合作应对推广挑战

12.3.1 积极参与生态建设，探索综合性适配测试

终端安全厂商应摒弃观望心态，改变以往以项目或者安全事件推动的被动应付策略，积极参与、加大研发投入，配置更多的人力物力，扩大兼容适配的种类和范围，争取更大的主动。当前环境下，要认识到终端安全产品与国产芯片、操作系统、数据库及应用的兼容性互认证只是基础性工作。应该积极开展综合性适配测试，在试验环境下尽早发现问题，共同排查解决问题，为用户提供成熟稳定的组合方案，减少现场测试带来的时间消耗，缩短响应迭代时间，增强用户信心，进一步促进国产化应用推广。

12.3.2 实现终端安全一体化、集约化防护

国产化终端安全的最佳路径是对现有分散在终端安全产品上的安全能力组件化、集约化，建立一个集成多种安全能力的一体化综合性解决方案，逐步取代目前堆砌多个产品的方式。

首先，一体化平台为用户提供集约化的安全防护能力以及方便快捷的安全管理工具。用户通过一体化平台为各类终端设备提供安全防护。平台不仅

提供统一的管理界面，还能根据用户需求进行定制化配置，以满足各行业的特殊安全需求。平台还可以对终端上报的告警日志进行综合关联分析，从多维度做风险分析和呈现，从全局视角依据不同优先级聚焦各类威胁，实现更精准地溯源和处置，改善防护产品“各自为战”的状况。

其次，能力模块按需灵活配置。用户只需在终端安装单一终端安全产品，根据自身终端防护范围的约束，按需搭载能力组件，既可对不同终端设备提供差异化的安全防护，又可以避免多个安全产品间的能力重复和冲突，提高整体防护效果，减小维护难度和成本。

12.3.3 从满足合规要求向提供有效安全防护价值转型

随着各行业领域国产化逐步推进，市场对终端安全防护能力的要求也逐步在原有以“满足合规要求”为目标的基础上，发展为以“提供有效安全防护价值”为目标。针对更高的能力要求，国产化终端安全防护能力的优化，可以从强化终端安全加固和威胁检测处置能力两方面进行综合考虑。

终端安全加固不仅仅是基于规范要求对系统进行加固，还需要将加固与实际业务相结合。基于终端类型和场景进行细粒度的数据采集，并依据数据分析的结果，制定有效的安全加固方案。

终端威胁检测处置能力应该得到持续提升。首先是全面提升检测范围，集成丰富的威胁检测引擎、环境检测引擎、网络流量检测引擎，同时整合威胁情报，对终端文件信息、运行状态、环境特征、流量信息等内容具有检测能力。其次是构建终端上全量执行体细粒度检测处置能力。针对不同类型执行体，系统应支持设置约束规则，控制执行体的执行权限、操作动作、网络访问等行为，确保低信誉执行体不会具有访问敏感数据或执行威胁行为的机会。

本章编写人员：

北京安天网络安全技术有限公司 辛颖

北京安御道合科技有限公司 李永明

北京网御星云信息技术有限公司 王斌

北京可信华泰信息技术有限公司 杜君、贾胜男

北京天融信网络安全技术有限公司 梁连燚、吕佳

四川航天七零六信息科技有限公司 马书磊

上海上讯信息技术股份有限公司 韩璐

第 13 章 云计算安全

2022 年，我国云计算市场规模达 4550 亿元，较 2021 年增长 40.91%[7]。相比全球 19% 的增速，我国云计算仍处于快速发展期，预计 2025 年整体市场规模将突破万亿元。上云之后，云安全成为用户重点关注的问题之一。据统计，近 5 年我国云安全市场保持 45% 以上增速，2022 年市场规模达到了 176.9 亿元，同比增速为 46.7%[8]，显示出云计算安全市场的巨大潜力。

13.1 云计算产业快速发展，出现新的安全薄弱点

13.1.1 云原生采纳率持续攀升，安全问题日渐突出

云原生技术在部分行业快速应用。互联网、金融、电信、能源等行业对云原生已有较高采纳度，并逐渐加大在云原生领域的投入规模。云原生技术架构改变了传统应用设计、开发、部署和运行模式，其不但继承了传统应用的安全问题，也带来了新的安全风险，如镜像、容器、镜像仓库、集群等新基础设施的安全防护问题；微服务模式导致的工作负载间东西向流量监控问题；基于云原生架构的 DevOps 全流程安全监控问题等。云原生技术带来的高密度动态调度、敏捷快速迭代等特性，也加大了安全防护难度。过去一年，有 94% 的组织在其容器环境中遇到安全问题，其中 69% 的组织检测到错误配置，27% 的组织在运行时遇到安全事件，还有 24% 的组织发现了严重的安全漏洞[9]。如果没有实施有效的安全防护，黑客可以利用漏洞攻击容器上的服务，或者访问容器云上的敏感信息，进而获取服务器特权，对容器云进行修改并最终完全控制服务器。

---

[7] 中国信通院《云计算白皮书（2023 年）》

[8] 赛迪研究院《年报 |2020-2022 年中国云安全市场研究年度报告》

[9] StackRox《容器和 Kubernetes 安全态势报告》

13.1.2 信任风险由人员向云计算基础设施转变

人员信任风险一直是云计算安全关注的问题。随着云计算的普及，运营方对人员的访问权限进行了更加细化和严格的管理，加上云计算环境下的自动化和标准化可以减少人为操作引入的错误，使得人员信任风险相对减少。

随着新型基础设施建设步伐的加快，IT 基础架构的多云、混合云部署已逐渐成为新常态，采用大规模虚拟化、分布式架构和自动化管理的云计算环境增加了云计算基础设施的复杂性和关联性。一旦云计算基础设施存在安全漏洞，就可能破坏数据的保密性、完整性或可用性。缺乏统一的安全架构极易导致云上缺少整体的安全规划和一致的安全策略编排，这使安全管理变得更加复杂。

13.1.3 安全左移导致责任划分不清晰

传统安全建设中，安全责任更多的是在安全团队内部进行划分，较少会涉及到其他部门，边界相对清晰。在应用云计算技术后，参与基础设施与安全建设的角色范围有所增加，涵盖了云服务供应商、安全服务供应商、运维团队以及安全团队，因此安全与云基础设施呈现出融合的态势，安全团队在进行建设时往往需要与云基础设施运维团队进行互动，从而使安全责任的边界变得愈发模糊。此外，云服务供应商或云基础设施运维团队可能会出于云平台稳定性或业务性能的考虑，对云安全措施提出相反的意见。

另外，随着云原生和DevOps的发展，传统安全责任的划分正在发生改变，安全责任越来越多地被左移至开发和运维人员，这需要各部门之间更加密切的合作和沟通，才能确保安全措施的实施和落地。一方面，开发和运维人员需要更多地了解安全最佳实践、安全配置和漏洞修复等方面的知识，并将其应用到工作中。另一方面，安全团队的角色也发生了变化，他们需要了解业

务开发流程并与开发和运维人员密切合作。这种变化使得安全建设变得更加困难。

13.2 安全体系建设滞后于新技术、新业态、新模式

13.2.1 云原生技术复杂度高，安全能力储备不足

云原生技术生态覆盖广、复杂度高，涵盖了容器化、微服务架构、持续交付、弹性基础设施等方面，客观上加大了安全防护难度。用户和厂商对云原生及相关安全技术的储备不足，也是现实情况。

从 IT 基础设施视角看，云原生底座包含容器运行时、编排系统、服务网格、Serverless 等，以编排系统 Kubernetes 为例，核心组件包括 kube-apiserver、etcd、kube-scheduler、kube-controller-manager、kubelet、kube-proxy、内部 dns、网络组件等。此外，还包含管理界面、资源监控、日志审计等辅助组件。这些组件自身可能（或一定）存在安全漏洞，同时每一个组件的配置问题都可能引发安全风险。

从 DevOps 视角看，传统技术架构只需将安全能力融入到从软件开发到上线的各个环节，只重点关注代码的安全性，但云原生技术基于镜像，形成了不可变基础设施理念，安全关注的方向也由代码转变为代码及其依赖的整体环境，在整个流转的过程中，还需关注镜像仓库、持续交付的工具 / 平台等。

从业务运行视角看，业务进程基于云原生技术进行了一次封装。容器作为业务载体，在运行过程面临逃逸、横向移动等安全风险，在传统技术无法获取安全数据的情况下，安全人员需要建立新的防护手段。另外，基于容器实现机理，业务容器由于升级迭代、故障漂移等情况消逝时，在运行过程中的行为以及自身基本信息不会留存，这对溯源造成了困难。

13.2.2 多云、混合云业态加剧了安全信任风险

因迁移灵活、性价比高，多云和混合云正成为企业部署的热点。为此，云计算厂商依据多云、混合云策略，推出多种加速数字化转型的产品和解决方案。相关解决方案将涉及到基础设施支撑、业务应用支撑和企业数据存储等多个领域。由此也产生一系列安全信任风险，如虚拟机系统面临的安全风险、多租户安全风险；由云服务提供商对数据的直接控制导致的数据安全风险；由大量 API 导致的接口安全机制风险；由监管缺失导致的用户恶意使用云平台的风险等。

13.2.3 传统 IT 架构安全职责无法适用于云计算安全体系

云计算技术架构打破了传统 IT 架构的安全责任划分。当云计算建设和安全建设独立时，往往安全责任边界相对清晰，但当云计算融合安全共同建设时（特别是当引入云原生技术后），运维部门和安全部门需要协同合作，一旦业务或安全出现问题，各部门之间的责任划分相对难以界定。

云原生业务环境承载在传统 IT 架构之上，而正是传统 IT 架构导致了安全职责的分裂。不同部门对云原生安全的关注点是不同的，如主机平台部门负责服务器和容器云平台的部署，关注点是主机和平台环境安全；网络部门负责服务器和容器云网络的管理，关注点是主机和容器的网络安全；开发维护部门负责容器镜像、实例的构建、业务的运行维护，关注点是容器镜像（代码）和业务安全；安全部门对企业整体安全及合规负责，关注点是标准、规范以及实战安全水平。随着开发人员、测试人员被纳入到云原生安全责任模型中，安全措施从应用开发之初就被引入，安全责任需要追溯到多个职能部门，如果没有清晰的安全责任划分，就会出现各自为战的情况。

另外，不同部门根据自己的安全能力需要各自部署的产品或工具之间存

在大量重叠和兼容性问题，例如主机平台部门部署的 EDR 产品同时兼有微隔离能力，而网络部门部署的微隔离产品同时也兼有主机安全能力。这会导致不同云原生安全产品争夺相同监控对象，对云原生主机环境和计算资源造成影响。

13.3 多方面入手，助推云计算安全

13.3.1 建立云原生安全体系，形成业务全生命周期防护

云原生技术生态还在不断发展，在开展云原生安全体系建设过程中，面临着前所未有的技术复杂、企业组织文化冲击等方面的挑战。在云原生安全建设上需从两方面着手：

一是补强技术短板，理解和接受云原生理念。云原生技术引入了镜像、容器、编排系统等新的资源对象，因此不论是用户还是厂商，都需要在关注传统安全威胁的同时，加大对云原生相关技术的关注度，快速补强技术短板。另外，由于云原生在防护对象、架构、管理模式等方面与传统计算模式存在较大差异，在技术能力补强的同时，还需要充分理解云原生理念，如在云原生环境下，业务容器只换不修；安全关注点由代码转变到代码及运行所需的环境；业务接受动态调度且固定标识由 IP 变换为标签等。

二是建立云原生安全体系。当前云原生安全建设不再是在云原生应用上线时一次性的安全扫描，而是将“安全前置”到云原生应用的开发阶段，并且将“安全后移”到云原生应用运行阶段的全生命周期，从业务需求分析、业务软件开发、业务软件测试、业务软件发布并一直延伸至业务软件的运维，让安全不存在“间隙”。

13.3.2 由被动防御向主动防御转变，打造整体可信链条

传统的云计算安全防护手段没有从安全威胁发生的源头即计算平台自身

着手解决问题，而是把注意力放在对系统的外围保护上。只有构建从底层硬件平台到上层可信应用，建立起全网安全互联的纵深网络空间信任体系，才能彻底改变“封堵”“查杀”的被动局面，确保各类云计算平台处于预期、稳定的安全环境，网络应用处于可信、可控的状态，形成覆盖全网的主动防御、自身免疫的可信云计算空间，提高网络空间安全防护能力。

从被动防御向主动防御转变，是一个科学问题，也是技术发展的必然趋势。主动防御技术从逻辑正确验证、计算体系结构和计算模式等多个方面，在云计算环境中构建独立于云计算系统的可信云架构，提供可信服务并为云计算环境安全机制提供可信支撑。云计算环境所有节点可信元件通过可信协同方式构成的云可信框架，可支持在进行云计算的同时实施安全防护，为云计算安全提供基础。

基于主动防御的云计算安全管理防御体系能够深入解析安全威胁，增强预警风险，协调安全性信息反馈，实施阻断与修复，以可信的链接平台体系为内核，透过对用户身份验证、数据加密、授权管控等多层次的安全控制，采用静态度量、动态度量、可信报告等主动防御手段形成了云计算安全管理防御系统的可信架构，为云计算技术的运用提供强有力的基础保障。

13.3.3 打造一体化云计算安全职责体系

云原生业务环境虽然承载在传统 IT 架构之上，但早已呈超融合之势。云原生安全能力自然也随着云原生业务环境的融合而融合才能达到最佳效率。全面保护云原生应用程序需要使用来自多个供应商的多种工具，这些工具很少进行融合集成，而且通常只为安全专业人员设计，而不是与开发人员合作。对于组织而言，这种孤立的方法在确定实际风险的优先级方面无效，并导致过多的警报和浪费开发人员的时间。云原生应用保护平台（CNAPP）提供了一种集成方法，可实现跨团队协作，以保护日益复杂的攻击面。

因此，由安全部门牵头建设集多种云原生安全能力于一身的云原生应用保护平台（CNAPP），进而打造一体化的云原生安全职责体系，由主机平台部门、网络部门、开发维护部门根据各自的安全能力需要，按需使用云原生应用保护平台（CNAPP）提供的不同功能，共同配合安全部门实现整体安全目标，是解决安全职责划分问题的思路之一。安全部门牵头组织其他部门进行云原生安全能力的整体建设，完成整体安全合规及实战安全保障工作；主机平台部门可用的安全能力有主机防病毒、EDR、主机 DLP、主机 & 平台配置合规扫描；网络部门可用的安全能力有容器网络流量可视化、微隔离；开发及维护部门可用的安全能力有容器镜像扫描、代码扫描、IaC 扫描、容器入侵检测 API 扫描、Web 应用防火墙。

本章编写人员：

北京小佑网络科技有限公司 袁曙光、白黎明、左伟震、杨冬富

北京可信华泰信息技术有限公司 王杨、齐洪东

北京信安世纪科技股份有限公司 焦靖伟

北京山石网科信息技术有限公司 任亮

北京天融信网络安全技术有限公司 夏威

北京神州绿盟科技有限公司 刘丽

湖南麒麟信安科技股份有限公司 杨鹏举

精壹致远（武汉）信息技术有限公司 李勇

第 14 章 数据安全

随着数据的应用越来越广泛、形式越来越多样，数据安全产业也得到了快速发展。产品门类从传统的数据加密、数据库审计，拓展到了包括数据资产管理、数据监测、数据共享、隐私保护、追踪溯源等在内的数据全生命周期。同时，深化数据安全应用、有效保障行业用户的数据安全，也面临意识、技术和生态等方面的问题需要解决。

14.1 深化数据安全应用面临多重挑战

14.1.1 数据安全治理观念没有得到充分认可

数据安全防护产品已经相对成熟，但数据安全防护在多产品联动、多形态一体化方面还有所不足，体系化开展数据安全治理还需要时间和场景化检验。存在的问题主要体现在以下三方面：

一是重产品轻服务。相对于传统的网络安全，数据安全与业务结合更紧密，更需要依靠专业的技术服务来完善防护体系。如果没有从实际业务角度出发，单纯依靠数据安全产品很难发挥作用。目前，除金融和电信行业用户相对习惯服务交付外，多数行业还停留在认为产品堆砌即能解决问题的层面。

二是缺乏全面的安全策略。数据安全涉及到数据的收集、存储、传输、使用、交换、销毁等多个环节 (DSMM)，需要综合考虑法律法规、管理、技术、工程、人员等多方面因素。现实的情况是，部分用户仅针对检查项进行补充，没有从业务和数据全生命周期角度考虑数据安全问题；另外，由于数据分类分级难度大，导致数据安全措施集中在传输和存储环节，数据使用环节缺乏规划或采而不用。

三是担心影响业务而持观望态度。对存量数据的改造投资大、周期长，同时可能会对现有业务造成较大影响，所以很多用户对数据安全建设持观望态度。

14.1.2 数据安全技术发展与数据应用规模不匹配

在新技术的驱动下，数据量呈现爆炸式增长，数据安全保护范围不断扩大。同时，新兴技术的发展也带来了新的安全威胁。传统的数据安全防护重传输和存储，在数据使用环节的安全保障有缺失，与业务逻辑的结合不够充分，因而难以适应数据应用的新场景（如文件外发通道复杂化、供应链攻击获取敏感信息，内部人员对抗数据防泄露措施等）。面对快速迭代的数据应用场景，数据安全技术研究与实际应用之间的转化速度比较慢。随着数据的价值和重要性不断提升，数据安全防护手段有点跟不上数据应用的步伐。

14.1.3 多技术路线给数据安全应用推广制造困难

当前多技术路线并行的产业现状使得下游数据安全厂商在适配方面面临时间和成本压力（这不仅体现在研发上，运营投入也是不可忽视的成本）。同时，复杂的信创产业生态对于数据安全产品的应用推广也造成了一定的困难。由于数据安全处于产业链下游，上游技术相互交叉融合、场景化适配以及版本迭代更新，都使面临的威胁急剧复杂化，数据安全产品和解决方案在需求侧需要面对的技术路线组合呈指数级增长。

14.2 从标准化、技术创新和产业生态看数据安全问题

14.2.1 具备顶层设计，但缺少实施细则

随着《网络安全法》、《数据安全法》等法律法规的颁布施行，以及一系列数据安全国家标准、行业标准、团体标准的发布，相关的顶层设计已经

初步建立。但在实际工作过程中往往会发现，由于实施细则和标准体系还有待完善，在项目落地时普遍存在抓手不足、没有参考依据等问题，如难以制定合理的数据安全策略、难以进行有效的合规性管理、难以评估安全产品的有效性等。这在很大程度上影响了数据安全（特别是数据安全治理）产品和解决方案的推广。

开展数据安全保护工作，数据的分类分级和标签是对数据场景化安全防护的基础性支撑。除金融和电信等少数行业外，其他行业尚缺乏清晰明确的数据分类分级标准，导致组织在开展数据分类分级工作时，需要投入较大的成本去梳理模板，且存在梳理出来的模板和后续正式发布的标准不一致的风险，进而导致组织在开展数据分类分级工作时存在一定的顾虑。

行业级数据分类分级标准不健全问题的原因是多方面的。从业务的角度看，数据分类分级与场景化的数据安全需求以及数据安全时效性强相关，不同行业（甚至同一行业的不同单位）对于数据安全的需求存在较大差异性，因此需要结合业务流程制定有针对性的分类分级标准。从技术的角度看，数据的多样性、规模性、安全场景化、与业务强关联等特质对分类分级造成困难。一方面，数据来源和格式日益复杂多变；另一方面，数据规模庞大且快速增长，使得分类分级过程十分复杂，对计算资源也提出了更高的要求。

14.2.2 数据安全技术需要响应数字化需求

数据安全涉及的技术面非常广，包括数据防泄漏、数据加密、数据脱敏、隐私计算、身份认证、威胁检测等。随着新技术的不断出现，在实际应用中全面覆盖各个行业的数据安全需求难度越来越大。

从需求侧看，不同行业的技术基础不同，数据保护的层次、程度和要求各异，要全面覆盖行业需求，就要针对不同行业特点制定相应的数据安全解

决方案。如数据在其生命周期过程中不同阶段的变化，在不同区域会面临不同的安全风险。内循环涉及组织内部对数据的保护、管理、审计；外循环涉及数据在组织之间的传输、共享、合作，需要考虑合规性、隐私保护、信任建立等问题。

从供给侧看，数据安全涉及技术、管理和制度等多个维度，要全面覆盖行业需求，不是厂商单方面就能完成的任务，需要各方面协同配合、形成合力。另外，随着新技术的不断涌现，攻击者也在不断寻找新的漏洞和攻击方法。这意味着数据安全技术必须不断跟进，以响应新的威胁。

14.2.3 产业链对数据安全业务有较大影响

一是对数据安全产品的影响。由于国产化基础硬件在性能、稳定性等方面与国际先进水平相比略有差距，导致国产数据安全产品在处理大规模数据时出现性能瓶颈。此外，国产软硬件在价格方面处于相对劣势，导致数据安全产品成本上升。

二是对数据安全产业的影响。技术路线分散问题对于信创产业的下游厂商来说是共性问题，主要体现在以下几个方面：首先，技术标准不统一导致产品的互操作性差、互联互通难度加大。其次，产品与服务的多样化给用户选型乃至集成和维护造成困难（包括技术、人员、资金等）。第三，全栈国产化意味着企业需要投入更多的研发资源，导致运营成本上升。

14.3 提高能力、解决问题，促进数据安全产业发展

14.3.1 健全数据安全标准制度体系

一是建立健全数据分类分级制度，制定国家层面数据分类分级的基本原则和方法，明确数据分类分级的标准和流程。二是制定各行业的细化方案，

结合行业特点制定数据分类分级细则，明确各类数据的保护要求和责任主体。三是完善数据安全标准体系，加强数据安全标准的研究和制定工作，实现各行业数据安全保护工作有据可依。四是建立健全数据安全治理体系，落实数据安全主体责任，从组织、制度、技术和人员方面持续提升数据安全保障能力。

14.3.2 加强基础通用技术研究

基础通用技术的不断发展为数据安全技术创新提供了有力支撑。在国家对信创支持力度不断提升的大背景下，产业链各节点要持续加大基础通用技术的研发投入，为提升数据安全关键技术提供支撑。如，通过人工智能技术帮助识别和分析数据安全风险，支撑数据分类分级，提高数据安全水平；通过数据标识结合驱动级透明加解密技术支撑结构化和非结构化数据的分类分级，并对数据的使用权限进行控制；通过数据水印技术支撑安全事件的溯源反制，同时降低合规风险；通过数据血缘技术支撑动态的数据监控，让数据安全与业务的耦合更加紧密顺畅，同时也为安全监控和审计提供证据链条。

14.3.3 打造数据安全新业态

在技术方面，积极参与各产业节点的技术交流与合作，通过完善相关标准规范逐步建立最优技术路线，降低研发和适配成本，提高市场竞争力。在产能方面，通过智能化生产线和精细化管理，提高生产效率和产能，加强供应链的抗风险能力，确保国产基础硬件供应链的安全。在数据安全自身的生态建设方面，具有“头雁”效应的大型企业要努力做大做强；中小微企业要增强内生动力，走“专精特新”的发展道路；单项产品市场占有率较高的企业要瞄准单项冠军，走特色道路。

本章编写人员：

精壹致远（武汉）信息技术有限公司 李勇

哈尔滨安澜科技有限公司 常景辉

山石网科通信技术股份有限公司 李莅

北京安御道合科技有限公司 谢依夫

杭州亿格云科技有限公司 崔双硕

北京得意音通技术有限责任公司 黄小妮

北京久安世纪科技有限公司 刘博文

北京时代亿信科技股份有限公司 沙勇

中国软件评测中心 白惠文

上海众人智能科技有限公司 付宗玉

浙江华途信息安全技术股份有限公司 吴进波

北京神州绿盟科技有限公司 王晓丹

杭州安恒信息技术股份有限公司 程文博、刘少鹏、郭立文

上海上讯信息技术股份有限公司 吴阳

北京炼石网络技术有限公司 白小勇、张齐军

北京天融信网络安全技术有限公司 张志颖

湖南麒麟信安科技股份有限公司 彭勇

科来网络技术股份有限公司 张津、李萌

第 15 章 高级威胁防御

高级威胁是指由攻击者使用高度复杂和先进的技术，针对特定目标发起的长期、隐蔽的网络攻击。为了应对高级威胁，组织需要采用多种安全产品与服务构建纵深防御体系。

15.1 攻防两端技术演进共同推动高级威胁防御市场发展

15.1.1 高级威胁防御从合规驱动转向效果驱动

随着网络威胁的日益复杂和高级化，单纯依靠合规驱动的安全防御已经无法满足实际需求。APT 活动近两年大幅增长，高级威胁对抗已然进入白热化阶段。2023 年，全球公开披露的攻击活动涉及 APT 组织 162 个，同比增长 21 个，其中首次披露的 APT 组织 66 个，同比增长 12 个。网络攻击活动涉及的 APT 组织数量和首次披露的 APT 组织数量，均比 2022 年大幅增加。我国遭受的 APT 攻击越来越多，包括来自不同网空威胁能力层级的组织行为体。同时，得益于攻防演练的实际检验效果，越来越多的组织开始转向效果驱动。高级威胁的检出率和误报率成为衡量防御效果的重要指标，直接反映了安全体系对潜在威胁的发现和识别能力。

15.1.2 高级威胁防御在行业应用上有较大差异

建设高级威胁防御体系是一个复杂的过程。自 2016 年以来，高级威胁防御体系的建设速度明显加快，一些行业与地区已初步完成整体建设，新建系统不再依赖单一的技术手段，而是将多种安全技术和策略进行融合，从单点被动防御逐步演化到动态综合防御阶段。

从本章编写单位的实践看，高级威胁防御体系建设具有明显的行业特征，政府、金融、电信等行业是高级威胁产品的主要应用领域。其中，政府对高

级威胁的投入处在领先的地位，在体系建设上较为关注防御窃取数据、数据勒索、APT 攻击，目标是避免攻击导致数据泄露或者公共服务瘫痪；金融行业防御高级威胁的需求增速明显，尤其关注网络金融钓鱼、漏洞攻击、勒索等威胁；电信行业通过增强自主研发能力，综合采用外采、自研与技术合作等多种模式，逐步完善高级威胁防御体系，相对更注重防范服务拒绝攻击、数据篡改、设备劫持等威胁类型。

15.1.3 高级威胁防御体系面临异构和信创的挑战

行业用户在构建高级威胁防御体系时，往往采取异构策略。一方面，异构可以在一定程度上提高安全能力；另一方面，也在实际部署和运行过程中给集成、互联互通和互操作带来障碍。这在一定程度上又降低了防御体系的整体效能。用户在管理和维护多个高级威胁防御产品时，会遇到日志和报警信息格式不统一的问题。这导致分析研判、协同处置与溯源对人工处理的依赖过大，增加了运营成本，降低了防御效率和准确性。

政府、国防军工、信息技术、金融、科研等行业历年来一直是高级威胁攻击的核心目标领域。随着行业信创的深入、应用软件的成熟，信创产品将渗透至更多核心业务场景，这必然会引入新的网络安全风险。举例来说，信创生态跟不上行业增长需求，适配工作繁重，包括原有系统的迁移、历史软硬件版本的兼容、行业特色软件的使用、非信创环境与信创环境的组合等复杂情况，暴露了诸多攻击面，存在防御薄弱点。以高级威胁中常见的供应链作为攻击路径而言，可利用多阶段多层次的攻击手段，依据不同的基础软件目标（操作系统、数据库、中间件、桌面云等）部署不同的武器工具和渗透入侵策略。体现出信创在应对高级威胁活动中的供应链威胁上下游的组件、代码缺陷等检测变得愈发复杂，与之相关的主机、网站等遭受未知威胁组织长期渗透入侵的情况难以被发现。

15.2 高级威胁攻击和防御具有强烈的技术驱动属性

15.2.1 攻击技术快速发展，攻击行为越来越多

从技术角度看，AIGC（生成式人工智能，Artificial Intelligence Generated Content）技术的快速发展为网络攻击者提供了新的机会。在前几代人工智能中，人们将社会对现实的某种理解提炼为程序代码，而当下的机器学习人工智能与之不同，它们在很大程度上是靠自己对现实进行建模。AIGC 降低了网络攻击门槛的原因在于：第一点，黑客可以将人工智能生成的结果直接用于网络攻击活动当中，而不需要了解人工智能是如何学习的或者学到了什么。第二点，黑客基于某类目标系统环境的建模，一旦应用成功可大规模部署网络攻击活动。

从风险角度看，我国遭受的 APT 攻击越来越多，包括来自不同网空威胁能力层级的组织行为体。重点包括来自美国 NSA-TAO 入侵西北工业大学的攻击事件和武汉市地震监测中心遭境外网络攻击曝光；来自越南海莲花组织借助商业军火武器和利用 0-Day 或 1-Day 入侵网络设备作为跳板的系列攻击活动；以及白象、绿斑等 APT 组织紧随时事热点以邮件、网站或社交平台等作为攻击入口，采用机会主义游击战术攻击我国重点关键基础设施行业和科研院所系统单位。

15.2.2 高级威胁的检测能力仍然不足

在威胁持续加剧的情况下，安全厂商也逐步推出不同的高级威胁防御产品，使用了包括新一代恶意代码检测引擎、内存安全检测、人工智能检测、溯源分析等新技术解决高级威胁问题。然而，不可否认的是，高级威胁的检测能力仍然不足。

2023 年，全球范围内披露 APT 分析报告数千篇，虽然报告数量众多，

但其中大多是一般能力的 APT 组织，针对顶级的 APT 攻击组织披露寥寥无几。究其原因，一是高级威胁防护产品和服务本身能力上的不足；二是由于对手的先发优势和技术投入，攻防两端存在多维度的差距；三是攻防本身就是不对等的较量，防御方要面面俱到，而攻击方只需要找到一个弱点突破。因此，当前防御者面对顶级的攻击技术手段难以快速发现异常或告警，导致针对顶级的网络攻击很难发现。实际上，当下网络空间环境中，网空霸权和地缘安全博弈依然是当前网空攻击的主要持续性动机和因素，该类攻击代表当前网空攻击的最高能力，其目标广度和深度均全面覆盖，造成的后果也最为严重。

15.2.3 高级威胁情报可能因 AIGC 失效

随着技术发展和 IT 场景演进，传统的内外网硬性边界划分已经模糊，传统防护思路已不再适用，安全边界需要伴随着资产的弹性范围和接入动态延展，将其最小化并弹性连接为一个防御体系也是必然趋势。AIGC 降低网络攻击门槛的同时，高级威胁活动的技术、战术和过程中存在的 AIGC 应用可能因目标不同而不同，高度的定制化情报导致缺少攻击组织的信标或者画像信息。分析人员需要针对人工智能生成的成果进行分析，但可能由于高级威胁情报的碎片化而形成线索无法拓线。

网络纵深和欺骗防御等安全建设也伴随着复杂度的增加，在安全能力单元各自为战的环境下导致高级威胁情报缺乏共享、存在孤岛现象，高级威胁穿透或绕过防御薄弱点直达价值资产的过程中并无关键线索留存。在对抗高级威胁过程中，一方面基于情报知识、主动扫描等技术，试图从非告警数据中挖掘异常痕迹，进而确认是否存在潜在的高级威胁攻击活动来进行主动狩猎高级威胁；另一方面，通过快速响应事前所布置的规则或黑名单等触发的安全告警，拓线研判并将其归类到组织或团伙进行被动狩猎。被动狩猎与主

动狩猎往往在情报侧由于出现新的攻击手段、目标资产、场景的不同，产生的结果难以契合，缺少联动。这使得安全人员很难获取全局的安全视图，无法对安全事件进行全面的分析、响应，难以联防联抗。

15.3 高级威胁检测发展趋势与建议

15.3.1 加快单点产品自身能力迭代

网络安全体系是由不同安全产品共同构建起来的，通过“层层设防，层层监控”的方式应对网络威胁。在高级威胁对抗逐渐白热化的背景下，新的攻击手段不断涌现、容器业务形态开始在信创环境使用，对于网络安全产品来讲，更应该迭代自身能力深度，适应变化的环境，提供更强大的防御和保护能力。

在检测能力上，在具备基础反恶意代码、联动威胁情报的基础上，安全产品还应该对更底层的内存、更新的容器业务形态予以关注，构建协同网络流量、应用、系统、内存等多层次的高级威胁检测和防御能力。安全产品通过研究 ATT&CK 框架跟进威胁情报，了解攻击者使用的战术、技术特点，一方面监控行为点并针对多点行为场景化关联分析，提升威胁检出率、降低误报率，同时将检出的威胁进行可视化图谱溯源展示，完整还原攻击链路，分析出攻击者使用的具体入侵手段，发现零日漏洞攻击、APT 攻击和有针对性攻击等行为；另一方面，高级威胁逐渐呈现低频隐蔽、复杂多步的特征，安全产品通过引入人工智能技术，加强攻击样本构建、复杂网络攻击检测、检测模型可解释性等智能分析水平，研究基于图的复杂网络攻击检测技术，实现对多步复杂等高等级威胁的“检测 - 溯源 - 预测”，提高未知威胁攻击的检测能力。在容器这种新的业务形态上，合理地运用容器“职责单一化”的特性，落地基于行为模型的未知威胁检测方式，通过持续、长时间的监控容器进程、文件、网络等行为刻画业务行为，结合人工智能技术利用快照、

历史、基线、异常检测相结合的逻辑组合实现异常行为发现，从而确定未知的攻击行为。

安全产品也应该针对信创操作系统、云原生业务形态进行适配。一方面，安全产品应该能够适配安装在这些信创系统上，并支持防护上层的云原生业务。这需要产品与信创操作系统的架构和特性兼容，以确保软件能够正确地安装和运行，同时能够与信创系统的版本协同演进，并且能够与系统的应用程序和服务进行无缝集成，以提供全面的保护。另一方面，安全产品还需要能够针对信创系统的特点进行增强，利用其具有一些独特的特点和安全机制，构建全面而有效的安全防护。

15.3.2 构建以运营中心为枢纽的纵深防御溯源体系

高级威胁纵深防御溯源体系的基本思路，是以安全运营中心为枢纽，将安全防护措施有机组合起来，针对攻击窃取过程的全生命周期进行层层检测、分析、响应和阻断。因此需要将攻击过程全生命周期的网络行为、主机行为等数据进行全量采集和高价值数据萃取，建立起数据底座；结合高级威胁对抗的实战经验，建立保护对象资产的正常行为基线；构建网络异常行为和主机异常行为模型，通过机器学习等方式在海量数据中发现隐匿性高级威胁，结合高效的安全决策执行机制，实现快速有效的安全防御。在这个过程中需要重构建威胁发现能力和威胁溯源能力。

15.3.3 引导行业建立信创威胁研究体系与相关标准

为了有效应对由信创引入的新的安全威胁，应引导行业逐步建立信创威胁研究体系和相关标准。一方面建立信创威胁研究体系，有助于行业用户深入了解威胁源头，为防范和应对威胁提供科学依据；同时有助于快速发现和预警潜在威胁，为行业用户提供充足的应对时间。另一方面，通过制定信创

威胁相关标准，可以规范行为，便于监管和评估，促进形成良好的行业秩序，同时也有助于为技术创新和产业发展提供良好的市场环境。

本章编写人员：

安芯网盾（北京）科技有限公司 文谱、姚纪卫

安天科技集团股份有限公司 邢宝玉

科来网络技术股份有限公司 陈伟清

南京南瑞信息通信科技有限公司 刘苇、魏兴慎、周剑

厦门服云信息科技有限公司 陈俊杰

第 16 章 漏洞管理

随着信创产业的发展，安全漏洞问题也日益凸显。漏洞管理成为信创的重要议题：一方面，漏洞管理的重要性和必要性越来越被业界认可；另一方面，漏洞管理也面临着诸多挑战。

16.1 漏洞管理获得初步认可，但还面临不少挑战

16.1.1 漏洞管理在信创产业中的价值获得认可

随着《网络安全法》、《网络产品安全漏洞管理规定》的深入落实，以及“信创政务产品安全漏洞专业库”的建设与运营，一批基于国产芯片、操作系统等关键组件的自主创新漏洞管理类产品得到广泛应用。这些产品针对国产操作系统、数据库、中间件、浏览器、安全产品、办公软件，帮助组织及时发现漏洞风险，建立规范的漏洞研判处置流程，取得了显著成效。

在政策环境不断完善的情况下，漏洞管理产品逐渐走向“重发现、重处置”阶段。企业开始采购漏洞扫描平台、加入产品众测、发展内部安全测试团队、采购第三方厂商安全服务等，同时加紧了内部漏洞闭环机制的建设，结合资产管理、人员管理、流程管理，不断完善漏洞管理体系。

16.1.2 漏洞管理在信创市场的应用不断深化

企业的漏洞管理体系（漏洞发现、报告、分析、修复等环节）是一个逐渐建立和完善的过程，相关的流程和管理制度也需要逐步优化。新的漏洞扫描工具、漏洞管理平台和安全解决方案不断涌现，这些技术创新有助于企业更高效地发现和修复漏洞。此外，信创市场中的企业和组织开始建立联合的漏洞管理机制，通过共享漏洞信息和安全情报，共同应对安全威胁。这种合作模式有助于提高整个行业的安全水平，共同抵御网络攻击。

16.1.3 信创市场的漏洞管理需要良好的共享机制

漏洞管理在信创市场也面临挑战，主要表现为漏洞发现不及时、漏洞误报、漏洞修复困难等。用户采购的信创产品越多，需要执行漏洞管理的范围就越大，也就越需要全面和及时的漏洞发现能力。这个能力可以是用户自己建设，也可以通过从安全厂商购买漏洞发现产品和服务来实现。对用户来说，建设自己的漏洞发现能力需要获取厂商的安全通告，以判断是否有设备受到漏洞影响；对安全厂商来说，需要有自主创新产品的指纹和漏洞通告来进行漏洞识别。在自主创新产品越来越多，漏洞来源越来越广的情况下，相关各方并没有建立良好的安全漏洞共享机制，这使得漏洞的发现、通报、修复等机制不能顺畅流转，从而产生一系列问题。

16.2 漏洞管理瓶颈源于生态和技术双重主因

从生态角度来看，信创产业生态封闭性明显，同时漏洞管理上下游企业各司其职。这些利益相关者之间的合作和协调形成了复杂的关系网络，往往存在一定的生态协同问题。从技术角度来看，信创产业通常涉及高新技术和前沿科学领域，这些领域的技术发展迅猛，所以要求漏洞管理必须能够应对快速变化的技术环境，及时识别和解决新出现的漏洞。此外，漏洞管理还需要不断跟进技术发展的步伐，及时更新和升级相关工具和解决方案，以满足不断变化的安全需求。

16.2.1 自主创新产品生态封闭

信创产业的生态体系庞大且复杂，其中漏洞管理面临着诸多挑战。由于大多数生态产品采用专有技术和封闭平台，仅对内部安全团队开放，限制了外部漏洞管理产品的接入和使用，导致这部分漏洞发现能力大大降低。同时，也增加了漏洞误报、漏报的几率，导致自主创新产品漏洞库规模和质量都存

在明显不足。

首先，网络安全厂商与自主创新产品供应商之间尚未建立有效的信息共享生态。安全厂商缺乏获取自主创新产品信息的渠道，无法及时了解自主创新产品的指纹信息，导致对自主创新产品的漏洞检测识别不准。此外，自主创新产品的开发往往依赖开源软件，如果对开源软件的依赖关系、影响范围、破坏程度等信息缺乏足够了解，将给自主创新产品带来极大的安全风险。

目前，自主创新产品的漏洞尚未引起广泛关注，这主要是因为自主创新产品尚未大量普及，且漏洞库中的信息较少。随着自主创新的规模化推广和国外敌对势力的针对性研究，可以预见自主创新产品的漏洞问题将越来越突出。

为了改善这一状况，部分自主创新厂商已经建立了漏洞通告机制，定期发布安全漏洞及相应的补丁。但这一机制并未在所有厂商中得到落实。部分产品只能依靠零散的网络信息获取安全漏洞及修复补丁，有些漏洞甚至无法找到修复补丁。此外，部分厂商的安全通告缺乏标准输出格式，不利于自动化获取和解析。

另一方面，各自主创新厂商对漏洞分类分级制度的标准不统一。例如，对于漏洞的“严重等级”，不同厂商根据自身情况设定了不同的取值，如“严重”、“超危”等，这给统一管理信创产品的漏洞带来了困难。

16.2.2 资产多元化的状态下漏洞检测机制不足

在资产多元化的状态下，自主创新产品的漏洞检测机制存在明显的不足。随着信创产业的快速发展，各种类型的信息资产不断涌现，包括芯片、操作系统、中间件、虚拟化、数据库、云服务以及行业应用等。因为不同的资产有着不同的技术架构和运行环境，漏洞的检测和修复变得更加复杂和困难。

目前，自主创新产品的开发与应用尚处于探索阶段，技术人员需要不断熟悉国产化开发环境、积累软件代码安全编写经验并加强软件开发治理能力。然而，这一过程往往导致从代码编写、适配到测试方面产生一些先天性的缺陷和问题，使得自主创新产品的安全风险在可预见的一段时间内比传统应用系统的风险还要大。同时，由于缺乏大规模应用和未经长期用户及工业场景的验证，其安全性面临着更大的挑战。

现有的安全漏洞检测手段已经无法满足激增的自主创新产品。依靠人工检测，检测效率无法覆盖代码的增长速度；而依靠漏洞库提供的漏洞特征进行检测，又因为自主创新产品与通用软件的技术架构和运行环境的差异，使得 CNVD、CNNVD、CVE 和 NVD 等通用漏洞库并不能完全适用于自主创新产品。因此，需要积累专属于自主创新产品的漏洞库，提供更加准确的技术支撑和数据支持。

此外，优化漏洞检测机制、补充漏洞定位及复现能力也是必要的。这可以降低自主创新产品漏洞误报率，提高漏洞处置效率。虽然通过已知漏洞特征的比对可以发现已知漏洞，但对于未知漏洞却无能为力。因此，对未知漏洞的挖掘是当前最为缺失的能力。

16.2.3 产业化漏洞协同机制有待深化

目前，信创产业各方的漏洞协同机制尚未完全建立。首先体现为信息共享不足，这使得漏洞的发现和修复速度受到限制，增加了安全风险。其次，自主创新软件领域缺乏统一的漏洞标准和规范，导致不同厂商和组织对漏洞的定义、分类、评估和修复存在差异，使得协同工作变得困难。第三，由于自主创新软件与通用软件的技术架构和运行环境存在差异，通用漏洞库并不能完全适用于自主创新软件。第四，协同机制中缺乏明确的激励机制，导致合作和信息共享的积极性不高。最后，自主创新软件领域缺乏具备专业知识

和技能的人才，以及能够支持漏洞协同机制的技术平台和工具，使得各方在合作中可能遇到技术障碍和沟通难题，影响协同机制的推进。

16.2.4 漏洞管理专业性强，市场化进展缓慢

漏洞管理是一项专业性极强的任务，在市场化过程中，漏洞管理面临着诸多挑战和困难。

首先，漏洞管理对专业知识和技能要求极高，需要相关人员具备丰富的安全知识和实践经验，加之网络安全技术发展变化太快，新的漏洞和攻击方式不断出现，使得漏洞管理的市场化教育成本较高。

其次，漏洞管理的复杂性和多样性也是导致市场化困难的原因之一。漏洞管理涉及到多个技术领域，每个领域都有自身的复杂性和特殊性，需要漏洞管理人员具备更广泛的知识和技能，以便能够应对各种类型的漏洞和攻击。

此外，网络攻击和漏洞利用技术的不断进化也给漏洞管理带来了挑战。为了应对这些变化，漏洞管理人员需要及时跟进最新的安全漏洞和威胁情报，并具备快速适应和应对的能力。这需要投入大量的人力和资源，增加了漏洞管理的成本和难度。

最后，漏洞管理需要大量的资源和工具支持。为了保持最新版本和适应不断变化的威胁环境，这些工具和设备的购买和维护成本相对较高。

16.3 产业生态协同，共融共建漏洞管理新局面

漏洞管理行业的发展需要深入洞察行业需求，推动生态协同，共同开创漏洞管理的新局面。

首先，深入行业是关键。漏洞管理涉及到各个行业和领域，因此需要

针对不同行业的需求特点和发展趋势，进行深入的研究。通过深入洞察行业需求，可以为不同行业提供定制化的漏洞管理解决方案，满足行业的特殊需求。

其次，生态协同是核心。漏洞管理的生态协同包括多个方面，如企业与供应商、客户、竞争对手、研究机构等之间的协同，以及国家、监管单位各方对行业的有效监管和有力支持。通过建立良好的生态协同关系，可以共同应对漏洞管理面临的挑战，分享资源和信息，提升整个行业的安全水平。

最后，共创漏洞管理新局面是目标。漏洞管理行业的发展需要不断创新和进步，通过不断提升产业协同联动能力、提升技术融合与顶层建设加码加力，多措并举，共融共建漏洞管理新局面，推动整个行业的进步和发展。

16.3.1 打破信息壁垒，建立行业生态体系

兼容性、扩展性、标准化、规范化等问题是现阶段信创产业安全发展的主要挑战，其主要原因在于行业具有较高的信息壁垒，尚未与上下游各机构单位间形成良好的行业闭环生态体系。

建立信创产业安全生态是一项长期的、艰巨和复杂的任务，当前看来，主要有以下几点可供借鉴：其一，探索建立信创产品相关安全风险、安全事件、安全技术、安全应用等信息共享与风险通报机制，统筹信创领域漏洞管理，推动定期开展自主创新产品安全风险评估工作；其二，制定统一标准，制定行业内的统一技术标准和规范，确保各类产品和服务的兼容性与安全性，实现信息的互联互通；其三，促进产学研用资创合作，整合各方资源，推动技术研发、成果转化和产业应用。全产业链凝心聚力，协同攻关，使自主创新安全真正变成一种长期机制运转起来。

16.3.2 AI 等新技术融合，提供漏洞管理新思路

遗传算法、神经网络等 AI 技术开始与模糊测试技术相融合，为安全漏洞检测和修复带来了极大的推动作用，也为漏洞管理提供了新的思路。

在模糊测试中，遗传算法可以生成更多不同类型的测试用例，通过改变输入数据的长度、格式或内容，以模拟各种异常情况。这些测试用例可以有效地测试应用程序的边界情况，增加测试的覆盖率。

神经网络则可以用于构建模糊测试的目标函数，通过学习大量的数据来进行分类、预测和优化等任务。在模糊测试中，可以使用神经网络来评估测试用例的质量，判断测试用例是否能够触发应用程序的漏洞或异常行为。通过不断地训练神经网络，可以逐步提高其评估测试用例的准确度和效率，提升模糊测试的效果。

随着 AIGC（生成式人工智能，Artificial Intelligence Generated Content）等大模型的兴起，模糊测试技术得到了进一步的提升。实践证明，AIGC 融合模糊测试在漏洞检测和修复方面取得了显著的改进，可谓是一次颠覆性的创新。在漏洞检测方面，通过使用大模型的能力，可以更好地了解被测程序的语义、参数、函数接口等信息，从而指导代码模型自动化生成测试驱动，有效提升模糊测试工具的自动化程度，降低其使用门槛。模糊测试还可以不依赖已知漏洞信息，通过针对软件的输入进行随机或有目的的模糊变异。这能够发现那些尚未被公开披露或被收入漏洞库的漏洞，可以弥补自主创新软件漏洞库的不足。在缺陷修复方面，通过将存在漏洞的代码片段与模糊测试的分析结果作为测试用例输入大模型，可高效生成修复后代码，加快漏洞修复速度，提升代码质量。

此外，模糊测试技术还可以与 SAST（静态应用程序安全测试，Static Application Security Testing）和 SCA（软件组成成分分析，Software Composition Analysis）等工具共同协作，提高漏洞检测的精度和覆盖率。模

糊测试可以生成各种类型的输入数据，包括异常数据、边界数据等，以模拟各种异常情况。这些测试用例可以作为 SAST 和 SCA 的输入，帮助它们发现更多潜在的漏洞。同时，模糊测试还可以提供更丰富的异常场景和错误行为信息，有助于改进 SAST 和 SCA 的检测算法和规则库。

16.3.3 完善信创漏洞管理顶层建设

国家已经颁布了一系列漏洞相关的标准和监管要求，建立起了“信创政务产品安全漏洞专业库”国家级漏洞共享平台，这为漏洞管理提供了基础框架。但在实际操作中仍存在一些问题，如各部门之间的协调不足、政策执行不到位、缺乏长期规划等。因此，需要加强政策环境的建设，完善机制、推广标准，提高政策的有效性和协调性，促进形成产业合力。为了更好地完善漏洞管理机制，建议出台相应规定，统一漏洞数据格式及分类分级标准，以减少用户获取不同来源漏洞公告的技术难度。同时，设立安全厂商准入机制，符合准入机制的安全厂商可以共享 NVDB 数据，以提升安全厂商的漏洞发现能力。

16.3.4 深入行业场景，推行可落地的行业漏洞管理方案

漏洞管理与资产之间存在紧密的关联性。全面的漏洞发现依赖于更加全面且准确的资产信息，资产的变化也会影响漏洞风险的存在。这意味着不同的行业场景需要匹配不同的漏洞管理解决方案。由于大多数企业并不具备专人专职管理的条件，漏洞管理方案更应切合企业实际，以场景化的解决方案帮助用户实现漏洞管理需求。

首先，针对不同行业的特点和需求制定漏洞管理策略和规范，包括对行业标准的梳理、安全需求的识别、风险评估的方法、漏洞修复的流程等。在制定漏洞管理方案时，还要充分考虑业务连续性、数据安全性、合规性等问题。

其次，建立完善的漏洞发现和报告机制。建立全面的漏洞发现体系，包括定期的漏洞扫描、实时的监控和告警、对异常行为的及时响应等。建立漏洞报告机制，鼓励内部员工和外部合作伙伴及时报告漏洞，并对漏洞报告进行及时分析和处理。

本章编写人员：

三六零数字安全科技集团有限公司 胡晓娜、闫小涛、冯飞、王佳敏

北京天融信网络安全技术有限公司 黄栋

北京神州绿盟科技有限公司 刘美君

北京启明星辰信息安全技术有限公司 蒋发群、张苗苗

北京云起无垠科技有限公司 沈凯文、王书辉、夏营

上海碳泽信息科技有限公司 贾玉彬、董惠

第 17 章 反恶意代码引擎

绝大部分网络攻击都依赖恶意代码的投放与执行，对恶意代码及其衍生物的快速识别、检测分析、分类命名和响应处置能力是各类网络安全产品和整个网络安全体系的基石。随着威胁数量与复杂度的持续增加、攻击的场景不断泛化，信息系统复杂性、资产规模和网络带宽不断加大，给反恶意代码引擎的检测能力、检测效率、算力成本和精准分类命名提出了新的要求。

17.1 反恶意代码引擎面临日趋复杂威胁对抗形势

17.1.1 威胁形势日趋复杂

国家背景的威胁行为体发起的网络攻击和有针对性的攻击达到了前所未有的强度，网络威胁攻击越来越复杂和多样化。恶意代码即服务的兴起和人工智能的发展降低了网络犯罪分子利用恶意代码发起攻击的成本和技术门槛。网络钓鱼攻击变得更加复杂，有针对性的钓鱼攻击越来越多。勒索软件攻击更加频繁，勒索威胁不再以经济作为唯一犯罪动机，出现“政治化”攻击动向。俄乌冲突期间频频出现“破坏式”勒索软件。勒索攻击已经在早期的“数据加密”之上，发展出了包括窃取数据、曝光数据（泄露或出售）、数据破坏等在内的更多勒索攻击类型。跨平台勒索软件帮助威胁行为体渗透到更多的复杂环境中，给反恶意代码检测引擎的检测分析能力带来了新的挑战。安全威胁泛化已经成为常态，物联网、工业互联网等新兴场景下的恶意代码攻击事件持续增加，对反恶意代码引擎的新场景适配和场景化专属检测能力提出了新的诉求。面对复杂的威胁形势，反恶意代码引擎需要不断优化检测能力，在持续提升识别解析、特征匹配、启发式分析、虚拟执行和行为分析等基础能力之上，采用增强级的检测技术，如机器学习和人工智能，与基础技术能力互补，形成多层有效的威胁检测能力，更有效地应对新威胁。

17.1.2 算力危机加大了检测能力与成本代价之间的矛盾

半导体危机和“卡脖子”带来了相应的安全算力危机。同时，严峻的威胁形势产生了更高的安全防护能力需求，给安全产品和反恶意代码引擎等带来了效能和算力代价均衡的挑战。安全高度依赖算力，算力的成长为安全能力的持续叠加增长提供了支撑，算力危机也必然导致安全危机。

基于通用计算平台的高速检测引擎发展遇到瓶颈。反恶意代码引擎分支众多、预处理深度加深，带来计算处理资源的压力；热数据集规模庞大、局部性差，也会导致 cache 失效等性能恶化。此时，安全检测所需要的算力能力并不能完全获得摩尔定律的支持。

“卡脖子”导致的被动算力降级。国产自主的 CPU 能力已经有了长足进步，但其实质性的计算能力（特别是对高安全需求的算力任务承载方面）仍与 Intel 等主流 CPU 存在着较为明显的差距，为反恶意代码引擎带来了诸多挑战。

算力危机可能导致检测能力与成本代价之间的矛盾进一步凸显。当算力而非安全能力变成首要制约项时，算力就会拉平强安全能力厂商和弱安全能力厂商之间的差异，从而导致安全能力的负淘汰。

17.1.3 业界缺乏统一的恶意代码分类命名标准

目前业界还未形成统一的恶意代码分类命名标准。国际上有多个机构与组织积极推动恶意代码分类命名相关的标准化工作，但未达成普遍一致的共识。1991 年，计算机反病毒研究组织（CARO）推出了 CARO 命名方案，约定恶意代码样本的命名规范。2005 年，美国计算机应急小组和 MITRE 公司推出了恶意代码类型枚举（CME）计划，采用共享的、中立的标识符交叉引用不同厂商的病毒名，以改善业界的恶意代码信息共享。2011 年，MITRE 公司

推出了恶意软件属性枚举和特征描述（MAEC），对恶意软件进行统一描述。

几乎所有复杂的和规模化的攻击行动都依赖恶意代码的投放和执行。反恶意代码引擎对恶意代码的检出和精准命名是安全防护的基础，各种安全产品与安全平台也需要借助恶意代码的分类命名进行相应的事件告警、关联分析和优先级排序等。因此统一的恶意代码分类命名标准愈加重要。缺少规范的恶意代码分类命名规范，难以有效支撑统一的事件告警、关联分析、风险判断、应急响应和信息共享等工作。用户信息资产场景的安全防护与响应、社会层面的安全治理、监管单位的风险预警通报、威胁情报共享等都需要科学清晰的恶意代码分类标准和命名规范。

17.2 反恶意代码引擎需要解决“内部”问题

17.2.1 传统反恶意代码引擎的效能正在衰减

传统反恶意代码引擎对海量已知威胁的精准识别已成为网络安全中不可替代的核心能力。由于其本身是易获得、可免杀绕过的资源，导致其面临着效能衰减的挑战。随着安全威胁的持续不断演进，攻击者获得各种安全产品，进行对抗绕过测试已经是高级攻击中的必选动作。特别是，攻击者通过编写新的病毒样本或替换模块、对已被查杀的样本进行各种免杀修改、利用窃取主流厂商的数字证书给样本签名绕过白名单机制、广泛使用无文件攻击手段、攻击者更多使用开源性攻击工具甚至改造现有工具逃避检测，都成为攻防中的常态动作。同时，更先进的网络钓鱼方法和新的社会工程技术不断出现。高级威胁行为体更多使用复杂的 UEFI 固件 Rootkit/Bootkit 实现持久化和隐蔽攻击。

17.2.2 反恶意代码引擎的高检测能力需要算力支撑

反恶意代码引擎依赖算力完成对输入对象的检测，高检测能力必然产生高

算力需求。引擎对于待检测对象的预处理、分析和检测匹配工作上有大量的解密、解码、解压、虚拟执行、多种 hash 算法以及多种匹配的算法，这些都对算力有重度依赖。从威胁对抗的角度看，恶意代码的规模和复杂度均在不断增加，反恶意代码引擎势必加强相关的能力，包括更全面的格式识别拆解能力、更深度的预处理能力和更细粒度的检测能力等，这些变化都产生了更大的算力需求。

17.2.3 主流厂商有自己的恶意代码分类命名风格

各主流厂商在持续的捕获分析、规则提取和更新升级等恶意代码检测分析一级威胁对抗工作实践中，形成了自身经验和视角下的恶意代码分类命名风格与规范。部分厂商更多继承了历史上约定俗成的风格，并未形成统一的分类；有的厂商以流行的恶意代码作为分类标准，局限于特定操作系统平台上的恶意代码；一些厂商以恶意代码的特定行为作为分类标准，但随意添加分类。整体来看，各厂商形成了差异化的恶意代码分类命名方法。

17.3 发挥反恶意代码引擎价值，赋能核心威胁检测能力

17.3.1 构建全场景赋能的共性安全能力和公共知识体系

国内引擎厂商为业界生态提供以反恶意代码引擎为代表的共性安全能力，并基于大规模基础设施支撑和引擎的输出形成了一套恶意代码公共知识体系。

17.3.1.1 为全场景赋能共性的可嵌入式安全检测能力

国产引擎厂商提供了全系统场景的可嵌入安全检测能力，基于国内外主流基础软硬件技术路线构建了适配各类场景环境的安全内核和反恶意代码引擎，把安全基因作为一种可集成的能力兼容到各种体系结构和环境中，为终端场景（传统终端、信创终端、移动终端、工业主机、云主机、虚拟化和容器等）、流量场景、云端、业务场景（邮件服务器、OA、文件交换等）以

及工业智能场景提供可嵌入式安全能力。截止目前，国产反恶意代码引擎通过供应链融合的方式，已经融入到了超过 100 万个云原生节点、超过 5000 万台传统 PC 节点、超过 130 万台网络安全设备，以及超过 30 亿部手机和智能终端。每一台 2018 年之后出厂的国产手机和 2019 年之后出厂的国产 POS 机，都有国产的反恶意代码引擎。

17.3.1.2 构建并持续完善恶意代码公共知识体系

国内的引擎厂商积极推动知识体系的建设与完善，基于广泛的反恶意代码引擎赋能、长期的特征工程和知识工程实践积累，结合大模型形成了一套名为“计算机病毒分类命名知识百科”（后文简称计算机病毒百科）的公共知识体系，并面向互联网开放。计算机病毒百科以严格的分类命名索引为基础，按照基础分类、运行环境、家族名、变种号和核心行为标签的结构展开。计算机病毒百科从基础分类出发，按照恶意代码的运行环境逐层展开，粒度达到恶意代码家族级别。计算机病毒百科目前涵盖超过 5 万个家族知识词条，覆盖了超过 99% 已知的恶意代码家族，并且在不断地更新迭代。计算机病毒百科将逐步发展成恶意代码领域的公共知识，可供研究界、学术界、产业界和公众所使用。

17.3.2 双管齐下优化反恶意代码引擎的算力使用

为了在有限资源和用户可接受代价下实现更有效的恶意代码检测和威胁对抗，需要从软件和硬件两个层面优化反恶意代码引擎的算力使用。在软件层面，通过优化预处理机制、精细化检测逻辑和改进特征匹配算法等一系列工程化方法，最大限度地发挥现有算力的潜力。

随着通用算力的使用已接近极限，硬件层面的优化（如 GPU 加速和专用安全检测芯片）成为必经之路。将适合 GPU 执行的逻辑，如哈希计算、模式匹配等能高度并行的计算任务，从 CPU 转移到 GPU，充分利用硬件资

源，发挥相应硬件计算优势，从而提高检测速度。尽管 GPU 扩展了计算单元，但仍存在一些结构上的瓶颈，且功耗成本更高。国内引擎厂商开始尝试扩展专用安全算力，研发专有安全算力芯片以实现更高的计算性能。反恶意代码引擎结合专用算力芯片将实现性能优化和“算力”卸载，有效提升引擎性能，满足用户对检测能力、效率以及算力成本之间平衡的迫切需求，为整个网络安全生态体系提供更强大、更快速的核心威胁检测能力。

17.3.3 推进恶意代码分类命名标准工作

为了解决由于缺乏恶意代码分类命名标准导致各方在恶意代码的判定、命名和共享等工作方面无法统一的问题，促进安全生态协作、助力核心关键技术创新发展，推动网络安全产业高质量发展，国家计算机网络应急技术处理协调中心牵头，联合安天科技集团、三六零、蚂蚁集团、国家信息技术安全研究中心、西安邮电大学、奇安信等产学研单位共同编研了《信息安全技术 互联网恶意软件定义与描述格式》。该标准已进入征求意见阶段。这一标准的研制为互联网恶意软件提供了清晰的定义、分类和判定准则，并规定了恶意软件命名格式和描述格式。标准正式发布后，将为各方开展威胁检测、安全预警、信息共享、应急响应等工作提供规范化参考。

本章编写人员：

安天科技集团股份有限公司 童志明、李石磊、韩耀光

安芯网盾（北京）科技有限公司 杨芳、文谱

第 18 章 安全管控

信息系统的复杂程度和开放性不断加深，从技术的角度对安全管控体系带来了巨大的挑战。市场上对安全管控的定义也不一致，包含了网络安全产品管理和控制、态势感知、安全运营等多种形态。但安全管控作为政企网络安全管理和运营的综合型平台，所带来的价值和作用逐步得到认可，安全管控已成为政企构建网络安全体系的核心。

基于安全管控在市场侧的多种概念，本文所提的安全管控概念包含了网络安全产品管理和控制、态势感知和安全运营等 3 种形态。

18.1 安全管理在精细化实战方面表现差强人意

网络安全管控已从等保合规进入到攻防实战阶段，对技术和产品的实战要求逐年提高。现有的安全管控技术和产品在智能辅助决策、异构设备的纳管以及个性化安全场景的覆盖等方面的表现差强人意，技术创新和产品升级势在必行。

18.1.1 安全管控的智能化辅助安全决策效果不佳

事件响应是政企网络安全团队的重要工作内容之一。安全设备每天会产生海量告警，安全分析人员需要找出高危告警，并对这些告警进行分析和追踪溯源，做出合适的处置操作。管理者需要根据自身业务的发展与网络安全建设效果进行整体网络安全战略制定和未来网络安全规划等。

理想的情况是期望通过建设网络安全管控体系，为安全人员和管理者提供风险评估、应急响应、安全规划的决策支撑。但现实情况是，现有的安全管控技术缺乏一定的智能技术，在高级威胁分析溯源、自然语言联动、安全策略生成等方面存在一定的缺陷，无法给出精准的辅助安全决策信息。

18.1.2 异构安全产品纳管效果不理想

网络安全建设是一个随着 IT 环境升级不断变化的动态的过程，政企单位的网络环境中部署了大量的不同品牌的安全产品。通常情况下，一个小型单位大概部署 15-20 种不同的安全产品，中型单位 50-60 种，大型单位超过 150 种。根据安全牛等咨询机构发布的年度网络安全全景图可以看到，网络安全的细分领域有 3180 项[10]，这其中至少涉及了数千个不同品牌的产品。这些产品包括防火墙、IPS/IDS、WAF 等传统安全产品，以及近年来流行的 SDP、EDR、XDR、UEBA、资产视图等新型安全产品。

在网络安全的技术演进中，理想的情况是期望通过安全管控平台类产品实现对这些不同安全产品的统一纳管。但现实情况是，大部分安全管控平台仅可较好地纳管自有品牌产品。对于第三方产品，由于各品牌安全设备遵循的协议、标准、技术架构差异较大，且产品之间接口互不开放，无法有效的互联、互通、互操作等现实原因，造成了安全产品的生态难以融合，导致安全产品的纳管效果一直不尽如人意。

18.1.3 行业差异化场景覆盖能力不足

安全管控平台应用正在向行业化、场景化发展。不同行业对网络安全的考核、管理要求差异较大。如金融机构永不离线已经成为常态，安全运营成为生命线，系统面临着巨大的并发压力。通信行业的安全风险主要表现在 5G、云计算、人工智能等新技术新应用带来的数据保护、通信、用户权限控制、终端安全等风险与能源、交通、公共服务等行业领域深度融合产生的业务安全风险。互联网企业由于存在大量的内部或外部的数据服务接口，通过 API 接口导致的安全事件层出不穷，API 安全问题已成为互联网企业需要直面的首要难题。即使同一行业不同规模的用户，随着企业业务的发展，也不

[10] 网络安全行业全景图（2023 年 4 月第十版） https://www.aqniu.com/focus/95236.html

断涌现出个性化的安全需求，例如工业互联网安全管控、物联网安全管控、数据安全管控等。同时在网络安全建设程度和资源保障上，大型企业通常需要投入更多的资源和技术来保护自己的网络系统，而中小型企业则可能缺乏专业的网络安全人员和设备，更依赖于外部的服务提供商。

理想的情况是期望通过建设网络安全管控体系，具备强大的场景覆盖能力，能自适应的覆盖各行业差异化网络安全场景。但现实情况是，各行业安全场景差异巨大，同行业不同体量的客户也存在巨大差异。当前的安全管控产品除了核心能力外，厂商需根据客户的需求提供定制化的开发服务来满足这些差异性需求。

18.2 安全管控技术和产品需要创新发展

经过多年的发展，安全管控体系在政企网络安全体系中的核心价值已得到市场认可，同时现有的安全管控技术和产品在网络安全实战化方面的部分效果乏善可陈。从技术层面分析，主要原因在于缺乏安全数据、安全能力原子化的标准规范；缺乏快速满足客户网络安全新需求的技术手段。因此，当前的安全管控技术和产品急需创新发展。

18.2.1 中台化成为安全管控实战能力的基础

安全管控需要具备整合企业内各应用系统、安全系统的能力，需要进行跨职能部门的资源协调，支持与保障企业的数字化战略。这种多层次的协调联动对安全数据的多级流转和原子安全能力的协同互操作提出了非常高的要求，安全数据和原子安全能力是安全管控体系建设的两大基础。同时缺乏安全数据、安全能力原子化的标准规范，也极大影响了安全管控体系的辅助决策和安全产品纳管效果。

由于各类数据的格式、协议、接口等不一致且传输过程中存在丢包等因素，大量异构安全数据汇聚后，原始数据的质量无法保障，如自动发现的资产数据和资产管理系统导入的资产数据存在不一致、不同安全设备产生的告警存在矛盾等问题，极大的影响了上层的数据分析准确性和安全业务的开展。因此通过构建安全数据中台，建设一个完善的信息资源共享服务技术体系，建立信息共享的标准和规范，实现对原始数据的完整性、规范性、一致性、准确性与唯一性等指标进行检测评估；上层建立完整的信息共享资源目录和信息资源服务能力；提供统一的大数据处理服务能力，提升信息资源服务能力，解决网络安全业务对海量数据的深度挖掘、分析、应用的迫切需求。

在《2023 网信自主创新调研报告》中，我们已经分析过安全能力中台将成为安全管控的基础。未来的安全管控体系将以中台和安全业务平台的形式存在，即利用数据中台构建一个完善的安全信息资源共享技术支撑，建立安全信息共享的标准和规范，为上层各类安全业务提供统一的数据服务；利用安全能力中台构建企业网络安全的核心枢纽，以资源化、原子化、服务化和标准化的方式打通组织内外部网络安全职能边界，正在实现全局视角的网络安全管控体系。

18.2.2 低代码保障安全管控具备更强的适应性

由于网络安全需求存在较大差异性，在短期甚至未来的很长一段时间内，安全管控平台的定制化服务不可避免，且定制开发周期比较长。相应的，对于需求方而言，期望可以大幅降低自身网络安全需求的定制开发周期和降低定制带来的人力和经济成本；对于厂商而言，急需一种可以简化定制开发过程、提高开发效率的技术和方法。

低代码（Low-code）[11] 技术提供了一种良好的解决思路和方法。当安全

[11] Low-code development platform https://en.wikipedia.org/wiki/Low-code_

管控平台核心功能建设完成后，通过使用低代码技术提供更高效的网络安全业务应用开发工具，保障定制开发的效率快速提升，缩短项目交付周期，让平台快速上线。从而保障安全管控具备更强的适应能力，实现快速覆盖各行业用户的差异化网络安全需求。

18.2.3 提升用户体验可以尝试人工智能技术

AIGC 等人工智能和自动化技术的融合有助于进一步提高安全运营的效率和质量，提升用户体验。如，大语言模型可以通过分析大型数据集、识别可疑指标和关联事件，帮助主动寻找威胁，并根据最佳实践和合规标准辅助制定安全策略；自然语言检索能让用户通过简单的自然语言输入，快速检索到所需的安全告警信息；自然语言联动支持用户通过自然语言下发联动指令，实现设备之间的智能协作，简化操作流程，实现高效自动化控制和管理。

18.3 多维度提升安全管控综合产业能力和技术价值

随着新技术和方法的引入和使用，安全管控体系将逐步解决安全人员使用过程中面临的专业层度要求高、安全成果度量难以及实战效果不太理想等问题。未来的安全管控技术将具备良好的人机互动和较强的自适应能力，将可以快速满足各类差异化网络安全需求，并进行决策或者辅助决策。

18.3.1 强化学习，增强安全实战能力

随着人工智能大模型的兴起，通过网络安全私域模型训练，将会提高安全管控体系的知识管理应用、对话式应用，能够极大地提升最终客户的使用体验，并大幅提升面对网络安全事件的检测与响应效率。通过引入安全大模

development_platform

型等新技术，可实现安全管控如下能力的提升：

(1) 高级威胁分析与溯源。大语言模型可以通过分析大型数据集、识别可疑指标和关联事件来帮助主动寻找威胁。帮助检测 APT 攻击并发现容易被忽视的秘密攻击活动，实现高级威胁分析的准确率和溯源完整的攻击过程。

(2) 自然语言检索。通过大模型自然语言处理能力，实现让用户通过简单的自然语言输入，快速检索到所需的安全告警信息。这种直观、便捷的界面交互方式，降低了平台的使用学习成本，减少操作复杂性，加快了告警信息的查找速度，帮助用户更高效地发现和应对潜在的安全威胁。

(3) 自然语言联动。借助人工智能大模型和自动化技术，支持用户通过自然语言下发联动指令，实现设备之间的智能协作，简化操作流程，提升了用户的使用体验，实现了更高效的自动化控制和管理。

(4) 安全策略生成。制订全面的安全策略和指南是一项耗时的任务。大语言模型可以根据最佳实践和合规标准协助制定此类策略。实现现有策略分析、找出差距并提供增强安全策略的建议。

(5) 增强安全运营能力。用户可以通过与智能助手对话的方式，提出各种网络安全运营相关的问题，如安全策略、威胁情报、安全告警报文解读、安全事件响应等。通过在安全管控中加入安全大模型智能助手，将根据模型的训练和理解，提供相应的解答和建议，帮助用户更好地理解和应对各种安全运营问题，而且让安全工作变得更方便、更有效率，提高整体安全运营的能力。

18.3.2 牵头引领，提升安全生态融合

信创适配中心的成功为安全产品生态融合提供了良好的建设思路和解决

方法。为了解决安全管控面临的各类异构品牌安全产品对接的生态融合难题，可以通过联合共建或各省或大型行业企业独立建设的方式，建立适配中心，落实网络安全产品对接和管控标准。

由国家和行业监管单位牵头，创新行业特色的产业生态合作模式，建立安全产品对接适配中心，制定和执行网络安全产品的对接和管控的执行规范，提供网络安全产品的适配服务，可以推动网络安全产品的生态建立（包括网络安全产品的研发、测试、认证等环节），提高网络安全管控产品的质量和效率，促进网络安全产业的发展。

18.3.3 深耕行业，提供精细化的服务

安全管控平台正在面向行业化、场景化方向发展，与通用的行业属性不同，网络安全天然处于交叉行业，安全管控方案的供应商除了为用户提供核心能力外，仍需根据用户的行业属性需求提供定制化开发服务。安全管控体系的行业差异需求覆盖是需求方和技术提供方共同努力的方向。

对于需求方而言，当安全管控体系建设完成之后，如何体现安全价值及根据企业的业务发展持续改进非常重要。因此需求方应当与技术提供方充分配合，将网络安全度量方法整合到安全管控体系中，做好安全度量，以定量评估安全性能、风险和防御能力，深度分析自身的网络安全新需求，这有助于企业及时发现自身问题，确保安全防御体系在实战中处于最优的姿态。

对于技术提供方而言，随着安全管控技术和产品整体综合能力的成熟，各供应商应当考虑深耕行业需求，深度了解不同行业的网络安全风险和管理需求以及相关的法律法规和考核标准，推出行业解决方案，以满足差异化的行业需求，为行业用户提供更加专业和有效的服务。同时各供应商也需要引入低代码、人工智能、自动化等新技术，以进一步增强方案和产品的扩展能力，

以适应网络环境的变化和客户的新需求。安全管控方案也应当兼顾中小型企业的网安需求，可以通过MSS（安全托管服务）、公有云版安全管控平台等，帮助这些普遍缺乏足够人力和相应技术的中小型企业应对网络安全攻击。

本章编写人员：

杭州安恒信息技术股份有限公司 聂桂兵、孙佳

中电长城网际系统应用有限公司 刘鹏

科来网络技术股份有限公司 张卫云

安天科技集团股份有限公司 苗佳艺

第 19 章 工控安全

党的二十大报告指出“推进新型工业化，加快建设制造强国”。新型工业化是指融合人类先进的科学技术，在已有的工业技术技能和管理范式的基础上进行装备高端化、数字智能化、能源绿色化、供应自主化、技术创新化、体系结构化的高质量可持续性转型升级。本章所探讨的新型工业化背景下的工控安全，涵盖传统工控安全、工业信息安全、工业互联网安全[12]。

19.1 工控安全国产化进入加速期

19.1.1 工控安全主动防御技术不断涌现并开始落地

国内外工控安全大都围绕以白名单技术为基础构建纵深防御解决方案，相关技术领域的产品已发展成熟。我国国产化生态的内生 / 可信安全类、安全终端类、以白名单为技术特色的访问控制类、检测分析类、综合管理类等产品持续迭代并已实现市场化落地。

工控安全创新的主动防御技术思路和解决方案不断涌现。主要包括三个方向：一是以可信计算和零信任等技术为代表的主动防御技术体系；二是内生安全，即工控安全与业务深度融合、互为驱动的主动防御技术体系；三是随着人工智能技术的快速突破，人机共智的主动防御与运营新阶段开始萌芽。其中，以内生安全和可信计算为技术主导的产品广泛应用在电力、新能源汽车及其配套充电设施等领域；以零信任为代表的技术流派在工业物联网、工业互联网平台已开始使用。

[12] 工业信息安全、工控安全、工业互联网安全相关概念见《2019 年工业信息安全标准化白皮书》。国际上通常将细分的工控 / 工业数据安全领域统称为 ICS（Industrial Control Security），即工控安全。

19.1.2 工控安全蓬勃发展，但国产化覆盖不足

《中国工业信息安全产业发展态势研究 (2022 年—2023 年)》报告显示，2022 年我国工业信息安全产业规模达到 204.86 亿元 [13]，工业信息安全市场从产业资本、技术、人才各方面加速聚合，整体发展迅猛。

随着我国工控安全产业规模不断扩大，各工业行业对工控安全产品的国产化需求同步逐渐提高，出现了一大批基于国产化生态研制工控安全产品的厂商，市场上开始采用国产化的产品和解决方案。虽然工控安全的国产化与发展进程保持同步，但国产化工控安全产品的市场整体占比还处于较低水平。原因在于各细分工控行业的购买力不同，如果行业的购买力强，则工控安全国产化的发展速度就相对较快。如已执行的工控安全国产化项目，近 60% 来源于电力行业。

19.2 新型工业化面临多重安全挑战

19.2.1 新业态带来新的技术挑战

新型工业化要求工业领域融合新技术、新应用构建新业态快速发展。这既给工业领域带来了巨大的发展机遇，也给工业控制系统引入大量新的网络和数据安全风险。

由于网络攻击工具越来越容易获得，并且越来越自动化，网络攻击的门槛逐步降低。普通灰黑产业人员即使不具备强大的技术背景和专业知识，也可以开展攻击并造成严重危害。针对新型工业的攻击工具、技术服务化已经开始出现。全球的工业网络安全攻击事件表明，工业现场 PLC 这种相对固化、低算力、小存储的计算单元也可以成为攻击 OT/IT 网络的跳板，针对工控数

[13] https://news.cctv.com/2023/11/09/ARTIc0xcUXgeLa02UH7WYRZM231109.shtml

据的勒索攻击导致价值成百上千亿的工业生产线全线停摆。对工业信息基础设施漏洞的重新发现和利用，不断刷新着人们对工控安全的认知。

19.2.2 供应链安全保障能力不足

工控安全的国产化需要构建从芯片、整机、操作系统、中间件到工业应用软件一系列 ICT 国产化的完整生态。目前，国内工控安全生态链方面存在以下问题：

一是供应链核心技术的安全监管和应对不足。供应链的国际化为工业互联网引入了许多不受主要供应商和用户控制的第三方角色，扩大了潜在攻击面。极端情况下，工控安全的供应链保障能力不足。硬件和装备方面，CPU/GPU/NPU、内存、网络交换、存储主控等核心高端芯片，以及高端工业制造装备仍依赖国外；软件和系统方面，多数工业行业的基础操作系统、工业设计软件、大型工业控制系统、工业管理软件和工业数据库等依赖国外。在缺少供应链安全监管平台和供应链安全评测规范的情况下，针对封闭的工业系统，如何管控复杂、动态的供应链安全是需要引起高度重视的问题。

二是国产化产品的成熟度有待提高。国产化的工控安全产品种类相对较全，但基础软硬件在技术上与国际领先水平存在差距，使得产品的成熟度和可靠性不高，导致用户对国产化产品验证时间长、应用推广进程缓慢。

19.2.3 工控安全观念需要提升

目前，工控安全主要围绕基本安全需求和合规进行防护建设，但合规是基线，而不应该是工控安全的目标。在攻防对抗中暴露出来的跨专业、横纵向联防联控和安全响应机制不完善的问题，很大程度上源于工控安全建设“重设备、轻人才，重建设、轻运营”的现象。

工控安全是一个综合的系统工程，依靠设备的堆砌远远不能有效的解决工控安全问题，需要结合考量合适的安全技术、人员安全意识与技能和有效的管理制度多个方面进行体系化的能力提升。

19.3 强化技术与服务创新，促进工控安全高质量发展

19.3.1 融合新技术，持续开展创新

技术创新是推动工控安全行业发展的核心动力。企业在筑牢国产化关键技术底座的同时，需要不断开展技术和服务模式的创新（如新型工业化下的人工智能、数字孪生等新兴技术与工控安全的深度融合发展），以应对新的威胁和挑战。

人工智能大模型可以在工控系统安全运营、辅助决策、人员培训等多方面赋能。例如，通过大模型技术将行业知识与专家经验工具化，以数字身份扮演安全运营角色，基于授权策略，实现全天候值守；利用大模型系统的智能安全运营能够自动解析和解读告警信息并进行智能研判，提供实时的辅助决策，推荐最佳响应方案；根据工业企业的实际情况进行个性化的安全培训和教育，甚至开展模拟攻击训练，让工业企业更快速、更全面地提高员工的安全认知和技能水平。

数字孪生为工控安全提供了物理现实与数字化安全融合的新途径、新方法。数字孪生技术已经在工业攻防靶场、工业安全态势感知的虚实结合方面取得了一定应用，但还需继续深化应用研究，加速产业化落地。

19.3.2 建设高质量的安全服务能力

在关键信息基础设施安全保护中，需要在理解业务流的基础上，开展关键资产、风险等的识别后再开展其他网络安全活动；在工业数据安全保护中，

需要以业务数据流为基础，梳理数据和业务的关系再规划和开展数据生命周期的保护。这两种服务均要求服务者在具备以设备资产和应用系统安全服务传统能力的基础上，进一步理解现场业务和数据，提供更专业的安全咨询、安全培训、安全建设与实施、安全托管服务。推动国产化工控安全技术和产品与业务场景融合，将安全控制策略与生产过程关联，实现面向工业生产环境的行为安全管控，让安全懂工业，让工业懂安全。

另外，工控安全在新型工业化时代需要进一步加强多方协同监测及威胁情报共享，提高企业对工控安全系统性的理解和应对网络攻击事件的响应能力，这也是安全服务提质增效的前提。

19.3.3 构建实战化的主动防御体系

单点的产品或者不成体系的防护手段已经难以对抗新常态下的工控安全威胁。要有效应对多点和复合式网络攻击，需要构建基于实战化的主动防御体系。

实战化方面，加强模拟演练、红蓝对抗等实际攻防验证手段。通过建设高逼真的工控演练系统进行安全推演，了解系统弱点，优化安全策略；通过红蓝对抗模拟真实攻击，培养跨专业和工种的工控网络安全团队的紧急响应和协同合作意识。

主动防御方面，通过可信度量和计算保障计算环境的加载启动和运行安全，以攻击者的视角监测识别完整的网络攻击面，持续身份鉴别，动态调整授权和访问控制策略，最大程度地减小潜在的攻击面。

构建实战化的主动防御体系能更全面地识别潜在威胁，验证安全策略的有效性，及时调整和优化安全措施，增强工控系统的整体安全性和应对未知威胁的能力。

本章编写人员：

长扬科技（北京）股份有限公司 汪义舟、张亚京、赵华

江苏云涌电子科技股份有限公司 方艳湘、陈凯迪、黄婉静

北京惠而特科技有限公司 赵承刚

北京天融信网络安全技术有限公司 金忠龙、刘超、樊强

科来网络技术股份有限公司 孟召瑞、张卫云

北京久安世纪科技有限公司 刘博文

北京可信华泰信息技术有限公司 郑锟、杜君

北京珞安科技有限责任公司 梁宁波

北京启明星辰信息安全技术有限公司 蒋发群

杭州安恒信息技术股份有限公司 安成飞、高倩

中电智能科技有限公司 孟德俊

第 20 章 电子数据取证

电子数据取证是国内安全领域的一个重要方向，但在推广进程中，存在一些难点和挑战，制约了电子数据取证产业的国产化发展。

20.1 电子数据取证产业国产化推广进程缓慢

20.1.1 最终用户未形成普遍的、规模化的市场需求

电子数据取证领域的市场需求主要集中在公安、纪检、海关缉私、税务稽查、市场监管等执法机关以及有内部审计需求的企业，其他行业的最终用户对此类产品的需求较小，尚未形成规模。对于执法机关客户而言，非国产化电子数据取证产品与国产化产品相比，在功能、性能、价格等方面更具优势。此外，由于电子数据取证产品的专业性和复杂性，大众对其认知度和了解程度有限，也缺乏足够的意识和重视。这些因素导致国产化取证产品的市场需求相对较小，难以形成规模化的推广和应用。

20.1.2 国产化取证产品的标准化工作还在酝酿

目前，国产化电子数据取证产品还未形成相关标准。这导致了不同厂商的取证产品在数据格式、协议解析等方面存在差异，难以实现互通和互操作。厂商对于国产化取证产品究竟应该实现哪些功能，达到何种性能也尚未形成共识，在这样的环境下，用户也难以评价国产化取证产品的质量优劣。同时，由于标准化工作的滞后，国内厂商在技术研发和创新方面也受到了一定的限制。

20.1.3 取证厂商开发国产化产品积极性不高

目前电子数据取证行业仅有少数厂商开展了国产化工作，市面上通用的国产化电子数据取证产品种类较少。与一些其他高科技行业相比，国产化电

子数据取证产品市场的规模相对较小，电子数据取证行业的利润空间相对有限，并且由于涉及到的技术和领域较为复杂，开发出高质量的电子数据取证产品需要具备强大的技术实力和人才储备。这使得一些厂商在考虑开发国产化产品时，可能会面临技术难度大、开发周期长等问题，从而降低了开发国产化产品的积极性。此外，由于电子数据取证产品的使用涉及到敏感的司法问题，产品的质量和可靠性对于用户来说至关重要。因此，厂商在开发国产化产品时需要面临更高的风险和责任。一些厂商可能会因为担心产品的质量和可靠性无法达到用户的要求，而选择不开发国产化产品。

20.2 电子数据取证产业国产化推广进程缓慢的原因

20.2.1 电子数据取证国产化产品具有高度定制的特点

目前电子数据取证国产化产品以平台类居多，表现为基于国产化服务器、操作系统、中间件、数据库等实现的数据综合分析类平台。由于此种项目建设成本较高，且需要接受客户的高度定制化需求，无疑增加了产品开发和推广的难度。对于厂商来说，需要投入大量时间和资源来了解每个用户的特定需求，并进行定制化的开发。而对于潜在用户来说，要在众多产品中选择最适合自己的，也需要花费大量时间和精力。

20.2.2 取证产品本身仍然缺乏统一的行业标准

公安部于2019年发布了《法庭科学 电子物证检验实验室建设规范》标准，规定了电子物证检验实验室的设备配置清单等内容，各地司法鉴定管理部门对涉及电子数据检验的司法鉴定机构也有设备清单要求，但这些标准和要求中对于各取证设备具体应当符合何种功能和性能要求却并未做出明确规定。当前国内大部分电子数据取证厂商将主要资源投入产品研发和技术服务，并未深度参与取证产品的标准制定工作。目前，非国产化取证产品的标准化工作尚未完善，更遑论国产化电子数据取证产品。

20.2.3 部分取证产品国产化还存在技术难点

电子数据取证的对象在硬件层面包括计算机、手机、服务器、移动存储等设备，在软件层面包括网站、数据库、软件、APP、流量等。目前国产化平台下的电子数据取证产品对于计算机、服务器类的存储介质取证提供了一定的支持，但在部分产品的国产化实现上还存在困难。例如，根据目前主流的手机取证技术路线，需要解析手机与操作系统之间的通信协议以实现手机数据的提取，但对于国产化操作系统而言，在连接种类繁多的品牌型号的手机时还存在诸多问题。这些技术难点使得国内厂商在研发和生产方面面临一定的困难，也影响了国产化取证产品的质量和竞争力，耗费大量人力物力，也带来了系统的不稳定，使得最终用户对国产化取证产品仍然心存疑虑。

20.3 把握机遇，加快电子数据取证产业国产化推广进程

20.3.1 自顶向下，以点带面

电子数据产业的国产化推广需要自顶向下，从政策层面开始，政府和相关部门应当给予国产化产品更多的支持和鼓励，包括政策扶持、采购倾斜、技术研发资金支持等。通过政策引导和市场机制的推动，逐步提升国产化产品在电子数据取证领域的应用广度和深度。同时，可以选择一些具有代表性的国产化产品和企业，进行重点培育和支持。通过给予这些产品和企业更多的市场机会和资源支持，打造出具有国际竞争力的电子数据取证产品品牌。鼓励这些企业在技术研发、生产制造、市场营销等方面进行创新和探索，形成可复制的成功经验，进而带动整个电子数据取证产业的国产化进程。

20.3.2 加快标准化工作进程

国家应制定电子数据取证领域的国家标准和规范，推动不同厂商的取证

产品实现互通和互操作。应制定相关政策法规，明确国产化产品的应用范围和推广目标，并建立完善的标准体系，规范国产化产品的研发、检测、使用和评估等环节。这样可以确保国产化产品的质量和可靠性，提高用户对国产化产品的信任度和认可度。

20.3.3 产学研相结合进行研究攻关和示范应用

对于电子数据取证国产化过程中遇到的技术难题、规范难题，可发挥机构、高校在科学研究方面的优势，依托强大的研究能力和技术人才储备，为取证厂商提供先进的技术支持和解决方案。取证厂商则具有市场推广和应用示范的经验，可以将研发成果转化为实际的产品和服务。通过高校和科研机构的培养和教育，可以为企业输送更多高素质的人才，提升团队的整体素质和创新能力。同时，政府也应加强引导和支持，推动电子数据取证产业链上下游企业进行合作和创新，形成产业协同发展的良好格局。

本章编写人员：

广东中科实数科技有限公司 丁丽萍、杜漠

第 21 章 软件供应链安全

近年来，针对软件供应链的攻击越来越多，相关的安全保障问题逐渐被业界关注。

21.1 软件供应链安全尚未得到足够重视

21.1.1 软件供应链高度依赖开源组件或国外技术

近 5 年，开源代码在应用中所占的比例由 40% 增至 78%-90%，混源开发成为主要模式，平均每个应用包含 147 个开源组件[14]。据统计，在物联网、网络安全、计算机硬件、半导体、能源等行业的代码库中有 100% 是开放源代码，其余行业存在 93%-99% 的开源代码库[15]。开源组件的广泛应用，在提高软件开发效率的同时，也带来了潜在的安全风险：技术的开放性和透明性降低了漏洞被发现和利用的难度。此外，一些用户对国外技术的依赖也较为严重。

21.1.2 用户对软件供应链安全认知存在误区

一是忽视软件供应链安全基础，将安全视为一个附加的功能，而不是基础功能。二是缺乏长期安全规划，没有建立完善的软件供应链安全治理与运营体系。三是存在片面的安全观念，认为安全只是技术问题，忽略了安全的复杂性和多维性。四是缺乏协同合作。

21.1.3 软件供应链安全实践的可复制性较低

国内软件供应链安全领域头部企业实践案例的低可复制性现状主要表现为行业属性差异、软件供应链安全产品和解决方案的适配性问题，以及长期

[14] 2022 OSCAR 开源产业大会

[15] 新思科技《2022 开源安全与风险分析报告》

性和持续性的投入问题。一是不同行业对软件供应链安全的需求存在显著差异，导致头部企业的实践案例难以直接应用于其他行业。二是头部企业在选择软件供应链安全产品和解决方案时，通常会根据自身需求进行定制化开发或配置。这些产品和方案在功能和性能上不一定适合其他企业，而规模较小的企业又无力进行定制化开发或配置。三是头部企业在软件供应链安全方面的投入和实践往往具有长期性和持续性，这种投入对于中小企业而言难以承受。

21.2 软件供应链安全供需双方都需要提高

21.2.1 国产软件供应链安全产品自身能力需要持续提升

一是国外开源项目的发展历史悠久，经过多年的市场验证，其可信度、成熟度和性能稳定性都相对较高。相比之下，国内开源技术起步较晚，仍面临成熟度不足的问题。

二是一些厂商将国外产品引入国内，简单修改后宣称完全自主。这种做法导致技术含量低、运维能力差，在实际应用中可能存在兼容性问题，甚至可能导致业务系统崩溃，给企业的运营带来巨大风险。

三是部分用户较长时间使用国外产品，迭代过程中需要考虑兼容性等问题，这不仅涉及技术层面的挑战，还涉及业务流程、人员培训等多个方面。

四是软件供应链安全情报共享机制不健全，在一定程度上影响了软件供应链安全的产品效能。

21.2.2 部分网络运营者软件供应链安全观念薄弱

尽管近年来有政策和事件的双重驱动，但目前很多企业仍无暇顾及“并未发生的安全风险”，认为软件供应链安全是奢侈品，而非必需品。尤其是中小企业，受现实竞争压力所迫，更关注于短期的业务发展和利润增长，往

往忽视安全对于长期稳健发展的重要性。

网络安全的意识仍停留在传统安全的产品或服务层面。部分从业人员认为只要部署了传统安全产品（甚至采购了安全服务），就能够确保软件供应链的安全。实际情况是，传统的安全产品或服务很难应对复杂多变的供应链安全挑战。另外，投入高、收效难以直接体现，也是导致企业软件供应链安全观念薄弱的原因之一。

软件敏捷开发和安全成本之间难以平衡。在敏捷开发模式下，开发周期通常只有几个月甚至几周，这就意味着在短时间内要完成大量的开发工作，开发者考虑安全问题的可能性比较小。另外，为了提高开发效率，敏捷开发通常会大量使用外部库和开源代码，这必然会引入新的漏洞或恶意代码，而安全团队的介入又相对滞后，这就错过了修复安全问题的最佳时机。

21.2.3 用户对新技术的接受度较低

技术复杂性和高门槛是企业对新技术接受度低的原因之一。新技术往往具有较高的复杂性和专业性，对用户的技术实力和人才储备有较高的要求。因此，对于一些技术实力较弱或缺乏相关专业人才的企业来说，新技术的接受和应用就变得困难。另外，对不确定性的谨慎态度，应用新技术的成本考量，以及行业标准和规范的不完善都是影响新技术、新产品广泛应用的因素。

21.3 积极应对挑战，保障软件供应链安全

21.3.1 完善软件供应链安全管理和技术体系

软件供应链安全管理需要建立在对软件供应链生命周期各阶段风险的深刻理解之上，确保供应链的完整性、保密性、可用性和可控性。目前，我国对软件供应链安全管理尚未形成完整链条。在大力推动软件供应链安全管理体系落地过程中，重点的工作方向包括建立具备前瞻性与适应性的法规体系，

推进技术标准的国际化，研发风险评估工具，以及构建开放的创新生态等。

特别是在技术体系建设方面，要构建软件供应链安全检测与防御体系，建立上游安全检测机制、建立供应链安全情报中心、完善软件开发安全体系、优化软件安全交付流程、强化软件安全运营能力。在评估工具方面，要考虑功能完备性、自动化与集成、漏洞数据库更新频率、可定制性和灵活性、报告和可视化能力。

总之，要构建软件供应链安全检测与防御体系，需要多方参与协同共治，方能实现安全工具供应商、软件采购方、软件供应商三者循环互信的可信软件供应信任链。

21.3.2 提升软件供应链安全意识

一方面，强化内部安全与开发团队建设，提高对开源软件的安全治理能力。这包括采用先进的持续运维手段、加强数据备份，以及在国产化替代过程中解决兼容适配、平滑替代、数据迁移等关键问题。另一方面，要强化安全管理与意识建设，通过培训、交流、考核、合作等多种方式确保安全团队和软件开发团队紧跟先进技术趋势不掉队。同时，对于开源软件和技术，要避免简单的“拿来主义”，而应进行深入的评估、测试和改进，确保其与自身的业务需求和安全标准相符合。

21.3.3 建立软件供应链安全生态圈

构建一个覆盖全产业链、全员参与、全方位保障的软件供应链安全生态圈是我国软件产业健康发展的重要基石。只有通过生态圈内各方力量的协同合作，才能真正实现从源头把控安全风险，保障软件供应链的稳定可靠。具体来讲，首先要建立软件供应链威胁情报共享平台，基于云计算、大数据分析、人工智能等技术，建立符合软件供应链威胁情报共享标准的体系，及时采集、

汇总、研判、共享、发布软件供应链威胁情报信息，促进有关部门之间的威胁情报共享，并满足实战化需求，达到对软件供应链安全事件进行联防联控的效果。其次要建设供应链上下游企业间的透明度与互信机制，提倡软件供应链安全审查和认证服务，以便下游用户做出决策。第三要加强产学研一体化，鼓励科研机构、高校与企业合作研发更加先进的软件安全保障技术，培育具有自主知识产权的安全解决方案，为软件供应链安全生态圈提供源源不断的创新动力。

本章编写人员：

北京安普诺信息技术有限公司 子芽、陈超、杜玉洁

中国移动通信有限公司研究院 李政

北京安天网络安全技术有限公司 陈灵锋，郑剑萧

北京启明星辰信息安全技术有限公司 杨天识

北京云起无垠科技有限公司 沈凯文、王书辉、夏营

杭州孝道科技有限公司 刘永瑞、朱雅汶

湖南泛联新安信息科技有限公司 覃子桐

后记 1

随着《2023 网信自主创新调研报告》统稿完成并通过专家评审，第 6 个网信产业调研和编写工作已经告一段落。如果连续 6 年的编写工作能得到业界的认可，将是对参与这项工作的全体人员莫大的鼓励。

回顾过往的 6 年（2018 年 -2023 年），编委会一直“坚持脚踏实地、坚持实事求是、坚持集思广益”编写原则。我们给自己确定的目标不是系统性、全面性、典型性，不去刻意要求教科书式的表达方式，而是站在业界和参编成员的视角、从参编单位的实践出发，写实地阐述我们一年来的创新努力和取得的成效，尝试着对具有代表性的问题做出我们的分析，提出对策的思考和建议。正是这个特点，报告受到了相关单位和人员越来越多的关注，得到了越来越多的支持，而且参与编写单位一直在逐年快速增加。

在呈现形式上，编委会一直追求逻辑性和简洁。《2018 网信自主创新调研报告》的主题是展示创新成果，逻辑是从技术创新、产品创新、工程创新和应用创新 4 个维度展开。当初《2019 网信自主创新调研报告》以供应链安全为主线，对各个领域面临的供应链安全问题进行了分析和梳理，从一线厂商的视角回答了供应链安全“是什么”、“为什么”和“怎么办”3 个问题。《2020 网信自主创新调研报告》站在“十三五”收官之年，一方面回顾过去 5 年取得的成绩和存在的问题，另一方面从用户需求、国内外差距或新技术新应用带来的挑战等角度分析当下的创新发展目标，同时结合数字化转型、双循环等大环境和大趋势，展望了未来 5 年的创新发展路径。《2021 网信自主创新调研报告》再一次以创新成果为主题，展示了自 2018 年以来我们的技术、产品取得的进展，分析了这些技术和产品的应用情况，探讨了未来一个时期的发力点。《2022 网信自主创新调研报告》第一次以深化自主创新为主题，

尝试着呈现和分析替代的现状（提出问题）、原因（分析问题）和实现路径（解决问题）。

如今《2023 网信自主创新调研报告》再一次以“深化自主创新”为主题。主要原因在于，编委会在调研中深切感受到，随着产业界技术创新和产品化工作的不断推进，目标已经从单纯的党政办公自动化系统转向支撑关键信息基础设施应用领域，供给侧和需求侧之间的协同是进一步深化自主创新的关键问题。因此，本年度的调研和报告着重关注了“问题导向”。

报告成文后，为了更好地掌握和分析数据，编委会对各产业节点提出的影响深化自主创新的问题（包括现状、原因、对策中涉及的可能关系以及该主题的各种要素）做了统计分析。统计数据如图 1 和表 1 所示：

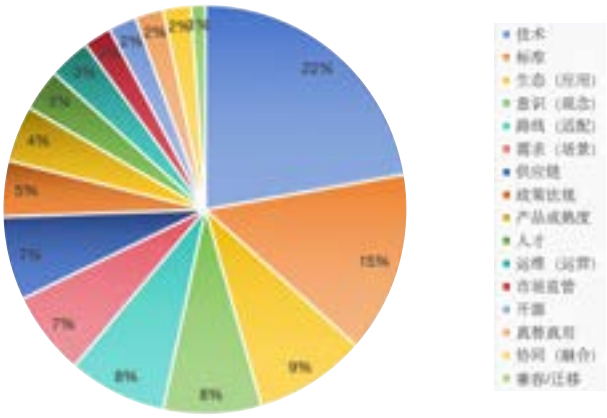


图 1 数据分布

从统计数据看，21 个产业领域共涉及了 16 类问题，包括技术、标准、生态（主要指应用系统）、意识（主要指需求侧的观念）、技术路线（主要关系到适配的人力成本、时间成本和经济成本）、需求（主要指应用场景和产品的匹配）、供应链、政策法规、产品（主要指成熟度，也包含性能、性价比等因素）、人才、运维（也包括运营）、市场监管、开源（既包括开源

带来的安全风险，也包括需求侧采用开源工具而不是商业化版本）、真替真用、协同（主要指技术和产品的融合）、兼容 / 迁移（主要指软件的品牌和版本的兼容，以及替代后的数据迁移）。

技术问题被提及的最多，21 个产业节点中的 20 个都提到了与技术创新相关的话题。可见，影响深化自主创新最主要的因素还是核心技术受制于人或关键技术水平的相对落后。这与编委会的预期是一致的，影响关键信息基础设施国产化替代的首要因素是技术能力与应用需求之间的差距。

排第二位的问题是标准，共有 13 个产业节点提到了标准化问题。这里的标准既包括技术规范，也包括信创标准。值得关注的是，在信创目录不再更新、信创标准迟迟没有出台的情况下，很多行业的国产化工作继续参照信创目录，这导致很多成立较晚的厂商根本就没有机会参与相关工作。另外，即便是之前入围了信创目录的厂商，由于其新产品错过了信创目录，也只能用两三年前的老产品参与某些领域的工作。这在一定程度上阻碍了技术创新和产品迭代工作。

排第三位和第四位的问题是生态和技术路线，分别有 8 个和 7 个产业节点提到了相关问题。实际上这两个问题是一体的两面，对于产业链上游来说，每一条技术路线都希望基于该路线完成适配的应用数量越多越好；而对于产业链下游来说，每一个应用都深感技术路线分散带来了巨大的适配压力。

并列第四位的问题是用户的意识和观念，共有 7 个产业节点提到了相关问题。这一问题主要存在于办公软件和网络安全领域，主要表现在对正版软件的支持、对开源软件的选择，以及重硬件、轻软件，重产品、轻服务等方面。

排在第六到第十六位的问题涉及的产业节点数相对较少，这里不再赘述。

除了进行纵向比较外，编委会还将统计数据从基础篇和安全篇两个视角

表 1 数据统计

序号	问题	涉及节点数	芯片	固件	OS	存储	数据库	中间件	整机	办公软件
1	技术	20	■	■	■	■	■	■	■	■
2	标准	13	■	■		■	■	■	■	■
3	生态（应用）	8	■		■	■		■	■	
4	意识（观念）	7		■						■
5	路线（适配）	7	■		■			■	■	■
6	需求（场景）	6			■					
7	供应链	6				■		■	■	
8	政策法规	4				■			■	
9	产品成熟度	4			■				■	
10	人才	3		■						
11	运维（运营）	3					■			
12	市场监管	2				■				■
13	开源	2						■		
14	真替真用	2							■	■
15	协同（融合）	2								
16	兼容 / 迁移	1					■			

进行了横向对比，相关数据如下图 2 所示。

图 2 横向对比

从统计数据看，技术问题被提及最多是基础篇（包括基础软硬件、整机、应用软件和打印设备）和安全篇共同关注的问题。相对来说，基础篇更关注

打印设备	软件测试工具	商用密码	终端安全	云安全	数据安全	高级威胁	漏洞管理	反恶意代码	安全管控	工控安全	安全取证	软件供应链安全
■	■	■	■	■	■	■	■	■	■	■	■	■
■	■	■				■		■			■	
							■		■			■
	■			■	■					■		■
			■		■							
		■	■				■		■			■
■					■					■		
■		■										
	■										■	
	■	■										
			■			■						
												■
		■					■					

标准、生态和技术路线问题，安全篇更关注应用场景（供需对接）问题。用户的意识（观念）和供应链问题都得到了一定程度的关注，但关注的程度并不是很高。而基础篇关注的生态、真替真用、市场监管问题，安全篇关注相对低一些。安全篇关注的应用场景问题，基础篇关注也相对低一些。

由此，编委会认为可以提出以下观点：首先，深化自主创新工作，最重要的是做好技术创新；其次，通过完善标准体系（不仅是技术标准，还有信创标准），有助于解决技术路线分散导致的适配和生态问题；第三，提升用户的信创和安全意识，对于促进创新成果应用推广至关重要，而政策引导对于行业市场也是不可缺少的引导推动手段。

《网信自主创新调研报告》主编 田霞

2024 年 4 月 19 日

后记 2

《2023 网信自主创新调研报告》和大家见面了。今年，是中华人民共和国成立 75 周年，是实现“十四五”规划关键的一年。对于网信自主创新工作来说，亦是如此。

记得在 2023 年初，编委会对《2023 网信自主创新调研报告》做最后的统稿工作时，大家普遍预感到 2023 年对于网信自主创新企业来说将会是极不容易的一年。一方面，党政领域的信创工作告一段落，重点行业的国产化替代工作开始启动；另一方面，也开始感到三年抗疫后的经济环境和国际形势的影响给企业拓展市场带来的压力。

如今，当我们回顾 2023 年的时候，发现实际情况与当时的预感基本一致，行业内各个产业节点在 2023 年都承受到了上述压力。我们的《2023 网信自主创新调研报告》以“进一步深化自主创新”为主题。编委会在确定这个主题的过程中，与大量业界专家进行了广泛和深入的沟通，多数人认为我们目前的创新成果在各个行业应用落地的效果并不理想。

本年度的报告由 200 多家网信厂商、近 400 名网信从业者，历时 7 个多月经过调查、分析、编写、汇集完成。报告从网信行业 21 个产业节点的视角，从应用推广的角度研究分析了当前我国网信产业面临的现状和问题。尽管如此，编委会深知由于参与编写单位有限等原因，报告在深度和广度上还有很大的上升空间。比如，在人工智能算力方面，在英伟达的 AI 算力芯片被美国政府一而再再而三的封堵时，华为的 AI 芯片昇腾 910 为我国打造自主稳定可靠的 AI 云基础设施提供了有力的支持。而华为麒麟 9000S 的突破和鸿蒙 4.0 的推广以及即将出台的鸿蒙 5.0，也给了自主可控的国产移动终端产品

以创新性的支撑。我们期待，对类似问题的调研分析，将在《2024 网信自主创新调研报告》中会有所体现。

2024 年 3 月 5 日，国务院总理李强代表国务院向十四届全国人大二次会议作政府工作报告时提出：综合分析研判，今年我国发展面临的环境仍是战略机遇和风险挑战并存，有利条件强于不利因素。我们认为，网信自主创新工作，也面临着同样的机遇和挑战，加快自主创新、深化自主创新成果的应用落地非常必要。我们要坚持稳中求进、以进促稳、先立后破。稳是大局和基础，进是方向和动力。 网信自主创新工作也存在稳和进的对立统一。一方面，产业界要在基础性核心技术和产业生态建设上稳扎稳打，不断提高产品的性价比和稳定性、可靠性，为进一步做好深化自主创新工作打好基础。毕竟行业市场的最终决定因素是产品的市场竞争力。另一方面，我们也想代表产业界呼吁有关部门和行业主管部门，要在破的问题上加大力度，对真正自主创新的企业和产品在采购、替代和使用上给予明确引导和坚定有力的支持。

最后，在《2023 网信自主创新调研报告》的编写工作即将完成，报告即将发布之际，编委会向参与报告编写工作的单位和个人表示衷心地感谢，向为报告提出指导意见的各位专家表示衷心地感谢。六年的坚持，我们最大的收获仍然是必须始终学习贯彻习近平同志关于核心技术自主创新的战略思想，在具体工作中“坚持脚踏实地、坚持实事求是、坚持集思广益”。

让我们“撸起袖子加油干”，为我国的网信自主创新工作继续努力！

网信自主创新调研报告编委会

2024 年 4 月 19 日

扫一扫关注公众号