2021
网信自主创新
调研报告

网信自主创新调研报告编委会

2022年4月

专家委员会

主　任：倪光南

副主任：严　明、霍　炜、胡伟武、窦　强

委　员（按拼音排序）：

曹　冬、陈晓桦、丁丽萍、杜跃进、冯燕春、冯裕才、
高　南、国　强、郭守祥、韩乃平、贺建楠、胡红升、
黄玉钏、黄志刚、江　海、金　波、李　斌、李　冰、
李　超、李璐瑶、李智虎、刘龙庚、刘闻欢、刘学忠、
刘　毅、陆宝华、卢　卫、罗东平、罗建东、孟　楠、
任卫红、唐　彬、汤学军、田俊峰、吴　锋、项　勇、
肖新光、杨纪文、杨小晔、翟起滨、张　滨、张焕国、
张　凯、张　强、张　彦、张宇翔、赵　波、赵　甫、
赵晓燕、赵战生、郑静清、祝国邦

编委会

主　编：田　霞

副主编：李　勇、张　戈

编　委（按拼音排序）：

白　华、陈　鹏、陈　强、陈小春、陈晓光、陈雪鸿、
崔文喆、崔煜华、戴凯乐、樊海珍、樊　山、冯　源、
付　伟、高喜宝、郭同彬、韩耀光、胡金山、黄　健、
黄　岩、贾　宇、蒋发群、寇增杰、康　毅、李安伦、
李保丰、李利军、李亚军、李震宁、凌　飞、刘　彬、
刘明哲、刘　缨、刘云龙、刘晓蔚、路　娜、罗　芳、
罗俊松、吕　冰、马　静、马士民、马志仁、马　原、
聂桂兵、欧庆于、任宏洋、任　亮、孙　亮、唐前临、
屠故园、王春伟、王金龙、王　鹏、王伟光、王小东、
王英键、王中斌、向　科、徐明迪、徐　宁、徐　洋、
严　飞、杨　昆、杨庆华、杨　涛、张长河、张　磊、
张木梁、张琦滨、张晓琴、张　昳、张一彬、张　映、
赵泉城、赵晓溢、郑　金、郑　良、朱　琳、朱正美

倪光南

中国工程院院士

《网信自主创新调研报告》专家委主任

中国科学院计算技术研究所研究员，中国计算机学会终身成就奖获得者，2018年获得中宣部、科技部和中国科协“最美科技工作者”称号。倪光南院士秉承核心技术不能受制于人的信念，为中国计算机事业的发展做出了重要贡献。

田霞

《网信自主创新调研报告》主编

曾任中关村可信计算产业联盟秘书长、国家信息中心《信息安全研究》杂志社副主编，主持编写了基础软硬件自主创新、可信计算、网络安全人才培养等一系列专刊，组织研究并发布了《网络安全人员角色分类和能力要求框架》（团体标准），创办了“大学生网络安全尖锋训练营”公益组织，荣获2021年度武汉“新时代巾帼英雄”称号。

2021 网信自主创新调研报告

网信自主创新调研报告编委会

2022 年 4 月 19 日

版权声明

免责声明

责任编辑：伊敏娜

校　　对：黄 怡

美　　编：赵泉城

开　　本：720 X 980　1/16

版　　次：2022 年 4 月第 1 版

印　　次：2022 年 4 月第 1 次印刷

本报告咨询联系方式：cii_zgc@163.com

刊首语

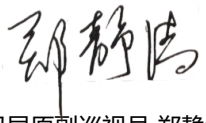
《2021 网信自主创新调研报告》和大家见面了。2021 年是我们党第一个百年，我们在自主创新上取得了长足的进步。这期调研报告分 23 个专题，向大家介绍了我们在网信自主创新当中取得的成果。相信大家读了以后，会对我们自主创新的现状、下一步的方向和我们遇到的问题，都会有所启发。

——中国计算机学会计算机安全专委会荣誉主任 严 明

《网信自主创新调研报告》在过去三年中，着眼发展、聚焦企业、探索实践，积聚了丰富的经验。相信今年国家相关法律法规实施后，该报告一定能为相关领域、生态伙伴带来更具参考价值的成果。

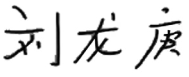
——中国电子商会自主创新与安全技术委员会理事长 冯燕春

《2021 网信自主创新调研报告》客观、真实地反映了十四五开局之年网信创新发展的良好局面，以及现阶段面临的共性难点，同时也分析提出了解决这些问题的思路与路径，为国家相关管理部门的工作人员和网信领域的各界同仁，提供了极具参考价值的珍贵资料。



——公安部网络安全保卫局原副巡视员 郑静清

《2021 网信自主创新调研报告》客观呈现了我国网信产业取得的最新成果和存在的主要问题，提出的建议与思考，为开展补链强链专项行动，加快解决关键技术与产品的自主可控，明确了攻坚方向。



——中国软件评测中心副主任 刘龙庚

《2021 网信自主创新调研报告》延续了脚踏实地的风格，较详细地介绍了这三年来我国信创基础硬件、基础软件、应用软件和信息安全四个方面的发展和应用落地情况，以及下一步的发展方向。阅读本报告的信创产业从业者和国产化工作者可以从中获得有益的借鉴和参考！

——中国铁道科学研究院集团有限公司研究员 张 彦

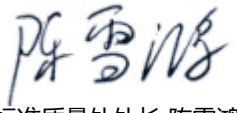
ICT 供应链安全已经上升到国家安全的高度，是关键信息基础设施保护的重点内容。《网信自主创新调研报告》已经连续发布多年。该报告立足我国实际，调研工作扎实，成果可支撑网信安全政策制定，助力关键信息基础设施的国产化替代工作。

——公安部信息安全等级保护评估中心专家委员会研究员 任卫红

近期发生的国际事件，再次证明了开展网信自主创新工作的必要性。近几年来，我国在网信技术和产品的自主可信方面取得了显著的成果，但这些还远远不够，还需要进一步加强技术创新、加快应用推广，不断推进产业生态良性发展。希望《2021 网信自主创新调研报告》能对大家今后的工作有所帮助。

——中国智能终端操作系统产业联盟秘书长 曹 冬

《2021 网信自主创新调研报告》对通用处理器、操作系统、数据库等基础软硬件，防火墙、反恶意代码等安全产品在近几年中取得的技术创新和应用成果进行了总结。相信这将有助于推动网信自主创新事业的发展，为做好关键信息基础设施保护工作提供支撑。



——国家工业信息安全发展研究中心标准质量处处长 陈雪鸿

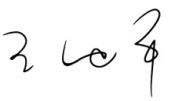
《2021 网信自主创新调研报告》客观地反映了网信企业在突破核心技术的过程中开展的创新实践和遇到的问题，对未来网信产业创新发展进行了分析，为网信核心技术自主创新提供有效的参考价值，值得关心网信技术创新的从业者深入阅读。

——龙芯中科技术股份有限公司董事长 胡伟武

网信产业的持续、深入发展，需要集众人之智，合众人之力。《2021 网信自主创新调研报告》凝聚了众多专家、网信从业者的心血，在习总书记 419 重要讲话 6 周年之际，发布这个调研报告，意义重大，必将对新时期的网信工作产生重要的指导价值。

——飞腾信息技术有限公司总经理、首席科学家 窦 强

《2021 网信自主创新调研报告》视角多元、剖析深刻、洞见长远，既是一份网信产业的权威报告，也是一份行业同仁的学习手册。

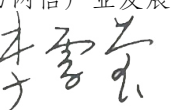


——统信软件技术有限公司董事长 王继平

《2021 网信自主创新调研报告》是网信人持续努力、砥砺前行、坚持走自主创新之路的呈现。报告的发布代表着我国网络安全和信息化领域创新成果的展示和宝贵经验的总结。麒麟软件为代表的网信企业将持续发挥自身在网络安全领域的核心优势，为打造安全可信数字底座、提供体系化安全防护体系、促进国家网信事业发展贡献科技力量。

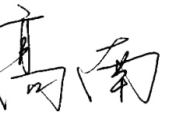
——麒麟软件有限公司高级副总经理 韩乃平

《2021 网信自主创新调研报告》凝结了网信产业科研侧、需求侧、供给侧等领域众多专家的智慧结晶，从产业政策、用户需求、产业发展、应用实践等全方面客观、真实的展现网信产业发展过程中遇到的困难、创新性地突破以及取得的成果，为推动网信产业发展提供了重要参考。



——天融信科技集团董事长兼 CEO 李雪莹

《2021 网信自主创新调研报告》来源于从业人员的客观实践，内容详实、观点前沿，相信会为各位同仁带来有价值的参考。



——江苏云涌电子科技股份有限公司董事长、总经理 高 南

《网信自主创新调研报告》从国产基础软硬件平台、网信产品、网信应用和网信人才队伍建设等四个维度，梳理国内网信企业的技术创新、产品创新和应用创新，是信创产业发展与产业链协同的催化剂与助燃剂。

——北京中船信息科技有限公司董事长、总经理 张 凯

《2021 网信自主创新调研报告》客观、真实地反映了网信企业在突破核心技术的过程中开展的创新实践和遇到的问题，得到了广泛的关注。“ 惟其艰难，才更显勇毅；惟其笃行，才弥足珍贵 ”，我们将继续努力、砥砺前行，坚持走自主创新之路，不断在网信核心技术自主创新上取得新突破。

——沈阳东软系统集成工程有限公司董事长 杨纪文

《网信自主创新调研报告》从基础领域到应用领域再到安全领域，全面、客观、真实地展示我国网信自主创新的丰硕成果，并分析各领域的创新活动以及遇到的问题，为我国自主创新产业指明方向。

——启明星辰信息技术集团股份有限公司高级合伙人 李春燕

通过《2021 网信自主创新调研报告》，我们看到了网信产业不断发展的丰硕成果，也看到了产业当前面临的主要问题与挑战。报告为网信企业继续开展自主创新工作提供了助力，为整个产业的后续发展提供了前瞻性的思考。

——北京天地和兴科技有限公司董事长 王小东

《2021 网信自主创新调研报告》是该系列调研报告的第 4 个年头，这也让我们看到了坚持的力量！随着国际形势的日益复杂多变，网信事业的重要性与日俱增，自主创新也变为最强音。本报告既盘点了过去一年各厂家取得的丰硕成果，也可作为用户单位选择的参考，非常具有实用价值！

——深圳市东进技术股份有限公司总裁 贺建楠

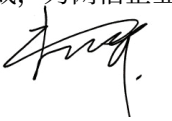
《2021 年网信自主创新调研报告》通过对自主可控生态的深入研究，真实的呈现了近年来网信产业发展的成果，为关基行业国产化替代提供了方向和引导，成为网信产业发展的风向标。

——友虹（北京）科技有限公司总经理 徐志东

立足“十四五”新发展阶段，我们比任何时候都更加需要把科技自立自强作为国家发展的战略支撑。《网信自主创新调研报告》是我国网信企业在自主创新的道路上凝心聚力、砥砺前行的一个缩影、一面旗帜。

——北京金山办公软件股份有限公司副总裁 吴庆云

《2021 网信自主创新调研报告》记录了我国网信产业取得的成果和亟待解决的问题，从新的角度审视了用户需求以及新技术、新应用即将带来的新机遇、新挑战，为网信企业发展路径规划，提供了重要且详实的参考依据。



——北京东方通科技股份有限公司执行副总裁 李利军

《2021 网信自主创新调研报告》持续以真实的数据、丰富的内容、明确的观点为我国网信领域发展提供强劲助力，充分展示了网信产业的发展成果，对构建绿色、安全的信息技术生态体系发展有重要意义。

——国科微电子股份有限公司存储事业群总裁 康 毅

《2021 网信自主创新调研报告》通过系统、深入的调研，收集了大量的资料和信息，呈现了最新成果，分析了现状，指出了问题和不足，展望了发展趋势和广阔前景，为相关单位更加深入地开展网络安全、信息安全和数据安全工作，提供了有价值、前瞻性和战略性的参考。

——重庆市信息通信咨询设计院有限公司总工程师 张晓琴

参与编写单位（按拼音排序）

阿里云计算有限公司
阿米华晟数据科技 (江苏) 有限公司
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
北京安宁创新网络科技股份有限公司
北京奥星贝斯科技有限公司
北京柏睿数据技术股份有限公司
北京辰光融信技术有限公司
北京得意音通技术有限责任公司
北京东方通科技股份有限公司
北京东方通网信科技有限公司
北京东土科技股份有限公司
北京海泰方圆科技股份有限公司
北京机智科技有限公司
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
北京六方云信息技术有限公司
北京珞安科技有限责任公司
北京奇虎科技有限公司
北京人大金仓信息技术股份有限公司
北京神州绿盟科技有限公司
北京升鑫网络科技有限公司
北京数字认证股份有限公司
北京天地和兴科技有限公司
北京天融信网络安全技术有限公司
北京网迅科技有限公司
北京威达泰克信息技术有限公司
北京信安世纪科技股份有限公司
北京亚控科技发展有限公司
北京亦心科技有限公司
北京易捷思达科技发展有限公司
北京有略测评技术有限公司
北京云思畅想科技有限公司
北京长亭未来科技有限公司
北京中安星云软件技术有限公司
北京中船信息科技有限公司
北京中电瑞铠科技有限公司
北京中科网威信息技术有限公司
北京尊冠科技有限公司
超越科技股份有限公司
重庆市信息通信咨询设计院有限公司
大庆中基石油通信建设有限公司
飞腾信息技术有限公司
广东安证计算机司法鉴定所
广东中科实数科技有限公司
国科微电子股份有限公司
国网智能电网研究院有限公司

瀚高基础软件股份有限公司
杭州安恒信息技术股份有限公司
杭州立思辰安科科技有限公司
杭州世平信息科技有限公司
杭州盈高科技有限公司
恒安嘉新（北京）科技股份公司
湖南麒麟信安科技股份有限公司
华北理工大学
江苏云涌电子科技股份有限公司
江苏长城计算机系统有限公司
精壹致远（武汉）信息技术有限公司
科东（广州）软件科技有限公司
科来网络技术股份有限公司
龙芯中科技术股份有限公司
迈普通信技术股份有限公司
南京联成科技发展股份有限公司
南京南瑞信息通信科技有限公司
平凯星辰（北京）科技有限公司
奇安信科技集团股份有限公司
奇安信网神信息技术（北京）股份有限公司
奇虎 360 科技有限公司
麒麟软件有限公司
启明星辰信息技术集团股份有限公司
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
厦门市易联众易惠科技有限公司
山东九州信泰信息科技股份有限公司
山石网科通信技术股份有限公司
上海缔安科技股份有限公司
上海观安信息技术股份有限公司
上海上讯信息技术股份有限公司
上海算石科技有限公司
上海云轴信息科技有限公司
上海众人智能科技有限公司
深圳昂楷科技有限公司
深圳市安证保全数据处理有限公司
深圳市安证区块链技术发展有限公司
深圳市东进技术股份有限公司
深圳市网安计算机安全检测技术有限公司
沈阳东软系统集成工程有限公司
苏州市立医院
太极计算机股份有限公司
天津神舟通用数据技术有限公司
天津赢达信科技有限公司
统信软件技术有限公司
同方计算机有限公司
无锡沐创集成电路设计有限公司

武汉达梦数据库股份有限公司
亚信安全科技股份有限公司
永中软件股份有限公司
友虹（北京）科技有限公司
元心信息科技集团有限公司
长扬科技（北京）有限公司
浙江华途信息安全技术股份有限公司
浙江齐安信息科技有限公司
浙江远望信息股份有限公司
郑州信大捷安信息技术股份有限公司
中电科技（北京）股份有限公司
中电科申泰信息科技有限公司
中电智能科技有限公司
中国电力科学研究院有限公司
中国软件评测中心
中国移动通信有限公司研究院
中航鸿电（北京）信息科技有限公司

支持单位（按拼音排序）

北京嘶吼文化传媒有限公司
北京通明湖信息技术应用创新中心
国家网络安全产业园区（通州园）
武汉赛博网络安全人才研究中心
中国智能终端操作系统产业联盟
中国电子商会自主创新与安全技术委员会

鸣谢

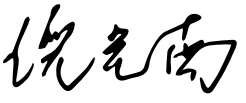
本报告的编写、审校过程采用北京金山办公软件股份有限公司支持的金山 WPS 软件完成，在此对北京金山办公软件股份有限公司表示感谢。

序一

2013 年 12 月 20 日习近平总书记《在中国工程院一份建议上的批示》上指出：“ 计算机操作系统等信息化核心技术和信息基础设施的重要性显而易见，我们在一些关键技术和设备上受制于人的问题必须及早解决。要着眼国家安全和长远发展，抓紧谋划制定核心技术设备发展战略并明确时间表，大力发扬‘ 两弹一星 ’和载人航天精神，加大自主创新力度，经过科学评估后选准突破点，在政策、资源等各方面予以大力扶持，集中优势力量协同攻关实现突破，从而以点带面，整体推进，为确保信息安全和国家安全提供有力保障。 ”正是在习总书记的这一指示以及其他重要指示的指引下，这些年我国信创工作蓬勃兴起，取得了重大成果，现在正从政府办公领域扩展到各行各业，有力地推动了我国科技自立自强和建设网络强国的进程。

随着“ 信创 ”工作的深入开展，在这个历史大背景下，《2021 网信自主创新调研报告》也如期与大家见面了。该报告以国产 CPU、操作系统、数据库、整机等等为代表，阐述了我国在网信技术方面的自主研发能力不断提升，生态愈发繁荣，核心技术不断取得突破、关键产品从基本“ 可用 ”到“ 好用 ”“ 易用 ”大跨步发展。当前信创工作呈现出在重点行业领域解决方案的自主水平不断提升的良好局面，产业生态也在重构的过程中不断融合发展，逐渐形成了良性循环的态势。但同时我们还有很多不足和短板需要迅速补齐，为此我们要踔厉奋发、笃行不怠，坚定科技自立自强的国家战略思想，在网信领域必须做好战略部署，顶层设计，随时应对潜在的风险危机。

《网信自主创新调研报告》已经连续编写 4 年了。该报告近几年越来越多地受到政产学研用各界的关注和支持，希望这本报告能对我国网信工作的开展起到助推器的作用。



2022 年 3 月 20 日

序二

《2021 网信自主创新调研报告》发布了。

这一年，是“十四五”开局的一年，是开拓新局面的一年。

这一年，我们乘胜利完成“十三五”规划的势头，在继续抗疫和反对无理制裁和霸凌中，在以习近平同志为核心的党中央团结带领下，克服困难，排除万难，继续朝着实现伟大复兴的目标奋勇前行。

这一年，在信息化和网络安全方面，我国推出了一系列重要的法律法规，将我们的信息化和网络安全进一步推向法制化和完善保护规则的途径。

在 2021 年里，在各方面因素的推动和激励下，我们的网信自主创新再一次取得了长足的进步。《2021 网信自主创新调研报告》集思广益，从联盟群体的实践和思考的角度汇总和诠释了这一进步。

我觉得，调研报告秉承一贯的指导思想，坚持脚踏实地，实事求是，继续在“实”字上下功夫。既有对本年度取得进步的情况的汇集陈述，也有对当前存在问题的思考分析，相信读后会对网信业界同行、管理部门和相关研究者都有所裨益。

我向编写《2021 网信自主创新调研报告》的专家、厂商和网信从业工作者们表示我的敬意。

还是那句话：“惟其艰难，才更显勇毅；惟其笃行，才弥足珍贵”。诸多事实告诉我们，我们必须坚持不断努力，砥砺前行，必须坚持走自主创新之路，必须要以这样的信念和追求，不断在关键核心技术研发上取得突破，为实现中华复兴的大业做出贡献。

谢谢！

2022 年 3 月 20 日

目录

前 言 …… 01
概 述 …… 03
基础篇 …… 09
1 芯片 …… 10
1.1 国产芯片在架构、性能、生态等方面取得全面进展
1.2 国产芯片在重点行业领域应用落地 …… 13
1.3 跨指令集结构的兼容和人才培养是可持续发展的关键 …… 14
2 固件 …… 16
2.1 国产固件具备全面支撑国产计算机产业的能力 …… 16
2.2 国产固件已在重要领域推广并不断扩大应用范围 …… 17
2.3 国产固件将进一步融合计算机产业链 …… 17
3 操作系统 …… 19
3.1 操作系统创新发展驶入快车道 …… 19
3.2 国产操作系统在重点行业得到广泛应用 …… 21
3.3 国产操作系统创新发展要两条腿走路 …… 22
4 数据库 …… 25
4.1 国产数据库突破部分关键技术 …… 25
4.2 数据库在政务、互联网、金融等领域大规模应用 …… 26
4.3 国产数据库针对行业需求不断深化技术创新 …… 27
5 中间件 …… 30
5.1 国内中间件技术和产业发展态势良好 …… 30
5.2 国产中间件在重点行业广泛应用 …… 31
5.3 进一步打开国产中间件市场空间 …… 33

6 办公软件 …… 36
6.1 产品和技术协同性、智能性和安全性持续提升 …… 36
6.2 国产办公软件的应用规模显著增长 …… 38
6.3 国产办公软件厂商坚守自主研发初心 …… 40
7 整机 …… 42
7.1 整机产品的功能和性能基本能够满足市场需求 …… 42
7.2 整机产品应用的广度和深度不断提升 …… 42
7.3 国产整机发展道阻且长 …… 44
8 IP 网络 …… 48
8.2 自主 IP 网络解决方案在部分行业部署并发挥作用 …… 49
8.3 自主 IP 网络仍需加速技术和应用创新 …… 51
9 云计算平台 …… 54
9.1 云计算平台实现国产化迭代升级 …… 54
9.2 云计算平台已经在多个领域广泛应用 …… 56
9.3 加强自主可控，促进云计算产业生态的可持续发展 …… 57
10 安全浏览器 …… 60
10.1 安全浏览器在虚拟化和源数据加密方面取得进展 …… 60
10.2 创新技术成果逐步开始在政企业务场景中取得应用 …… 61
10.3 未来需进一步加大浏览器核心技术的投入 …… 61
11 外设 …… 63
11.1 外设类产品在自主创新和安全管控方面取得进展 …… 63
11.2 国产外设产品在政务和金融领域获得广泛应用 …… 64
11.3 尽快打造高性能、全覆盖的产品系列 …… 65

安全篇 …… 66
12 商用密码 …… 67
12.1 商用密码技术、产品和服务形态取得突破 …… 67
12.2 商用密码与应用场景的结合日益紧密 …… 68
12.3 商用密码要和产业链上下游进一步融合发展 …… 70
13 边界安全 …… 73
13.1 边界安全产品向协同、联动、融合的方向发展 …… 73
13.2 边界安全的融合创新成果已经发挥了重要作用 …… 75
13.3 边界安全产品向高性价比和绿色节能方向发展 …… 76
14 反恶意代码引擎 …… 78
14.1 反恶意代码领域在理论、技术和工程方面持续完善 …… 78
14.2 自主核心反恶意代码技术应用促进安全生态可持续发展 …… 80
14.3 反恶意代码厂商需要不断创新并加强产业赋能 …… 81
15 高级威胁检测 …… 83
15.1 高级威胁检测思路手段不断丰富 …… 83
15.2 我国高级威胁检测技术的典型应用 …… 85
15.3 跨界融合提升高级威胁检测防护能力 …… 86
16 漏洞管理 …… 89
16.1 漏洞管理产品向智能综合方向演进 …… 89
16.2 漏洞管理产品在部分行业发挥重要应用 …… 90
16.3 漏洞管理向协同联动方向发展 …… 92
17 安全管控 …… 94
17.1 安全管控的技术创新成果全面开花 …… 94
17.2 安全管控解决方案在各行业的应用范围逐步扩大 …… 95
17.3 安全管控需要在四个方面持续发力 …… 97

18 终端安全 …… 100
18.1 自主创新的终端安全防护体系已基本建立 …… 100
18.2 终端安全产品在各行业领域广泛使用 …… 102
18.3 推动终端安全自主创新 …… 103
19 云计算安全 …… 105
19.1 传统安全产品和技术向云的演进基本完成 …… 105
19.2 云安全产品有力地支撑了等级保护建设 …… 107
19.3 新的场景和业务需要新的云安全产品 …… 108
20 数据安全 …… 111
20.1 数据安全厂商在多个专项技术上不断深挖 …… 111
20.2 数据安全技术与多个行业领域的业务场景深度融合 …… 113
20.3 数据安全需要与业务场景实现紧耦合 …… 115
21 工控安全 …… 118
21.1 工控安全产业开始注重国产化问题 …… 118
21.2 国产化的工控安全产品在电力和制造业获得应用 …… 119
21.3 工控安全产业需要进一步做大做强、做专做优 …… 119
22 安全服务 …… 122
22.1 安全服务仍处于探索阶段 …… 122
22.2 安全服务已在重点行业发挥作用 …… 123
22.3 安全服务需要加强能力建设 …… 123
23 电子取证 …… 126
23.1 电子数据取证产品种类繁多、形态多样 …… 126
23.2 电子数据取证存证在各领域得到应用 …… 129
23.3 提高效能是电子数据取证产业发展的关键 …… 130

案例篇 …… 132
龙芯中科技术股份有限公司 2021 年自主生态建设成果 …… 133
中电科申泰信息科技有限公司申威 3231 处理器 …… 136
北京计算机技术及应用研究所天熠 TR4261 便携式计算机 …… 138
北京中船信息科技有限公司边界安全防护解决方案 …… 141
江苏云涌电子科技股份有限公司远程浏览器隔离解决方案 …… 144
珠海金山办公软件有限公司 WPS Office 2019 for Linux 专业版 …… 147
精壹致远（武汉）信息技术有限公司网络攻防教学演练平台解决方案 150
友虹（北京）科技有限公司友虹电子文件链控平台 …… 155
北京东方通科技股份有限公司东方通应用服务器软件 TongWeb …… 158
湖南国科微电子股份有限公司终端安全加固解决方案 …… 161
南京联成科技发展股份有限公司安思易安全集中运维管理平台系统软件 165
安思易安全集中运维管理平台系统软件 …… 165
深圳市东进技术股份有限公司信息系统因产密码应用方案 …… 168
后 记 …… 171

前 言

一年一度，《网信自主创新调研报告》又和大家见面了。2021 年也是习近平总书记 419 讲话的五周年。2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上再一次强调了网信自主创新，他说：“我们要掌握我国互联网发展主动权，保障互联网安全、国家安全，就必须突破核心技术这个难题，争取在某些领域某些方面实现“弯道超车”。他还说，“供应链的‘命门’掌握在别人手里，那就好比在别人的墙基上砌房子，再大再漂亮也可能经不起风雨，甚至会不堪一击。”

几年来，网信自主创新取得了长足的进步。为了展示自主网信产业取得的创新成果，树立行业用户对自主网信产业的信心，同时也是为了提出和分析企业作为创新主体在现实工作中面临的困难、探索未来发展的道路，在中国工程院倪光南院士指导下，编委会自 2018 年以来连续四年组织业界专家同仁共同编写发布了年度的《网信自主创新调研报告》。编写工作组、专家委和编委会秉承“坚持脚踏实地、坚持实事求是、坚持集思广益的指导思想”，在编写过程中不以系统性、完整性为目标，不去追求教科书式的表述方式，努力将网信创新主体在各个方面的研发、生产和服务过程的实践活动汇集起来，进行分析，将取得的进步，遇到的困难，进行的思考，提出的建议都呈献出来，供业界同仁、政策研究者和管理者参考以利于更好的推动我国的网信自主创新事业。

回顾以往，《2018 网信自主创新调研报告》从技术创新、工程创新、产品创新和应用创新四个角度呈献了参与编写单位的创新成果；《2019 网信自主创新调研报告》以供应链安全问题为主线，对网信行业各个领域面临的供应链风险进行了分析和梳理，回答了供应链安全问题“是什么”、“为什么”和“怎么办”三个问题；《2020 网信自主创新调研报告》相对全面地回顾了参与编写单位在十三五期间开展的工作，并对十四五的发展前景做了展望。

如今，距离《2018 网信自主创新调研报告》的发布已经过去了三年。2021 年作为十四五的开篇之年，网信产业当仁不让地承担了数字经济建设的排头兵角色。三年来，网信技术快速发展、网信产业不断壮大，不论是技术、产品、解决方案还是相关的服务，都有了较大的进展。同时，我们在网信领域面临的国际态势也更加严峻和复杂。

《2021 网信自主创新调研报告》归纳了三年来取得的创新成果，分析了这些创新成果在各行业数字经济建设中发挥的作用，同时以产业一线的视角探讨了未来一个时期网信核心技术自主创新和产业生态建设的方向和发力点。虽然报告中体现的 23 个章节还不能做到覆盖网信技术的全部领域，但是立足于全体成员的具体实践，相信大家读来会有实实在在的收获。

进入 2022 年，我们开始了十四五规划的实践。“十四五”规划在信息化建设中部署了全面的目标。毫无疑问，坚持自主创新是完成十四五规划的关键。我们希望，这一份专注于我国自主创新的实践的调查报告，能够为迈入新征程，实现十四五规划尽一点绵薄之力。

编写组、专家组和相关工作人员为本期调研报告付出了辛勤的劳动，在此特向他们表示衷心的感谢。

概 述

本报告主体分为三个部分，按照23个专项分别对网络安全和信息化的部分领域进行了信息采集、分析和讨论。第一部分为基础篇，主要讨论基础软硬件（芯片、固件、操作系统、数据库、中间件）、信息化设备（整机、IP网络、云计算平台、外设）和相关软件产品（办公软件、安全浏览器）的技术、产业和生态问题。第二部分为安全篇，主要讨论网络安全（商用密码、边界安全、反恶意代码引擎、高级威胁检测、漏洞管理、安全管控、终端安全、云计算安全、数据安全、工业控制系统安全、安全服务、电子取证）的技术创新和产业发展问题。第三部分为案例篇，展示了部分参与编写单位近三年来取得的创新成果及其应用情况。

从报告采集的数据看，近三年来我国自主创新的网信技术和产业取得了快速发展，但在核心关键技术方面还没有取得阶段性突破。受益于政策因素，自主创新的网信产品在一定范围内获得了应用，客观上促进了产品性能和易用性的提升，但与国外同类产品相比仍存在不同程度的差距。随着有关工作的扎实推进，供应链被卡脖子的问题有所缓解，但仍不容乐观，基于开源软件的产品，是否面临断供风险，这需要引起高度关注并做深入研究。

现将报告中涉及的23个领域，及其反映出的现状、问题和建议概括如下，以便读者查阅：

1、以CPU为代表的国产芯片在架构、性能、生态等方面不断取得新的进展。龙芯发布了LoongArch自主指令集架构，最新发布的3A5000芯片单核性能提升50%以上；申威、飞腾等CPU产品的性能也有大幅提高。在生态建设方面，国产CPU形成了至少2000家以上的自主生态体系，业务应用软件配套正在逐步补齐。当前面临的主要问题，除生产测试环节的“老问题”外，解决由于指令集结构不同而导致的适配迁移成本高和难度大的问题值得重点关注。需要研究如何建立统一应用编程框架，统一规范API接口，做好编程框架的演进规范，实现跨指令集结构的兼容。

2、国内专业从事固件产品研发生产的厂商相对于其他领域显得十分集中。目前，国产固件产品具备了全面支撑国产计算机产业的能力，并在以党政办公为代表的重点行业获得了广泛应用。下一步关注的重点是加强产业链协同，促进技术成果转化和产业资源的有效利用。

3、国产操作系统在内核、服务和应用等各技术层面都取得了显著成果，操作系统产业向专业化和精细化方向发展，相关产品也在重点行业得到广泛应用，生态建设接近临界规模。需要引起重视的是，国产操作系统（桌面、服务器、嵌入式、移动端）均源于开源 Linux 操作系统，尽管国内厂商在开源社区的贡献度不断提高，但不完全掌控核心技术的的困境仍然存在。从产业的角度看，解决现实需求和突破核心技术，需要两手抓，并且两手都要硬。

4、国产数据库在集中式数据库和分布式数据库两方面都取得了较大的技术进展，同时在政务、互联网、金融等领域得到了大规模的应用。未来一段时间，对于已经部署国产数据库的领域，需要解决易维护性、易开发性、系统稳定性等问题；对于正在部署和未部署国产数据库的领域，需要针对具体应用场景尽快形成解决方案，满足用户差异化需求。

5、国内主流中间件厂商已经完成了较为充分的技术积累，核心技术基本自主可控，具备在极端情况下应对开源风险的能力。相关产品的技术和产业生态发展态势良好，应用范围也日益扩大。未来需要重点关注的问题，一是深入了解行业的应用需求，积极打造安全可信中间件；二是加强开源生态建设，提升话语权；三是倡导构建国产中间件供应链管理体系，同时注重人才队伍建设。

6、办公软件章节主要讨论了文档处理软件、安全邮件和图像处理软件。在上述领域，部分产品已经逐步跨越了从“可用”到“好用”的门槛，但在稳定性、复杂文档的兼容效果上与国外产品相比还存在一定差距。近年来，办公软件厂商在协同办公、安全可信等方面的能力持续提升，在重点行业领域的应用规模显著增长。未来一段时间，国内办公软件厂商需要在技术创新的同时做好市场创新，提升用户对相关产品的认知度和忠诚度。

7、国产整机在核心部件和元器件的国产化率方面不断取得突破，在功能、性能、易用性和安全性等方面有了较大程度的进步，在重点行业领域应用的深度和广度不断提升。同时，国产整机存在性能低、成本高、利润少的现实情况。相关厂商也面临着技术路线分散、适配工作量巨大的困难。针对这些问题，报告提出加强研发生产能力、成立联合攻关中心、加大人才培养力度等建议。

8、国内网络设备厂商推出了基于国产基础软硬件的产品和解决方案，核心元器件的国产化率达到了较高的水平。在产品方面，性能指标基本与采用非自主核心元器件的产品达到了同一水平；在解决方案方面，基本具备了满足行业应用需求的能力。

9、国内云计算在部分核心技术上已经达到国际领先水平。近年来，云计算平台厂商开始关注基于国产化架构的技术研发工作，集中对国产化底层基础设施进行了攻关适配，在优化性能、解决兼容性问题方面取得了一定的进展。关于后续发展，报告提出要加强自主可控的核心技术研发和适配，同时也提到了建设开源云计算社区。

10、安全浏览器在产品的安全性和易用性方面取得一定的进展，并得到了更大范围的应用，但仍面临着核心技术依赖开源软件的现实问题。报告提出浏览器厂商需要加大核心技术的研究与投入，打造国产浏览器的开源社区，并提出了将浏览器产品逐步切换到自主内核的目标。

11、本报告涉及的外设产品包括打印机、复印机、扫描仪、一体机、高拍仪等。相关厂商解决了多种底层技术路线兼容适配问题，自主产品与Windows操作系统兼容问题，以及非国产芯片外设产品的安全可控问题，产品的功能和性能不断提升，在重点行业领域的应用规模逐年扩大。未来产业界需要着力解决技术协同和产品适配问题，提高产品稳定性，打造高性能、全覆盖的产品系列。

12、密码和业务应用融合的趋势已基本形成，业务系统密码改造在各行业初步展开。虽然在一段时期内“密码要用”与“业务可用”的供需矛盾还将存在，但这既是商用密码获得更大发展必须要直面解决的问题，也不失为激发产业动能的另一个契机。报告提出，商用密码厂商在未来一个时间需要加强与传统安全产业和新兴技术的融合。

13、网络边界的概念随着云计算、人工智能、威胁情报技术的发展，已经逐渐被破除，并朝着服务化、应用化的方向发展，被动边界安全防御机制逐渐失效。国内安全厂商应势而动，构建了云网端协同的主动安全防御体系，拓展了边界安全能力和应用范畴。相关产品和解决方案已经在众多行业领域得到应用推广。未来，边界安全产品将向着高性价比和绿色节能方向发展。

14、自主创新的反恶意代码核心技术总体不落后，并在一定范围内很好地起到了为产业赋能的作用。近年来，反恶意代码领域在理论、技术和工程方面持续完善，新一代安全防御能力框架、向量级情报运营和智能未知威胁检测技术、后端支撑工程体系、移动反恶意代码引擎等一系列成果面世。

15、国内厂商在高级威胁检测方面的手段日趋丰富和成熟，并在越来越多的场景下发挥了重要作用，但仍面临能力投入相对离散、协同能力不足等问题。报告提出，今后应加强跨界融合，提升检测防护能力。

16、面对传统的漏洞扫描工具不能实现真正意义上的漏洞修复和管理的现状，漏洞管理产品正在从单一的漏洞评估工具向更全面、更有安全价值的方向演进。目前国内厂商在漏洞基建运营、智能漏洞检测管理、人工智能和自动化编排、DevSecOps 等方面有所进展并有相当范围的应用。后续漏洞管理将向着云地协同的方向发展。

17、安全管控在网络安全领域是一个相对较新的方向。尽管专业从事安全管控的厂商不多，但业界在近几年在安全业务、系统性安全风险、全局性安全管控等方面也取得了较为全面的创新成果。未来，这一领域需要从技术创新、体系框架、自身安全和人才培养等几个方向发力。

18、国产化终端安全产品和技术成熟度尚无法与国外厂商相比肩，但已逐渐步入成熟阶段并从被动防御转向为主动、自适应的防护。报告提出，今后终端安全需要将风险可视化作为重点，将业务和安全结合，探索构建上层管理接口和底层技术接口的统一，通过融合创新促进可持续发展。

19、国内云计算安全厂商配合云计算业务，基本上完成了传统安全产品和技术向云的演进，并在不同行业和不同业务场景下得到广泛应用。云工作负载安全、云原生安全、云数据安全将成为国内未来几年云安全领域的主流发展方向。

20、数据安全技术和产品在大形势推动下蓬勃发展，新技术与传统数据安全技术相融合，相关产品和服务在各领域的应用程度逐渐提升。相对于标准法规的日趋完善，数据安全的技术标准、评估手段还有所欠缺。报告提出，未来数据安全的发展方向是与业务场景紧耦合。

21、国内工控安全厂商普遍提高了对国产基础软硬件适配的重视程度，大量基于自主核心元器件的产品面市。同时，可信计算开始与工控安全场景结合，在部分行业领域发挥了重要作用。报告提出，未来一段时间，工控安全厂商需要着力做大做强，通过龙头企业形成辐射带动作用；同时工控安全的第三方检测技术、标准、工具需要尽快加强，以规范市场的发展。

22、国内的安全服务还处于探索阶段。特别是针对自主创新的网信产品以及基于这些产品构建的信息系统，目前的安全服务能力还远远不够。关于加强安全服务能力建设，报告提出一方面要关注针对自主产品的服务，另一方面要加强人才队伍建设。

23、电子数据取证产品快速发展，并在实际工作场景中发挥了重要作用。该领域未来的发展方向主要在于：一是对国产化操作系统、数据库、办公软件、浏览器等进行电子数据取证，形成国产化取证体系；二是运用人工智能和大数据技术，快速发现案件中的关键线索，组建可视化分析网络，形成平台化的应用支撑。

通过对上述23个领域进行对比分析，发现存在以下几个共性问题：一是专项技术不断取得突破，但核心技术仍然没有完全摆脱受制于人的局面；二是产品性能快速提升，已经有部分产品实现了“好用”的目标，但多数自主产品的性价比尚低于国外产品；三是产业生态日趋完善，但是和实际需要相比还远远不够；四是跨界融合成为产业发展的热点，但达到“1+1>2”的效果距离还很大；五是多个领域开始关注安全与业务的紧耦合问题，但缺少现实可行的具体工作路径；六是越是产业链下游，面临的适配压力越大，如何解决这一问题需要加大推动力度；七是人才短缺仍然是各领域普遍面临的问题。

基础篇 »

1、芯片

2、固件

3、操作系统

4、数据库

5、中间件

6、办公软件

7、整机

8、IP 网络

9、云计算平台

10、安全浏览器

11、外设

1 芯片

近年来，以通用处理器为代表的国产芯片产品谱系越来越完整，生态越来越完善。龙芯推出了自主指令集 LoongArch，申威自主处理器架构和 SW64 指令集不断迭代发展，飞腾等厂商获得了指令集的永久授权。国产通用处理器芯片对海外指令集的依赖程度逐渐降低，性能越来越接近国际主流水平。与此同时，不可忽视的是随着美国最新打压措施的实施，华为的麒麟高端芯片已经面临流片被阻断的问题。因此，在芯片领域（特别是高端芯片的生产，而不是设计），我们被卡脖子的情况仍然严峻。

1.1 国产芯片在架构、性能、生态等方面取得全面进展

1.1.1 芯片性能和安全性不断提升

（1）通用处理器芯片

龙芯先后发布了基于 LoongArch 自主指令集架构（龙芯架构）的 3A5000/3C5000L 芯片。3A5000 芯片采用 12/14nm 工艺节点，4 核，主频 2.5GHz，相对于上一代 3A4000 芯片，单核性能提升 50% 以上，功耗下降 30% 以上。3C5000L 芯片是龙芯中科新一代高性能服务器处理器，采用 12/14nm 工艺节点，16 核，主频 2.2GHz，相比上一代 3B4000 服务器处理器性能提升 7-8 倍，性能达到国际主流服务器处理器水平。龙芯 3A5000/3C5000L 芯片内置国密算法和可信模块，加解密性能可达到 5Gbps 以上。

申威自主处理器架构和 SW64 指令集经过不断技术迭代，CPU 单核性能提升 2.6 倍，多核性能提升 40 倍。2020 年发布自主研发的 32 核 Core3B 核心申威威鑫 3231 服务器处理器，主频 2.0-2.5GHz，支持 DDR4-3200，IO 聚合带宽达到 160GB/s，支持 2/4 路互连。2021 年申威发布自主研发的 8 核 Core3B 核心申威威焱 831 桌面及嵌入式处理器，内置 1 个异构主动安全管

控模块，实现计算和安全管理分离，最高主频 3.0GHz。2021 年申威完成新一代处理器核心 Core4 研制，从指令架构上增加对国密等算法的指令支持，微结构上增加了内生安全的设计。

飞腾于 2019 年推出 FT-2000/4，集成 4 个飞腾自研 FTC663 处理器核，主频 2.6GHz，典型功耗 10W；2020 年推出飞腾腾锐 D2000，集成 8 个飞腾自研 FTC663 处理器核，采用境内先进工艺，相比 FT-2000/4 的性能进一步提升 70%。在高性能服务器 CPU 领域，飞腾于 2018 年推出 FT-2000+/64，集成 64 个自研 FTC662 处理器核，是国际上首款 64 核 ARM 架构通用服务器 CPU；2020 年推出飞腾腾云 S2500，集成 64 个自研 FTC663 处理器核，支持 2-8 路处理器直连。2019 年，飞腾首次推出自主处理器安全平台架构规范 PSPA1.0，目前已在 FT-2000/4、D2000、S5000 等桌面和服务器 CPU 中支持，实现 CPU 内生安全。

（2）其他芯片

在网络控制器芯片方面，网迅发布的万兆和千兆以太网控制器芯片，基本可以满足 X86 平台和国产化通用平台下 PC 和服务器硬件平台需求，其中单、双、四接口和宽温环境产品已在商业、工业、专用等领域应用推广；定制的专用网络控制器芯片，可以支持硬件国密算法，网络底层硬件上实现灵活配置和卸载各层网络安全协议。沐创自主研发了双口 40G 智能安全网络芯片；高性能安全芯片的单片方案可以满足 25G 网络的数据加解密需求，多芯片方案可以满足 100G 网络带宽的数据加解密需求。

国产 SSD 主控芯片在近几年的研发过程中取得了高速的发展。在性能上，国科微从传统的 SATA 接口，转换到新的 PCIe Gen3 甚至 PCIe Gen4 接口，带宽性能得到了 10 倍的提升，达到 6GB/s 的带宽性能，同时 IOPS 性能达到 1M IOPS 的等级。在安全性方面，国产 SSD 主控芯片支持了国密 SM2/SM3/SM4 的加密算法，搭建了国产 SSD 的安全体系。

1.1.2 芯片技术不断创新实现突破

（1）通用处理器

龙芯发布了 LoongArch 自主指令集架构（龙芯架构）。近 2000 条指令（包括基础架构部分和向量指令、虚拟化、二进制翻译等扩展部分），吸纳了现代处理器架构中各种先进指令技术优势，运行效率更高，功耗更低。龙芯架构支持通过二进制翻译等技术实现高效率的 X86、ARM、MIPS 指令集到 LoongArch 指令的翻译，实现跨指令平台应用系统兼容，降低其他架构向 LoongArch 架构的迁移成本，快速的完善的自主指令集架构生态。

申威处理器始终坚持从指令集源头创新的自主可控路线，不断完善和提升“申威 64”自主指令集架构。在通用 CPU 芯片的微结构上突破了同时多线程技术，突破了多路直连技术，单 DIE 实现了 64 核架构，支持 4 路直连；安全核心和计算核心管用分离的双平面架构，奠定了芯片级安全架构的基础。在领域通用类芯片上实现了单 DIE 集成 390 核心的众核架构创新。在配套芯片上，实现了 PCIe Switch、GPU、VPU、南桥功能的高度集成，提供了采用 2 颗核心芯片形成主板的高国产化率解决方案。

飞腾在设计上优化了高效乱序多发射超标量处理器设计技术以及多核片上并行体系架构，支持最高 512 核规模的 cache 一致性维护；实现了 CPU 内生硬件安全防护技术，从底层支持可信计算 3.0，并支持多项 CPU 级 RAS 特性；推出自主 CPU 加自主套片的洞庭平台提高整机效率和可靠性、降低成本；采用面向性能、功耗与面积均衡的多目标综合优化物理设计技术，以及深度定制优化、多模式融合、分区收敛等技术提升主频、保障质量。

（2）其他芯片

在以太网网络控制器芯片整体架构的高速通道设计、低延时设计、国

产化兼容及安全性设计上，网迅突破了传统高速数据通路的设计架构，实现了一种超多 DMA 队列的方法，设计了分层 DMA 队列架构，节约传统资源的 50% 以上；设计了支持叠加网络层协议的可编程流表结构，实现了 ACL 和路由表的动态加载，以及物理网络拓扑的动态配置；发明了报文分片传输方法，突破了报文并发条件下的关键加速等技术；片内设计硬件国密算法 SM2/SM3/SM4 引擎，实现了网络控制器配置的不透明安全传输模式，并支持片内硬件密钥产生，在网络硬件底层实现了安全和认证等机制。

在后量子密码芯片的研究上，沐创针对 NIST 即将标准化的后量子密码算法，有针对性的提出了混合计算阵列架构、基 2 和基 4NTT 乘法架构等，研发完成了全球首款支持基于不同数学问题算法的后量子芯片。其中，针对后量子密码签名算法 Dilithium 提出的高效紧凑的硬件架构，是全球首个同时支持三个安全等级密钥生成、签名、验签的算法硬件架构。

国产 SSD 主控使用 LDPC (Low-density Parity-check，低密度奇偶校验）技术愈发成熟，国科微能够以更少的纠错码实现更多的纠错 BIT 数。SSD 主控芯片的 LDPC 算法引擎纠错能力越来越强，纠错的性能稳步提高，同时纠错所消耗的功耗也在逐步降低，相关技术水平逐步接近国际领先水平。

算石科技基于国家标准研发了 TPCM 芯片，完全支持国内可信计算 3.0 双体系结构，以计算机的三个启动运行阶段（待机、启动、运行）为依据，配合三类物理接口通路设计，为计算机建立起可信运行环境，并对可信环境进行主动动态监控，实现对计算机全生命周期的可信度量和控制。

1.2 国产芯片在重点行业领域应用落地

近三年，国内芯片技术高速发展，性能已接近国际先进水平，实现“自主研发”和“安全可信”的深度融合。基于自研芯片的服务器、桌面电脑、嵌入式设备、交换路由网络设备、存储设备已经在重要领域完成百万套量级

的批量应用，形成了至少 2000 家以上的自主生态体系，业务应用软件配套正在逐步补齐。

国产 CPU 芯片在党政、金融、能源、电信、交通、教育等关键行业都有应用落地，芯片的性能可以满足办公、行业自助终端、基础的办公业务系统的要求。在党政办公领域，国产 CPU 芯片已覆盖全国各省市及上百个部委，芯片出货量达到数百万颗，满足党政办公场景的基本需求；在金融行业，基于国产 CPU 的桌面电脑、专用机、金融机具、服务器等多个类别产品，已经部署服务银行、证券、保险领域多家金融机构，贵阳银行等金融机构核心业务系统也已经开始在国产 CPU 平台上部署应用；在电信领域，国产 CPU 已经在营业厅办公电脑、办公系统、5G 小站、5G 核心网方向与三大运营商及伙伴展开合作，浙江温州、金华和湖州等地完成了基于自主基础软硬件的电信营业厅落地，国产 CPU 中标运营商集采项目；在交通行业，基于国产 CPU 平台的信号控制系统、交通行业工控机、智能城市检测系统、高速公司 ETC 等系列产品，已应用于车联网、交通信息化等领域；在能源行业，基于国产 CPU 平台的数据采集、控制系统、网关单元等实现了控制系统的国产化替代，集中监控和智慧电厂项目也开展国产化应用；在医疗行业，基于国产 CPU 的自助医疗设备已经在北京、湖南和山西省等多地医院上线使用。

国产网络控制器芯片和国产 SSD 主控芯片也已经在国家党政、金融、海关、能源、轨道交通、保密等关键行业的办公设备和业务平台上得到了应用和推广。

1.3 跨指令集结构的兼容和人才培养是可持续发展的关键

国产通用处理器由于指令集结构不同，增加了行业软硬件产品的适配迁移成本和难度。因此，建立统一应用编程框架，统一规范 API 接口，做好编程框架的演进规范，同时从系统层面整合优化应用软件、中间件、数据库、

基础库，做实做强性能测试和兼容性测试，有利于进一步完善生态，实现跨指令集结构的兼容。

国内芯片行业从事芯片生态建设的人员数量、研发投入不足，极大制约了生态可持续发展。国产芯片生态尚不完善，人才数量不足，人才培养与实际需求结合不紧密，难以填补行业市场不断发展的人才缺口。国产芯片、国产基础软硬件教材不足，国内高校开展的相应课程不多，基于国产平台做实验的条件不足，限制了基础技术、核心技术的人才培养。

本章主笔人员（按拼音排序）：

龙芯中科技术股份有限公司 郭同彬、柳军

本章贡献人员（按拼音排序）：

北京网迅科技有限公司 耿涛、胡金山、钱利国

飞腾信息技术有限公司 屠故园

国科微电子股份有限公司 游毓

上海算石科技有限公司 黄坚会

太极计算机股份有限公司 张洪明

无锡沐创集成电路设计有限公司 王孟元

中电科申泰信息科技有限公司 韩磊

中航鸿电（北京）信息科技有限公司 严华锦

2 固件

国产固件目前主要包括两类产品：一是国产 BIOS（基本输入输出系统，Basic Input Output System），二是国产 BMC（基板管理控制器，Baseboard Management Controller）。面对产业链上游技术路线分散、兼容适配难度较大的现状，国产固件厂商开展了尽可能广泛的适配，目前已基本具备了支撑产业链上下游协调联动的条件。

2.1 国产固件具备全面支撑国产计算机产业的能力

我国的主流国产通用处理器包括4种架构、6种主流品牌，技术路线分散，上下游厂商的兼容适配难度较大。国产固件系列产品已经在龙芯、申威、飞腾、鲲鹏、海光、兆芯等主流国产处理器平台以及麒麟、统信、普华等国产操作系统中进行了应用。国产 BIOS 屏蔽了六种处理器平台的硬件细节，提供统一的操作系统引导路径，起到了承上启下的关键作用。另外，国产固件厂商已研制了全国产的 BMC 固件产品，并在党政军多个项目的服务器中进行了使用，改变了 2017 年以前国内 BMC 多使用台湾地区信骅公司的 AST 系列产品的被动局面。

在产品化的同时，国内中电科技等固件厂商联合华为等整机厂商开展了固件的标准化工作。在全国信息安全标准化技术委员会推动和支持下，相关厂商共同制定了《计算机基本输入输出系统（BIOS）技术要求》、《服务器基板管理控制器（BMC）技术要求》和《计算机基本输入输出系统（BIOS）技术要求》等固件标准规范，体现服务器 BIOS 发展方向，导入先进的技术理念，并兼容国际标准。上述标准健全了国产计算机标准体系，为计算机固件的创新发展指明了方向。

固件除了能提供对底层硬件的初始化和操作系统引导外，还能够提供底

层硬件管控能力。通过对固件安全能力进行封装，可以配合可信计算等安全理论体系，构建上层安全支撑接口，实现对终端的多维度管控。目前，中电科技正在进行相关产品研发，并已在某些领域进行试用。

2.2 国产固件已在重要领域推广并不断扩大应用范围

国产固件产品是网信自主创新产业的的重要节点，已在党政军等重要领域国产计算机上得到广泛应用，并在电子、金融、教育、通信、能源、交通等重点行业中大量使用，累计出货量超过百万台 / 套，年产值近亿元。

昆仑固件可适配所有国产自主处理器平台，支持 50 余家主流计算机整机生产商和主板厂商，研发了自动化的固件级自动测试系统，并已在实际项目中使用。昆仑 BMC 开创性地引入了可信计算体系，能够完成可信度量、身份认证、三权分立等安全可信功能，还研发了采用国产自主芯片的 BMC 硬件板卡，并支持基于国产自主处理器的服务器设备。在自主创新的网信产业链上，已适配的主板硬件款型已达到百余款。昆仑固件正在打造适用于主流处理器平台和配套操作系统的统一集成开发环境，实现多厂商、多机种、多版型集中并行开发、适配和验证，实现问题共享、经验分享和技术复用，解决重复适配、厂商协调困难等问题。目前，昆仑固件在国产化领域市场占有率在 85% 以上，占据绝对领先地位。

2.3 国产固件将进一步融合计算机产业链

面向国产计算机大规模应用的趋势，国产固件需要进一步聚合产业力量，重点推进三方面的工作：一是要持续加强关键技术研究，形成核心竞争力，引领产业创新与发展；二是要全方位凝聚各界力量，持续壮大固件产业生态建设；三是搭建固件产业信息共享与技术交流平台，积极与相关技术组织开展合作，进一步结合上下游优质企业的产业发展和用户需求，促进交流与协

同，推动固件技术成果的共享、共用，进而推进产业资源的有效利用。

在具体的技术层面，国产固件将继续适配国产新型处理器平台和配套操作系统：国产 BIOS 将围绕产业的自主可控需求，打造核心产品体系，扩展可信计算、安全审计等安全功能模块，统一固件层硬件平台和操作系统的安全接入和管理接口，形成固件安全系列标准规范；国产 BMC 将基于国产新型芯片，设计和实现服务器 BMC 远程管理全国产解决方案，扩展国产 BMC 固件适配范围，在支持市场主流 AST 系列芯片的基础上，实现支持采用国产自主芯片的 BMC 硬件板卡，并支持全系列国产自主处理器服务器设备，以支持需要全国产化的高安全应用场景。

本章主笔人员（按拼音排序）：

中电科技（北京）股份有限公司 陈小春、孙亮

3 操作系统

近几年，国内操作系统产业迎来历史最好的发展机遇，已在技术与产品、市场环境、开发者社区、产业链上下游等生态建设方面取得了长足的进步。银河麒麟和统信在终端和服务器操作系统领域的市场份额稳步增长。根据公开的资料[1]，鸿蒙操作系统自发布以来，用户数已超过 2.2 亿，据称 2022 年上半年将发布鸿蒙 3.0 版本。然而不可否认的是，绝大多数国产操作系统的内核仍基于开源项目，由此导致的供应链风险仍然存在（尽管此类风险弱于显性的“断供”风险）。同时许多领域与国际先进水平还存在较大差距，因此，正视问题、迎头赶上，是操作系统产业未来几年的主要课题。

3.1 操作系统创新发展驶入快车道

3.1.1 核心技术兼容开源路线

国内主流的桌面和服务器计算机操作系统均源于开源 Linux 操作系统，在嵌入式和移动终端领域，国内厂商的技术路线也与开源操作系统有着很深的联系。近年来，操作系统企业在核心技术上不断加大研发力度，在操作系统内核、服务和应用各技术层面都取得了显著成果。

内核方面，CPU 中断驱动和硬件交互子系统是国内已重点突破的技术，在国产 CPU 和国际主流 CPU 平台上，实现了同源支持，内核用户交互上，提供统一的操作界面和用户体验；在开发接口上，提供统一的标准规范和开发接口，减少适配和应用开发的工作量，从而加快了国产操作系统应用生态的建设进程。服务层是内核和应用交互的桥梁，国内在图形开发与显示、管理配置、运行时兼容、备份还原等服务层技术上已重点突破。目前国产操作

[1] https://baijiahao.baidu.com/s?id=1718440140572345412&wfr=spider&for=pc

系统的桌面环境，已经移植到主流 Linux 发行版本中。应用软件，包括软件中心、更新管理器、软件助手、显示切换、输入法、截图软件、影音软件、通讯软件、国产办公软件、刻录软件等大量涌现，极大的丰富了国产操作系统的使用场景。

3.1.2 产品向专业化和精细化方向发展

在桌面和服务器操作系统方面，主流的国产操作系统全面支持飞腾、鲲鹏、龙芯、海思麒麟、瑞芯微等主流国产 CPU 和国外 CPU 平台。部分操作系统产品面向关键行业全面支持物理、云或超融合环境上构建生产环境，通过连接传统和新基础设施简化 IT 环境；另有部分产品通过云服务安全引擎对 KVM 和容器服务进行保护，同时通过内置的 AI 数据卫士使得操作系统对绝大多数勒索病毒具有免疫能力。在嵌入式操作系统方面，相关厂商围绕产业方向进行了处理器的多样化支持和应用系统适配工作。

3.1.3 国内厂商在开源社区的贡献度不断提高

2020 年，中国在 GitHub 的贡献者数量增长迅速，目前仅次于美国，数量位居第二，占据 GitHub 活跃贡献者中的 14%[2]。其中，华为对 Linux 5.10 的贡献超过国际厂商排名第一；麒麟软件在 OpenStack 社区开源云基础设施软件的第 24 个版本（开发代号 Xena）中贡献排名全球第三；统信软件在操作系统核心组件如 kernel、gcc、binutils、glibc、cmake、elfutils、libtool、clang、boost、gdb 等领域累计适配集成补丁超过 5000 个，自研开发并反馈上游社区补丁超过 500 个，并在 Qt 贡献排名全球第五。

[2] GitHub 2020 年调研报告

3.1.4 生态建设接近临界规模

操作系统产业的核心在于生态建设，而生态系统建设的核心在于尽快突破“临界规模”。一旦突破“临界点”，用户会因为开发商的丰富度而加入，开发商也因为用户数量级而投入开发，从而形成一个良性循环。近三年来，通用操作系统实现了认证测试过程的标准化和信息化管理。主流厂商的生态合作伙伴数量已超过数千家，适配软硬件数量已达到十万量级。截止 2021 年底，国产操作系统的装机量累计已达到千万量级。为解决应用软件不足的问题，通用操作系统厂商基于 Android 和 Windows 平台的兼容技术将常用软件迁移到国产操作系统，并支持多种体系架构，实现了多端生态融合应用。另外，在全力推进通用软硬件产品适配的同时，操作系统厂商针对重要行业研发安全创新的行业共性开发框架、应用中间件，研究制订行业递进式关键部件、整机、系统平台、应用等方案，积极推进行业应用迁移适配。

3.2 国产操作系统在重点行业得到广泛应用

目前，国产桌面和服务器操作系统在重要行业中逐渐被认可。移动智能操作系统大量应用在政务、公安、司法、金融、电力、水利等重点领域，嵌入式操作系统在细分领域逐步扩大市场份额，改变了原有开源系统、国外操作系统一统天下的局面。

目前，国产操作系统在党政办公系统应用套数达到千万级，覆盖全国各省市自治区，从性能、稳定性、安全性、易用性等方面已经可以满足党政办公的需求，在大规模推广应用中基本通过了考验。针对办公领域用户非常关注的性能、兼容性、生态等主要问题，主流的国产桌面操作系统都提供了企业级应用商店，实现应用分发、补丁推送、外设驱动更新等实用功能，并在云打印方案等方面积极解决应用环境国产化改造的难点，为用户业务平台提供有力的后台保障。

国产操作系统作为信息系统安全底座，在金融行业正在从边缘应用向核心应用迁移。国产操作系统在银行业的应用从非核心业务系统开始，在安全稳定性得到确认后不断深入。目前，网银的前置系统、资金清算系统、手机银行等准核心业务系统已经采用国产操作系统。大型国有银行、股份制银行、大型商行、城商行、银保监会、保险公司均在外设适配、应用迁移、压力测试等环节验证了国产系统的安全性和可靠性。

在电信行业自主创新工作中，联通实验室与麒麟软件完成了十三款应用软件的迁移适配工作，多个业务平台迁移至银河麒麟服务器操作系统。某电信运营商完成了多个业务系统基于统信服务器操作系统的迁移。

国产操作系统已逐步在电力等能源行业取得应用。“华电睿蓝”DCS（基于银河麒麟）在国内超超临界火电机组上的首次实现示范应用和全厂一体化控制。某中央直管国有能源企业基于统信完成了 Windows 及 CentOS 替换项目。国家电网调度系统省 / 市调度中心机房部署了麒麟信安操作系统。国家电网、南方电网及多家发电企业的电力监控系统部署了南瑞瑞盾安全操作系统，在专用安全防护装备及调度数据网实现了规模化应用。

3.3 国产操作系统创新发展要两条腿走路

我国操作系统产业与发达国家的差距，始终在于不完全掌控核心技术。解决这一核心问题，不但需要科研和产业界的持续投入，也需要应用的支撑和牵引。因此，未来一个时期操作系统企业应在解决重点行业现实需求和解决核心技术尽快突破两个维度共同发力，两手抓、两手都要硬。短期内争取突破部分关键核心技术，基本形成国产操作系统技术标准与生态体系，在金融、电力、能源等关乎民生的重点行业应用普及率大幅提高；争取未来几年在绝大部分核心技术取得突破，完全形成自主的操作系统及其标准体系，实现封闭市场的全覆盖，在开放市场具备一定竞争力。

3.3.1 建立自主社区版操作系统

借鉴国际成功开源社区模式，在国外内核的基础上，研制自主的社区版操作系统。国内操作系统厂商基于社区版做发行版，可有效促进操作系统统一，减少操作系统厂商在包选取验证、漏洞检测、补丁研制等方面的投入，以及下游基础软件、应用软件、外设等厂商的适配工作，有效解决技术分裂问题，缓解国内操作系统企业“分散而不强”的局面。社区版操作系统从开源规范、流程工具、组织结构和治理模式、标准接口方面统筹发展，打造版权清晰、兼容开放、技术领先且被广泛使用的开源社区，避免上游发行版停服事件、断供风险。

目前欧拉（openEuler）、龙蜥（OpenAnolis）、优麒麟（Ubuntu Kylin）、深度（deepin），是中国最活跃的操作系统代表性社区。目前，已有多家企业及机构等基于 openEuler 社区版操作系统研制、发布了商业发行版，并在金融、能源、医疗、自然科学研究等领域实现应用。社区集合了中国最优秀的操作系统技术成果。初步探索出了“贡献 - 获取 - 积累 - 盈利，再到贡献”的可持续的商业模式。鉴于这些初步成功的案例，有理由持续探索，将活跃并具有代表性的社区，明确作为中国操作系统的上游社区。

3.3.2 产学研联合提高技术更新迭代能力

在高校方面，落实相关课题、课件、相关教师资源、实验环境和开发环境等，开设相关专业课程，引导在校学生学习操作系统相关知识。此外，在学习国际相关先进技术的同时，还要加大高校与产业界的对接，创新国内操作系统相关技术，鼓励更多年轻人投身于国产化事业。在产业方面，鼓励企业与科研院所的合作，成立联合实验室、促进技术迭代创新，加速关键领域核心技术突破，以及相关的成果转化，推动企业及行业的整体发展。

3.3.3 面向行业需求加速技术攻关

调动国内用户对国产操作系统的积极性是国产操作系统普及应用的关键。借鉴党政办公和金融领域国产操作系统应用推广的成功经验，面向重点行业，在操作系统内核、基础运行库、基础工具、安全技术，以及开源社区基础运营环境等方面加大研发力度；避免在核心代码、托管平台和开源许可协议等层面发生断供或法律纠纷风险；针对产业不同时期的重点需求开展定向攻关工作。通过 5 到 10 年的系统性规划补齐短板，达到核心技术、运营环境等自主自立，实现操作系统核心领域完全自主。

本章主笔人员（按拼音排序）：

麒麟软件有限公司 崔文喆、李震宁、王亚萍

本章贡献人员（按拼音排序）：

北京东土科技股份有限公司 周爱平

北京机智科技有限公司 杜占源

北京凯思昊鹏软件工程技术有限公司 陈鹏、李云翔

长扬科技 (北京) 有限公司 徐宁

湖南麒麟信安科技股份有限公司 陈松政

科东（广州）软件科技有限公司 邱学强

南京南瑞信息通信科技有限公司 刘苇、祁龙云、闫珺

统信软件技术有限公司 牛战争、孙建民、熊兰天、于伟、郑阳阳

元心信息科技集团有限公司 黄浩东、欧阳任勇

4 数据库

数据库是除操作系统之外另一个重要的基础软件。国产数据库在集中式数据库和分布式数据库方面都取得了较大的技术进展，在政务、互联网、金融等领域得到了大规模的应用，未来需要针对不同行业的需求尽快形成成熟的解决方案。

4.1 国产数据库突破部分关键技术

4.1.1 集中式数据库

数据库共享存储集群技术是数据库支持网络计算环境的核心技术，具有高可用、高可恢复性、负载均衡等特性，旨在帮助企业加强核心业务系统健硕性，解决多类型、多数量的核心应用服务持续运营问题。该集群技术的突破打破了国外在共享集群技术的垄断，填补了国内在高端数据库领域的空白，已实现支持 8 节点集群规模。

SQL 优化与执行作为数据库的核心技术，负责完成用户数据访问请求的解析、优化和执行。SQL 优化与执行技术的优劣直接决定了数据库的 SQL 执行性能。基于左深树的 SQL 路径探测方法、基于代价的优化器、编译执行的 SQL 执行器等技术和方法，实现了高效复杂 SQL 解析、评估、优化、执行过程。

短期内国产数据库不得不做的一件事是兼容 Oracle 等国外数据库。目前国产数据库普遍实现了 Oracle 数据库到国产数据库的快速迁移。实现的路径主要有两条：一是改造国产数据库的执行引擎，从数据库核心语法层实现对国外数据库语法的兼容，这种方式的优点是通用性好，迁移体验好，但对国产数据库厂商的核心技术掌握能力要求高；二是在数据库内核的外围通过自动化工具进行语法转换，该方法技术难度相对较低，好处是可以避免迁移技

术难题阻塞在数据库厂商，适用性更广，缺点是迁移工作量相对更大，存在一定的迁移改造时间。

4.1.2 分布式数据库

分布式数据库通过计算节点承担访问请求接入、SQL 解析与优化等技术，根据数据库并发压力负载按需增加或减少节点，对已有负载无影响。以 OceanBase 数据库为例，支持超大规模集群（节点超过 1500 台，最大单集群数据量超过 3 PB，单表数量达到万亿行级别）动态扩展，实现了按需扩展功能。

基于改进的多主机 XA 协议、基于分布式环境的多版本并发控制等技术，保证分布式数据库对事务 ACID 规范的支持，满足金融、交易等具有强事务需求的业务模型。

通过引入 Paxos 、Raft 一致性协议，在工业级的分布式一致性协议支撑下，多副本数据的数据一致性和系统可用性之间实现平衡，保证正常业务的 I/O 低延迟体验和数据强一致性。

通过 DBaaS 服务，可构建不同的租户资源来满足业务个性化需求，管理员按需调整租户的资源配置，灵活对租户资源进行扩容和缩容。同时，租户之间资源相互隔离，通过权限控制确保不同租户数据的安全性，各个租户也可以选择不同的兼容类型。

4.2 数据库在政务、互联网、金融等领域大规模应用

到 2022 年底，党政机关将完成基于国产数据库的应用系统改造和建设工作。国产数据库的大范围大规模应用，证明了国产数据库在安全性、可靠性、可用性、以及性能上满足国家的战略需要，满足党政机关基于国产数据库的

信息化系统的建设需求。

国产数据库在国防军工单位完成了大规模部署和应用，支撑了国防信息化建设，并支撑了多项重大工程，证明了国产数据库在安全可靠方面达到了先进水平。

国产数据库突破了分布式存储计算等关键技术，为电子商务以及新零售等基于互联网的业务提供了有力的支撑，解决了对海量数据的快速检索和分析等问题，为互联网经济提供了优秀的解决方案。

越来越多的线上金融系统开始使用国产数据库。典型的案例包括：中国银行运维监控系统、工商银行对公理财系统、建设银行粤龙云系统、光大银行理财公司新一代财富管理平台、北京银行网联支付清算平台和银联无卡快捷支付系统、南京银行互联网金融平台、网商银行金融交易系统、浙商银行电信反欺诈和外汇交易以及管理驾驶舱业务、浙商证券互联网用户中心、招商证券历史收益系统、中国人民健康保险股份有限公司互联网保险、中国人寿 CMDS、中国人寿企业年金、梅州客商银行核心系统等。

4.3 国产数据库针对行业需求不断深化技术创新

4.3.1 对于已全面应用国产数据库的行业

对于党政、国防军工等已经开展了数据库国产化的行业领域，国产数据库已经满足了数据库的安全性、可靠性、可用性、实时性等关键需求。今后几年，产业界要结合行业应用，解决数据库的易维护性、易开发性问题，全国产化环境下的系统稳定性，专业领域的定制需求等。一是自适应数据库配置、诊断、修复。通过选择性地运行样例脚本库，采集、分析、处理信息，数据库依据配置模板和内置的故障库，自动生成配置方案或诊断结果，并对方案或诊断结果进行试运行评估，评估完成后进行自动反馈和修复。

二是支持新技术框架及接口，如 Node.JS、Python、GoLang、SpringBoot、Mybatis、Hibernate、Apache Shiro、Disruptor 、ehcache、Jquery、BootStrap 等。三是持续开展兼容适配，在国产数据库之间向上屏蔽差异，减少移植适配成本，在纵向层面实现跨领域的、深层次的综合优化工作。四是面向专业领域数据库功能和性能的拓展开发，提升国产软硬件生态的支撑能力。

4.3.2 对于正在启动数据库国产化的行业

医疗行业对数据库的要求，除了安全可靠外，还有一些行业特点：一是数据的采集量大，地理分布广；二是数据分析的数据量大且实时性要求高。针对这些特点，数据库将综合使用分布式数据库技术、HTAP、MPP 等解决方案，为医疗行业的应用做好技术支撑。

金融行业对数据库的要求主要体现在：一是强一致性、稳定性；二是高并发、高性能。国产数据库在接下来的几年里将着力解决分布式数据库、数据库集群技术在金融行业应用所面临的问题。例如，共享存储集群技术作为数据库面向中高端应用领域的核心技术，虽然已实现技术突破，但在金融核心业务中仍处于应用初期，需要尽快形成成熟的解决方案。

4.3.3 对于新场景新技术的应用

对于中小客户，未来几年数据库将持续优化系统内部模块级内存使用限制，突破小规格限制，支持在小规格机器上部署并稳定运行。在性能方面，对数据库内核不断优化，针对内存写入平滑性、系统并发执行、系统可用会话池、收发包内存等内存使用方面进行性能增强优化，进一步降低数据库对内存资源消耗，提升数据库对内存资源的利用率；通过数据存储压缩等技术，降低成本和存储空间。在云支持方面，帮助用户实现多节点跨云部署，满足用户差异化的需求。

本章主笔人员（按拼音排序）：

天津神舟通用数据技术有限公司 项钦之

本章贡献人员（按拼音排序）：

阿里云计算有限公司 曲山、于巍

北京奥星贝斯科技有限公司 王枫、王栩

北京柏睿数据技术股份有限公司 车岩磊、谷振宁

北京人大金仓信息技术股份有限公司 白志辉、金学东

瀚高基础软件股份有限公司 谷永舫、马继超

平凯星辰（北京）科技有限公司 兰元

武汉达梦数据库股份有限公司 冯源

5 中间件

中间件产品根据应用领域划分，可大致分为三类：基础类、数据类和云计算类。不同种类中间件所使用的技术不同，涉及的核心技术也不相同。总体上看，国内中间件厂商在产品必要功能方面已经完成了较为充分的技术积累，大部分核心技术已经掌握。

5.1 国内中间件技术和产业发展态势良好

5.1.1 中间件厂商已掌握大部分核心技术

基础类中间件最为成熟。该类产品主要包括应用服务器、消息中间件、交易中间件、企业服务总线、工作流中间件、可管理文件传输中间件、安全和统一认证中间件等，涉及的核心技术包括分布式内存网格、集群通信框架、基于内存的无锁消息队列机制、分布式事务协同调度、服务编排和引擎调度、复杂流程建模及控制管理、运行时自我防护等。东方通消息高速传输平台TongHTP在国产高配置服务器环境中，同步消息吞吐性能超越同类开源产品，取得了自主创新中间件历史性突破。

数据类中间件涉及的主要技术已取得突破。数据类中间件指涉及数据缓存、处理、交换和集成、治理等领域的中间件，相对基础类中间件，更靠近具体业务。该类产品包括数据交换和集成中间件、数据缓存中间件、数据治理中间件、ETL 中间件、数据同步中间件、分布式数据访问中间件等。数据类中间件涉及的核心技术包括高性能数据缓存、集群部署和弹性伸缩、元数据全链分析、动态建模、分布式任务调度等。如分布式任务调度技术，属于国家“2020 年基础支撑软件项目 - 中间件”重要研究内容，解决了集群环境分布式部署情况下，任务调度重复执行的问题。

传统中间件产品正在向云化方向演进。云计算类中间件包括分布式服务

框架、API 网关、服务网格、分布式任务调度中间件、分布式链路跟踪中间件、服务注册发现中间件、配置管理中间件等。该类产品涉及的核心技术包括无侵入接入技术、离群实例摘除技术、高性能网关、高性能可扩展容器网络技术、跨网格多集群技术、调用链路关联技术、雪崩保护、热生效等。东方通应用服务器 TongWeb 目前已实现对微服务化场景的运行支撑，可以无缝衔接 SpringCloud 微服务应用开发；消息高速传输平台 TongHTP 已具备支持微服务架构应用所需的各项能力特性，如高并发接入处理能力、海量消息堆积能力、灵活的弹性扩展能力等。

5.1.2 中间件产业生态体系日趋完善

中间件软件在整个应用系统架构中处于承上启下的位置，与上下游产品的认证测试，特别是与产业链伙伴的合作十分重要。国内中间件厂商积极寻求与相关厂商开展合作，并配合地区和行业做好兼容适配认证工作。

5.2 国产中间件在重点行业广泛应用

根据计世资讯的研究报告[3]，党政、金融、电信是中间件市场中占比最大的三个领域。2018 年和 2019 年连续两年，市场主占有率最高的都是党政领域，金融和电信行业分列二、三位。此外，制造、能源和交通等行业也正在面临新一轮信息化应用和信息基础设施转型升级，对中间件软件的需求在持续增加。

5.2.1 党政领域

纵向上看，以数据为主线的政务信息化项目催生出大量对于中间件产品

[3] 计世资讯《2018-2019 年软件基础设施（中间件）市场发展趋势研究报告》、《2019-2020 年软件基础设施（中间件）市场发展趋势研究报告》

的需求，通过数据类中间件实现重要数据逐级汇集，进而衍生出各种信息产品，辅助开展宏观调控、市场监管、社会管理、公共服务等工作。横向上看，在国产中间件的支撑下，政务数据共享交换平台完成与所辖区域政务部门、基础信息资源库、主题信息资源库及其他社会信息库的对接，形成了横向联动的数据共享交换体系。东方通数据交换平台 TongDXP 广泛应用于 15 个省级数据交换平台、200 多个市级数据交换平台。另外，国产中间件也支撑了中央部委和各级政府构建政务云平台。

5.2.2 金融行业

金融行业是使用国产中间件的先行者。2020 年起，金融主管机构推动两期改造试点，打破了已经固化的中间件供应格局，国产中间件在金融行业的应用越来越广泛。2020 年金融一期试点中，超过 90% 的单位选择了应用服务器中间件 TongWeb，未来国产中间件将持续应用于金融行业的扩点、扩容。此外，随着金融行业互联网化、数字化转型的不断发展，用分布式替代集中式、云架构替代传统 IT 架构是大势所趋。可以预见，云计算类中间件为代表的新需求正在释放。目前，商用云计算类中间件产品还相对较少，部分已经云化的基础中间件产品在金融行业的应用已经取得突破。

5.2.3 电信行业

电信行业是使用国产中间件较早的行业。网络类业务、支撑类业务、管理类业务普遍需要应用服务器中间件提供运行支撑；数据传输业务需消息中间件构筑安全可靠的数据传输通道；多个系统集成需要企业服务总线进行服务集成；数据加工处理类业务需要数据集成交换中间件对数据进行加工处理。近两年各大运营商总体 IT 建设正在逐步转向集中化建设方向，系统架构以实现资源的动态调度、容器化、微服务化、PaaS 中台化和全面云化转型为目

标。运营商正在积极与专业中间件厂商合作，加快解决方案、技术研发、组织机构的融合协同，通过联合创新促进业务和能力的双提升。

5.2.4 其他行业

在制造业，信息系统的优化集成贯穿于产品设计、制造、服务全生命周期。中间件是实现多个应用系统优化集成的关键，如整合系统服务接口，实现系统间互联互通，完成流程再造；整合数据，通过数据驱动实现价值延伸。

能源行业的核心信息系统主要涉及生产营运、经营管理、信息基础设施与运维三大领域。生产营运平台以工业控制系统为核心，国产中间件应用案例较少，大量应用案例主要集中在后面两个领域。

在交通行业，2003 年东方通中间件应用于京沈高速公路联网收费系统，拉开了交通行业全面采用国产中间件序幕。近几年，国产中间件在城市轨道交通领域有大量应用。在全国高速公路联网收费系统中，基于东方通消息中间件 TongLINK/Q 搭建的省份占 80%。

5.3 进一步打开国产中间件市场空间

“十三五”以来，越来越多的网络运营者在数字化转型的背景下意识到软件基础设施的重要性。国产中间件市场保持了较好的发展态势。今后一个时期，核心受制于人的形势将更加严峻，产业侧、监管侧、用户侧需要紧密配合，进一步提升国产中间件产品的替代能力，扩大市场占有率。

5.3.1 加强核心技术掌控能力

技术创新是国内中间件持续发展的动力，相关产品的规模化应用是不断加强技术创新和生态建设的关键。中间件厂商需要充分利用国家政策和资金

支持，紧跟新技术发展，全面对标国外产品，找差距、补短板，开展产学研用联合攻关，加强中间件领域核心基础技术研究，同时深入了解行业的应用需求，积极打造安全可信中间件，促进研究成果落地。

在开展技术创新过程中，中间件厂商要积极拥抱开源、贡献开源、投入开源生态的建设。目前开源中间件软件主要来源于国外各大开源基金会和相关社区，如 Apache 基金会、Linux 基金会、云原生计算 (CNCF) 基金会等。国内中间件产品应充分借鉴同类开源软件的先进技术，激发自己产品的技术创新。同时，国内中间件企业要注重对开源中间件的贡献度。贡献越多话语权越大，这样就可以逐步主导项目的发展方向。目前，以 Apache Dubbo、Apache RocketMQ、Apache APISIX 等为代表，国内企业已经开源了一批成熟的中间件软件。

5.3.2 建立软件供应链管理体系

构建国产中间件供应链管理体系，在防范国外软件供应链技术体系壁垒、提升国产中间件安全性、促进国产中间件生态持续健康发展等方面都有着十分重要的意义。中间件厂商需要从以下几方面推进供应链管理体系的建设：一是与上下游厂商、用户及行业主管部门共同制定供应链管理标准规范；二是开展与中间件相关的供应链管理工具研制，保障中间件供应链管理活动能有效执行；三是推进供应链管理体系生态建设。

5.3.3 打造良好的生态体系

目前，中间件与产业链上下游产品的适配尚处于 1.0 阶段，随着中间件在金融、电信等行业的大规模应用，基于复杂业务场景进行适配的 2.0 阶段即将到来。中间件厂商需要积极推进上下游合作伙伴的协同发展，一方面与行业侧共研共创，围绕产品创新持续发力；另一方面，建立面向集成商和用

户的产品认证培训体系，为合作伙伴和用户赋能；同时，寻求建立统一的产品适配认证中心，降低大量适配给厂商造成的成本压力；此外，还要注重人才培养，鼓励校企协同育人，基于实操性教程（如《TongWeb 中间件实用教程》）在高等学校和中等职业技术学校开设中间件课程。

本章主笔人员（按拼音排序）：

北京东方通科技股份有限公司 刘玉杰、于滨峰、俞立平

6 办公软件

目前业界对于办公软件尚无统一的定义。本报告调研的办公软件包括文档处理软件（桌面 / 在线）、安全邮件和图像处理软件。在上述领域，部分产品已经逐步跨越了从“可用”到“好用”的门槛，并在协同办公、安全可信等方面的能力持续提升，在重点行业领域的应用规模显著增长。

6.1 产品和技术协同性、智能性和安全性持续提升

随着云计算、AI、大数据等技术的发展，流式办公软件逐步从云存储入手，将个人办公场景迁移到在线办公，以云端协同的产品形态为用户提供综合办公服务。版式办公软件实现了文件在系统服务端解析、渲染，本地不需要安装阅读器或者插件实现在线阅读。图像处理软件产品能够支持 10 亿级像素的图像文件处理。安全邮件实现了 1 亿封邮件深度全文检索只需 0.001 秒的至高性能，在极端情况下也能保证速度一致。

6.1.1 文档处理的云端协作和智能化日趋成熟

国产办公软件产品借助云平台为用户提供协同办公服务。金山、永中等办公软件已支持对 Word、Excel、PPT 等格式文档的多人实时协同编辑。通过文档云端存储技术，可实现多人、同时、通过不同终端访问和编辑同一文档，实现无延迟协同办公；通过身份认证、权限管理、传输加密等手段，保证文档在协作编辑过程中全生命周期安全。目前，金山办公的在线协作平台月活用户突破千万，漫游文档开启率达到 90%。同时，国产办公软件的平台效应正在显现，办公软件融合邮件、即时通信、音视频会议、日历、内容创作资源、行业业务系统等应用服务，可针对跨地域场景提供定制化的协同办公解决方案。

国内办公软件厂商专注于计算机视觉、自然语言处理等算法研究，开发

了智能辅助写作、文档校对、智能校对、PPT 智能美化、智能翻译、智能排版等近百项 AI 能力。WPS Office 2019 推出的文档校对工具，通过大数据技术和强大的纠错引擎，检测并修正 Office 文档中的拼写、语法、知识和格式错误。永中智能一键排版功能支持自定义规则，对文件进行一键排版。金山 WPS 全文美化功能可对 PPT 进行全局换肤、排版、配色和字体美化。此外，金山办公自主研发 OCR 和机器翻译技术支持快速完成英汉互译，BLEU 值[4]达到世界领先水平。

6.1.2 版式办公软件完成全国产化适配并实现“在线轻阅读”

国产版式办公软件产品完成了与国内主流基础软硬件和应用软件的全面兼容，稳定性、安全性和易用性不断提高。在基本满足用户各种需求的同时，“在线轻阅读”产品形态逐渐成熟，在文件的阅读过程中实现按需推送，本地不留痕，保证文档阅读的可信、可控、安全。友虹科技的在线轻阅读软件、数科网维的网页轻阅读、福昕鲲鹏云阅读、永中版式阅读器等产品，实现了版式文件的跨平台、跨终端、跨操作系统阅读。

6.1.3 图像处理软件精度进一步提高

近年来，国产专业图像处理软件取得了长足进步。以悟空图像为代表的国产专业图像处理软件能够支持 10 亿级像素的图像文件处理，实现了与 PSD 文件的双向兼容；在操作方法上从图像文件的底层结构出发，以异构对象取代传统的图层方式，兼顾非专业用户和专业用户的需求。

[4] BLEU 值：Bilingual Evaulation Understudy 的缩写，意为双语评估替补，是一种自动评估机器翻译的方法。

6.1.4 安全邮件性能和安全能力大幅提升

国产主流安全邮件系统采用企业级底层架构，通过分组块存储引擎、双数据引擎、自主 Web 2.0 引擎，以热数据克服性能缺陷。安宁邮件实现了 1 亿封邮件深度全文检索不超过 0.001 秒，同时可以保证在极端情况下速度一致。在安全设计方面，国产邮件系统从身份鉴别、安全访问、权限控制、发信、敏感信息过滤、传输、收信、存储到安全审计，实现邮件全生命周期安全闭环。如安宁邮件针对多种部署环境要求进行体系化、全方位的安全设计：底层采用沙箱架构，既减小了邮件系统的攻击面，又降低了内网横向渗透的可能性；上层采用透明盾牌架构，过滤针对 WebMail 所有的输入输出的请求；数据传输采用双重加密技术，数据存储采用双重指纹技术；云端安全中心定期更新特征库和病毒库，并及时下发安全策略到安全网关。

6.2 国产办公软件的应用规模显著增长

艾瑞咨询公布的数据显示，2020 年中国协同办公市场规模达到 440 亿元，疫情带来了大量的新用户，使得市场规模增速显著提升，同比增长率为 43.5%[5]。截至 2021 年 9 月 30 日，国产办公软件代表产品 WPS Office 月度活跃设备数达到 5.21 亿 [6]，是 2019 年 3 月 3.18 亿的 1.64 倍 [7]。根据《2021 中国企业邮箱安全性研究报告》数据显示，目前活跃的国内企业邮箱用户规模约为 1.6 亿，比 2018 年的 1.3 亿增加约 19%；2021 年全国企业邮箱用户共收发正常电子邮件约 2695.1 亿封，这一数字在 2019 年约 2454.1 亿封的基础上增长 9%。

[5]《2021 年中国协同办公市场研究报》http://report.iresearch.cn/report/202103

[6] 金山办公（688111）2021 年第三季度报告

[7] 金山办公（688111）2019 年年度报告

6.2.1 云协同和智能办公产品广泛应用

作为云办公最主要的载体之一，国产办公软件先后向阿里、百度、腾讯、华为、字节、360 和京东等在内的生态伙伴开放了在线文档处理能力，通过合作伙伴为亿万用户提供在线文档协同编辑能力。金山办公 WPS Office 全线产品全面搭载智能办公能力，为政府、能源、金融、互联网等行业超过 5 亿用户提供了服务。永中智能办公在政府、出版编辑等领域广泛应用，保障了公文、新闻、论文、出版的编辑质量和效能，其中常用的永中 PDF 工具集产品实现了多种文件格式的互转，文件转换成功率已经达到了 99%。2020 年一季度，超过 2 亿 WPS 用户通过云端文档实现在线协作办公。截止 2021 年 6 月 30 日，个人及“WPS+”用户通过公有云服务上传至云端的文件数量从 2018 年 93 亿份增长约 11.66 倍至 1085 亿份，较上年同期增长 56.02%。永中软件的云协同办公产品获得了金融电子合同模板协同编辑、检务文书协同编辑等多场景应用能力，有力支撑了政企单位文稿协同编辑、流转查询及统一管理。

6.2.2 版式办公软件在部分领域形成规模化应用

受益于政策推动，版式软件产品应用领域逐步扩大，市场份额逐年增加，部分领域已形成规模化应用。特别是电子公文系统的国产化为版式软件发展提供了难得的历史机遇。电子公文以及公文归档、电子发票、电子证照、电子档案等领域逐渐采用国产版式软件产品，有的形成了规模化的应用。友虹科技等国产版式软件厂商深度参与了医疗行业的电子健康档案开放共享、财政行业的非税票据管理、保险行业的保函开具等业务场景。

6.2.3 国产图像处理软件逐步获得用户认可

一直以来国内图像处理软件市场被国外产品 Photoshop 牢牢占据。近年

来，随着国产图像处理软件技术的不断进步，市场占有率情况也逐步发生变化。以悟空图像为例，在统信、麒麟、Windows、MacOs 及 Linux 平台上均已发布对应的产品，向相关党政机关和大型国企发放了数千份授权，并发展了数十万用户（在统信的软件应用市场中，悟空图像的用户增长率是 Photoshop 的 3 倍）。

6.2.4 安全邮件规模效应显现

国产安全邮件从前期的小规模、试点化应用，逐步呈现出大规模、集团化应用趋势，在政务、军工、金融等行业逐步推广并顺利实现跨单位、跨网络的数据安全交换，大大提高了整体产品设计、交付、业务联动效率。

6.3 国产办公软件厂商坚守自主研发初心

6.3.1 加大短板技术的攻关力度

目前，国内办公软件产品在中文用户所需功能、性能方面基本追平了国外产品，但在稳定性、复杂文档的兼容效果上与国外产品相比还存在一定差距。如国产安全邮件在易用性、便捷性方面设计不足，整体视觉感观尚待提升；国产图像处理软件在功能、文件格式和外设支持等方面与国外产品还有一定差距。瞄准差距加大科研投入，力争尽快固强补弱，是相关厂商的当务之急。

6.3.2 构建办公软件产业生态

数字化转型已成为各行各业的重要课题，办公软件之间的安全互通是用户的普遍需求，建设高质量生态体系是办公软件产业发展的核心和关键。完善网络安全生态，以联合攻关机制促进软硬件技术水平整体跃升，同时做好前沿技术布局，形成办公软件安全互通的解决方案，是办公软件厂商可持续发展的关键动作之一。

6.3.3 扩大应用推广提升品牌影响力

主流国产办公软件虽然已实现从“可用”到“好用”的跨越，但品牌宣传方面还较为滞后，而跨国公司办公软件产品已在国内市场培养了良好的品牌认知度和用户忠诚度，导致国产办公软件应用推广还存在一些困难。未来一段时间，国内办公软件厂商需要在技术创新的同时做好市场创新，提升用户对相关产品的认知度和忠诚度。

本章主笔人员（按拼音排序）：

北京金山办公软件股份有限公司 刘彬、马静

本章贡献人员（按拼音排序）：

北京安宁创新网络科技股份有限公司 王献芬

北京亦心科技有限公司 韦祖兴

永中软件股份有限公司 陈涛、王国文、吴庆敏

友虹（北京）科技有限公司 黄岩、张升平

7 整机

近年来，国内整机（由于参与编写单位业务范围的原因，本报告在整机领域调研的对象主要是服务器和桌面终端，暂不包含移动终端）厂商致力于提高核心部件和元器件的国产化率，在整机功能、性能、易用性和安全性等方面有了较大程度的提升，相关产品在重点行业领域应用的深度和广度不断提升。同时，国产整机也存在着性能低、成本高、利润少的现实情况，相关厂商面临着技术路线分散、适配工作量巨大的困难。

7.1 整机产品的功能和性能基本能够满足市场需求

目前，除 CPU、固件实现全面国产化之外，在显卡、内存、SSD 硬盘等部件的国产化率方面取得了重要进展，电阻、电容、电感等元器件的国产化率不断提高，在实际量产机型中得到了大范围的应用和检验。目前，不同产品形态和性能的国产整机产品基本能够满足各种应用场景的需求。此外，随着生产工艺、稳定性验证等方面生产技术水平的大幅度提升，国产整机产品的质量（开箱合格率）也在不断提升，部分厂商一次开箱合格率已经达到 99.85% 以上。

7.2 整机产品应用的广度和深度不断提升

在政策和业务双轮驱动之下，国产整机产品在各重点行业的使用率不断提高，现已从政府、国防等行业延伸至金融、能源、交通、医疗、教育及央企国企等多个领域，为社会治理、民生服务、产业发展等全面赋能。当前国产整机在重点行业的应用可大致分为三个梯队：党政和金融行业使用率较高，处于第一梯队；电信、石油、电力、交通、航空航天等处于第二梯队；教育、医疗领域使用率相对较低，处于第三梯队。

对于党政办公场景来说，“国产处理器 + 国产操作系统”的整机在性能、

易用性、兼容性等方面已经可以满足政务办公需求和期待。现阶段，党政办公计算机主要以台式机为主，一体机为辅。在产品性能方面，国产整机满足党政日常办公需求的情况基本令人满意，但仍有进步的空间，尤其是打开大型文件，响应速度有待提高。在生态适配方面，网信产业链上下游兼容适配的多年发展在本年度取得了成效，流版签软件、社交软件、浏览器软件、办公软件、打印扫描设备等均有适配产品，同时操作系统也匹配了一键安装软件方便用户的使用。

金融行业的整机需求更多的是承载业务系统的 IT 基础设施，如计算服务器、存储服务器、应用服务器等，对产品性能和稳定性的要求较党政办公系统更高。过去金融行业的 IT 基础设施以国外品牌为主，随着相关工作的深入推进，国产整机在性能和稳定性方面的水平不断提高，部分金融单位已经开始采购基于“国产芯片 + 国产操作系统”的服务器。在实际业务场景中，部分服务器已经可以实现超过 99.999% 的高可靠性，在一定程度上性价比可媲美国外设备。以银行为例，除六大行开始试点并逐步提升自主产品占比之外，越来越多的城市银行、股份制银行已经加入国产化替代的实践中。

目前电力行业的基础软件适配率可以达到 95% 以上，外设和业务系统的适配率为 70% 左右。其中部分业务系统，如设计软件、采集系统等未能适配完成或只能采用国外的软件产品，这也是国产化进程在电力行业的最大制约因素。随着试点工作的开展，不断暴露并解决问题，电力行业的国产化进程会进入一个发展的高速通道。

教育行业整机设备的使用年限为 5 年左右，2021 年是《教育信息化 2.0 行动计划》全面落地实施的关键年。2021 年 7 月，教育部等六部门发布指导意见，指出将可信安全新型基础设施作为教育信息化重点发展方向之一，提出推动可信应用这一明确要求。在教育行业推动网信整机落地的方式除了直

接采购外，以 CPU、操作系统为核心，整机为重要组成部分，构建完整的网信基础生态也是发力点之一。智慧大屏、网信实验室终端、云桌面服务器、云终端、教学平板电脑等不同整机的参与形式，配合网信人才的培养机制，满足了教育信息化的需求。

7.3 国产整机发展道阻且长

7.3.1 差距和不足

对标国外同类产品，整机产品在现阶段还存在一些问题：一是成本和价格偏高；二是技术路线相对分散，产品适配复杂，部件更新迭代快，适配周期短，批量应用产品的成熟度有待提高；三是供应链服务生态体系不完善，厂商的项目实施服务能力不足；四是特定场景下的解决方案与成熟体系比有一定差距。

（1）性能低成本高利润少

整机产品性能强依赖于上游处理器、内存、硬盘等部件的技术水平。现阶段，国产处理器、内存、硬盘与国际同类产品相比还存在一定差距，制约了整机的性能。与成熟的 Wintel 生态体系相比，整机产品的生态体系尚未完全成熟，与国产基础软硬件产品组合对性能的提升不明显，与相同价格的国际同类产品相比，性能有一定程度的差距。

受设计、制造、研发等环节成本高的影响，国产处理器、内存等部件价格普遍较高，并且整机厂商受限于产业链位置等因素，对部件的议价能力有限。与国际同类产品相比，产品研发、生产、适配、服务等多个环节的投入大，造成了整机产品成本偏高。由于市场竞争造成的价格与成本的比例不协调，压缩了整机厂商的利润空间，造成整机厂商缩减研发方面的投入，进而影响了整机研发进程的提速、水平的提升及网信事业的良性可持续发展。

（2）技术路线分散，适配工作量巨大

自主整机产品技术路线多，研发力量分散，除了造成研发适配工作量增长以外，还很难保证产品质量的一致性。六大 CPU 与数款操作系统可搭配组合，不同组合产品的开发要求不同，如何保证所有技术路线的产品品质，对整机厂商的技术研发、人才培养、资源整合都是很大的考验。

同时，处理器、操作系统、应用软件在技术与产品上升级迭代过快，造成整机开发、适配周期短。生态链上下游厂商每次都需要重复进行设计、适配、验证及测试流程，工作量巨大。部分情况下出现大幅度调整还容易造成无法有效继承老平台改进优化的成果，导致从零开始的情况。从用户的角度看，每一代产品都不能持续改进，用户使用的产品始终处于不完善状态，影响用户的使用体验，不利于网信产业的持续稳步推进。

（3）特定场景下的解决方案缺乏竞争力

面对重点行业（特别是金融、电信）用户的差异化需求，国产整机产品在性能、可靠性、稳定性等方面都与国外同类产品和解决方案有一定差距。因此，目前多数情况下只能用于外围系统。

7.3.2 从整机厂商的角度看今后一个时期的发力点

（1）保障整机厂商利润空间

以当前的市场体量，上游部件厂商在研发成本、生产成本和市场运作成本等方面还不足以通过规模化效应摊销成本。加大国产部件在各厂商整机中的使用占比，提高国产部件的整体的产能需求，以整体需求的体量，支持国产部件厂商降低生产成本，从而降低整机厂商的成本，是未来重点要考虑的工作之一。同时，要破除掉那些影响网信市场的利润空间的不可持续发展的因素，提升整机厂商利润空间。

（2）提升产业链的研发和生产能力

自主创新的网信产业蓬勃发展的同时，也伴随着部分合作伙伴进入实体清单、新冠疫情造成的核心芯片产能不足等情况，整机供应链的供货能力不足问题，有从 CPU、内存、显卡、主板等核心部件向关键元件漫延的趋势。

首先，要解决研发能力问题。只有具有了相关产品的研发能力，才能保证供应的连续性和稳定性。现阶段，还有部分关键部件国内不具备设计、生产和制造能力。部分能在国内研发和生产的部件，距离完全实现对国外先进产品的替代，还有很多问题要解决。

其次，要解决生产能力问题。无论是 CPU 还是内存、闪存，国内厂商在设计水平、设计能力方面与国际品牌的差距正在缩小，有的已经达到或接近国际先进水平，能够在一定范围内实现对国际品牌的替代，但是受限于生产能力，还不能满足市场的实际需要。

（3）成立联合攻关中心

目前，大部分兼容适配的认证是基于纯净系统环境进行的，还没有在集成应用系统的特定应用场景及日常工作环境下进行验证。在实际应用场景和生产环境下，集成的硬件设备、软件系统数量巨大，存在的问题也相对较多。只有通过实际生产环境的验证，才具有推广的基础及可能性。针对上述问题，整机厂商已经与上下游厂商组建联合攻关中心、适配基地等，验证复杂环境下的底层架构、应用进程等问题，致力于从根本上解决问题。

（4）多层次培养人才

已验收项目在日常设备使用方面、系统应用场景方面均暴露出一些问题。造成这些问题的原因，除了客观情况之外，还有部分是主观的使用习惯、运维能力等原因造成的。为解决这些问题，需要基于自主创新的网信技术大力

推动各类人才的培养，包括前端培训人才，即能够给一线使用人员、操作人员、维护人员进行针对性培训的培训讲师等；项目咨询、建设人才，即能够提供网信项目咨询、方案规划、系统集成及安装实施、运维的人才；核心研发、适配、测试专业人才，即在整机及上游产业链内实际需求的专业人才。

本章主笔人员（按拼音排序）：

同方计算机有限公司 邓忠良、李亚军、张伟

本章贡献人员（按拼音排序）：

百信信息技术有限公司 侯飞

北京计算机技术及应用研究所 杨超

超越科技股份有限公司 冯磊、刘维霞

江苏长城计算机系统有限公司 景思哲

8 IP 网络

IP 网络是指基于 IP 协议簇的网络，本章主要探讨与 IP 网络相关的设备和解决方案的创新和应用情况。目前，国内主流的网络设备厂商推出了基于国产基础软硬件的产品和解决方案，核心元器件的国产化率达到了较高的水平。在产品方面，性能指标基本与采用非自主核心元器件的产品达到了同一水平；在解决方案方面，基本具备了满足行业应用需求的能力。

8.1 自主 IP 网络设备和解决方案逐步成熟

8.1.1 IP 网络设备

路由器的国产化，其核心是基础软硬件的自主。硬件层面主要是 CPU、转发芯片、存储芯片；软件层面主要是协议栈。国内网络厂商推出了基于国产基础软硬件的自主路由器，产品的种类和档次逐步完善，具备了在不同的应用场景下逐步完成国产化替代的条件。

交换机的国产化，在技术层面与路由器类似。目前，从低端园区盒式接入交换机，到高端数据中心多槽位分布式架构交换机，核心元器件国产化率已达到 100%，整机元器件国产化率已达到 80% 以上，并仍在不断提升中。功能上，除传统的 L2/L3 网络协议以外，可支持一虚多、M-LAG、VxLAN、Trill、EVPN 等数据中心功能。

WLAN AP 产品核心部件为 CPU、Wi-Fi 芯片（射频芯片、FEM 等）/ 模组、内存、存储器件、交换芯片等。Wi-Fi 芯片是 WLAN 网络设备的关键器件，其市场集中度非常高，高通、博通以及联发科占据约三分之二市场份额。国产 Wi-Fi6 芯片目前相较于国际先进水平仍有差距，主要原因是起步较晚，前期积累不够、人才匮乏、技术基础不足。

8.1.2 IP 网络解决方案

数据中心网络提供从应用到物理网络的自动映射、资源池化部署和可视化运维，构建以业务为中心的网络业务动态调度能力，主要涉及网络虚拟化、大规模二层网络、M-LAG 双规接入、服务链、微分段、虚拟机流量导出等关键技术，以及服务器、智能网卡、Spine-Leaf 业务交换机、存储交换机、云平台、管理交换机、网络分流器、数据中心网络控制器等产品。目前，相关解决方案已基本具备替代条件。在云网一体化管理方面，阿里云、腾讯云、中国电子云等云厂商与迈普、H3C 等网络厂商开展协作，从云管向云网融合方向延伸，形成接口标准、加大互认证力度，提供统一的云网融合解决方案。

软件定义广域网解决方案（SD-WAN）通常由广域网络控制器和路由器共同组成，可广泛应用于骨干网场景、纵向网场景、分支接入场景，可满足网络快速部署、业务路径动态规划、网络深度透视呈现等需求。SD-WAN 方案采用自主广域网控制器，以业务为视角，解决了数字化转型过程中广域网面临的自动化程度低、智能化程度低、网络不可见、运维成本高等难题。

基于自主交换机和园区网络控制器的智能园区解决方案具有整网的协同安全、极简接入和策略随行、智能运维等特点。软件定义分支方案（SD-Branch）将广域和园区网络打通，同时解决广域接入、园区接入、无线接入、安全防护、策略不一致等问题，提升企业网络的一体化管理水平，降低运维难度，实现网随人动，网络为业务服务。

8.2 自主 IP 网络解决方案在部分行业部署并发挥作用

国内厂商大规模投入 IP 网络解决方案的打造，推动了方案成熟落地，已经基本能够代替国外产品满足国内市场需求。当前自主 IP 网络解决方案已在部分行业得到大规模应用，主要集中在政府、金融等自主安全要求较高

的行业，其他行业如医疗、能源、教育、制造等，还需要进一步推动落地。

8.2.1 数据中心网络解决方案助力云基础设施建设

数据中心网络采用 SDN 技术重构传统网络架构。当前国内主流网络设备厂商均推出了自主数据中心网络设备，在公有云、私有云、混合云、政务云场景中得到广泛的应用，已部署在金融、邮政、政府等各种规模的数据中心。金融行业数据中心解决方案使用智能 SDN 网络，实现业务自动化交付；基于数据中心网络控制器的逻辑组网，通过端到端的网络流程仿真，自动下发配置，提供灵活的计算、网络、负载均衡和安全防护能力。

8.2.2 软件定义广域网打通企业云网互联

软件定义广域网广泛应用于金融、运营商、政府、能源、交通行业，以及商业中小客户群体。2021 年，国有大型商业银行基本均已完成骨干网向 SD-WAN 网络升级。在股份制银行、城商行、农信银行等机构中，SD-WAN 方案也在逐步落地，随着数据中心 SDN 化的快速推进，这些金融机构的骨干网 SD-WAN 换代已列入日程。同时工商银行、农业银行已在省级分行启动了现网 SD-WAN 方案的试运行。预计未来两年内，SD-WAN 金融网络大面积铺开广泛应用。在商业市场上中小型企业可以选择购买 SD-WAN 服务，形式包括运营商直接提供 SD-WAN 线路服务、云厂商借助企业上云提供 SD-WAN 方案、安全接入服务商拓展广域网接入市场、传统数通厂商打造 SD-WAN 方案协助自建等多种方式。

8.2.3 智能园区解决方案提升网络安全性和运维效率

主流整机厂商推出了以自主网络设备为基础，融合园区网络控制器的智能园区解决方案，在政府、金融等行业得到广泛的应用。如金融行业某二级

银行园区网络，通过园区网络控制器对不同的安全接入区域配置不同的安全策略模板，对同一个安全接入区域的接入设备下发统一的安全策略；基于终端识别技术自动识别终端设备类型，根据终端类型下发对应的认证策略，提供同一终端用户多场景方便快捷的接入；可查看局域网中不同业务数据的转发路径、流量带宽、转发延迟、组网拓扑等可视化信息；支持拓扑自动发现、设备自动化配置下发、变更策略批量修改、故障自动定位等功能，实现园区网的自动化快速部署运维。

8.3 自主 IP 网络仍需加速技术和应用创新

8.3.1 发展智能网络技术

智能网络技术主要包括可编程网络、基于意图的网络、网络数字孪生技术等。采用智能网络技术可进一步增强自主 IP 网络，利用自主网络设备和网络控制器，使网络能够满足未来业务发展需求，提升企业生产效率。

可编程网络基于软件定义网络，将网络设备配置平面和部分控制平面独立到软件平台，采用应用编程接口（API），通过编程语言向网络设备发送编程指令，由软件驱动的中央控制节点自动化控制网络。

基于意图的网络（IBN）是一种基于业务意图配置网络基础设施的网络技术。IBN 综合了多种现有的技术，它将网络从以设备为中心的模型转变为以业务为中心的模型。IBN 通过分析用户意图，将意图转译为相应的网络策略，最终实现网络感知和控制策略的自动化部署。

数字孪生技术应用于网络，创建物理网络设施的虚拟镜像。数字孪生网络平台通过拓扑透视和流量全息、从设备到组网的全生命周期管理、网络实时闭环控制、网络优化方案高效仿真等多种技术手段，能够实现低成本试错、智能化决策和高效率创新，将成为未来网络规划、运行、管理和运营的新方向。

下一步需要明确数字孪生网络的定义和架构，在关键技术上持续深入研究，选取典型应用场景开发数字孪生网络验证系统，验证数字孪生网络的架构、流程、功能和接口，促进数字孪生网络技术的成熟和应用，推动其标准化工作。

8.3.2 发展智能网卡技术

随着云计算、大数据、AI 及机器学习的发展，现有的数据中心网络解决方案已经无法完全满足业务的需求。基于智能网卡完成网络卸载和特定业务卸载的要求越来越强烈。基于智能网卡技术的发展，未来有可能对服务器当前的基础硬件架构进行重定义。继 CPU，GPU 之后，DPU（Data Processing Unit）成为数据中心场景中的第三颗重要的算力单元，为高带宽、低延迟、数据密集的计算场景提供计算引擎。当前作为 DPU 主要的应用领域，网络厂商基于国产化器件研发生产智能网卡产品，围绕服务部署解决服务器性能不足问题，协助各种业务功能应用卸载，在体系结构上探索与服务器操作系统、服务器虚拟化、容器等技术的结合。

8.3.3 深化工业互联网应用

工业互联网需要保证业务流高可靠、低延时支撑生产业务需求，基于自主创新的 IP 网络设备深化工业互联网应用，可以从多个方面入手。一是通过时钟同步、频率同步、调度整形、资源预留等机制，满足确定性网络确定性时延、抖动、丢包率、带宽和可靠性等要求；二是通过 FlexE 实现网络切片，支撑带宽资源弹性灵活的分配和保障；三是通过高可靠通信、切片等技术保障带宽和时延需求。

本章主笔人员（按拼音排序）：

迈普通信技术股份有限公司 林茂

本章贡献人员（按拼音排序）：

迈普通信技术股份有限公司 董威、郭久明、雷晓龙、罗向征、唐仁圣

重庆市信息通信咨询设计院有限公司 张晓琴

9 云计算平台

国内云计算在部分核心技术上已经达到国际领先水平。近年来，云计算平台厂商开始关注基于国产化架构的技术研发工作，集中对国产化底层基础设施进行了攻关适配，在优化性能、解决兼容性问题方面取得了一定的进展，初步建立了自主创新的云平台生态环境。

9.1 云计算平台实现国产化迭代升级

9.1.1 可持续演进的私有云加速 IT 架构升级

随着数字技术的快速发展，传统私有云技术出现了不适应政企上云需求的情况，主要由于传统私有云主要采用新建或割接的升级方式，容易造成版本碎片化，导致“运维难、使用难、升级难”等问题。新一代私有云采用多种新技术手段，能够兼容适配多样化技术路线的数据中心基础设施，较好地解决碎片化和复杂性问题。

产品级“一云多芯”架构将复杂多样的硬件资源抽象、池化，形成统一的云化资源平台，解耦了应用对底层硬件的依赖，屏蔽了底层芯片和设备的差异化，可构建同时兼容多种主流国产化芯片和 x86 架构芯片的私有云平台，解决了传统私有云建设、部署和运维的碎片化和复杂性问题。

全平面统一接口设计采用数字原生架构。系统架构和应用架构采用统一的 API（应用程序接口，简称接口）架构风格与约束，满足应用与服务的东西向和南北向调用。总体架构采用两层接口架构，一层是通过 Kubernetes 统一编排接口，用于统一不同组件的接口风格，使全平面可编程、可编排；另一层是平台中各种开源组件的原生接口，保持与开源生态完全兼容。该架构以事件网格组件为中枢，以可编排为原则，可进化为总体目标，应对组件在升级过程中事务完整性和业务补偿之间的平衡问题。

云平台与云服务分离。云平台与云服务的分离使云平台彻底解决了在私有部署场景中建设周期结束即是平台能力边界终点的短板，更好地应对数字化转型过程中云计算技术的变化，与传统的软件交付方式比较，效率提升了上千倍，同时提升了业务连续性。

9.1.2 专有云快速实现国产化落地

主流云计算平台通常采用自主设计的底层系统架构，适配多种芯片和操作系统，在一朵云内，实现多种芯片的资源池交付。这种一云多芯的承载设计可以很好的适应当下国产芯片多样性的发展趋势，也可适用于复杂的多区域、多维度、多种云架构的混合业务场景。通常一套管理界面即可异构纳管包括混合云、专有云在内的全部资源的技术体系，有助于在跨网络和区域的场景中统一管理云资源基础设施，降低技术风险。依托于自主研发的云计算平台底层，在功能、应用上符合技术驱动的发展要求。

9.1.3 桌面云轻量级完成自主化转型

基于虚拟化技术的桌面云已成为和传统计算机桌面相并列的新模式。桌面云向下兼容硬件 CPU 平台，向上为用户提供国产桌面操作系统，有效地解耦国产操作系统和底层硬件平台，实现用户端自主化和轻量化。

桌面云以同一技术架构、同一技术产品，有效整合信息创新软硬件生态链。覆盖服务端和用户前端，全面兼容支持多类自主异构 CPU 平台，实现异构混合部署；支持推送国产操作系统，降低操作系统与终端硬件的关联性。支持在国产操作系统上运行 Wintel 体系应用软件，可有效快速的打通国产化生态与 Wintel 体系的新老应用衔接；支持在国产自主硬件下的高清视频播放。

9.2 云计算平台已经在多个领域广泛应用

9.2.1 私有云成为党政、金融等领域的新型基础设施

随着数字化转型升级的深入以及云计算技术的发展，越来越多的政府、金融、电信、能源等国计民生行业用户选择私有云平台作为承载业务的基础设施，近些年出于安全性和可控性的考虑，用户会优先选择国产化私有云平台部署自己的业务模块。

新一代私有云的特点可以极大的降低政府部门财政支出。一云多芯解耦厂商与 CPU 路线，可以适配各类硬件，满足多技术路线发展需求。一体化架构在不论是前期建设阶段还是中后期运维阶段，都可以大大降低建设成本与运维成本。

金融行业作为实现信息技术应用创新的排头兵，目前超过 200+ 银行、TOP20 券商和大型保险公司，均采用私有云平台推进目标计划，并且不同细分领域的用户都需要有针对性的全栈金融云自主解决方案，帮助金融机构更快更稳更好地实现自主可信的目标。

9.2.2 专有云加速教育、广电等行业应用创新

专有云针对教育和广电等行业云平台使用特点，提供资源利用灵活高效，可统一管理，组网灵活、扩展灵活的云平台解决方案，将用户私有云业务和公有云业务无缝联接起来，实现资源的灵活调度。

教育行业近些年结合云计算、大数据、人工智能等技术为高校以及科研机构提供在线教育、智慧高校、课题研究等场景解决方案。某高校完成专有云平台构建后，响应院系信息系统资源需求分配云资源，并将当前传统架构的校园信息系统逐步上云。

广电行业纷纷在原有的影视和娱乐产品基础上增加了直播、富媒体等多样化传媒内容和服务。某广电集团在技术上采用基于公有云和自建私有云的专有云平台，以互联网架构和广电级安播模式逐步构建安全、稳定、可扩展和承载海量视频内容的生态云平台，为广电公司各业务发展提供基础承载与技术支撑。

9.2.3 桌面云助力党政办公国产化平滑过渡

桌面云厂商围绕信息创新技术应用场景下各行业自主创新应用需求打造用户端自主化和轻量化的桌面云解决方案。在国家部委和地方政府若干项目中陆续得到落地应用。桌面云最大程度上降低了用户使用的虚拟桌面操作系统与终端设备的耦合度，提升了用户数据的安全性，降低了管理员的系统运维工作。

9.3 加强自主可控，促进云计算产业生态的可持续发展

9.3.1 构建开放、多元的云计算生态体系

我国云计算从 2010 年发展至今，经过多年的发展及技术更迭，在我国 IT 基础设施，尤其是关键信息基础设施建设过程中，形成了“云平台、容器、裸金属”三足鼎力的局面。国产化厂商应积极建设符合我国国情、面向全球的开源云计算社区，构建一个开放、多元的云计算生态体系，集中国内龙头企业，逐步掌握技术主动权，引领云计算技术发展方向，保障核心技术自主可控。

9.3.2 建设中国特色的开源云计算社区

事实证明，开源已经成为全世界最成功的科技创新模式。我国云计算厂商也通过参与国际开源项目提升了云计算领域的自主创新能力，开源软件已

经成为云计算产品的重要组成部分。在拥抱开源的同时，核心技术依赖开源的问题应该得到足够的重视，并将相关的供应链安全问题上升到国家安全的高度来对待。

9.3.3 加强兼容适配能力

2021 年 10 月，国务院印发了《国家标准化发展纲要》，提出：新时代推动高质量发展、全面建设社会主义现代化国家，迫切需要进一步加强标准化工作。加强云计算产品与国产中间件、操作系统、数据库、芯片等兼容适配标准研制和应用，不仅是引领云计算领域新业态新模式健康发展的需要，也是提升产品质量，满足数字化转型需求的重要途径。

9.3.4 积极面对“双态”共存的市场竞争格局

当前，我国云计算产业迅速发展，各行各业将云计算作为推进区块链、人工智能与实体经济融合的重要抓手。由于历史原因，在市场竞争格局上形成了以国外芯片为主的存量云市场和以龙芯、鲲鹏、飞腾等国内芯片为主的增量云市场。从用户需求和实际的部署情况来看，Intel 与龙芯、鲲鹏、飞腾等云资源池混合部署将会是常态化。

本章主笔人员（按拼音排序）：

北京易捷思达科技发展有限公司 陈翔、吕薇

本章贡献人员（按拼音排序）：

北京云思畅想科技有限公司 韩利超、孟芳

湖南麒麟信安科技股份有限公司 徐鹏

上海云轴信息科技有限公司 步松涛

中国软件评测中心 李安伦

10 安全浏览器

随着信息化应用的深入，安全浏览器作为业务应用的基础入口，具有高可用性、高可扩展性以及高可管理性的特点，成为国家信息化体系中不可或缺的一个关键组成部分。近年来，国内浏览器厂商在产品的安全性和易用性方面取得一定的进展，得到了更大范围的应用，但仍面临着核心技术依赖开源软件的现实问题。

10.1 安全浏览器在虚拟化和源数据加密方面取得进展

随着国产终端的普及，大量基于 IE 内核开发的业务系统面临迁移改造问题。安全浏览器厂商通过服务器虚拟化技术，在服务器后端创建云发布应用服务器，在应用服务器上安装“远程虚拟浏览服务”，通过远程虚拟化的方式访问原有业务系统，无需对于现有的业务系统和网络进行改造，还可以有效地阻断恶意代码，实现数据隔离和协议隔离。同时，国产安全浏览器的关注点不只放在解决数据传输安全问题上，更注重了源数据的加解密技术，用以保护网页中高价值数据免受攻击。

在涉及浏览器的网络攻击中，浏览器本身和插件等附属部件是主要攻击目标。虚拟化浏览器可以系统地解决安全问题，将浏览过程从桌面浏览器移至基于云的浏览器服务中，通过重置虚拟化的浏览服务为业务系统增加安全隔离带，将有风险的页面浏览行为与业务系统隔离起来，保护内部高价值目标，阻断勒索病毒、漏洞攻击等安全风险。

浏览器源数据加解密技术可以让用户利用浏览器内置密码能力在浏览器端来保护其身份数据和隐私数据，适用于浏览器中用户或服务的认证、文档或代码的签名、数据的机密性与完整性保护等。在浏览器上原生实现密码功能，相对于 JavaScript 调用的方式，更有助于解决浏览器的安全缺陷和性能问题。

10.2 创新技术成果逐步开始在政企业务场景中取得应用

近年来，国产安全浏览器的应用逐步得到了普及，客观上促进了浏览器行业向着安全、高效、透明的方向发展。但是，随着安全浏览器的应用越来越广泛，各个行业领域不同的应用场景对安全浏览器提出了细分的功能要求。这对于浏览器厂商来说，加大了开发的成本。另外，在全面支持自主创新生态建设方面，国产安全浏览器需兼容适配开发于不同历史时期、基于不同内核技术的应用系统，导致业务系统迁移改造投入大、成本高、进度缓慢。对于浏览器厂商来说，也是一笔巨大的投入。虚拟化浏览器的出现，在一定程度上解决了上述两个难题。现在一些政企用户尝试采用虚拟化浏览器技术，客户端不需要再关注业务系统兼容性问题，在服务器后端创建云服务，通过远程虚拟化的方式即可实现原有基于 IE 内核开发的业务系统访问。另外，在系统迁移过程中，无需对现有的业务系统和网络更改，只要保障云服务器与业务系统的通讯即可。预计在 2022 年将有越来越多的政企用户应用虚拟化浏览器技术。

在金融领域，安全浏览器主要实现对业务系统链路级的安全防护。随着监管要求的不断完善，用户对浏览器源数据加密的能力越来越关注。从 2021 年起，国内逐步有部分商业银行在网银系统中采用了浏览器内置的源数据加解密技术。预计在未来一段时间内，浏览器源数据加解密技术将逐步在金融领域推广。

10.3 未来需进一步加大浏览器核心技术的投入

国内浏览器在渲染引擎和 JavaScript 引擎等核心技术领域大多依赖开源产品，自主的技术研究长期处于空白状态。目前国内外主流厂商浏览器均是基于开源 Chromium 内核基础上二次开发，而 Chromium 项目由美国公司 Google 主导。如果 Google 关闭许可，国内浏览器厂商将面临无法继续使用

最新 Chromium 代码的风险。也就是说，国内厂商在核心组件方面仍然存在断供风险。因此，需要加大核心技术的研究与投入，保证安全浏览器产业的健康发展。具体路径可考虑打造国产浏览器的开源社区：先从国密算法支持、浏览器安全性加固、自主硬件适配优化等技术维度切入，通过开源社区的持续运营，逐步提升开源内核的成熟度和影响力，适时将国内浏览器切换到自主内核，更好地支持 W3C 新标准，保持与其他浏览器的兼容和自身的竞争地位。

本章主笔人员（按拼音排序）：

北京海泰方圆科技股份有限公司 王鹏

本章贡献人员（按拼音排序）：

北京奇虎科技有限公司 赵丰泽

江苏云涌电子科技股份有限公司 杨望星

奇安信网神信息技术（北京）股份有限公司 李良杰

上海缔安科技股份有限公司 林艺芳

天津赢达信科技有限公司 彭竹

11 外设

外设产品的品类十分庞大，本报告重点关注打印机、复印机、扫描仪、一体机、高拍仪等产品和相关的技术和产业发展情况。近年来，相关厂商集中力量解决了与多种底层技术路线兼容适配的问题，特别是在芯片厂商的支持下较好地解决了自主产品与 Windows 操作系统兼容的问题，产品的功能和性能不断提升。此外，国内厂商基于可信计算技术加强了对非国产芯片外设产品的安全管控，相关产品在重点行业领域的应用规模逐年扩大。

11.1 外设类产品在自主创新和安全管控方面取得进展

11.1.1 外设产品部件国产化率和安全性日益提高

外设产品创新发展的核心是建立自主可控的技术底层架构和标准。受益于相关政策，打印机、复印机、扫描仪、一体机、高拍仪等一大批国产外设产品集中涌现。外设产品的主控芯片逐步转为国产 SOC 芯片，核心器件、控制板卡、内核系统、驱动等关键部件由国内企业设计生产的比例越来越高。在国产化率不断提高的同时，外设产品的功能也逐步从可用迈向好用，应用场景越来越丰富。例如，激光打印机产品在打印机核心技术和自主知识产权上有所突破，已经成功采用龙芯、飞腾等国产芯片研发出一系列产品。在加强国产化的同时，相关企业充分发挥自身技术特点，在打印扫描、文档处理、通信控制和协议解析等方面加强管控，充分保障了数据输出安全。

11.1.2 外设产品的安全管控能力逐步提升

外设产品在国产化率不断提高的同时，安全管控水平逐步提升。国内主流外设厂商推出了基于可信计算的外设产品。打印机嵌入式板载 TPCM 产品的成功开发，在安全 BOOT、可信内核、应用执行控制、动态度量技术、可

信安全架构五个方面实现系统级的可信度量，保护打印机固件不被篡改，保障用户的数据不被窃取与泄露，实现打印机全生命周期的主动防御，填补了多项国内外设可信领域技术空白。

11.2 国产外设产品在政务和金融领域获得广泛应用

11.2.1 外设和文印管控产品在电子政务领域的应用

随着在电子政务行业应用经验积累，国内推出了多种类型的外设产品。如红黑打印机在电子公文和红头文件、电子印章等方面满足党政公文打印的需求并获得广泛应用；安全增强型打印机在内部打印、打印文件加密、打印传输加密等场景获得应用。基于可信计算技术的安全外设也逐步推向市场，文印管控平台在电子政务市场上也有广泛的应用。

11.2.2 外设产品在金融行业的应用

金融行业涉及的外设产品主要包括打印设备、复印设备、扫描设备、移动智能终端、金融柜外清、影像采集仪（高拍仪）等。上述产品的国产化版本均已实现广泛应用。

采用国产 SoC 片上系统、适配统信桌面操作系统的针式打印机成功应用于各大银行，可在一张凭证上实现字符打印为黑色、印章打印为红色的功能，同时支持纸张自动纠偏、自动寻边、自适应厚度打印，可以支持存折、证卡、各种尺寸的单页纸、多层拷贝纸等的打印，部分产品还提供了打印扫描一体化的功能，显著提高了产品可靠性及易用性。

移动智能终端设备目前已完成各技术路线的适配工作，相关产品主要应用于金融移动办公或业务办理场景。在移动办公过程中，配合平板电脑完成部分介质类功能，补充了平板电脑不具备的银行卡读写卡、存折读取、二代

证读取、专用指纹库认证、实体加密键盘输入、电磁签名等必备功能。

金融柜外清系列产品主要应用于银行柜面服务，实现银行在客户交互过程中的高效服务及无纸化办公，目前在全国二十多家银行均获得较好的应用。银行无纸化系统的建设与推广大大提升了银行业务受理的高效性与便捷性，结合柜面智能终端的手写签批、双目活体检测摄像头、二维码扫描、数字人民币交易等功能，形成了新一代柜外清产品，让客户体验到更加便捷安全的服务。

影像采集仪（高拍仪）产品也已完成各技术路线的适配工作，设备具有证照识别、证照扫描、人脸识别、录音拍照录像等功能，广泛应用于银行、保险、政务等行业的文件归档、OCR 识别、录音录像、人脸识别、活体检测、认证比对等业务场景。

11.3 尽快打造高性能、全覆盖的产品系列

通过近几年核心技术的积累和产业的发展，国内外设厂商已经具备了一定的创新研发能力，并在外设产品国产化解决方案上取得了不错的成绩。未来一个时期，国产品牌应始终坚持以技术自主、研发创新、设计可靠、细节精细的理念，尽快实现全面的自主可控。

在这一过程中，需要着重关注并突破高端核心组件技术，加大协作力度，着力解决技术协同和产品适配等问题，提高产品稳定性，打造高性能、全覆盖的产品系列，做到有序发展。同时，考虑到未来中长期的发展，需要从组建产业联盟和构建标准规范等不同的角度，促进专利的交叉授权和零部件供应商的共享，打造融合、开放的产业生态。

本章主笔人员（按拼音排序）：

北京辰光融信技术有限公司 杨香玉、张志龙

安全篇 »

12、商用密码

13、边界安全

14、反恶意代码引擎

15、高级威胁检测

16、漏洞管理

17、安全管控

18、终端安全

19、云计算安全

20、数据安全

21、工控安全

22、安全服务

23、电子取证

12 商用密码

近年来，密码和业务应用融合的趋势已基本确定，业务系统密码改造在各行业初步展开。虽然在一段时期内“密码要用”与“业务可用”的供需矛盾还将存在，但这既是商用密码获得更大发展必须要直面解决的问题，也不失为激发产业动能的另一个契机。

12.1 商用密码技术、产品和服务形态取得突破

12.1.1 基础和新兴密码技术取得进展

密码芯片在制造工艺、综合性能、存储容量、接口类型、安全性等方面取得长足进步；密码模块与整机产品种类不断丰富，性能不断提升；密码分析及安全防护技术不断增强；可信计算技术体系日益完善。上述成果已在关键信息基础设施和重要信息系统得到规模化应用。

在新兴技术密码应用方面，基于高性能云密码产品的多种密码服务等取得重要进展；隐私计算技术得到了迅速的发展，并在金融行业获得应用；基于量子密钥分发的量子通信与传统密码技术融合创新，出现了量子增强型数据加密与认证系统。

12.1.2 商用密码产品形态不断丰富

密码与信息化产业的融合既包括与 IT 底层基础软硬件的融合，也涵盖与面向业务的信息化应用的融合，国内厂商已具备了相对成熟的支撑能力，一批融合创新产品集中面世：如在高速密码处理器方面，基于可重构计算技术研发的高速密码芯片；在云密码应用方面，基于国产处理器研发的 TEE 软件密码模块；在智能网联汽车领域，支持商用密码的车规级安全芯片等。

面对密码与业务的融合过程中出现的“难用、难管”问题，基于“面向

切面的数据安全技术”将安全与业务在技术上解耦、但又在能力上融合交织，提供轻量级改造应用的密码应用实施模式，实现主体到应用内用户、客体到字段级的防护，让密码“好用、好管”。同时，应用开发商、上游安全厂商、服务机构等非业内角色也依托各自的优势，积极尝试解决密码应用融合的问题，极有可能为密码行业带来新的变革。

12.1.3 新型密码服务快速发展

随着密评合规工程的快速推进，用户对密码厂商的需求，已不再是提供单一的密码产品，而是要求基于密码技术，提供平台化的产品技术支撑和一体化的服务能力。目前部分商用密码厂商已经推出了咨询、整改、一体化交付等多种新型密码服务形态。同时，密码产品在应用侧正向着标准化、平台化的方向发展。密码厂商相继推出了具有鲜明的应用特色的密码服务平台产品，通过统一对接应用减少运维和管理的成本。随着实践的深入，密码服务平台逐步尝试与风控及测评服务、安全态势感知、数据安全治理等安全理念融合，形成了密码的安全管控中心的雏形。

12.2 商用密码与应用场景的结合日益紧密

随着新兴信息化技术与传统产业的融合，业务应用对商用密码产品和解决方案的需求越发迫切。密码应用不再停留在原有单一的应用场景，开始随着业务形态的不断变化，形成以密码为核心的创新型行业安全应用。

12.2.1 可信终端安全解决方案在电力行业广泛应用

以密码技术为基因，可信计算平台已广泛应用于电力行业的网络安全隔离装置，通过对固件、操作系统、应用及业务软件等计算部件进行度量和检测，从根源上建立了对恶意程序攻击的免疫机制，使其能够抵御恶意代码、漏洞

利用、病毒等攻击。

12.2.2 密码服务支撑云计算安全建设

集约化建设的行业密码运营服务平台陆续开始为行业应用提供专业化、平台化、服务化的统一密码服务。全栈式密码云服务平台实现了从构建在本地设备上的密码服务到构建在云平台上的密码服务的转变，提供基于 IaaS、PaaS、SaaS 模式的多种云架构密码能力，提供面向云化业务的新型密码技术架构和服务模式，满足多场景、多层次的敏捷密码应用需求。

12.2.3 密码服务支撑解决物联网和车联网安全问题

基于可信标识系统形成的物联网感知层设备的综合解决方案，在石油、电力、智能制造、智慧城市、轨道交通等行业的广泛应用，解决了物联网感知层设备的密码安全应用问题。基于商用密码的车联网信任体系，通过信任基础设施解决了典型应用场景下的身份认证、数据溯源和隐私保护问题。工业互联网密码服务平台为车联网、物联网标识体系提供密码基础服务，解决了工业互联网应用中的身份认证、隐私保护等问题。

12.2.4 密码技术在数据安全领域发挥重要作用

基于密码技术的大数据全生命周期安全体系，将密码技术对敏感数据的防护提升到应用层，在解决数据检索和计算问题的同时，构建了独立的第三方数据安全权限体系。多终端融合的数据防泄露解决方案，实现和优化了商密算法库在文档加密领域的适用性和灵活性，在航天、制造、金融等领域均达成了上千个终端用户的常态化应用。透明接入方式实现的云平台虚拟机数

据存储加密解决方案，解决了 OpenStack 架构下的虚拟化敏感数据保护问题。固态硬盘控制器芯片在企业级固态存储硬盘中获得广泛应用。

12.3 商用密码要和产业链上下游进一步融合发展

12.3.1 与传统安全产业的融合

在国产化信息技术体系中全面应用密码将成为新的需求和增长点，对传统形态的密码产品产生深刻影响。从商用密码厂商的角度看，当前面临着商密产品技术相对于需求的滞后性问题。密码技术如何与安全产品深度融合，以及密码产品存在的门槛高、面世周期长等问题，需要商用密码厂商进一步关注。

12.3.2 与云计算等新兴产业的融合

云计算等新兴技术的发展促进了传统信息业务的变革。传统以密码设备、密码系统为主的交付方式，已逐渐难以满足业务的需求，越来越多的业务需要更加便捷、可靠、安全的密码功能来保障业务的安全性和合规性。商用密码厂商将在以下两个方面进行探索：一方面以云服务方式的提供密码功能的研究、设计和开发，如云密码机、云签名服务、云电子合同服务、云密钥管理等；另一方面在智慧城市、智能交通、智慧医疗、互联网 + 电子政务、电子商务等领域探索云密码服务应用模式。

12.3.3 与数据跨境需求的融合

随着数据跨境跨域流动成为新的安全和合规焦点，密码技术将作为有效的数据保护手段之一。在通过密码技术与其他安全技术和管理的结合解决数据跨境问题的同时，密码行业面对国际国内密码标准、算法和协议混用的场景时，还缺乏有效的机制和手段。如何通过密码技术建立国际互信机制，维

护数据主权完整，促进大数据的充分利用，是对商用密码行业的挑战。

本章主笔人员（按拼音排序）：

三未信安科技股份有限公司 鹿淑煜

本章贡献人员（按拼音排序）：

北京海泰方圆科技股份有限公司 王学进

北京计算机技术及应用研究所 王永安、吴宇、于然

北京炼石网络技术有限公司 白小勇、钱晶、魏婷

北京数字认证股份有限公司 张妍

北京天融信网络安全技术有限公司 刘治平

北京信安世纪科技股份有限公司 焦靖伟、汪宗斌

国科微电子股份有限公司 窦步纹

湖南麒麟信安科技股份有限公司 彭勇、申锟铠

江苏云涌电子科技股份有限公司 高渊

启明星辰信息技术集团股份有限公司 程昌明

厦门市易联众易惠科技有限公司 林静

上海众人智能科技有限公司 丁震宇

深圳市东进技术股份有限公司 吕冰

深圳市网安计算机安全检测技术有限公司 洪跃腾、彭洁瑶、孙少波、

唐启楠、朱思霖

无锡沐创集成电路设计有限公司 王孟元

浙江华途信息安全技术股份有限公司 叶俊卫

郑州信大捷安信息技术股份有限公司 梁松涛、刘为华、刘献伦

中国移动通信有限公司研究院 李邦灵、马爱良、彭华熹、张艳、张杨

13 边界安全

云计算、人工智能、威胁情报技术的发展，逐渐破除了网络固有的物理边界，朝着服务化、应用化的方向发展。从而导致传统的边界安全防御体系难以适应云化、虚拟化网络发展，被动边界安全防御机制逐渐失效。国内安全厂商融合 AI、威胁情报、零信任和物联网等新技术，通过与威胁情报中心、零信任和物联网管理平台智能协同，构建了云网端协同的主动安全防御体系，拓展了边界安全能力和应用范畴。

13.1 边界安全产品向协同、联动、融合的方向发展

13.1.1 边界安全与威胁情报融合

为了应对被动边界安全防御机制逐渐失效的困境，各厂商积极参与情报生态系统的建设，通过云端提升安全威胁检测能力，实现多维度、全方位的情报感知，帮助安全管理人员及时了解系统安全态势，动态调整安全策略，快速部署可行的安全响应战术，变“被动防御”为“主动防御”。通过多源安全情报整合，赋能网端，不断提高防火墙、网络入侵检测 / 防御、Web 应用防火墙等边界安全设备对未知威胁、恶意文件、异常流量、隐秘通道等多方面的检测能力。

作为边界安全防御的重要角色，下一代防火墙积极的通过协同机制与安全防御体系各个组件交互信息，不仅与终端、网络端形成协同防御，还借助云端威胁情报以迅速获取最新安全能力，从而实现从静态特征检测向智能动态感知转变，从被动应对向主动响应转变，从事后应对向事前防御转变。国内厂商在智能下一代防火墙的研发方面取得了较快的进展：采用全新硬件架构设计的智能下一代防火墙，通过与威胁情报中心联动，突出了智能感知、情报集成、融合安全能力，在检测未知威胁事件、检测内网失陷主机、管控物联网设备等方面相对于传统防火墙有了较大进步；另外，在防火墙一体化智能检测引擎方面取得了较大进展，将 AI、多网元协同防御、云检测协同

融入下一代防火墙产品，提升了防火墙的综合防护能力。

13.1.2 边界安全零信任方案落地

零信任在边界安全领域的应用和解决方案涵盖了原有 SSL VPN 技术的应用场景，对终端状态的检测更全面、更动态。为实现零信任安全方案，网络安全厂商在以下三个方面开展了重点攻关：一是持续动态收集终端状态信息、确保接入终端始终可信；二是零信任网关动态配置终端与应用间的策略；三是零信任管理平台实现全局策略编排和下发。通过以上三者联动，构建以身份和终端状态为中心的、持续动态的鉴权与访问控制体系，保障应用和数据安全。

国内边界安全厂商提出的零信任安全解决方案中，应用不再信任网络内外任何单元，且将用户 / 终端访问权限限制为完成特定任务所需的最低限度，不仅融合了 SDP（软件定义边界）理念，并强化了 SPA（单包认证）落地，使得应用对用户 / 终端隐藏，构建以身份为中心的动态访问控制机制，提供更为精准、有效的资源访问安全管控。

13.1.3 物联网安全管控能力提升

随着物联网设备的广泛部署，其他安全风险也日益受到重视。加强物联网设备的安全管控，除了提升相关人员的安全意识和管理水平、提高前端设备自身安全性之外，通过边界安全设备加强对物联网终端的检测和管控也十分重要。

国内厂商针对边界安全设备的物联网安全管控能力开展了技术攻关并取得了突破：通过网络地址和物理地址等信息的确认杜绝物联网设备私自接入；在设备信息辨识方面，通过感知设备指纹信息实现精确分类统计；在安全检测和管控方面，对设备行为进行监控，发现异常行为后可对相关设备进行隔离。

13.2 边界安全的融合创新成果已经发挥了重要作用

13.2.1 威胁情报与智能防火墙联动的方案获得广泛应用

威胁情报技术已成为边界安全产品的核心威胁防护能力之一，被各安全厂商广泛应用于防火墙、入侵防御系统。边界安全与威胁情报的融合，有效提升了安全运营的保障能力。网络安全厂商与威胁情报联动的边界安全产品和解决方案，在政府、医疗、教育、能源等行业领域获得了广泛应用。在攻防演练和重保活动中，在威胁情报与边界安全体系的联动保障下，及时向网络运营者推送安全漏洞、恶意 IP、产品和舆情通告等情报信息，为组织提供战时情报预警服务，并借助专家级分析研判与应急处置能力，实现了对安全事件的风险闭环管理。

13.2.2 零信任解决方案在金融等行业初步应用

随着业务上云和移动化的趋势，办公接入方式也发生了巨大变化，并带来了新的网络安全挑战: 一是终端接入地点、时间复杂，内网安全边界被打破；二是个人终端不可控，终端安全状况难以统一。零信任理念引导安全架构从网络为中心转向身份为中心，通过细粒度的自适应访问控制，实现信任最小化、访问权限管控的效果。

以智能下一代防火墙为重要组成部分的零信任远程安全接入解决方案，能有效应对远程办公接入带来的风险。已发布的零信任远程安全接入解决方案在金融、政府等信息敏感行业获得了初步应用。实际的使用效果显示，零信任解决方案基于身份和终端状态动态进行授权判定，将网络位置作为验证身份和提供授权的重要依据，同时基于按需分配的策略控制访问范围，大幅降低了资源可见性，减少了远程攻击。

13.2.3 物联网安全监测与管控初步发挥作用

在日常管理物联网终端的过程中，由于管理意识的欠缺以及物联网终端

自身的漏洞，导致数据资产面临着较大的保密性和完整性风险。同时，随着物联网设备大规模的接入互联网，很容易成为网络安全防御体系的短板，对整体防御效果造成较大损失。智能下一代防火墙对物联网终端的识别、监测和管控能力在一定程度上降低了这一风险。在实际使用过程中，智能下一代防火墙能识别市场上主流摄像头并对其异常行为做出安全决策，同时可将摄像头物联网安全管控的信息对接至安全运营中心，在实际应用场景中打造了更全面、更智能的安全大脑。

13.3 边界安全产品向高性价比和绿色节能方向发展

边界安全是网络安全产业生态中相对最为成熟，也是竞争最为激烈的领域。为了构建健康、可持续发展的生态环境，各相关厂商需要更加关注差异化，在发挥各自优势的基础上，构建从设计研发到生产制造为一体的网络安全产业生态体系。另外，应积极探索网络安全与多产业协同发展的新途径，加快技术创新、加强产业协作与跨行业融合，推动多领域多层次网络安全技术框架落地。同时，要积极推进网络安全产业链的组织、优化与协同，推进各企业优势资源互补和优化配置，完善产业链协作配套体系。

在核心技术创新方面，加大对网络安全专用芯片的研发投入力度。传统CPU/GPU并不是网络安全处理专用芯片，当用于网络安全设备时，内部大量的冗余逻辑会导致网络安全应用效率较低。为了进一步提高边界安全产品的性能，各网络安全厂商需加大对网络安全专用芯片的研发力度，在满足产品功能和性能的同时，实现“网络＋安全”的专有特色，满足不断增长的数据处理和安全防护需求。目前，山石网科已经启动了首款网络安全专用芯片研发，将创新的网络安全芯片应用于下一代边界安全产品，提高数据处理能力和综合性价比。

在系统能耗方面，关注节能环保。“2030年碳达峰、2060年碳中和”的“双碳”目标，倒逼我国加快低碳转型，推动经济高质量发展。为了响应“绿色低碳”新型数据中心建设的需求，网络安全厂商积极推进技术升级，通过引

入一系列创新的绿色技术，满足节能环保的时代要求，在落实碳达峰、碳中和目标中发挥示范引领作用。

本章主笔人员（按拼音排序）：

北京山石网科信息技术有限公司 王中斌、温晶晶、姚鹏

本章贡献人员（按拼音排序）：

北京神州绿盟科技有限公司 张良玉

北京天融信网络安全技术有限公司 曹昊阳

北京网迅科技有限公司 耿涛、胡金山、钱利国

精壹致远（武汉）信息技术有限公司 陈强、赵泉城

恒安嘉新（北京）科技股份公司 李鹏超

江苏云涌电子科技股份有限公司 李新顺、练书成

北京中船信息科技有限公司 张德胜

上海缔安科技股份有限公司 陈炬

沈阳东软系统集成工程有限公司 陈静相、路娜、宋圣

郑州信大捷安信息技术股份有限公司 梁松涛、刘为华、刘献伦

中国移动通信有限公司研究院 何申、黄静、赵海燕

14 反恶意代码引擎

反恶意代码引擎有高技术难度、高开发量和高维护量的特点，是反恶意代码领域的最高技术门槛。绝大多数安全厂商的核心威胁检测能力来自于反恶意代码引擎。因此可以说反恶意代码引擎方面的技术和产业能力在一定程度上决定了整个安全产业、乃至国家层面的威胁检测能力和安全防御能力。对比国外厂商，我国自主创新的反恶意代码核心技术总体来说并不落后，在一定范围内很好地起到了为产业赋能的作用。

14.1 反恶意代码领域在理论、技术和工程方面持续完善

全球数以千计的网络安全厂商中，具备完全独立自主开发反恶意代码引擎的只有十多家（其中绝大多数是国外厂商）。我国反恶意代码引擎虽然在检出率方面与国际顶尖厂商的引擎略有差距，但是在检测效率、平台适配（包括国产平台）、检测对象深度拆解、检测结果命名体系化和检测配置灵活性与粒度等方面，我国的自主引擎更有优势。

14.1.1 新一代安全防御能力框架

为提升主动安全防御能力，改变攻防过程中的被动地位，安天提出了以“识别、塑造、防护、检测、响应”为特点的新一代安全能力框架。识别是网络安全管理的基础，构筑起网空防御地形认知基础；塑造是建立防御主动性的前提，通过塑造使攻击者处于不利的位置；防护是系统对威胁做出的行为，达成对威胁活动和违规行为的拒止；检测则是在对象中发现和标定风险活动；响应是处理、管理风险与威胁事件。通过对 IT 规划和场景的构建、重构和调整，形成环境、场景拓扑路径配置和安全策略的优化，并结合欺骗布防使攻击者处于不利的位置，从而提升防御方主动防御能力。该框架在借鉴当前国际先进的防御矩阵框架（NIST CSF 框架、SHIELD 积极防御框架和

D3FEND 知识图谱等）的基础上强调“塑造”环节，充分发挥建设方和运营者的先发优势，加大防御纵深、构筑欺骗环境，协助用户完成防御体系的能力组装，建设起体系化安全能力，达成体系对抗威胁，实现检测、干扰、阻断和呈现对手杀伤链的目标。

14.1.2 向量级情报运营和智能未知威胁检测

在情报运营方面，我国安全厂商将反恶意代码引擎的经验与能力向威胁对抗扩展，形成向量级威胁情报，实现向量情报生产、运营、消费的闭环过程，有效解决高价值威胁情报难以落地、传递性不佳、效用性不好、知识性不足的问题，支撑高级威胁的检测、揭示、对抗和溯源能力。安天全面跟踪和感知网络威胁行为体和威胁活动，基于威胁视角提取高级恶意代码的基因特征，将威胁情报从攻击载荷层面扩展到典型字符串、编译环境、身份信息、加密算法、通讯配置、关键代码片段等关键向量以及向量时序和向量间的逻辑组合关系。结合威胁框架完成向量级威胁情报的形式化运营，实现以引擎 SDK 形式完成向量级情报下发和落地，有效达成对高级威胁的载荷检测和组织关联，达到提升攻击成本、打造私有化检测能力的目的。

在未知威胁检测方面，国内厂商结合机器对海量威胁信息的处理、适应和扩展优势，叠加人类智慧和独创性，通过机器学习和人工智能进行高级检测和未知检测。典型的创新成果包括：基于跟踪全球高级威胁行为体形成的 APT 库以及全量恶意代码知识图谱，可快速将样本归因于 APT 组织，揭示背后的动机、方法和工具；基于安全大数据平台的深度学习引擎，可有效检测未知恶意代码并与终端安全防护软件联动；针对海量端点日志、利用 AI 建模分析能力，对端点日志进行分析、检测和研判；采用内存虚拟化技术和内存行为分析技术，通过对 CPU 指令级的监控和端点进程的监控，结合行为关联技术，对无文件攻击和内存攻击进行防护。

14.1.3 后端支撑工程体系

在工程体系建设方面，我国安全厂商将大规模捕获和分析体系的后端工程扩展为集捕获、分析、演训和情报于一体的威胁对抗工程体系。通过数万个计算节点构成的混合云支撑威胁的捕获和自动化分析研判、情报作业、溯源和对抗能力，将专家经验与 AI 自动分析结果快速持续转化为引擎、各类安全产品的识别、塑造、检测、防御和响应能力。

14.1.4 移动反恶意代码引擎

在移动端反恶意代码方面，我国厂商研发的自主引擎处于国际领先水平。在 2018 年和 2019 年 AV-TEST 测试中，安天以全年 6 期测评检出率皆为 100% 的成绩领跑全球移动安全杀毒引擎（包括但不限于小红伞、卡巴斯基和迈克菲等国际主流厂商）。在 2021 年的 AV-TESET 的测试中，安天移动反恶意代码引擎以强劲的查杀能力，零误报的实用性以及较低的 CPU 占用取得三项满分的佳绩。

14.2 自主核心反恶意代码技术应用促进安全生态可持续发展

14.2.1 赋能基础安全供应链

国内反恶意代码厂商通过赋能自有产品或第三方产品的方式支撑建立了一个良性的安全赋能生态体系。目前，安天的反恶意代码引擎覆盖全球超过一百万台网络设备和网络安全设备以及二十八亿部移动智能终端，为 50% 主流防火墙厂商和 100% 国产手机厂商提供安全底层，为全球亿万用户构建了智能安全生态防护能力。奇安信通过对自有端点安全产品、威胁分析平台等赋能威胁检测能力的方式为超过 5000 万政企终端提供安全防护能力。

14.2.2 威胁检测能力延展到新兴场景

国内安全厂商依托成熟的产业链支持和传统的积累，将反恶意代码技术和可信技术深度融合，拓展在物联网和工业互联网等新兴场景的战略布局。工业互联网恶意代码检测引擎在超过20家航天和船舶企业进行了应用示范，为其提供了有效的工业互联网安全内核。

14.2.3 提升自主网信产业的安全防护能力

国产化虽然有效降低了信息化产品中预置后门和断供等人为风险，但针对国产操作系统平台的病毒数量正在不断增加，国产系统也存在自身脆弱性问题。需要警惕的是随着国产平台的普及，威胁行为体对其的技术研究和攻击投入将会加大，安全防护面临更加严峻的挑战，甚至可能出现APT级别的攻击。针对上述问题，国内厂商与基础软硬件厂商开展了深度合作，将自主引擎与国产软硬件平台进行适配，研发了自主终端安全产品，对计算机进行全方位安全防控。国内安全厂商自主研发的反恶意代码引擎等安全产品已经完成了与主流国产CPU、操作系统和中间件平台的适配，解决了安全检测产品集成恶意代码检测引擎涉及的跨平台移植问题，为国产自主可控系统工程提供满足合规要求又具备实战化防护能力的引擎。

14.3 反恶意代码厂商需要不断创新并加强产业赋能

反恶意代码引擎厂商需要继续在自主创新方面深耕，努力输出更安全、先进、有效、方便、好用的反恶意代码引擎。在技术层面，持续提升基础识别拆解能力以及加大检测技术的研发与创新，向国际先进水准稳步推进。在检测能力方面，将持续夯实已知威胁检测能力并大力提升未知威胁检测能力，同时持续与国产化平台、操作系统、固件等兼容适配。在应用场景方面，基于传统的技术积累与安全产业链赋能经验，将威胁检测能力覆盖到人工智能、

5G、物联网、工业互联网和云计算等新兴场景，保障数字化转型与关键基础设施的网络安全。在安全产业生态方面，国内厂商将逐步在一般用户和商业机构中替代境外引擎，在党政军、关键信息基础设施等高信息价值、高防护等级和高威胁对抗的行业和客户提供专属化检测能力。

本章主笔人员（按拼音排序）：

安天科技集团股份有限公司 童志明、黄磊、韩耀光

本章贡献人员（按拼音排序）：

安芯网盾（北京）科技有限公司 陈洪龙、杨芳、朱燕涛

奇安信科技集团股份有限公司 宋加斌

亚信安全科技股份有限公司 李旻旻、王绪国、于忠臣

15 高级威胁检测

高级威胁（APT 攻击）是由国家、政治经济集团等发动，以战略目标、基础设施和特定高价值目标为对象，具有手段高级、时效持久等特点的一种攻击方式。当前我国在高级威胁检测方面面临能力投入相对离散、协同能力不足等问题。可喜的是，随着国家和社会各界对网络安全的重视程度不断提升，国内厂商在高级威胁检测方面的手段日趋丰富和成熟，并在越来越多的场景下发挥了重要作用。

15.1 高级威胁检测思路手段不断丰富

15.1.1 主动追踪高级威胁，赋能情报生产和威胁检测

主动追踪高级威胁，指从海量基础威胁数据出发，主动追踪高级威胁组织，了解其最新攻击手段、资产和目标等情况，基于规则和模型生产威胁情报知识，提升检测效率和防御效果。目前大多数厂商已经逐步具备 APT 活动的追踪和溯源能力，常见的主动追踪思路有两种：一种是被动式威胁狩猎，即快速响应事前所布置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；另一种是主动式威胁狩猎，基于情报知识、主动扫描等技术，力图从非告警数据中挖掘异常痕迹，进而确认是否存在未能检测到的攻击活动。目前采用的最常见的追踪方法是利用规则和模型等综合手段对攻击活动中产生的恶意文件进行检测，经过长期数据累积，可能发现新 APT 组织，并明确的给出组织的画像和证据。

越来越多的单位选择使用威胁情报进行高级威胁检测，提升安全运营能力。相关厂商在成熟开源情报技术（Open Source Intelligence）基础上演进出安全运营中心产品（Security Operations Center），通过定制化部署导入云端情报，联动所有安全设备，统一告警并快速发起威胁响应，进而阻断和缩短

APT 攻击时间。通过 SOC 及其团队，追踪 APT 组织的活动可以不再局限于恶意文件的检测和分析，而是可以利用情报数据和知识发现异常活动行为。利用失陷指标（Indicators of Compromise）信息中的 IP 和域名数据可以检测是否存在曾经访问恶意 IP、域名的主机，提取主机行为日志，可以进一步分析在连接恶意 IP 和域名时的主机行为和操作，定位感染源，完整还原入侵的攻击过程和活动过程。

15.1.2 基于内存保护实现运行态威胁检测

基于内存保护技术实现实时防御，是通过在内存中识别和分析敏感行为来检测威胁。该技术在程序的运行态着手解决威胁检测和防护问题，借助硬件虚拟化技术把安全防护能力从应用层、系统层下沉到硬件层，能有效突破操作系统的限制，直接对内存访问和指令运行等动作进行监控分析，判断程序运行的合理性，识别出异常行为或恶意代码的攻击，最后通过关闭恶意程序阻断攻击者入侵。内存保护技术在监控内存和系统异常方面具有天然的效率优势。相对于攻击样本的数量，其使用的敏感行为点相对收敛。只要触发到检测行为点，内存保护系统都会对其进行实时检测告警。目前国内厂商推出的内存安全防护方案，理论上可将二进制内存破坏型漏洞攻击的检出率提升到 85% 以上。

15.1.3 多阶段断链式检测建立 APT 攻击预警能力

断链式检测从杀伤链 (Kill Chain) 的各阶段对 APT 攻击进行综合检测，在侦查投递、漏洞利用、安装植入、命令控制和数据回传等等阶段建立更全面的 APT 攻击预警能力。该技术采用静态特征、动态行为、威胁情报和机器学习等多种检测手段，从多阶段进行综合检测，识别出完整的攻击行为并评估其造成的影响。相比于常见的单点检测，断链式检测技术能更容易地发

现网络威胁，对抗 APT 攻击方式。

国内厂商推出的为各攻击阶段分配针对性防御技术的深度检测方案，在侦查阶段采用特征匹配的方式识别口令爆破、端口扫描、漏洞探测；在投递阶段采用动静态结合的检测技术，检测邮件攻击、水坑攻击等典型 APT 攻击；在安装植入和利用阶段利用特征检测和行为检测技术识别恶意文件、0day 及 Nday 漏洞利用；在控制和渗透阶段通过主机控制检测、网站控制检测、隐蔽信道检测、DGA 域名检测等功能，检测远程控制、数据回传和内网攻击。

15.1.4 采集网络全流量建立全天候高级威胁识别能力

再高级的攻击都会留下网络痕迹，因此网络全流量分析是应对（发现、验证、阻击、溯源、取证）APT 攻击行之有效的手段之一。科来在该技术领域开展了研究，通过旁路采集和存储所有网络流量，通过多维的数据分析及深度挖掘能力，可以实现数据包级的追踪取证，发现高级未知攻击；同时，可通过安全事件关联分析，完整拓线各类事件数据，帮助用户进行影响面评估，发现安全弱点和盲点，并及时采取相应处置措施，阻止事态继续发展。

15.2 我国高级威胁检测技术的典型应用

2021 年，国内安全厂商在高级威胁追踪领域展现了不凡的能力，发布高级威胁分析报告达 90 篇以上，涵盖 23 个已知 APT 组织和 5 个新发现的 APT 组织，针对数十个高级威胁组织捕获数百起网络攻击事件，收集数千条高价值的情报数据。国内监管单位基于这些情报数据，可对境内受控情况进行定位排查，全年借此发现并阻断了众多来自境外的 APT 攻击活动。

内存保护技术在某次攻防演习中也发挥了重要作用，在域控环境中监测到攻击者利用远程命令执行漏洞开展的内网渗透行为。深度报文检测设备辅助 CNCERT 进行多阶段“断链式”检测，监测到了海莲花组织的网络间谍活动。

全流量安全回溯分析系统在部分重点行业领域部署后，采用异常行为模型、隐蔽信道检测等多种手段发现攻击，并实现对攻击事件从会话到原始报文的全程分析，精准还原再现整个攻击过程，研判攻击手法和攻击者背景，定位发现了多个 APT 组织和攻击行为。

15.3 跨界融合提升高级威胁检测防护能力

15.3.1 AI 技术与 APT 检测技术融合

应用人工智能技术检测未知威胁和高级威胁，将引发威胁检测领域对 APT 检测响应的思维模式从传统人工式响应持续向智能式响应转变，趋于智能式检测、智能式研判，构建全面的预测、基础防护、响应和恢复能力，对文件、流量、行为和事件等进行同源关联和性质研判能力将不断提升，显著提高大数量的高级威胁事件的检测和研判效率，抵御不断演变的高级威胁。

在部分高级威胁检测场景下，人工智能已经初显成效。未来基于智能化的安全防护技术在高级威胁检测领域将取得更多进步：一是基于机器学习、深度学习算法，同时结合大数据分析，将模糊、非线性、海量数据通过不同数据类型进行更好的聚合、分类以及序列化，持续训练优化检测模型，覆盖更多的检测场景，不断提高 AI 检测模型的安全检测效率、精准度和自动化程度；二是通过人工智能技术对各种网络安全要素数据进行归并、关联分析以及融合处理，通过大量安全风险数据进行关联性安全态势分析，综合分析网络安全要素，评估网络安全状况，预测其发展趋势，对网络安全性进行定量分析以及精细度量，进而构建关联性网络安全威胁态势感知体系，全面智能化感知内外部安全威胁；三是通过人工智能提高自学习应急响应防御能力，构建主动安全防御体系，推动网络安全防御向更快（机器学习、人工智能、自动化）、更准（行为识别、可视化）方向加速演进；四是借助人工智能的

学习和进化能力，应对未知的、变化的攻击行为，并结合当前安全策略和威胁情报形成安全智慧大脑，主动调整已有安全防护策略，形成全面感知、智能协同和动态防护的主动安全防御体系。

15.3.2 跨界知识与追踪溯源方法融合

基于溯源图的 APT 攻击检测方法，可被用于 APT 活动的追踪溯源。通过对设备日志的结构化解析，利用知识图谱和攻击路径的学习，对异常的执行路径和场景进行告警，进而发现 APT 组织的攻击活动。采用类似的思路和方法，可以规避人员直接操作系统日志和系统信息等敏感数据的问题，安全运营人员仅需要对异常数据进行分析即可发现攻击活动和路径。这样一方面避免了日常运行数据的泄露；另一方面解决了安全运营人员无法远程进行支持的难题；同时也降低了人力投入，提升了威胁发现、威胁狩猎的准确度和成功率。

15.3.3 知识图谱与推理研判过程融合

构建 APT 组织攻击知识库，可以解决完全依赖于运营人员知识积累的难点。知识库拥有比人脑更加完善的知识体系和数据，通过对 APT 组织的深度分析和攻击行为信息采集，能够在精准度上和研判速度上超越纯粹的手工作业。知识库体系与知识图谱等技术结合，可以实现攻击路径的推理和研判过程，进一步提升系统自动发现 APT 活动的可能性和准确率。

本章主笔人员（按拼音排序）：

安天科技集团股份有限公司 高喜宝、李登锋

本章贡献人员（按拼音排序）：

安芯网盾（北京）科技有限公司 杨芳

北京六方云信息技术有限公司 韩阳

北京神州绿盟科技有限公司 吴铁军

北京易捷思达科技发展有限公司 吕薇

北京长亭未来科技有限公司 张旭峰

恒安嘉新（北京）科技股份公司 李鹏超

科来网络技术股份有限公司 孟召瑞

上海众人智能科技有限公司 陈羽兴、徐肖顺

亚信安全科技股份有限公司 向剑岭

16 漏洞管理

随着信息系统规模的不断扩大，传统的漏洞扫描工具已不能实现真正意义上的漏洞修复和管理。漏洞管理产品正在从单一的漏洞评估工具向更全面、更有安全价值的方向演进。

16.1 漏洞管理产品向智能综合方向演进

16.1.1 漏洞基建运营

漏洞基建运营是通过建设一整套体系化、流程化、持续化的运营机制，围绕集漏洞情报、漏洞定向挖掘、专家响应，形成漏洞基建安全中心。区别于其他产品，漏洞基建不以单体企业漏洞管理需求和痛点进行业务规划，而是以战略视角看待漏洞管理问题，打造漏洞协同管控平台。典型产品如360安全大脑漏洞云，通过集成多个子系统建立规范化的漏洞运营流程，实现产品应用与数据互联，支撑漏洞全生命周期的运营管理。一体化安全漏洞管控中心和漏洞运营管理平台，通过结合漏洞情报、安全众测、漏洞管理等产品能力，实现漏洞闭环的集中处置，提高工作效率与漏洞响应处置速度。

16.1.2 智能漏洞检测管理

智能漏洞检测管理对用户的各类扫描工具与内置引擎进行统一调用，从漏洞挖掘、渗透测试、技术攻关、逆向分析、应急响应、溯源取证、安全分析、攻防能力等方面进行统一的数据融合与分析，提升全网自动化漏洞检测管理的能力。在智能漏洞检测管理过程中，确定漏洞优先级是基础，通过对漏洞进行优先级排序和流程化处理，可以大大提高漏洞处理效率。

16.1.3 人工智能和自动化编排

很多安全产品使用人工智能、机器学习技术进行自动化威胁检测和分析，

用于分析用户行为、检测未知危害、排序漏洞优先级等。除了与人工智能技术结合，漏洞管理与安全编排自动化响应 SOAR（Security Orchestration, Automation and Response）技术也广泛结合应用。该技术能够收集各种安全系统产生的告警，对事件分析与响应流程进行形式化的描述，并将漏洞样本送入漏洞管理平台进行分析管理，结合漏洞威胁情报进行资产校验，评估风险受控面。如果整个编排的过程完全依赖各个相关系统的 API 实现，就实现了自动化、标准化的事件响应。

16.1.4 DevSecOps

研发运营一体化模式下的安全概念 DevSecOps（Development Security Operations）逐渐走向成熟。该模式把安全能力嵌入现有开发流程体系，让安全不再置身于业务之外，也让其他人员参与到安全之中，对日常的应用安全和漏洞全生命周期管理保障工作起到指导作用。随着 DevOps 模式的落地，研发效能的提高意味着安全漏洞的数量随之上升。以往安全漏洞风险的管控会面临难修复、周期长等问题，一定程度上阻碍了业务持续交付，且解决漏洞的成本会越来越高。在软件开发生命周期的早期阶段开展 DevSecOps 建设，可以通过用自动化的方式检测软件应用程序中的各种漏洞，尽早发现编码错误。

16.2 漏洞管理产品在部分行业发挥重要应用

16.2.1 漏洞基建运营

漏洞基建安全平台应用于城市安全建设，通过深度结合漏洞运营管理业务，与城市漏洞运营管理者共同建立漏洞运营中心，打造了城市级漏洞运营体系，制定了高兼容性的漏洞运营制度，建立了城市级漏洞运营管理安全一体化平台，提高了城市级漏洞威胁感知能力，实现了针对重大漏洞爆发的快

速响应和处置。

漏洞基建中涵盖的漏洞情报订阅服务也为金融行业采购互联网漏洞通报及技术支持提供了支撑，通过漏洞情报收集体系，提供了“大安全”背景下的宏观漏洞全景防御，针对不同的场景提供漏洞风险预警，将关联漏洞进行统一聚类汇总，直观的发现高级漏洞威胁情报信息。同时，通过与安全平台（如 SOC、态势感知、全流量等）联动，可极大缩短威胁响应时间，起到“单点感知、全网联防”的效果。

16.2.2 智能漏洞检测管理

漏洞管理平台运营方案有效结合企业内部的管理流程，在一定程度上实现了漏洞管理的流程化、自动化，通过闭环管理有效减少了面临的风险：一是大大提升了安全管理员的工作效率；二是为漏洞修复提供了参考；三是制定了自动化的管理流程，做到过程、结果完整可追溯；四是标准化的漏洞处理；五是建立高效的风险定位机制，快速划分漏洞责任；六是满足基线配置规范要求；七是持续监控资产变化，达到持续优化弱点管理的基准要求。

16.2.3 DevSecOps

安全工具链集成至企业内部 DevOps 相关流程平台，通过安全左移，在需求阶段进行安全评审、识别安全风险、进行威胁建模。在软件开发和测试阶段，将 SAST（静态应用安全测试）、DAST（动态应用安全测试）、IAST（交互式应用安全测试）、SCA（软件组成分析）、AVC（漏洞关联分析）等工具集成到 CI/CD 中，提前发现安全漏洞并及时修复，从而在应用上线前解决安全风险，实现“出厂即安全”。在上线运营阶段，采用监控工具对应用程序进行实时跟踪，检测应用程序运行状态，当发现安全漏洞时根据漏洞自动跟踪工具追溯漏洞根源，及时进行漏洞的派发和修复，最后通过漏洞情报收

集、检测响应综合分析等对漏洞信息进行归档统计。

16.3 漏洞管理向协同联动方向发展

16.3.1 建立云地协同漏洞数据库

漏洞数据库需要本地和云端共同建设，单一的漏洞库很难发挥漏洞应急响应和管理的作用。本地漏洞数据库需要将本企业历史漏洞数据做统一的盘点、整合、拆解以及总结，可以为企业持续性的漏洞检测做指导，对漏洞修复做知识沉淀。云端数据库需要依赖第三方甚至外界海量的白帽子资源，第一时间发现漏洞风险后，及时同步到本地数据库做资产的联动以及应急响应。云端加本地双数据库并行的方式，可以将企业内部漏洞的梳理以及外部新漏洞发现的及时响应的优点汇集于一身，充分增强了企业对漏洞的管理能力。

16.3.2 加强云地数据库的协同联动

现阶段的漏洞管理需要加强第三方数据或者平台的联动，如漏洞管理可以同企业的漏洞威胁态势感知系统结合，动态了解当前面临的漏洞威胁；又如通过多方协作建立漏洞等级评估机制，以应对大量漏洞不能及时修复等问题。

16.3.3 加大在自主产品漏洞挖掘方面的投入

自主产品近年来部署量增大，在漏洞挖掘、存储和管理方面，也需要加入到云地协同的漏洞数据库中做联动处置。针对于自主网信产业面临的漏洞危机，增加对自主产品漏洞关注度及进行漏洞挖掘支撑相关产业的漏洞治理势在必行。一是要重视安全设计、安全开发等问题，从源头上减少安全漏洞；二是要不断完善第三方众测平台，加强针对国产化产品漏洞的检测能力；三是要重视漏洞技术生态力量，建议产品发布前先进行第三方安全测试；四是

加强开源组件应用的安全管理，构建安全的软件供应链环境。

16.3.4 加强安全加固工作

对于长时间无人维护的开源程序或组件，或不具备升级、重启条件的服务和系统，可根据漏洞的利用方式，在不升级或者不打补丁的情况下，通过禁用端口、修改配置、限制程序读写关键文件权限、删除或禁用不必要的服务等方法进行安全加固。不过，现在安全加固还只是针对有对外操作或者表现的漏洞进行加固修复，无法直接针对软件内部漏洞进行防护和补救。

本章主笔人员（按拼音排序）：

三六零数字安全科技集团有限公司 胡晓娜、李雅、冯飞

本章贡献人员（按拼音排序）：

北京神州绿盟科技有限公司 许伟强、李瀛

北京天融信网络安全技术有限公司 黄栋

杭州安恒信息技术股份有限公司 韩潇

恒安嘉新（北京）科技股份公司 李蓉、王泽政

江苏云涌电子科技股份有限公司 刘少鹏

苏州市立医院 柳维生

北京安普诺信息技术有限公司 张荣香、子芽

17 安全管控

安全管理和策略控制中心，既是安全业务的综合管理中心、策略控制中心，也是系统性安全风险的威胁感知中心、态势分析中心，同时还是全局性安全管控的决策研判中心、指挥调度中心，从而形成对安全、可信、合规能力进行综合管理、融通协同、一致行动的安全管理中心。

17.1 安全管控的技术创新成果全面开花

17.1.1 从安全业务的视角看

以人工智能、大数据、云计算、边缘计算等为代表的新技术带来企业业务发展的新模式。远程办公、业务上云以及无边界网络设计已成为近期的发展趋势。从安全业务的视角来看，安全管控逐渐演变为人员、技术和流程有机结合的复杂系统工程。国内网络安全厂商提出了综合管控的技术路线，通过为管理员提供一体化的安全管理门户，实现安全运维人员、工具和运营流程相结合的目标，为安全管理工作提供了技术、管理、服务资源上的支撑。创新产品和解决方案包括：基于 SOAR 实现安全策略的自动化编排系统、安全运营业务流程管理系统、覆盖全局视角的安全运营中心、基于管理体系与服务体系相融合的集中管控平台等，在金融、能源、运营商、公安等行业领域获得了广泛应用。

17.1.2 从系统性安全风险的视角看

随着攻击手段的不断变化，高级持续性网络安全攻击层出不穷，信息安全正在成为一个需具备全局视角的大数据分析问题，需要汇聚网络中所有安全事件信息、威胁信息以及相关数据，结合知识库和情报库，快速准确地发现网络异常和高级威胁。具备系统性的安全风险威胁感知、态势分析能力的

全局性解决方案，成为众多企业打造整体网络安全防御体系的首选。首先，从威胁感知技术来看，由传统的关联分析向智能分析、知识图谱、ATT&CK建模框架等技术综合应用，实现安全威胁高检出率、低误报率；其次，从态势分析维度来看，逐渐引入了安全知识图谱、网络空间地理学、数字资产测绘等技术，利用知识图谱技术关联多源数据，提供资产风险分析、威胁场景分析、威胁情报分析、态势可视化分析等多维度安全分析，实现安全威胁的可视化推理溯源，并进一步实现更高维度的“挂图作战”应用。

17.1.3 从全局性安全管控的视角看

从全局视角看，安全管控体现为决策研判中心和指挥调度中心。为了实现全局性的决策研判和指挥调度，需要构建多层级的统一管理场景，打通上下级之间的管理数据实现安全策略的统一制定和统一下发，同时能支撑上级单位对下级单位安全管理执行情况的监督考核。在指挥调度和应急处置方面，需要整合各级力量、优化多方资源，实现信息互通、资源共享、优势互补，高效应对各类突发安全事件。国内安全厂商在多层级安全管理架构的基础上，构建了以‘培训 - 预案 - 演练 - 指挥调度 - 结果处置’为核心的应急处置框架。相关负责人基于指挥调度功能，能够实现监控应急任务的执行状态，向应急人员实时下发指令，全局跟踪处置进展等目标。

17.2 安全管控解决方案在各行业的应用范围逐步扩大

17.2.1 从安全业务的视角看

近年来，各行业安全建设逐步从传统的“烟囱式”向集中化的安全管控转变。以铁路系统为例，随着铁路信息化应用面向互联网的开放，建设覆盖云、网、边、端、应用以及数据的综合安全管理体系，对全路各个层面的风险及威胁进行实时采集、感知及预警迫在眉睫。相关单位在安全厂商的支撑下，

横向涵盖互联网、外网及内网（含安全生产网），实现对整个铁路网络安全的总体风险预测及控制、安全态势感知平台与集中安全管理平台之间形成有效联动。

医疗行业逐步形成了以地方卫健委为核心的纵向网络与信息安全管控机制，建设了涵盖态势感知、预报预警、应急处置、督促整改等应用，通过SOAR 等技术实现了对下属医疗单位安全策略的管理，对重要网站安全的集中管理、批量处理、自动化安全监测，最终形成区域级安全威胁综合管理、安全策略规范化统一。

国家应急管理部在相关安全厂商的支撑下，利用互联网数字资产测绘技术，对全国网站漏洞不间断监测，实现网站和系统的全局审计和综合分析，达到了全国性的互联网安全态势综合管理目标。

17.2.2 从系统性安全风险的视角看

中国人民银行科技司在 2019 年 8 月正式下发了《金融行业态势感知与信息共享平台数据接入标准说明》，要求全国各金融单位“与人行进行安全事件数据对接，实现对行业内安全信息的总体监测、对态势数据的综合分析，建立上下统一调度的指挥平台，帮助成员单位快速共享情报，形成对行业内安全资产的风险管控”，并在 2021 年进一步加大数据的对接范围和情报共享等建设要求，初步建成了覆盖全行业的安全数据共享、安全威胁感知、安全态势分析的纵向级联体系。

在可预见的未来，会有更多的行业主管部门强化网络安全顶层设计，通过建设行业内部安全威胁信息的共享、安全能力的级联赋能，推进网络安全业务一体化建设工作。

17.2.3 从全局性安全管控的视角看

近年来，包括政府、金融、运营商、交通、能源在内的多个行业主管部门越来越重视打通行业内部数据孤岛，希望通过数据上报、情报下发形成行业合力，发挥行业主管部门的协调指挥作用。

在政务网络安全建设中，中国信息协会在2019年7月发布了《政务网络安全监测平台总体技术要求》（团体标准），要求各级政务网络安全监测平台“通过协同服务系统实现总体态势、告警日志、威胁情报、认证、报表等数据的级联对接”。

在水利系统，某省级水利部门在国内安全厂商的支撑下，采用多层级安全管理架构，部署实施了等保安全管理中心解决方案，通过部署集中管控平台，实现泵站本地化安全管理；同时在省调水中心部署管理中心平台，实现统一规范的安全管理和策略下发。

17.3 安全管控需要在四个方面持续发力

当前是“十四五”开局之年，网络安全管控技术的发展应遵循习近平总书记提出的网络安全发展的根本原则，贯彻落实《网络安全法》等法律法规和《网络安全等级保护基本要求》等标准规范的要求，紧扣《“十四五”国家信息化规划纲要》，在总体思路上可以把握以下三点：

一是持续技术创新。当前国际社会风云变幻，网络安全风险层出不穷，网络攻击手段千变万化，给网络安全管控技术提出了更高要求。未来，网络安全管控的能力建设要善于运用大数据、云计算、区块链、人工智能等前沿技术，以数字化运营管理中心为目标导向，构建统一网络安全运营管理策略，实现系统运行与管理服务过程的全面管控，切实支撑好网络安全监测、信息共享和通报预警、应急处置、考核评价、指挥调度等具象工作。

二是强化体系框架。从国家到地方的“十四五”规划建议，都体现了网络安全保障整体思路的改变，就是从局部考虑到体系规划。未来，网络安全管控的发展要遵循“同步规划、同步建设、同步运行”的原则，加强顶层规划、顶层设计，利用系统工程的思想构建科学、可靠、可信的体系框架，把网络安全管控理念有效有力地嵌入信息化建设的每一个环节，切实提升信息系统的安全防护水平。

三是夯实自身安全。在使用网络安全管控技术、运行管控平台的同时，运营者要充分认识到自身的网络安全责任和义务，要坚决落实各项法律法规和技术标准规范的要求。作为安全数据的中心，要加强数据收集、汇聚、存储、流通、应用等全生命周期的安全管理，建立健全相关技术保障措施，建立数据分类分级管理制度等，同时要强化自身的数据安全风险评估、监测预警、检测认证。

同时，我们要充分认识到，在“十四五”发展期间，网络安全也将从专业建设逐渐向学科建设转变，网络安全管控的技术发展也要生态化、标准化、学科化，需要领域内的各方协同共进，积极推进该领域的理论研究，加强共性基础技术交流，研究制定相关技术标准，探索构建人才培养机制，共建良好的协同创新环境，才能切实建立适应新时期下信息系统网络安全管控体系。

本章主笔人员（按拼音排序）：

南京联成科技发展股份有限公司 戴凯乐、凌飞

杭州安恒信息技术股份有限公司 聂桂兵

本章贡献人员（按拼音排序）：

北京东方通网信科技有限公司 韦凯

广东安证计算机司法鉴定所 钢锋、黄伟杰

山石网科通信技术股份有限公司 邱石

上海算石科技有限公司 王亮

上海众人智能科技有限公司 宋国徽

上讯信息技术股份有限公司 兰方、郑丹云

浙江远望信息股份有限公司 陈旭、卢普明、周征宇

18 终端安全

虽然当前的国产化终端安全产品和技术成熟度尚与 Windows 和 Linux 等基于 Intel、AMD 芯片组的传统平台的整体防护方案相比还有一定差距，但已逐渐步入成熟阶段并从被动防御转向为主动、自适应的防护。目前市场上适用于国产化平台的终端安全产品，主要功能包括安全登录、防恶意代码、主机监控与审计、打印刻录监控与审计等。这些产品基本上支撑了集防护、检测、响应、恢复于一体的终端安全防护体系的建设。

18.1 自主创新的终端安全防护体系已基本建立

18.1.1 移动终端安全

移动终端安全产品的国产化进程不断加快：在技术层面，全力支持操作系统、数据库的国产化，提升自主可控能力；在产品层面，构建移动终端安全闭环，规范 APP 隐私权限，保障用户个人信息安全；在应用层面，与物联网、车联网和工业互联网等应用场景紧密结合。同时，随着移动终端威胁的演变与迁移，移动终端安全从原本的个人终端安全保护，向着企业移动化管理的方向发展，进而向移动威胁态势感知演进。

目前产业界基本形成了以移动终端为基础的整体安全管控方案，主要包括针对移动终端的双域隔离系统和智能终端安全盒系统，通过安全隔离技术实现的个人和办公环境的隔离解决方案，基于国产密码算法的终端业务系统和安全存储产品等，在满足多场景安全需求方面发挥了重要作用。

18.1.2 PC 终端安全

在技术层面，把大数据和人工智能技术引入国产终端安全防护，针对系统环境打造专用反恶意代码引擎；在产品层面，通过云端查杀能力，执行恶

意样本快速鉴定，增强恶意代码的查杀效率；在应用层面，在多级部署架构下可以实现跨区域终端的管理，实现账号、权限的按需划分，版本升级和病毒库升级同步管理。

18.1.3 服务器终端安全

服务器终端安全产品正在向持续化、自动化、灵活化方向演进，针对国产终端系统环境，不断融合新兴技术，进行技术创新，并在产品能力上取得突破性进展，可为各类用户提供持续可靠的安全防护能力。在技术层面，已向云工作负载保护平台（CWPP）方向发展，进入了与多云架构全面适配阶段；在产品层面，向检测响应、隔离控制、行为检测等方向发展，在满足合规基线的基础上不断细化资产清点颗粒度，深化信息关联能力；在应用层面，持续安全运营、监测与响应、稳健灵活部署等成为方案重点，并为用户呈现态势可视的交互效果。

18.1.4 终端准入控制

终端准入控制已成为保证企业网络边界完整性、提升内网安全性的主要技术手段。目前第三代技术架构 Appliance-base NAC（单台设备实现准入，采用 PBR、MVG 等技术），由于其对接入控制设备的要求和依赖性较低，部署更加灵活，成为目前市场上主流的方案。该方案可以在很大程度上防止终端私自接入；可以灵活适配企业各种场景下的防终端私接需求；通过 SDN 技术联动接入交换机、路由器动态调度终端网络策略，可以实现终端策略的随行随动，满足灵活多变的业务要求。

18.1.5 终端系统加固

终端系统加固的主要目的是确保系统状态不被篡改、安全机制不被绕过。

主要的加固方案包括：一是基于可信计算 3.0 的主动免疫防护机制，对信息系统中运行的应用及其行为进行管理，确保仅有经过可信度量的代码能够运行，为系统上层安全机制提供基于硬件的密码保护；二是通过预验证安全访问控制（基于影子存储空间启动技术和多因子验证技术）的自加密固态硬盘和终端安全软件形成互补，避免通过拆盘、PE 光盘启动等手段绕过操作系统的验证从而获取硬盘数据的情况。

18.2 终端安全产品在各行业领域广泛使用

18.2.1 移动终端安全在警务领域的应用

在智能手机的基础上，基于密码芯片的定制智能终端，已经基本具备了满足电子政务移动办公需求的条件。以移动警务为例，通过定制警务通终端产品和安全接入等产品构建的移动警务平台，目前已经完成省级的移动警务平台建设，能够支撑现场执法和移动办公业务。智能终端安全方案也将逐步推广到检察院、法院、国税等相关部门。

18.2.2 PC 终端安全在政法系统的应用

通过将终端安全登录、防病毒、主机监控与审计、打印刻录监控与审计系统联动组合，实时监测终端状态，对内网终端系统安全风险的不间断的评估和控制措施调整，实现对终端的安全状态可视、安全风险可控，完成了整体终端安全体系建设。最终效果体现在建设了相对完备的终端安全管理体系，推进了安全事件管理规范化。

18.2.3 服务器终端安全在保险行业的应用

为解决用户在服务器终端安全层面缺少快速、集中的资产和风险管理手段，安全运营工作的推进缺乏技术层面的保障和审核能力等问题，构建一套

集中化、高效化服务器终端安全分析平台来处理繁杂的安全应急和安全管理工作。

18.2.4 哑终端准入控制在金融行业的应用

海量哑终端的管理和安全问题已经不容忽视，但常规的 PC 端的管控方式并不适用于哑终端类的管理。哑终端管理可实现终端智能发现、指纹级终端识别、全面资产管理等功能，提供终端统一安全接入认证、审批入网等安全功能，全面保护网络边界接入安全。相关方案已在某银行获得了使用。

18.2.5 可信计算 3.0 在电力行业应用

基于可信计算 3.0 技术实现对核电工控系统中 PLC、工作站、办公终端、安全边界设备等基础设施的可信构建，一方面对已有产品设备进行可信改造，另一方面在我国自主可控的核电工控系统中深度植入免疫机制，逐步采用国产自研的系统设备进行替代。同时根据“一个中心”管理下的“三重防护”体系框架，形成适用核电工控系统的纵深防御体系。

18.3 推动终端安全自主创新

终端安全是一个不断演变的领域。随着网络应用越来越广泛，固定终端和移动终端的应用发生了极大的变化，终端威胁形态也不断进化，黑名单、白名单等基于签名机制的防护手段在应对高级威胁时逐渐失效，终端安全威胁的复杂化正驱动终端安全技术向主动防御和威胁情报阶段演进。

未来网络安全态势愈发严峻，以传统模式规划和建设的网络安全体系存在的碎片化严重、协同能力差、弹性恢复能力严重缺失等弊病将被剧烈放大，达不到保障数字化业务发展的高标准要求。因此，终端安全需要与业务实现紧耦合，通过融合创新，促进可持续发展：一是将风险可视化作为重点，让

管理人员能够清晰的看到风险在哪、严重程度如何、整体安全防护效果的评估等管理信息，而不是技术数据细节；二是将业务和安全结合，从用户业务角度出发，将安全管控机制融入到业务当中；三是探索构建上层管理接口和底层技术接口的统一。这样既实现了安全防护，又不影响业务操作习惯，并且还能提供充分的管理效果、展示数据，将有利于提升终端安全行业的力量凝聚力。

本章主笔人员（按拼音排序）：

北京升鑫网络科技有限公司 卢动熠、陶臣

本章贡献人员（按拼音排序）：

北京可信华泰信息技术有限公司 杜君、王杨

北京天融信网络安全技术有限公司 张帅

杭州安恒信息技术股份有限公司 何柏宜

杭州盈高科技有限公司 张艺虹

湖南国科微电子股份有限公司 邓博

江苏云涌电子科技股份有限公司 陈凯迪、焦伟

迈普通信技术股份有限公司 袁懿

奇虎 360 科技有限公司 潘颖

上海上讯信息技术股份有限公司 韩璐

上海算石科技有限公司 李如前

郑州信大捷安信息技术股份有限公司 梁松涛、刘为华、刘献伦

19 云计算安全

与物理网络一样，云计算业务环境也同样需要网络和主机两个技术栈的安全产品。不同的是，传统网络安全产品多是硬件形态，无法直接部署到云计算环境中；另外，传统主机防病毒产品大多不适合直接部署在云主机上。尤其到了容器业务环境，传统的主机安全产品方案并不适应。在过去三年里，国内云计算安全厂商配合云计算业务用户基本上完成了传统安全产品和技术向云的演进，并在不同行业和不同业务场景下得到广泛应用。同时，新的场景和业务需要新的云安全产品和技术，云工作负载安全、云原生安全、云数据安全等成为国内未来几年云安全领域的主流发展方向。

19.1 传统安全产品和技术向云的演进基本完成

19.1.1 云网络安全

由于云网络的虚拟化，云租户无法再部署传统硬件网络安全设备来保护自己部署在云上的服务，云租户又需要继续在云上使用网络防火墙、Web 应用防火墙、入侵防御、防病毒、虚拟专用网、漏洞扫描、堡垒机、数据库审计、日志审计等产品和服务。为了满足用户在云上继续使用网络安全设备的需求，从 2013 年开始，国内主流安全厂商就开始提供虚拟化的网络安全产品。近三年来，国内绝大部分的传统网络安全厂商都已经完成了硬件网络安全产品的虚拟化，不仅能够提供单品的虚拟化安全网元供用户在公有云的 VPC 上使用，帮助云租户继续按照传统物理网络安全设备的使用习惯来为自己在云上进行网络安全建设，部分厂商还推出了安全资源池的解决方案。

随着 SaaS 化网络安全服务需求越来越迫切，从 2019 年开始，华为云、阿里云等云平台厂商已经逐步开始向云租户提供内置的网络安全能力（如防火墙、入侵防御等），并在向更多自研或者集成第三方安全能力的方向迈进。

由于网络安全产品的碎片化和客户需求多样化，网络安全厂商向云租户提供虚拟化的网络安全产品和方案与云平台厂商内置提供的安全产品和方案会长期共存。

19.1.2 主机安全

云租户的主机安全需求不再像传统 PC 机上主要以病毒防护为主，新的安全需求包括网络微隔离、漏洞管理、基线核查、入侵防御等。

网络微隔离是云环境中区别于传统物理网络的安全需求。在传统物理网络中，不同网络之间甚至是相同二层网络域内的服务器之间都有明确的物理边界，方便部署安全防护设备。在虚拟化网络中不同子网之间或者相同子网内，租户无法在云主机前再串入虚拟化安全防护设备。这就导致云租户内部东西向流量缺乏访问控制和可视化的安全能力。为了满足云主机的微隔离需求，从 2015 年开始，国内部分安全厂商开始为云计算环境提供微隔离网络安全产品，有基于虚拟交换机引流方式的网络防火墙方案，也有采用在云主机中安装 Agent 软件的主机防火墙方案。

由于云主机基本是作为服务器来使用，需要考虑资源的占用率，传统 PC 机的防病毒软件产品并不能很好的适用于云主机环境。另外，传统 PC 机上的恶意软件跟服务器上的恶意软件很多是不一样的，服务器上更多要做合规基线核查、主机漏洞扫描、入侵检测和防御、后门木马僵尸网络勒索等恶意软件的查杀，以及进程文件操作行为的学习和监控。目前国内多数安全厂商在云主机安全方面都能够提供相应的产品和解决方案。

19.1.3 容器安全

虽说容器安全技术属于主机安全技术范畴，但是传统主机安全产品方案并不适应容器业务场景，主要问题有三点：一是传统主机安全产品的终端代

理软件需要手动安装部署，对于有大量计算节点的容器业务环境，工作量很大且也不能自动跟随容器计算节点扩容；二是传统主机安全产品通常没有对接容器编排管理平台，对监控到的主机安全事件不能匹配到容器资产上，也不能围绕容器资产进行安全策略管理；三是容器镜像漏洞扫描和容器平台合规检查等技术超出了传统主机安全的技术范畴。

国内容器安全厂商主要参考了 Gartner 的容器安全控制分层体系，产品能够提供容器镜像安全、容器引擎和编排管理平台安全、容器网络安全、容器应用安全等多种安全防护能力。一些容器安全厂商在产品架构上，采用分布式安全容器 + 集中管理的方式，其中分布式安全容器在 Kubernetes 下以 Daemonset 形式部署，这样就能直接利用 Kubernetes 对安全容器直接进行扩缩容和状态监控以及故障恢复。领先的容器安全厂商甚至使用云原生技术来构架自己的容器安全产品，这是安全技术和 IT 技术走向融合的大趋势。

19.2 云安全产品有力地支撑了等级保护建设

19.2.1 云网络安全

云网络安全最大的应用场景是满足等级保护的合规要求。根据相关标准的要求，云租户业务系统和云平台采用分开定级的方式，其中云平台和云租户业务系统测评不仅需要满足安全通用要求还需满足云计算扩展要求。针对云平台的等级保护建设，云服务商需采购传统硬件安全产品去满足安全通用要求部分，而云计算扩展部分要求需要云服务商与第三方安全厂商共同完成。

无论是公有云、私有云还是行业云的安全建设，主要是向租户提供网络防火墙、Web 应用防火墙、入侵防御、防病毒、虚拟专用网、漏洞扫描、堡垒机、数据库审计、日志审计等产品和服务。公有云上以直接向云租户提供

SaaS 化网络安全服务为主；私有云和行业云主要是向云租户提供网络安全厂商的虚拟化网络安全产品，其中安全资源池的解决方案能够给云租户提供更多的易用性和便利性。

19.2.2 主机安全

云主机安全的应用主要是为了满足等级保护合规要求，如云计算安全扩展要求中安全区域边界的入侵防范部分明确要求应能检测到虚拟机与虚拟机之间的异常流量，并应在检测到网络攻击行为、异常流量情况时进行告警。无论是公有云、私有云还是行业云，通常云租户都要采用网络微隔离产品来满足这样的合规要求。基于虚拟交换机引流方式的虚机网络微隔离产品多应用于私有云，基于云主机中安装 Agent 软件的方式多应用于公有云和混合云。

19.2.3 容器安全

我国容器云的主要应用领域包含金融、互联网、运营商、制造业、能源等行业，其中金融和互联网行业对网络服务质量的要求较高。容器安全跟随容器云的应用而逐步开展，目前金融行业已率先投入容器业务的安全建设；运营商紧随其后，除了在 5G、边缘计算等技术规范中提出了容器安全的要求外，在自身的 IT 云安全技术规范中也做出了明确规划并逐步建设落地。

19.3 新的场景和业务需要新的云安全产品

19.3.1 云工作负载安全

云工作负载安全将是国内未来几年云安全的主流发展方向之一。云工作负载安全从云主机安全演进而来，主要强调跨混合异构环境的主机安全能力。混合异构环境包括物理机、虚机、容器，主机安全能力包括合规检查、漏洞

管理、网络微隔离和可视化、应用控制（白名单）、入侵防御、病毒防护等。可以看到云工作负载安全基本上覆盖了主机安全的功能和场景。虽然网络安全厂商把硬件网元都进行了虚拟化，但虚拟化网元在云中的部署和组网给租户管理员带来很多的工作。尤其是网络防火墙等需要流量串行经过的网元，部署难度很大。对于云租户东西向流量的微隔离需求，网络防火墙等网元在很多云环境中找不到合适的部署方案。在这种情况下，云主机中安装 Agent 软件的方案由于同云平台和虚拟化网络无关，因此深受青睐。

19.3.2 云原生安全

云原生安全是国内未来几年云安全的主流发展方向之一。在传统主机和网络安全场景下，安全跟业务一直都是相互独立的，而云原生安全要求安全能力跟随云原生业务流程开发、部署、运维的每个阶段。云原生安全从容器安全演进而来，强调面向云原生应用开发和生产的一整套安全和合规能力。其主要是面向Kubernetes的容器全生命周期的安全能力,包括合规检查(Linux 主机、Docker、Kubernetes）、容器网络微隔离、容器镜像漏洞扫描、容器镜像软件成分分析、基于容器应用行为的控制（进程、文件操作）、容器 Web 应用防火墙（应用层访问控制）等，另外云原生安全更注重安全左移（代码安全）。

19.3.3 云数据安全

近年来云计算市场规模持续增长，但数据泄露等安全事件频发。一方面，云环境中的实体（云服务提供商、云用户、第三方审计者、外部攻击者等）可能给云环境带来数据安全风险；另一方面，在云环境中的数据安全体制还有待完善，主要表现在静态防护策略无法保护数据安全、数据资产的权责不一致等。云数据安全将是国内厂商在未来重点关注的主流发展方向之一。

本章主笔人员（按拼音排序）：

北京山石网科信息技术有限公司 任亮

精壹致远（武汉）信息技术有限公司 陈强、赵泉城

本章贡献人员（按拼音排序）：

北京长亭未来科技有限公司 王兆蒙

北京神州绿盟科技有限公司 刘丽

北京升鑫网络科技有限公司 卢动熠、陶臣

北京天融信网络安全技术有限公司 夏威

北京信安世纪科技股份有限公司 陈晓萍、何秀峰

北京有略评测技术有限公司 颜佳威

北京中船信息科技有限公司 张德胜

湖南麒麟信安科技股份有限公司 孙利杰

启明星辰信息技术集团股份有限公司 郭伟华、田建丽

中国软件评测中心 李安伦、田峰、万晨阳

20 数据安全

过去三年，受益于数字经济的蓬勃发展以及政策因素的导向作用，国内在数据安全领域多个技术方向上取得了相对较为明显的进展，很多新技术与传统数据安全产品相融合，数据安全产品和服务在各领域的应用程度逐渐升高。

20.1 数据安全厂商在多个专项技术上不断深挖

20.1.1 数据加密技术日趋精细化

随着云计算、人工智能等技术的应用以及计算机系统性能的提升，各领域业务场景对数据加密的需求逐步细化。国内数据安全厂商立足国产密码算法，将加密技术与数据安全场景进行结合，推出了创新的产品和解决方案，如：电子签章、加密机，文档密标系统、数据安全传输系统、隐私数据保护网关、主机加固、区块链存证等，在金融、医疗、能源等行业获得了广泛应用。

20.1.2 数据防泄漏技术走向智能化

为了更好地满足监管要求，数据防泄漏技术开始跳出固有框架，寻找新的技术路线。首先，从检测技术发展来看，由传统的基础检测技术向高级检测技术（精确数据比对、指纹文档比对、向量分类比对）演进，提升了检测效率、准确率，同时也增加了数据适应类型。其次，从数据加密技术发展来看，加密技术经历了单缓存过滤驱动技术、双缓存过滤驱动技术和虚拟文件系统技术三个阶段。国内数据安全厂商将虚拟文件系统技术应用于数据库加密，提升了数据库加密性能，细化了管控粒度。第三，从管控细粒度来看，内容识别技术开始全面应用于数据防泄漏领域。此外，麒麟信安独创透明应用适配技术与不同应用场景进行对接，创新性地实现了对 OpenStack 云平台、

K8S 容器云透明加密存储，成功解决了云平台虚拟机数据安全存储问题。

20.1.3 敏感数据识别精度不断提高

敏感数据识别技术早期主要应用于数据防泄露领域，现已成为数据防泄露、数据分级分类管控和敏感数据加密、数据流转溯源等数据安全防护技术的基础。国内数据安全厂商在传统关键字识别的基础上，引入了规则匹配、自然语言处理、机器学习、内容识别、流量深度分析等技术，提升了敏感数据识别精度及智能化程度。

20.1.4 数据分类分级趋向自动化

数据分类分级是数据安全建设的起点，是国内外数据安全厂商研究的热点问题。国内数据分类分级标准逐步走向行业细分，为数据分类分级自动化实施奠定了坚实的基础。相关厂商从行业和法律法规两个维度研究形成了数据分类分级自动化模板，并应用于相关产品，提升了数据分类分级自动化程度。

20.1.5 数据脱敏技术逐渐成熟

数据脱敏技术主要被用于保护个人隐私数据。相关解决方案已经广泛应用于政务、金融、电信、互联网等行业领域。一是在大规模数据脱敏需求下，脱敏性能不断提高；二是脱敏数据类型由结构化向非结构化发展；三是内容识别技术取得了较好的应用；四是智能化程度越来越高；五是与各行业数据安全防护标准结合越来越紧密。

20.1.6 数据安全统一管控能力深入业务流程

在数字化改革背景下，信息技术、数字化技术与业务深度融合，使数据

安全风险更具有实质性的影响，数据安全问题成为数字化改革能否持续发展的重要因素。数据安全统一管控平台为数据一体化安全管控机制提供了一个全局的安全视角，将数据安全管控措施融入到业务流程和数据全生命周期，实现数据安全合规检测与响应常态化、数据资产分布与流动可视化、数据安全风险可测可控，并提供相应的预警及应急响应等支撑服务，可逐步提升数字化改革背景下的体系化数据安全能力。

20.1.7 动态生物识别技术开始兴起

随着疫情防控常态化，人脸识别技术得到大量应用，但也进一步引致了公众对于个人隐私泄露的担忧。国内主流厂商的研发路线开始从单纯追求快速、准确，向更注重隐私保护和数据安全演进：一方面，大幅提高识别精度并加入活体检测模块；另一方面，基于声纹、步态等动态行为特征的生物识别技术开始兴起。目前，声纹识别系统已被列入首批金融科技产品认证目录。

20.2 数据安全技术与多个行业领域的业务场景深度融合

20.2.1 促进医疗行业数据互联互通

随着电子健康卡的普及，电子健康档案共享成为“互联网 + 医疗”的重点应用场景之一，有关部门连续 5 年发文推动健康档案电子化和互联互通。目前，基于零信任架构的电子健康档案共享平台已开始在部分地区开展试点。该方案采用国产化版式 OFD 技术与数据安全技术，提供基于国密算法的文件标识和内容访问授权、基于索引的统一文件管理、无插件无留痕的安全在线阅览、移动互联网跨渠道分享、海量小文件的安全版式存储等创新性安全功能，为电子健康档案的生成、纳管、阅览、转换、存储、分享、授权、溯源提供全生命周期支撑能力，保证电子健康档案的真实性、完整性、安全性。

此外，在新冠疫情期间疾控数据安全报送体系发挥了重要作用。该方案基于国密算法确保报送数据在全生命周期的完整性和报送行为的不可否认性。

20.2.2 护航数据跨境传输安全

随着国家对个人信息和重要数据出境的安全管控不断加强，做好数据资产出境管理和安全防护工作，解决跨境数据的安全管控问题成为业界关注的新的焦点。数据安全厂商基于“整体性、关联性、合规性、价值性”原则，从“数据的全跨境过程”着手，综合运用数据防泄漏技术、数据脱敏技术、敏感数据识别技术等技术手段，对数据进行集中化、全过程管理，形成了立体、多维的数据管理和安全防护体系，在保障跨境数据的安全方面发挥了作用。

20.2.3 支撑运营商数据安全管控

运营商平台数据类型多、数量大，数据资产梳理困难，因此敏感数据难以得到很好地保护。针对这一问题，相关厂商基于敏感数据自动识别技术构建了数据安全管控平台：首先对收集到大数据平台的数据进行自动扫描、分类分级，为后续的数据脱敏、重点日志审计、安全态势感知提供基础。然后利用暗水印技术，为出平台的文档、结构化数据提供溯源能力。最后开展血缘分析和血缘信息存储，绘制用户画像与应用程序行为轨迹，为平台监测预警与用户行为溯源的实现提供技术支撑。

20.2.4 保障金融行业文档管控

近年来，金融监管机构出台了一系列文件，要求切实做好文件管控工作。世平信息基于数据分类分级管理，通过标记水印的方式提出了金融行业文档管控解决方案，对综合办公平台上的电子文档进行精准管控和溯源，减小文档扩散的风险，规范内部数据的使用。

20.2.5 保障政务领域数据安全合规

数据安全统一管控平台在政务领域发挥了一定的作用，实现了数据的统一管控，确保了归集数据的合法、合规，针对网络中传输的数据提供敏感内容识别、定位和实时预警，实现了流转监控。数据安全统一管控平台支持安全事件统一汇总上报，结合分析模型对数据安全进行预测和趋势分析，对安全事件进行分析展示，为网络运营者提供了决策依据。

20.3 数据安全需要与业务场景实现紧耦合

在数据安全领域，相对于法律法规的日益完善，技术标准、评估手段、产品和解决方案还有所欠缺：一是数据安全管理和评估标准不齐，导致某些行业在数据安全建设过程中，数据分类分级和风险评估工作推进起来面临阻力；二是数据使用场景日益复杂，急需新技术、新产品填补市场空白；三是大量老旧业务系统数据安全改造面临难题，需要创新的解决方案。

为了解决上述问题，在标准建设方面，需要结合行业特点，进一步细化数据分类标准，同时在数据安全风险评估关键、数据安全产品测试等方面尽快推出和完善标准体系，指导当前数据安全建设和产品研发工作。在技术研究和产品研发方面，需要转变传统的游离于业务之外的方式，推动数据安全技术与业务场景实现紧耦合，基于“面向切面的数据安全”理念探索新的方向；另外针对加密流量进行分析与建模，将会是未来数据安全技术发展的热点。

本章主笔人员（按拼音排序）：

北京中安星云软件技术有限公司 郑金、赵卫国

本章贡献人员（按拼音排序）：

北京得意音通技术有限责任公司 成舸、邬晓钧

北京炼石网络技术有限公司 刘晓光、张齐军

北京山石网科信息技术有限公司 钱贵涛

北京神州绿盟科技有限公司 王晓丹

北京天融信网络安全技术有限公司 张志颖、包英明

大庆中基石油通信建设有限公司 刘玮、桑圣洁、王春伟

广东安证计算机司法鉴定所 魏智煌

杭州安恒信息技术股份有限公司 聂桂兵、周芊芊

杭州世平信息科技有限公司 王世晞、张翠

恒安嘉新（北京）科技股份公司 许道远

湖南麒麟信安科技股份有限公司 彭勇、申锟铠

华北理工大学 陈学斌

江苏云涌电子科技股份有限公司 李天聪、黄婉静

三未信安科技股份有限公司 张驰

上海观安信息技术股份有限公司 胡芳

上海众人智能科技有限公司 张力强

深圳昂楷科技有限公司 蔡庆潤、郭小天

深圳市安证保全数据处理有限公司 陈东铉

深圳市安证区块链技术发展有限公司 江鑫

深圳市网安计算机安全检测技术有限公司 王水兵

友虹（北京）科技有限公司 黄岩、张升平

浙江华途信息安全技术股份有限公司 叶俊卫

中国移动通信有限公司研究院 何申、粟栗、杨亭亭

21 工控安全

近年来，随着工控安全顶层设计的不断加强，我国在工控安全管理体系、技术保障能力、产业规模结构等方面取得重大进展，涌现出了一批成长性高、创新能力强的企业。从产品上看，国内工控安全厂商普遍提高了对国产基础软硬件适配的重视程度，大量基于自主核心元器件的产品面市；从技术上看，可信计算开始与工控安全场景结合，在部分行业领域发挥了重要作用。

21.1 工控安全产业开始注重国产化问题

21.1.1 传统工控安全产品的国产化改造

近年来，我国工控安全产业规模不断攀升，产品以工业防火墙、工业网闸、主机加固、应用白名单、工控安全态势感知和监测系统为主，各个行业对工控安全产品的国产化要求不断提高。

国内工控安全厂商开始关注基于国产基础软硬件的产品开发工作，工控安全硬件平台开始从非国产向全国产的升级，自主创新的处理器、操作系统等核心组件在工控安全产品中的使用比例逐年上升，工业防火墙、工业领域的主机安全监视软件、自研专用安全操作系统、基于国产硬件和密码模块的安全管控设备等多种形态的安全产品大量出现并应用于军工、电力、能源、制造业等行业领域。

21.1.2 可信计算技术与工控安全需求深度融合

工控系统属于“生产型信息系统”，具备应用场景单一、版本相对稳定、升级周期长的特点。因此，可信计算技术与工控系统有着天然适配性。近年来，国内从事可信计算的厂商开始关注可信计算产品和解决方案在工控领域的应用。电力网络安全隔离装置、纵向加密认证装置、可信主动免疫防御系

统等在工业控制系统中发挥了重要作用，使工控系统拥有自免疫能力，保障其免受被未知漏洞、未知病毒、未知木马攻击而造成的风险，解决勒索病毒、幽灵、熔断等安全威胁。

21.2 国产化的工控安全产品在电力和制造业获得应用

在传统工控安全产品方面，国内厂商基于国产基础软硬件的工控安全产品在电力行业部分场景获得较为广泛的应用，在制造业也有应用。全国产化的隔离、加密、数据采集等产品和解决方案在电力二次安防系统有广泛应用；主机安全监视软件至今已在电力生产控制领域上线运行 6 万多套，7x24 执行设备安全监视；数控机床防护设备在军工行业进行了试点部署，降低了外界对数控机床系统环境的侵犯和内部数据外泄等风险。

在可信计算产品方面，以国家电网调度系统的可信计算项目为引导，可信计算产品与技术运用于新能源集控中心，通过部署于电力监控系统，使计算机信息系统拥有自免疫能力，以抵御未知恶意代码攻击，并且可实现与态势感知业务监控系统的数据融合。工控监测审计、入侵检测、工控防火墙、安全管理平台等方面的核心产品也逐步融入了可信计算技术，相关产品在电力、石油、石化、轨道交通、烟草、煤炭、钢铁及先进制造等行业均有应用。

21.3 工控安全产业需要进一步做大做强、做专做优

国内工控安全产业尽管取得了快速发展，但不可否认的是目前的产业规模仍然相对较小，产业内需亟待释放。存在的问题主要体现：一是工控安全防护体系建设长期以来受合规需求驱动，整体处于初级阶段，缺少体系化的安全规划和布局，对安全产品难以有效评估；二是工控安全市场竞争格局按地域和行业高度分散，产业规模整体处于低位，尚未形成骨干龙头企业，市场份额增长缓慢。

面对上述现状和问题，未来工控安全产业需要借助资本市场的力量，做大做强龙头企业，通过带动辐射作用引领产业发展。同时，第三方检测评估机构需要加快相关技术研究、技术标准制定和检测工具的改进，为工控安全特别是基于国产基础软硬件的工控安全产品建立技术有效、权威的评估手段，支撑行业快速、健康地发展。另外，中小企业要面向智能制造、工业互联网、工业大数据等新兴重点领域，深度聚焦、做专做优，打造拳头产品，做好优质服务，共同推动工控安全产业高质量发展。

本章主笔人员（按拼音排序）：

江苏云涌电子科技股份有限公司 方艳湘、黄婉静、练书成

本章贡献人员（按拼音排序）：

安天科技集团股份有限公司 王乃青

北京计算机技术及应用研究所 冯海楠

北京可信华泰信息技术有限公司 杜君、王杨

北京六方云信息技术有限公司 文武

北京珞安科技有限责任公司 门永超

北京神州绿盟科技有限公司 梁磐

北京天地和兴科技有限公司 刘乐农、覃汐赫

北京天融信网络安全技术有限公司 刘超

北京亚控科技发展有限公司 陈友越

北京中电瑞铠科技有限公司 冯坚

北京中科网威信息技术有限公司 李继磊、部云龙、吴磊

大庆中基石油通信建设有限公司 王柳青、王庆伟、宋小茜

国网智能电网研究院有限公司 王齐

杭州安恒信息技术股份有限公司 李显松

杭州立思辰安科科技有限公司 苗维杰

湖南麒麟信安科技股份有限公司 王攀

启明星辰信息技术集团股份有限公司 蒋发群

山东九州信泰信息科技股份有限公司 李龙飞

上海算石科技有限公司 黄坚会、李惠锋

长扬科技（北京）有限公司 赵华

浙江齐安信息科技有限公司 苏尧

中电智能科技有限公司 胡祥新、徐一凤

22 安全服务

近年来，国内网络安全头部厂商逐渐向安全服务倾斜更多资源。除了政策导向、法律法规的推进之外，日益增大的安全风险及自身安全需求也促使用户对安全服务的采购持续增加。尽管安全服务的市场不断扩大，网络运营者也越来越重视购买安全服务，但相对来说国内的网络安全服务还处于探索阶段。特别是针对自主创新的网信产品以及基于这些产品构建的信息系统，理论上存在更多未知安全风险，更需要针对性的安全服务来保障其安全稳定地正常运行。在这方面，安全服务还有很长的路要走。

22.1 安全服务仍处于探索阶段

22.1.1 安全服务的范围不断扩大

用户对安全服务的需求正在从过去的漏洞扫描、渗透测试、风险评估等专项服务向顶层建设升级，覆盖规划设计、实施建设及运行退网的全生命周期。在规划阶段，对自主产品进行可行性研究；在实施建设阶段，涉及方案评审、上线前安全评估、个人信息保护评估、数据安全评估、互联网新技术新业务评估、等级保护测评等；在运行及退网阶段，涉及漏洞扫描、渗透测试、基线合规检查、风险评估、符合性评测、应急演练、攻防演练、退网后安全检查、安全培训、安全咨询等。

22.1.2 针对自主产品的安全服务方兴未艾

自主不等于安全，自主产品存在安全缺陷是不可避免的。随着自主创新网信产品的广泛部署应用，其安全问题日益突显。为解决这一问题，各安全厂商从顶层设计到落地实施，形成了一套包括风险评估、用户个人信息保护合规评估、数据安全评估、等级保护测评、应急演练、安全规划及咨询、防

护有效性测评等服务项目的解决方案。不过由于各行业面临的风险和自身需求不同，自主产品安全服务还具有相当大的个性化因素，需要根据用户的特性制定适用的解决方案。目前各行业的自主产品安全服务解决方案已初显成效。

22.2 安全服务已在重点行业发挥作用

随着信息化水平的日益提升，各行业领域的网络架构和业务系统也越来越复杂，产品的优化也更为频繁。但随着能力模块的增多，网络风险也越来越高，安全服务是一个动态的、周而复始的、不断提升的过程，前置解决网络安全风险是安全服务的重点；同时需要从发现风险、呈现风险、处置风险、风险再评估各个阶段进行流程管控，形成事前预防、事中监控、事后审计的闭环管理。全方面提升企业整体网络安全防护水平。

安全服务产生的效益主要体现在以下三个方面：一是快速解决合规性问题，避免了由于安全措施落实不当造成的处罚；二是保障业务连续性，避免业务中断带来的经济损失；三是节省时间成本，实现网络安全事件快速定位和溯源，及时采取措施进行响应和补救。同时可以降低管理和人力成本。

22.3 安全服务需要加强能力建设

22.3.1 提高针对自主产品的安全服务能力

相对于国外成熟产品，自主产品本身可能存在更多未知漏洞。基于自主产品构建信息系统将导致脆弱性倍增，这是自主产品面临的一个挑战。而目前主流的漏洞披露渠道较为繁杂，且多为安全厂家设立。因此，需要加强针对自主产品的漏洞分析工作，建立规范的漏洞信息接收、处理和发布流程，建立信息通报、披露、共享、报告机制和统一汇聚渠道。强化自主产品漏洞

收集验证、安全风险感知、处置监督等方面的协同。加强网络攻防专业力量建设，建立自主产品的安全研究团队，建设网络安全靶场，打造自主产品的网络安全“演兵场”，常态化开展网络安全攻防演习，通过攻防实战来发现短板，增强网络攻击的发现和反制能力，健全自主产品网络安全攻防对抗机制，全面提升自主产品安全水平。

22.3.2 加强安全服务人才储备

随着安全服务市场的逐步扩大，网络安全人才需求快速扩张，安全管理型人才储备不足、专业人才流失、人才成长和培养落后于技术变革等问题日益凸显。导致这个问题的原因有二：一是安全技术能力分布失衡，相关人才主要聚集在各大安全厂商；二是人才供求地域失衡，网络安全人才多集中于北京、上海、深圳等一线城市；两者的根源问题为薪资水平和各地就业机会差异较大，各行业各单位对网络安全的重视和投入参差不齐。

为解决人才短缺问题，需要不断加强自主产品网络安全人才体系建设，按照“按需、分类、梯次”原则，加大自主产品网络安全人才培养，规范和鼓励社会力量、网络安全企业开展自主产品的网络安全人才培养。一方面，加强校企合作，支持高校与企业联合建设学生实训基地与企业培训中心；另一方面，建立自主产品网络安全专家智库，完善人才选拔、激励机制，形成专兼结合的自主产品网络安全教育师资队伍；同时，要推动开展网络安全人才能力评价，特别是针对自主产品的安全服务人员要做到持证上岗、规范上岗。

本章主笔人员（按拼音排序）：

重庆市信息通信咨询设计院有限公司 姜凌、张晓琴

本章贡献人员（按拼音排序）：

北京升鑫网络科技有限公司 林宝晶

北京有略测评技术有限公司 白晓贺

23 电子取证

随着信息技术的发展、普及和广泛应用，网络和电子信息技术已经被违法犯罪的各个环节所使用。这在一定程度上增加了执法单位进行电子数据取证的难度，从而催生出了电子数据取证的许多新场景。相应地，电子数据取证产品也快速发展并在实际工作场景中发挥了重要作用。

23.1 电子数据取证产品种类繁多、形态多样

目前，国内电子数据取证产品的种类可以分为手机取证、介质取证、网络取证、现场勘验、存证固证等，根据使用场景的不同，每类产品又可能具有多种产品形态。

23.1.1 手机取证

在手机取证方面，国内各取证厂商的产品主要包括手机综采、手机快采、手机云取证等。

手机综采产品主要用于案件中犯罪嫌疑人手机数据的综合提取分析，犯罪嫌疑人的手机作为案件线索的重要来源之一，对其综采取证能力的提高也将促进办案成效的提升。目前国内厂家的手机综采产品已经能够支持苹果、华为、小米、红米、VIVO、OPPO 等主流品牌手机共上千种机型的数据提取、删除恢复、密码绕过，支持获取数据的 APP 数量也增至 500 种以上，基本能够满足常见办案需求。

手机快采产品用于案件中受害人手机数据的快速定向采集，多用于电信诈骗类案件。各厂家的手机快采产品已经能够支持受害人人员信息和手机设备信息的采集，并能够快速提取受害人指定的与嫌疑人之间的通联记录，忽略受害人手机中其他与案件无关的个人数据，保护受害人隐私。同时，手

机快采设备通常还具有 APP 静态分析和动态分析的能力，通过对电诈相关 APP 的解析，实现对电诈团伙的追踪溯源。

手机云取证产品是手机综采和手机快采的补充。许多手机应用数据并非保存在手机本地存储中，而是保存在应用云端服务器中，手机云取证一般用于各类手机应用云端数据的下载固定。目前国内厂家的手机云取证产品主要支持云备份、银行、交易、购物、行程、邮件等类型应用云数据的取证，已经支持超过 100 款常用 APP。

23.1.2 介质取证

介质取证产品主要用于计算机、U 盘、移动硬盘等存储介质的数据提取和分析。在介质取证方面，国内各厂商已经能够较完整地提取常见存储介质和操作系统中的数据，能够实现磁盘镜像、磁盘分析、数据恢复等功能。介质取证工具通过将介质中的文件和数据进行分类和筛选，帮助取证人员高效地从大量数据中查找线索，相比国外的 X-ways、Encase 等取证厂商，国内厂商研发的介质取证产品操作简单、智能化程度高、对使用者技术要求低，更贴合国内取证人员的使用习惯。

23.1.3 网络取证

在网络取证方面，国内各厂商着眼于执法单位进行远程在线取证的需求，在服务器取证、网页取证、网络巡查等方面推出了成果。

服务器取证产品用于网络在线提取电子数据时对远程服务器的取证，主要针对服务器基本信息、网站、数据库、文件系统等数据进行取证，国内厂商研发的服务器取证产品具有远程磁盘镜像、内存镜像、数据库远程连接、网络抓包等功能，覆盖 Ubuntu、CentOS、Redhat 等 Linux 系统及各版本 Windows 系统。

网页取证产品专门用于远程固定网站及分析，适用于各种形式的网站和论坛。国内厂商开发的网页取证产品可以智能、快速地对数据量大、内容多、信息更新快的网站进行自动化处理，将网页按原样镜像到本地磁盘，使其能够在本地离线浏览，防止服务器上原网页被删除导致的证据灭失，取证过程中还提供了屏幕截图、屏幕录制等功能，满足了取证人员对网站取证的需求。

网络巡查产品用于解决网络执法巡查过程中，由于需要手工排查线索，在线巡查效率不高的问题，能够减少执法人员在网络日常巡查过程中的重复劳动，提高工作效率。网络巡查产品多用于文化执法的取证场景，通过对在线小说网站、视频网站、微信公众号等内容进行过滤，自动化地发现文化作品的违法违规线索，并即时进行多要素证据固定。

23.1.4 现场勘验

在现场勘验方面，为了帮助执法人员快速、规范地采集案件现场证据，国内厂家研发了形态各异的取证产品：智慧现勘设备，用于解决执法人员对办案现场的场所、人员、物证等信息快速采集、搜查扣押、物证发还等工作的法律文书的快速生成；多路硬盘复制设备，用于现场硬盘的不拆机快速复制镜像，通过多个传输通道实现多路并行获取以提高复制效率，节省现场时间；计算机快速取证设备，在现场实现对目标计算机的快速调查和数据提取；监控视频高速下载设备，对现场监控探头保存的视频进行快速采集。这些不同类型的取证产品各有所长、互相补充，能够满足执法人员在现场勘验中的各种取证需求。

23.1.5 存证固证

在存证固证方面，国内各厂商在探索利用区块链上数据不可篡改的特性，

进行电子数据证据的可信存证。区块链存证平台通常将需要存证的文件包进行哈希计算，并将哈希值保存在区块链中，在诉讼过程中，将区块链中保存的哈希值与法庭上文件包哈希进行比对，以此证明该文件包未被篡改。各厂家还将存证对接公证处、司法鉴定机构等，为用户提供证据保全的一条龙服务。

23.2 电子数据取证存证在各领域得到应用

目前，新型网络违法犯罪的打击治理不断深化，受害人报案时往往需要提交手机中的通话录音、聊天记录、涉诈 APP 等电子数据，为了保护受害人个人隐私，取证人员需要定向获取受害人手机中与案件相关的数据，忽略案件无关数据，并且需要快速获取所需的数据以提高警情处理效率。传统的手机综采取证方式难以满足此类需求，在公安部刑侦局的推动和指导下，手机快采产品需求不断增加。同时，对于新型网络违法犯罪中大量使用的虚拟拨号群呼设备，执法人员也需要获取其中的 SIM 卡信息、呼叫记录等，由此催生了针对群呼设备的专用取证工具。此外，利用虚拟币进行传销、赌博的新型犯罪还带来了虚拟币类案件相关取证产品的发展。

2018 年 9 月初，最高人民法院出台了《关于互联网法院审理案件若干问题的规定》，确认了存证在司法应用中的合法地位，使得电子数据的存证在金融、医疗、司法、政务等各个领域都得到了应用。如开户 / 信贷 / 交易流程中电子数据的存证、电子合同签约时的存证、医院电子病历等数据的存证、公证和诉讼服务中当事人提交证据的存证、政采招投标过程中标书的存证等。“十四五”规划提出推动数字经济和实体经济相融合，区块链、人工智能、大数据等技术与电子数据存证的结合，已经成为各产业领域数字化转型的可靠工具。

23.3 提高效能是电子数据取证产业发展的关键

随着电子设备不断升级更新，电子数据取证也必须适配软硬件版本的发展变化，并解决随之出现的技术难题。在手机取证方面，冷门手机品牌及型号的解锁和应用数据提取、加密备份文件的解密还原、删除应用数据的恢复等仍然值得研究。同时，随着安卓和 IOS 操作系统的不断迭代，取证手段也需要不断更新。介质取证中加密文件和加密磁盘的破解、隐写文件的识别和提取、各类应用程序的数据解析、各类物联网设备的数据提取等还不够完善。网络取证对于虚拟化云服务以及暗网的取证解决方案还有待优化和探索。解决电子数据取证中不断出现的难点问题，提高电子数据取证产品效能，是电子数据取证产业创新发展的关键方法。

目前电子数据取证设备更多地是针对 Windows、Linux 等操作系统。随着国产化进程的推进，如何对国产化操作系统、数据库、办公软件、浏览器等进行电子数据取证仍然值得研究。在取证对象国产化的需求需要满足的同时，取证产品本身的国产化也刚刚起步，具有国产化取证产品的厂家数量少，产品种类少。与国产化基础软硬件厂商开展合作，研究国产化取证技术，形成国产化取证体系，是电子数据取证创新发展的重要方向。

在执法办案的过程中，可能涉及到大量手机、计算机、服务器等设备中的电子数据。在对这些案件数据进行分析时，需要运用人工智能和大数据技术，快速发现案件中的关键线索。目前电子数据取证分析产品往往流于形式，在人物画像、关系分析、资金分析等方面难以得出准确、可靠的分析结论，在实践中仍然需要大量的人工分析工作。特别是在多个案件的串并时，涉及的对象和维度更加复杂。对于国内取证厂商而言，推出真正贴合实战、适用性广、准确度高的案件大数据分析产品，组建可视化分析网络，形成平台化的应用支撑十分必要。

本章主笔人员（按拼音排序）：

广东中科实数科技有限公司 丁丽萍、杜漠、刘栋

案例篇 »

1、龙芯中科技术股份有限公司 2021 年自主生态建设成果

2、中电科申泰信息科技有限公司申威 3231 处理器

3、北京计算机技术及应用研究所天熠 TR4261 便携式计算机

4、北京中船信息科技有限公司边界安全防护解决方案

5、江苏云涌电子科技股份有限公司远程浏览器隔离解决方案

6、珠海金山办公软件有限公司 WPS Office 2019 for Linux 专业版

7、精壹致远（武汉）信息技术有限公司网络攻防教学演练平台解决方案

8、友虹（北京）科技有限公司友虹电子文件链控平台

9、北京东方通科技股份有限公司东方通应用服务器软件 TongWeb

10、湖南国科微电子股份有限公司终端安全加固解决方案

11、安思易安全集中运维管理平台系统软件

12、深圳市东进技术股份有限公司信息系统因产密码应用方案

龙芯中科技术股份有限公司
2021 年自主生态建设成果

2022 年 1 月 13 日，在龙芯中科首届 LoongArch 生态创新大会上，龙芯中科重磅发布《龙芯生态白皮书 2021》，向业界展示了龙芯中科生态建设的成果与策略。

基于二十年的 CPU 研制和生态建设积累，龙芯中科于 2020 年推出了 LoongArch 指令系统，通过第三方权威知识产权评估机构评估，具备高度自主性与安全性。LoongArch 指令系统在设计时就充分考虑到兼容生态需求，基于 LoongArch 的二进制翻译方案，实现了 X86 体系下的应用软件以及打印机 Windows 驱动可以在龙芯平台上流畅运行。

基于自主的指令系统，龙芯中科已推出了多款 CPU 产品，随着龙芯 3A5000、3C5000L 系列新产品的问世，龙芯中科的商业应用也迎来了全面开花。

龙芯 3A5000 处理器芯片

龙芯 3C5000L 处理器芯片

紧密联合生态伙伴，龙芯中科已建立起两大产业链体系：信息系统（PC、服务器等）和工控系统（工业、网安、物联网）。

电子政务办公领域，龙芯中科多年来形成了成熟的应用方案。目前基于龙芯 CPU 路线的办公应用覆盖国家部委和全国各省市系统，每年销售上百万颗。

金融领域，主要覆盖金融机具、金融办公系统、金融业务系统。农业银行、工商银行等营业厅中已经开展基于龙芯方案的各种创新应用。2021 年，龙芯方案获得 30 余家机构选型入围，覆盖桌面、服务器、金融机具等场景。

工控与嵌入式领域，龙芯处理器在各种工业控制、智能仪表、机器人等场景积累深厚，基于 3A/C5000、2K0500 等边缘扩展服务器、边缘计算设备、态势感知设备、工业上位机等设备已广泛应用在交通、电力、石油石化等行业。

通信领域，中国移动在 2019 年就开始启动采用龙芯产品的各类终端。浙江移动完成龙芯 3A5000 终端在营业厅的部署，将生产环境的数据库平稳迁移至龙芯 3C5000L 架构服务器。

交通领域，龙芯 CPU 在高铁、地铁、公路交通等领域已经得到广泛应用。龙芯交通控制系统在安徽合肥、安徽六安、广东云浮等地区部署应用，龙芯 3A5000 工控计算机在粤西等地 ETC 车道部署应用，龙芯 3C5000L 用于高速雾区预警数据处理系统。

能源行业，龙芯中科为用户提供从 CPU 芯片、工业板卡、边缘设备、行业专用设备，到底层开发工具、嵌入式操作系统等各类成套解决方案，实现从芯片、板卡、设备整机到系统应用的全系统应用。

医疗领域，龙芯中科提供丰富的解决方案和产品。龙芯医疗自助终端设备已广泛应用于北京、山西等地的各级医院。基于龙芯开发的社区封闭管理系统、疫情监控系统，已在北京的大型社区部署上线，龙芯 3A5000 系列产品已经应用于长治市国家基本公共卫生服务信息平台。

网安领域，基于龙芯 3A/C5000 芯片的如防火墙、网关、通信终端等安全设备，在政企、能源等领域提供强有力的算力保障，提升安全防护能力。

教育领域，龙芯中科推出了覆盖小学、中学与高校的各类教材、教学平台、教学实验设备、智慧教室等一系列方案产品。在江苏、浙江、山西等地开展万套以上中小学信息教室应用，打造中小学教育信息化标杆。

如今龙芯中科基于 LoongArch 的自主生态建设已驶入快车道，龙芯中科愿和生态伙伴相向而行，共建生态。只有我们靠自力更生，才能彻底打破锁链、摆脱发展受制于人的命运。

公司简介

龙芯中科面向国家信息化建设需求，面向国际信息技术前沿，以创新发展为主题、以产业发展为主线、以体系建设为目标，坚持自主创新，全面掌握 CPU 指令系统、处理器 IP 核、操作系统等计算机核心技术，打造自主开放的软硬件生态和信息产业体系，为国家战略需求提供自主、安全、可靠的处理器，为信息产业的创新发展提供高性能、低成本的处理器和基础软硬件解决方案。

龙芯中科主营业务为处理器及配套芯片的研制、销售及服务，主要产品与服务包括处理器及配套芯片产品与基础软硬件解决方案业务。

中电科申泰信息科技有限公司
申威 3231 处理器

申威 3231 处理器是基于第三代“申威 64”二次优化版核心 (C3B) 的国产高性能多核处理器，主要面向高性能计算和高端服务器应用。

申威 3231 采用 CC-NUMA 多核结构和 SoC 技术，单芯片集成了 32 个 64 位 RISC 结构的申威处理器核心、8 路 DDR4 存储控制器接口、40lane 的 PCI-E 4.0 标准 I/O 接口以及 3 路直连接口。最高工作频率可达 2.2GHz。

产品特色

- 采用“申威 64”自主指令系统；
- 基于第三代“申威 64”二次优化版核心 (C3B) 32 64 位通用处理器；
- 采用 SoC 集成结构，片内包含 DDR4 存储控制器接口以及 40lane PCI-E 4.0 标准 1/0 接口集成 路直连接口，可构建 2 路或 4 路服务器系统；
- 计算性能：双精度浮点性能可高达 1126.4GFlops, 整数性能可达 774.4Gops；
- 访存性能：最大传输率为 3200Mbps, 最大总存储器容量 2TB;

● I/O 性能：双向聚合有效带宽可达到 160GB/s, 支持 I/O 虚拟化。

技术参数

核心数量	32
核心频率	最高可达 2.2GHz
峰值运算速度	浮点：每秒 11264亿次双精度浮点结果 @2.2GHz 整数：每秒 7744亿次整数结果 @2.2GHz
工艺特征	内核电源： 0.75V±5% I/O电源： 1.8V±5% 1.2V±5%
Cache 容量	每个核心包含两级 Cache，Cache 行长度为 128字节 一级 Cache：指令与数据分离，容量分别为 32KB 二级 Cache：指令与数据混合，容量为 512KB 32 个核心共享三级 Cache，容量为 64MB
存储空间	支持 53 位虚地址 支持 48 位物理地址
存储器接口	8 路 64 位 DDR4 存储器接口 ，支持可配置的 ECC 校验，最大传输率为 3200Mbps 支持的最大总存储器容量为 2TB 支持 X4、X8、X16三种颗粒 支持 DDR4 UDIMM/ RDIMM/ LDIMM存储器条 支持 3D 封装，最大支持 8H
I/O 接口	全芯片集成 40 个 lane 的 PCI-E 4.0链路 支持X4、X8、X16灵活配置维护接口支持芯片调试与维护
封装特性	采用 FC-BGA封装，引脚数为 4041 芯片尺寸为 65mm×65mm
功耗	热设计功耗： 200W@2.2GHz 典型运行功耗： 180W@2.2GHz（含 I/O功耗，与具体应用相关）

北京计算机技术及应用研究所

天熠 TR4261 便携式计算机

天熠 TR4261 便携式计算机以飞腾最新八核国产处理器平台——D2000 为核心，搭载国产昆仑桌面版固件和统信 UOS/ 银河麒麟桌面操作系统，适配国内主流软件，实现了产品从硬件到软件的自主研发、生产、升级维护的全程可控，保障工作过程中的信息安全。性能强劲，轻薄便携，集成指纹识别、一键还原等特色功能，轻松支撑各类办公场景。

产品主要特点

性能强劲——飞腾 D2000 核处理器，主频 2.3GHz, 搭载 8GB 内存（标配）+256GB SSD 硬盘（标配）+ 独立显卡，轻松应对各类办公、设计、娱乐需求；

超薄设计——整体采用航空铝材打造，整机厚度小于 20mm，重量小于 1.6kg;

超窄边框——采用全景超微边框设计，配备 14 英寸 FHD 超窄边框高清液晶显示屏；

180 ° 转轴翻转——显示屏支持 180° 转轴翻转，方便小型会议讨论，协同办公；

接口丰富——搭载 Type-C、USB3.0、HDMI、3.5mm 音频、网络接口等多类型接口，适应各类办公需求；

超窄边框——采用全景超微边框设计，配备 14 英寸 FHD 超窄边框高清液晶显示屏；

适配资源丰富——适配火狐浏览器、金山 WPS、永中 office、数科 OFD、福昕、中安源、金印等国内主流办公软件，支持奔图、天津光电等国产品牌打印机、扫描仪等外设。

应用场景

天熠便携式计算机轻薄便携，续航持久，除应用于固定环境中的日常办公、工程设计、系统维护等工作，还可较好满足出差办公、跨组织集中协同等工作。凭借完备的适配资源和强劲的性能，天熠系列便携式计算机已供应超 10 万台，广泛应用于国家部委、地方政府以及金融、能源等重点行业，支撑信创环境下的多类型应用需求。

公司简介

北京计算机技术及应用研究所始建于 1957 年，是我国最早从事计算机研究的大型骨干研究所之一。是以计算机软硬件研制及产品开发应用为主，集研发、设计、生产和服务为一体的计算机与控制技术核心研究所。作为国

家信创产业的“国家队”和“排头兵”"天甜"/“天焙”品牌信创产品累计供应 50 万台，用户覆盖 20 余家部委及 31 个省市自治区。拥有百万台级的现代化生产能力和 100% 覆盖全国地市的售后服务网络。

经过数十年的产品及技术积累，北京计算机技术及应用研究所围绕国产自主处理器和操作系统，形成了基千飞腾、龙芯、申威等国产处理器的基础软硬件产品，产品涵盖基础通用软硬件产品、平台及软件服务类产品、应用系统类产品及密码和安全产品，已广泛应用千党政、金融、能源、交通及特殊行业等领域。

北京中船信息科技有限公司
边界安全防护解决方案

面对日益紧迫的安全威胁，中船信息提出了突破传统检测引擎技术瓶颈的概念，采用基于威胁行为分析的方法，实现 L2-L7 层全面的威胁检测与防护，以保障用户应用安全为目标，通过对应用、用户、内容、地理位置等多维度业务场景感知，为用户提供可视化及精细化的应用安全管理。

中船信息边界安全防护解决方案采用全新硬件架构设计，具备硬件解密引擎、可扩展存储，拥有智能感知、情报集成、融合安全以及无限延展等能力，可有效检测未知威胁事件以及检测内网失陷主机，加强物联网设备的管控与防护，致力于向全行业全场景的客户提供领先的网络安全防护能力。

应用场景

互联网出口边界防护场景

智能下一代防火墙以网关模式部署于网络出口，通过链路负载均衡、NAT 等出口特性功能，实现多个互联网出口的智能路选。以用户资产为视角进行风险分析，构建对 IT 资产实现多维度的安全分析监控。内置 IPS、AV 能力引擎，抵御内外网的入侵防御，对网络中的病毒进行过滤查杀。威胁情报联动实现全网威胁实时同步，及时发现内网未知威胁。对网络社区 /P2P/ IM/ 网络游戏 / 炒股 / 网络视频 / 网络多媒体 / 非法网站访问等各种应用进行监控和管理，保障关键应用和服务的带宽。

关键业务串行防护场景

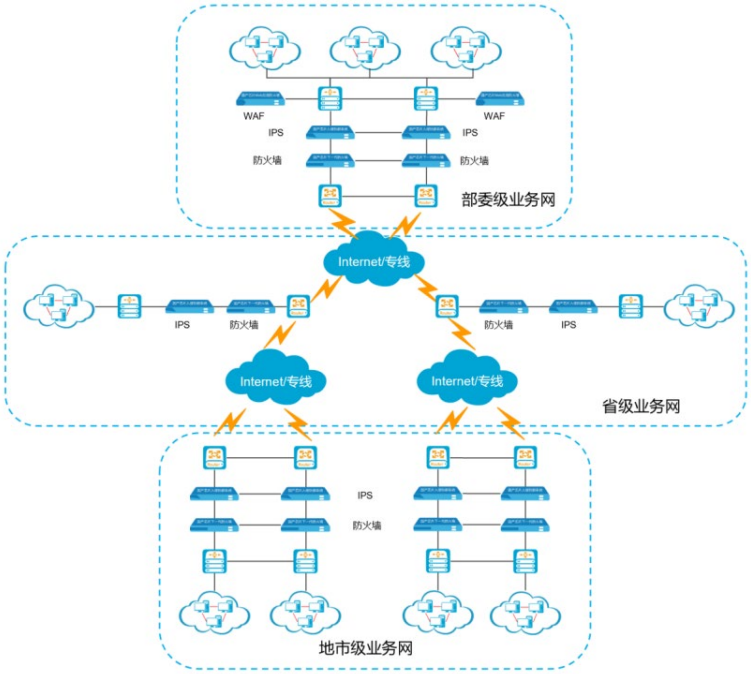
以串行路由或者透明方式部署于数据中心机房出口。通过智能下一代防火墙的资产发现功能，以用户资产为视角进行风险分析，构建对 IT 资产实

现多维度的安全分析监控。对外网针对数据中心的暴力攻击进行有效阻挡，对所有进出的封包均进行详细的七层分析。提供以资产和攻击维度的安全智能可视化的分析，便于管理员分析取证溯源。

总分型网络集中部署场景

以边界设备方式部署在总部和分支网络的出口。对大型总分型网络进行集中部署、集中监控管理，通过数据加密、验证及校验，防止数据泄密。通过 VPN 互联技术实现远程分支、移动办公、拨号接入等多场景互联，同时可基于员工身份进行访问控制，有效提升大型分支机构整体管理及安全防护水平。

典型案例



● 通过部署高性能、高可靠的船信防火墙，保障网络出口设备高效稳定运行。

● 按照各级单位权限，进行专网内灵活访问控制和入侵检测及防御。

● 智能的威胁检测防御，防止其他单位的渗透攻击、恶意程序、病毒木马等威胁。

● 支持丰富的日志功能，提供本地存储，安全记录一目了然。

公司简介

北京中船信息科技有限公司（以下简称中船信息公司）成立于2000年12月，由中国船舶集团有限公司下属中国船舶工业系统工程研究院、中国船舶工业贸易有限公司、上海外高桥造船有限公司等15家船舶行业知名企业共同出资设立的国有资本控股公司，注册资本3000万元，是北京市高新技术企业。中船信息公司作为信息技术行业的现代科技公司，坚持“做实平台、做精技术、做大产业”的使命。发展成为具有中船信息品牌的信息化集成商以及软件、仿真及信息安全等产品的供应商。截至目前，公司已有软件著作权138项，发明专利14项，实用新型专利20项。面向未来，中船信息公司将依托行业平台，秉承信息化、数字化、智能化推动信息技术产业快速、高效发展的历史使命，努力创造“创新、进取、健康、共赢”的企业文化，打造具有行业特色的中船信息品牌，为信息技术和网络安全产业发展提供有力支撑。

江苏云涌电子科技股份有限公司
远程浏览器隔离解决方案

云涌科技基于零信任技术打造的远程浏览器隔离访问方案，通过远程协议隔离和像素流实现两端数据摆渡访问方式，避免用户端直接通过浏览器访问内部网路，从而保护资源服务器的安全。

技术特点

零信任远程浏览器采用“2+1”安全架构：本机终端安全＋业务服务安全＋远程浏览器安全。其中本机终端安全：上网数据不落本地、不接受任何远端协议数据、本地不被恶意文件污染、本地不被恶意网站攻击、容器用后即毁；业务服务安全：被最纯净虚拟容器访问、每次访问均来自全新终端、有效防止 OS 注入和 XSS 等攻击、服务页面加载水印防截屏、无法拷贝粘贴数据到容器外、附件下载受策略管控。远程浏览器安全：服务隐藏、单包授权、国密隧道、实时审计。

应用场景

场景一：内网办公时需要访问互联网查资料

员工使用浏览器访问不安全网站增加受攻击风险，办公终端可能被污染成为肉鸡。

员工使用浏览器无意中下载了恶意文件，导致本地终端感染病毒，成为内网横向攻击的跳板机。

员工访问非法网站后又使用相同浏览器访问内网业务系统，导致业务系

统被 XSS 攻击或恶意代码注入。

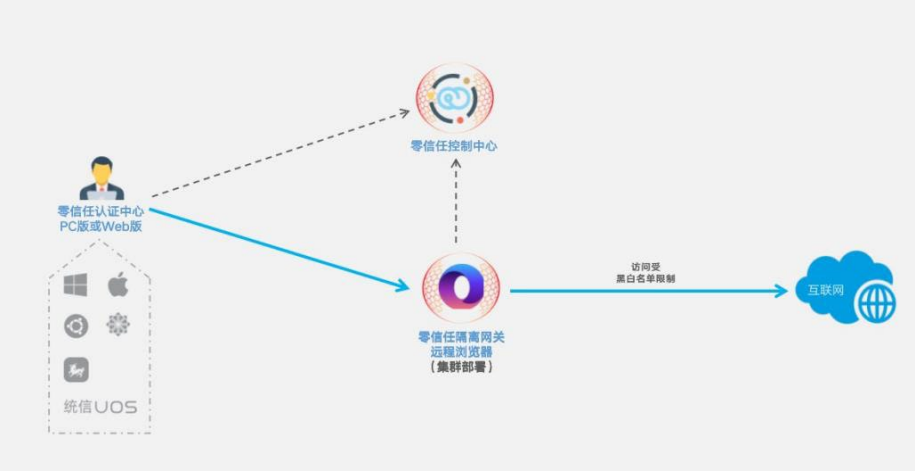
场景二：远程办公时需要访问内网系统处理业

员工借助 VPN 等工具，通过终端浏览器访问内网办公业务系统，因无管控导致企业敏感业务的数据外流。数据泄露包括敏感页面被截图、关键数据被拷贝、重要文件被下载到本地或打印等。

员工使用个人设备访问内网办公系统，由于终端无安全防护导致内网业务系统被污染。

典型案例

某互联网银行 IT 策略禁止内部办公网络访问互联网。这种策略阻碍了必要的实时外部沟通业务需求以开发团队的文档查询需求。2020 年企业选择试用了远程桌面解决方案，但发现存在成本高和上网行为审计粒度不够细等问题。在选用了云涌科技的远程浏览器系统后，通过横向扩容将系统推广到 500 个员工，在保证了安全策略的同时，满足了企业所有员工的安全上网需求，其部署成本比预期节约了四分之三。



公司介绍

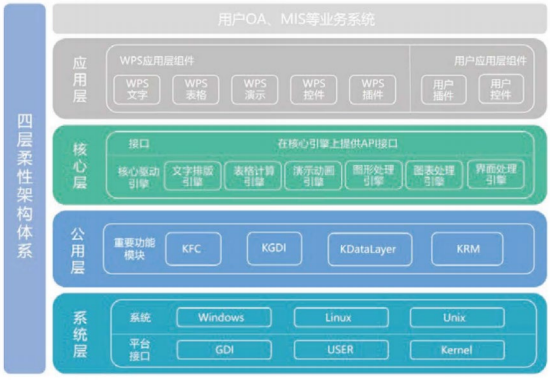
江苏云涌电子科技股份有限公司是一家致力于为能源电力、交通物流、石油石化等行业，提供工业互联网技术服务的高新技术企业。公司总部位于江苏泰州，生产厂房占地20000平方米，在北京、郑州、南京，深圳设有研发中心。2020年在上海证券交易所科创板成功上市（股票代码688060）。

云涌科技在嵌入式设计、密码技术、零信任安全，可信计算方面积累了丰富的经验，提供高性能RISC架构计算机平台，加密卡、网络隔离装置、主机加固、零信任安全接入等解决方案。在工业互联网飞速发展的今天，云涌科技将在“市场导向”与“技术创新”的双驱动下，秉持“平等、协作、开放、分享”的发展理念，与各位合作伙伴共同努力，风起云涌，聚创未来！

珠海金山办公软件有限公司
WPS Office 2019 for Linux 专业版

自 1989 年 WPS1.0 问世以来的三十余年间，WPS 办公软件从单一的文字处理软件逐渐充实为集文字处理、电子表格、电子演示为一体的数字化办公平台。WPS Office 2019 for linux 专业版于 2019 年 4 月发布，依靠 WPS 多年技术实力保障，该版本在兼容主流平台的同时，支持几乎所有平台的文档交互，并且支持跨平台分享和多人协作办公，实现文档实时备份。此外值得一提的是，WPS Office 2019 for linux 专业版融入了一系列全新应用来满足政府和企业等用户在日常办公中的需要，降低运维成本，提升办公效率。

WPS Office 2019 for Linux 专业版采用创新的“应用、核心、公用、系统”四层柔性架构模型，从产品内部结构的优化及系统的安全角度提供保障。系统层提供跨平台的系统接口服务，确保 WPS 核心功能可运行在各类操作系统上；公用层提供高度分离的共享功能模块，确保产品体系超小；核心层提供自主开发的文字排版、演示动画、表格计算以及图形绘制的四大核心引擎，确保在不同的操作环境下具有相同的底层驱动核心；应用层提供用户实际操作的应用组件。该四层柔性架构结构和目前市场上流行的其他 Office 在结构上的明显区别是直接在产品的核心层提供 API 接口服务，能够更好的实现和用户现有的各类业务系统的紧密糅合，具有开放、安全、易用三大特点。



应用场景

WPS Office 2019 for linux 专业版适用千各种办公场景，目前已在政府、金融、能源、航空等多个重要领域广泛应用，在政府办公场景下优势尤其明显，已成功应用千 30 多个省市自治区政府、400 多个市县级政府、90 多家央企以及 100 多家大中型银行。

WPS Office 2019 for linux 专业版的广泛应用，依赖于其与产业生态的融合共生，产品先后与龙芯、飞腾、兆芯、申威等 CPU 厂商，中标麒麟、银河麒麟等操作系统，数科等版式软件，以及打印机、签章、电子公文系统等软硬件厂商进行多次产品底层优化和产品互测，并出具互认证文件，全面提升产品的易用性和可靠性。

WPS Office 2019 for linux 专业版在应用中广受好评，这主要依赖于其在兼容性、安全性、便捷性等多个方面的卓越表现。秉承不丢失内容、不破坏数据、应用系统低成本迁移的三大兼容原则， WPS Office 2019 for Linux 专业版实现了文件格式、操作习惯、二次开发深度兼容。同时， WPS Office 2019 for Linux 专业版支持密级关键字检查，高效监控内部流转的涉密文档。

使用 WPS 打开电子文档，可自动进行全文检索，检测关键词信息，提醒用户文档涉密，并上传到服务器记录，管理员可以对敏感文档进行统计和管理。除此之外，用户通过 WPS Office 2019 for Linux 专业版可以访问 WPS+ 云办公线上服务，该服务是金山办公为用户打造的 SaaS 级一站式云办公服务的一部分，包括云文档储存服务、文档权限管理服务。

公司简介

金山办公主要从事 WPS Office 办公软件产品及服务的设计研发与市场推广。公司及其子公司拥有知识产权总数达 900 多项，两次获得国家科技进步二等奖，多次取得“核高基”专项基金支持，现已成长为中国科技自立自强的标杆品牌。公司主要产品月度活跃用户 (MAU) 已达到 4.94 亿，覆盖全球超过 220 余国家和地区，是国内拥有大规模市场化应用经验的民族软件企业代表。 2019 年金山办公登陆科创板，成为中国市值千亿的软件公司，也成长为全球能代表中国办公创新的民族龙头企业。 2020 年，金山办公成为北京 2022 年冬奥会和冬残奥会官方协同办公软件供应商。

精壹致远（武汉）信息技术有限公司
网络攻防教学演练平台解决方案

概述

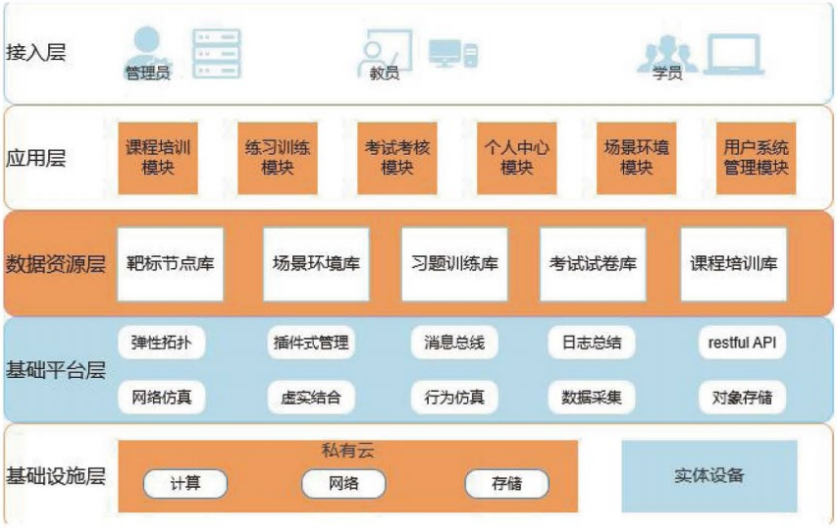
网络攻防教学演练平台解决方案由教学实验平台、实训平台、竞赛平台和演练平台构成，提供“学、练、赛、演”一体化设计，打通理论知识、操作技能和实战经验三个环节。

教学系统课程丰富

教学系统提供40类150门实训课程，总时长约2000课时，同时可针对高校的办学特色和人才培养目标提供定制化课程方案。

仿真环境贴近实战

实训、竞赛和靶场系统基于高度仿真的虚拟网络，动态模拟物理世界组网，实现网络攻防实操练习和能力评价功能，提供单兵演练、团队演练、红蓝对抗和系统测试等靶场功能和环境。



架构合理技术先进

方案采用 B/S 架构，后端基于私有云技术实现，支持多种虚拟化方式，同时采用缓存和负载均衡技术提升设备使用效率；前端展示模块具备完善的数据接口，除 U3D、GIS 等方式外还能支持用户自定义其他可视化方式；同时引入大数据分析系统对海量用户行为进行分析，综合展示用户能力。

应用场景

网络攻防教学演练平台解决方案对于高校培养网络攻防类人才具有重要支撑作用，通过教学、实训、竞赛和演练相结合的人才培养模式，有效提高学生的实际动手能力和接近实战的工作经验。该方案对于重点行业领域开展安全运维和服务人员的在职培训和能力评估有重要支撑作用，能有效提升相关人员的岗位能力，为培训、选才、用人提供重要的手段，能在控制风险的前提下提供接近实际环境的测试场景，为新产品、新技术、新方案提供上线前的安全测试条件。

在校教育

主要使用者为高等学校网络空间安全学院、开设网络安全专业的高职高专院校，作为网络攻防类人才培养的教学和演练平台。

在职培训

主要使用者为网络运营单位和网络安全服务提供单位，作为安全运维和服务人员的培训、能力评价和综合演练平台；

测试平台

主要使用者为关键信息基础设施运营者，作为敏感场景下网络安全从业

人员的培训、选拔、评价平台和攻防技术测试平台，以及针对新产品、新方案在准真实环境下的安全测试平台。

典型案例

武汉大学网络攻防演练课程

武汉大学国家网络安全学院为了加强网络安全学科建设，提升学生网络安全攻防实践能力，开设了《网络攻防演练课程》。该课程教学环境主要依托于精壹致远的实训平台、竞赛平台和教学靶场的云服务。

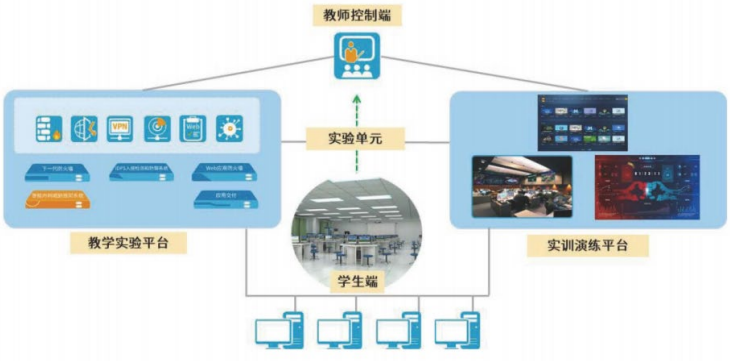
《网络攻防演练课程》具有理论和实践结合、攻防兼备的特点，围绕提升学生工程实践能力的总体目标，有针对性地解决武汉大学国家网络安全学

院实践课程面临的问题：一是对前序课程的知识点进行梳理和补充，解决覆盖面不全的问题；二是通过提升学生在操作系统核心层开展工作的能力，解决“飘在上面”的问题；三是着力把竞赛与真实的网络攻防建立联系，解决为竞赛而竞赛的问题；四是以人才培养方案为纲，定制开发课程和教学演练平台，解决课程与教学需求脱节的问题；五是针对武汉大学本科学生的知识和能力特点设计教学方案，解决课程针对性不强的问题。

学生普遍反映通过该课程的学习，对当前网络安全攻防的前沿技术有了深入的了解，深切体会到了理论知识不等于实践技能，认识到了自身能力与未来即将从事的工作之间的差距，对于明确自身定位、清晰职业规划、补足能力短板具有十分重要的意义和价值。

成都理工大学网络安全靶场

成都理工大学计算机与网络安全学院为加强网络安全学科建设，扩充人才培养方案，提高学院整体教学能力，锻炼学生动手实践能力，基于精壹致远网络攻防攻防教学演练平台解决方案建设了网络安全靶场。该项目从教学和课程学习、实训操作、比赛演练和仿真训练等不同层面对学生开展实践能力培养，针对学生在课程学习上进行查缺补漏，提升学生的动手能力，从实践课程到攻防演练最终在仿真环境中进行训练，稳步提升学生网络攻防水平。

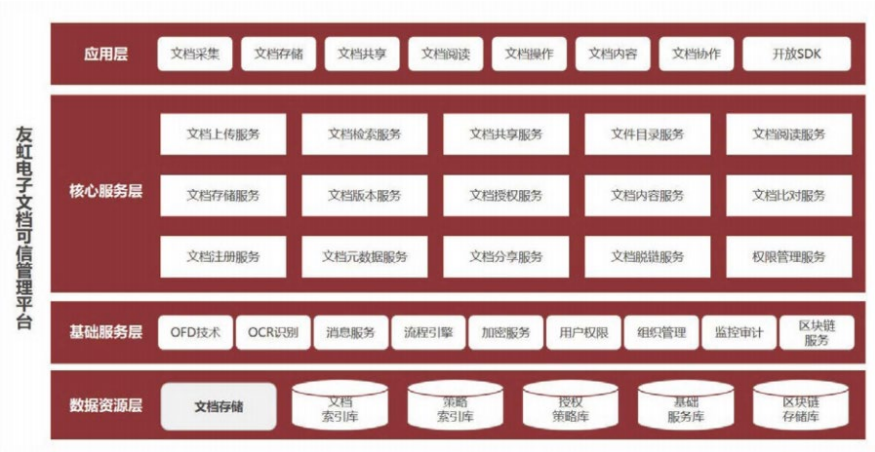


公司简介

精壹致远（武汉）信息技术有限公司以网络安全和信息化的自主创新为己任，致力于把最好的技术用在最需要的地方。精壹致远依托强大的技术底蕴，组建了国内领先的技术团队，产品体系覆盖边界安全、内网安全、云计算安全、数据安全、智能分析管理等领域，为卫生健康、教育、军工等关键信息基础设施提供自主可控、安全可信的网络安全产品、解决方案和服务。

友虹（北京）科技有限公司
友虹电子文件链控平台

友虹电子文件链控平台 SC-FCP 是采用国产自主知识产权 OFD 版式技术的文件管理赋能平台。链控平台基于国密标识技术建立了分布式文件索引，提供了无插件无留痕的文件在线阅览、基于属性的内容级授权、跨渠道便捷分享以及海量小文件版式存储等特色功能，为电子文件的生成、纳管、阅览、转换、存储、分享、授权、溯源全生命周期提供赋能支撑能力。



链控平台以“链”+“控”为产品设计理念，“链”保障用户可以高效便捷地使用各类电子文件，“控”保证用户的使用时刻处于安全受控的可信环境当中。

- 纳管：通过文件上传、系统对接等各种方式纳管企业 / 个人价值文档。
- 管理：赋予文档全局唯一的索引标识，实现“物理分散逻辑统一”的文件管理。
- 转换：支持 office wps pdf ofd png、网页等文件的流版图文互转。
- 处理：内置拆分合并、加解密、签章验章、插入删除、文字提取等。

处理功能在链阅览文件处千链控时，实现文档保存在归属地远程阅读，本地不留痕。

● 脱链阅览文件脱离链控时，提供密码信封、动态阅读码等方式的访问保护。

● 存储：不强制文档集中存储，支持分布式文档存储，支持远端文档访问。

● 分享：提供订阅 / 发布、请求授权、主动分享等分享方式，亦可扫码快速分享。

● 授权：遵循 XACML 访问控制架构，实现基于文件属性的细粒度访问控制。

● 文件级管控：以文件体为对象，管控文件的下载、复制、阅览、分享等操作行为级管控；以用户行为为对象，对文件的阅读期限、页码范围、授权对象等行为进行管控。

● 内容级管控：以内容信息为对象，实现文件图文水印、动态水印、特定区域掩膜、内容脱敏显示等隐私信息保护。

● 溯源：实时掌握阅读者信息、阅读时间、权限信息、分享链路等痕迹信息。

● 俯瞰：授权链机制掌握文件分享转发路径的全貌，随时掌握文档流转动态。

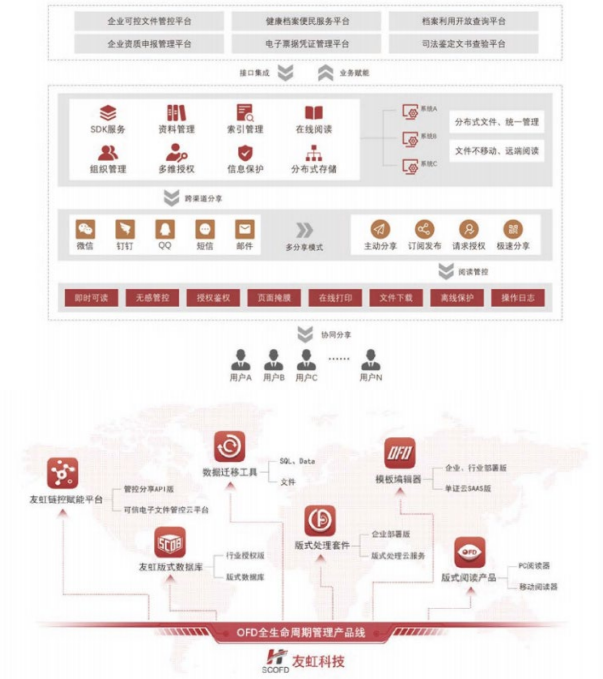
● 回收：对于授权链上的风险点，可及时回收阅览授权，阻止信息外泄。

● 归档：遵循电子档案管理与归档要求，实现文档的检测、归档与移交。

应用场景

链控平台 SC-FCP 问世以来，已经在卫生、档案、证照、票据、福彩等

行业进行了落地推广，为 20 多家行业合作伙伴进行技术赋能，支撑了诸如电子健康档案便民开放服务、档案检索开放与利用服务、电子证照安全可信应用、企业电子票据统一归档与验真查重服务等业务应用。链控平台推动了 OFD 产品生态的发展与完善，改变了国内版式应用一直依赖 Adobe 公司和国际标准 ISO 的现状，提升了企业 / 个人数字资产的安全防护能力与资源治理能力。



企业简介

友虹科技是国内后发领先的基础软件与平台服务提供商，以非结构化电子文件为主线，构建从阅读、生成、处理、分享、管控到存储全系列产品线，涵盖了 OFD 阅读器产品、高并发版式文件加工转换处理平台、文件授权管控赋能平台、结构化非结构化混存数据库（版式数据库）等系列产品，能够有效地为行业用户、合作伙伴及个人提供对严肃电子文件全生命周期管理的解决方案能力，打造版式文件基础软件平台，全面支撑国产 OFD 文件领域应用。

北京东方通科技股份有限公司
东方通应用服务器软件 TongWeb

东方通应用服务器软件 TongWeb 是遵循 Java EE 规范的企业级应用服务器软件，产品技术先进，功能成熟，可适应各类业务应用的基础环境及多种主流应用框架，实现应用部署、运行的集中管控。TongWeb 支持大规模高并发的集群化应用，内置负载均衡，支持弹性伸缩集群和智能路由，内置代码级定位的 APM 工具，满足全方位的应用运行、管理要求。

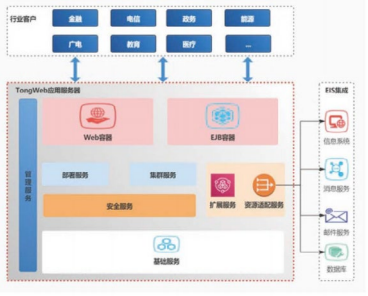
TongWeb 具有轻量易用、性能强大、高可靠性、高安全性等特点，既支持传统物理机、虚拟机，又满足微服务环境下的云平台、容器化环境应用。TongWeb 与国内上下游生态具有全面兼容性，已完成 1000+ 款产品的兼容性认证。TongWeb 在功能、性能等方面媲美国际同类的优秀产品，已在金融、电信、政府、能源、军工等重要行业核心系统广泛应用。

应用场景

作为国内最具影响力的应用服务器中间件，TongWeb 可为金融、电信、政务、能源、广电、医疗、教育等行业应用提供开发、部署、运行、维护等所需能力。

业务应用快速开发

TongWeb 具有安装简单、符合适用习惯、功能实用等特点，提供 Eclipse IDEA 开发插件，兼容主流开源框架，支持将开发的应用在 TongWeb 上进行部署、运行和调试，提高业务应用的开发效率。



业务应用稳定运行

针对各行各业对业务应用高稳定的运行要求，TongWeb 具有优异的健壮性和稳定运行能力，结合产品对 Java EE 标准的遵从性，为业务稳定运行提供强力支撑。

统一集中管控

随着业务发展，业务应用越来越多，用户需要一个统一的应用运行、管理平台，TongWeb 提供对应用的部署管理、监视能力，为业务应用的集中管理提供保障。

大规模高并发业务的应用支撑

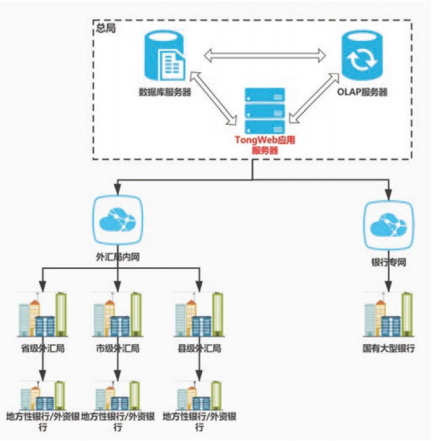
为满足电信、广电、金融等行业的大规模高并发应用要求，TongWeb 供了稳定可靠的集群应用能力，结合内置负载均衡，提升了应用的负载能力，保障业务的稳定性。通过其强大的集群管理工具可以方便的对大量服务器和应用进行统一的管理、维护和监控，从而降低维护成本，提高管理效率。

典型案例：国家外汇管理局

随着业务的发展和系统的不断增多，国家外汇管理局从建设和运维成本出发，考虑引入国产软件，以降低成本，提升安全管控能力。在此背景下，TongWeb 通过严格的业务测试成功入围。

银行结售汇统计系统升级项目是 TongWeb 在国家外管局中的第一个应用，该系统主要是从各个机构（银行、分支机构）采集数据，并进行统计分析，为行业监管及宏观经济提供决策支持服务。系统于 2010 年底成功上线，

部署示意图如下图所示：



通过前期的成功应用实践，TongWeb 在国家外汇管理局的应用范围逐步扩展到资管、案件等十几类业务应用，产品的稳定性、高效性和安全性得到了用户的高度认可。

公司简介

东方通 2014 年登陆创业板（股票代码：300379），是国内首家在上市的基础软件厂商，以“安全 +”和“数据 +”两大产品体系为基础，提供自主、高效的中间件、数据中台、网络信息安全及 5G 创新应用等产品和解决方案。

基于卓越的产品技术实力，以及高质量的综合服务能力，东方通获得业界的高度认可，产品及解决方案广泛应用于国内数千个行业业务，服务 5000 家行业用户，与 500 多家合作伙伴携手打造合作共赢的产业生态。

在中间件领域，东方通经过近 30 年的不断开拓和耕耘，不断引领中国中间件的发展与创新，是国家规划布局内重点软件企业，荣获国家科技进步二等奖等多项荣誉，承担多项国家重大科技专项的研制任务，主持和参与了 Java 企业版、中间件、SOA 及智慧城市等多项技术标准的制定，服务和推动关键行业领域的建设与发展。

湖南国科微电子股份有限公司
终端安全加固解决方案

随着信息化建设的深入发展，终端承载的信息价值越来越高，终端安全对与企业和单位显得愈发重要。国科微 5 系列安全加密固态硬盘是基于以上背景推出的一款用于桌面办公设备的安全存储产品。该款产品基于自研主控芯片、自研固件、国密算法实现的自加密机制和自研的预引导身份验证系统，为客户提供性能领先、安全可靠的终端安全加固解决方案。

传统的终端安全都是基于安全软件的防护，但是在安全软件未运行状态下，还存在启动不安全、数据泄露、数据被破坏等安全隐患。国科微 5 系列安全加密硬盘在终端设备启动时，影子空间上的预验证系统不可绕过，影子空间和用户数据空间物理隔离，多因子验证确保启动安全，全盘自加密技术确保数据存储安全。该方案能保证启动安全，保护数据不被破坏，避免通过拆盘等方式绕过操作系统的验证，获取硬盘数据，从而和终端安全软件形成互补，为终端提供全生命周期的保护。

应用场景

国科微 5 系列安全加密固态硬盘可提供单机版和网络版的安全加固方案，单机版可为终端提供安全启动，拔盘保护和数据加密存储；网络版在单机版的基础上通过安全存储管理平台，提供入网认证，统一的设备生命周期管理和安全管理，例如终端初始化、删除和修改，终端监管，终端设备升级，终端口令管理和终端安全策略管理。两种方案能为党政、金融、电力、医疗、教育、交通等行业的不同场景下的终端提供高易用性、高安全的加固方案。

移动办公电脑安全加固

笔记本电脑特点，可以带走，容易丢失，丢失后数据很容易被窃取和破坏。国科微 5 系列产品通过单机版的安全加固方案，比如对口令、本机特征值进行认证，实现设备丢失数据保证安全、设备重要配件被更换不能启动、单独盗走或者替换硬盘及时发现且数据不丢失以及 PE 启动无法获取盘片数据。

内网办公电脑安全加固

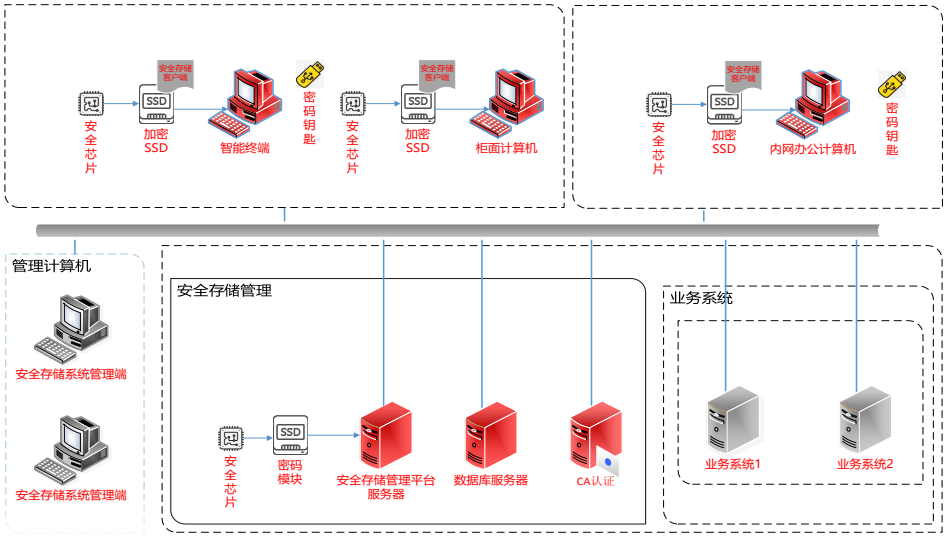
内网办公电脑通常会承载重要的机密信息，比如核心代码、财务报表、上市公司年报等。内网办公电脑不能与外网连接，关键业务只能通过内网办理，故而针对这种设备，需要在单机版安全加固方案基础上增加联网认证，可以保护设备在脱离原有网络环境状态下，不能正常启动，从而防止内网机密信息泄露到其他网络环境。

哑终端、边缘一体机设备安全加固

针对一些长期无人值守的哑终端和边缘一体机设备，比如银行 ATM 机，野外的一些数据采集 & 分析盒子，通过国科微 5 系列产品单机版安全加固方案，对该类设备实现安全加固，保证在设备被破坏或硬盘被窃取的情况下，数据不会泄露。另外，该产品还可提供快速恢复功能，能够为设备提供快速恢复业务的功能。

典型案例：某银行终端安全加固

由于金融机构的特殊性质，金融信息系统承载着重要数据信息，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益。



在此背景下，某银行通过国科微网络版安全存储加固方案对行内的关键终端设备进行了安全加固，终端设备增加了入网认证、硬件环境度量、网络环境度量、安全软件度量和拆盘保护。

方案达到的效果

- PBA 开启后，预验证无法绕过，保障数据安全；
- 盘片、设备丢失或者离开原有网络环境，保证数据不会丢失；
- 关键软件被卸载或篡改，无法正常启动；
- 硬盘全盘加密，加解密性能优异；
- 入网认证、统一的设备生命周期管理和安全管理。

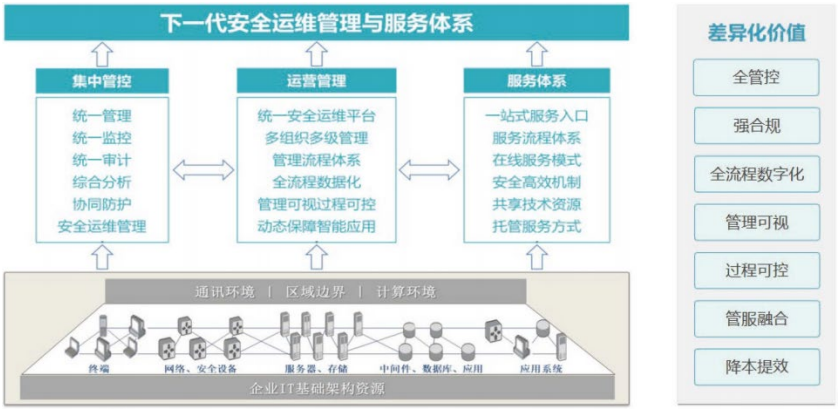
公司简介

国科微成立于2008年，总部位于长沙，并在成都、上海、深圳、北京、常州等地设有分子公司及研发中心。公司每年将营业收入的20%以上用于研发，先后承担了国家科技重大专项、国家重点研发计划等一系列重大科研项目。先后推出了直播卫星高清芯片、4K/8K超高清解码芯片、H.264/H.265高清视频编码芯片、固态存储主控芯片、卫星导航定位芯片等一系列拥有核心自主知识产权的芯片。公司持之以恒进行创新，为客户创造更多价值，推动数字经济高质量发展。

南京联成科技发展股份有限公司
安思易安全集中运维管理平台系统软件

安思易是以集中管控为核心的下一代安全运维管理与服务解决方案，遵循等保 2.0 标准。

安思易建立统一管理、统一监控、统一审计、综合分析、协同处置、持续安全运维，实现集中管控的安全运维管理闭环。采用流程化方式建设管理体系，将制度与技术结合，实现管理过程管控，避免人为因素风险，保障管理策略落地执行。通过全面的实时监测、数据采集与汇聚、多维度关联分析、智能响应与工单管理，把孤立的管理行为建立联动机制，数据驱动精细化管理，构建企业级运营管理智能大脑。



应用场景

安思易主要应用于三大方面：1. 实现等保 2.0 安全管理中心、安全管理体系建设，更全面地满足合规要求；2. 实现一体化运营管理建设，支持多级管理体系，实现统一监管、统一安全运维；3. 以集中管控为支撑，建立服务支持与体系，保障及时专业的远程服务。安思易帮助用户实现安全运维管理

能力、效率、体验的切实提升，同时降低管理服务成本，让用户更安全、更高效、更省心。

适用于政府、金融、能源、交通、医疗、教育、制造业等各行业，帮助实现一体化管理、一站式服务，共享海量技术资源，保障信息系统安全可信、可控、可视、可管。

典型案例

中企网络通讯技术有限公司

通过部署安思易产品建立起科学合理的安全运营体系，实现 IT 资产、资源、人员、流程的统一管理，形成事前预防、事中响应、事后审计的安全运营体系，极大提升了运维效率和规范性。

某融资租赁有限公司

通过应用安思易集中运维管理平台，该公司成功建立起信息系统安全运营管理体系，完成了技术、人才、资源、流程的整合目标，构建了系统安全运维管理的职能管理中心、在线服务中心、知识资源中心、技术人才中心、协同调度中心，打造了以业务为核心、资产为导向、事件为驱动、数据为基础，一体化、智能化、可视化的安全运维管理平台，建立符合规范的安全运营管

理机制，实现了集中管理、实时监测、快速响应、及时解决、全面预防的管理闭环，同时还建立了运行管理档案库，形成了数字化运营管理机制，加速数字化转型进程。

公司简介

联成科技于 2006 年创立于南京，是下一代安全运维管理与服务提供商，是集中管控的创造者。联成科技专注于集中管控技术、安全运维管理的研究探索，创新服务模式，发挥全管控、强合规优势，以安全合规、数据驱动精细化运营管理为目标，打造以集中管控为核心的下一代理安全运维管理与服务解决方案。

公司获得高新技术企业、双软企业称号，是信息安全标准化技术委员会成员、国家安全漏洞平台技术组成员、江苏省软件企业技术中心、南京市智能安全服务工程技术中心、灵雀企业、星级上云企业等，获得国家等级保护建设、安全集成、安全运维、风险评估、应急响应、 ITSS 等行业权威服务资质。

公司拥有三十多项软件著作权，申请了四十多项发明专利，获得了中国十佳安全方案商、中国信息安全领域创新企业、优秀软件和信息服务企业、CNVD 原创漏洞突出贡献、大数据行业创新产品等荣誉称号。

深圳市东进技术股份有限公司
信息系统因产密码应用方案

信息系统国产密码应用方案采用国产 SM 系列密码算法及相关技术，结合密码软硬件资源为最终用户打造一个可以为各类信息系统提供一站式密码服务的密码应用中台。方案及相关产品功能包括应用接入管理、设备管理、密钥管理、密码服务接口、监控与统计、审计与运维；方案技术特点包括安全合规、高性能的密码运算接口、灵活可靠的密码资源池、丰富的密码服务接口、全方位的状态监控和统计、安全的密钥存储和密码运算、完善的权限控制、运维简单。方案实现了对密码资源的统一管理、密码服务的统一调度、密码服务的统一监控、密码服务的统一运维。

应用场景

身份认证

在身份认证应用场景中应采用强身份认证手段或双因子认证方式，而强身份认证手段一般采用密码技术实现。

通信（传输）安全

应确保在通信过程中传输的业务数据完整且不被篡改。

重要和敏感数据加密存储

对于重要的和敏感的用户数据或业务数据应采用加密手段进行密文存储，防止明文数据泄露。

通信（传输）安全

对于敏感的业务操作需要操作行为留痕，且具备不可抵赖性。

典型案例

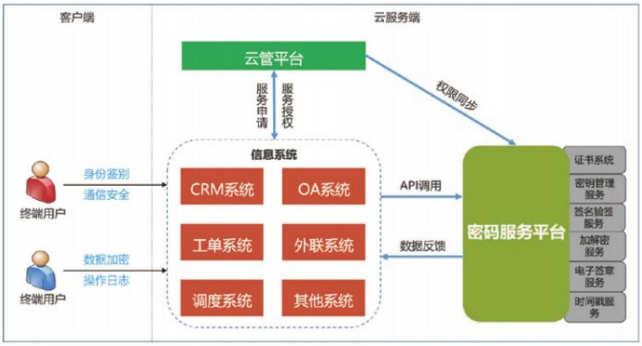
用户需求

某国营大型企业客户的多个业务系统构建于私有云环境下，业务系统的终端用户通过“用户名＋口令”的方式通过浏览器或客户端访问业务系统，且终端用户客户端与云服务端之间的通信是明文传输。此外云上的关键业务数据在数据库中以明文形式保存。

上述的业务应用现状已经凸显了终端用户身份认证的不严谨性、业务数据传输的不安全性、以及关键明文数据泄露风险。

解决方案

针对上述安全需求，东进提出基于密码服务平台方案面向终端用户提供强身份认证手段（数字证书）；客户端终端用户与云服务端业务系统通信采用 SSL 加密通道方式确保传输安全；云端关键业务数据经过加密后再保存至数据库，确保关键业务数据密文存储。同时密码服务平台上的各项功能可以由用户向云管平台进行申请，由云管平台审批用户需要的密码服务。解决方案架构如下图所示：



用户收益

此方案保障了终端用户与云应用系统之间的身份安全、通信安全；同时降低了云上敏感业务数据外泄的风险影响程度；从整体上提高了业务系统的抗风险能力，降低了安全运维成本。

公司简介

深圳市东进技术股份有限公司（简称东进技术）成立于 1993 年，是国内领先的网络安全和通信核心设备及解决方案供应商。公司已拥有 100 余项自主知识产权，近 50 项发明专利和 PCT 国际专利， 20 余款产品获得商用密码产品型号证书及认证证书。

以网络安全上升为国家战略为契机，东进技术抓住网络安全发展的历史机遇，践行民族企业的责任与担当，将公司历经多年基于通信领域的深厚底蕴和技术积淀，全面根植到网络安全行业，专注密码技术和网络安全，构建了覆盖密码设备和部件、加密传输网关、安全管理平台等品类的完整产品线，业务横跨数据采集、传输、存储到访问的全过程。

后 记

《2021 网信自主创新调研报告》的编写工作启动于 2021 年 9 月，整个编写过程历时近 7 个月的时间。回想 2018 年，编委会第一次组织网信企业编写这本报告的时候只有 30 多家单位参与。如今，参编单位的规模扩大了 4 倍，直接参与报告编写的人员规模扩大了 10 倍。大家的关注和支持，既是动力、也是压力，鞭策着编委会不断砥砺前行。

在今年的报告编写过程中，中国工程院院士倪光南，公安部第一第三研究所原所长、中国计算机学会计算机安全专委会荣誉主任严明，公安部网络安全保卫局原副巡视员郑静清、公安部信息安全等级保护评估中心专家委员会研究员任卫红、中国铁道科学研究院集团有限公司研究员张彦、中关村智能终端操作系统产业联盟秘书长曹冬、国家工业信息安全发展研究中心标准质量处处长陈雪鸿等近百位专家对报告的编写工作给予了大力的指导和帮助。在此，编委会向对报告编写工作给予指导的专家和参与报告编写的业界同仁表示感谢。

2021 年是十四五规划的初年。数字经济作为一种新经济形态，在经济发展中占据着越来越重要的地位。相应地，网络安全和信息化工作也将承担越来越重要的责任。在《国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》第五篇中，对数字化建设作出了系统部署，其中将加强网络安全保护提到了十分重要的位置。国务院印发的《“十四五”数字经济发展规划》在部署了优化升级信息网络基础设施、重点行业数字化转型提升等 11 项重点工程的同时，也提出要堵住安全方面的漏洞。

面对新形势、新任务，网信工作者更需要不惧艰险、迎难而上、勇攀高峰的精神力量。同时，做好技术创新、发展网信产业、完善生态环境，也需要产学研用各界的广泛参与和深度融合。脚踏实地、仰望星空，展示自主创新的力量、树立行业用户的信息，这依然是编委会编写这本报告的实训；“惟

其艰难，才更显勇毅，惟其笃行，才弥足珍贵”，这依旧是编委会坚持把这件事做下去、坚持把这件事做好的内心动力。

希望《2021 网信自主创新调研报告》能为广大读者带来些许帮助，也希望您能把意见和建议反馈给编委会。相信您的参与和支持将对下一年度的报告编写工作起到重要作用。

网信自主创新调研报告编委会

2022 年 4 月 19 日

扫一扫关注