DOI:10.19609/j.cnki.cn10-1255/f.2019.04.020

数字经济时代下新机遇与网络安全

数字经济时代对人类发展是极好的机遇，也是重大的挑战。十九大报告指出，建设现代化经济体系，在深化供给侧的结构改革的同时，更重要的是加快建设创新型国家，尤其是对网络强国、数字中国的建设。

□ 文 / 沈昌祥

数字经济时代的机遇与挑战

进入新时代，以互联网、大数据为代表的数字革命正深刻改变着经济形态和生活方式，建设数字中国，发展大数据产业，已经成为战略发展重点。

大数据给现有信息技术体系带来了新挑战，需要投入与创新，还需要营造有利于大数据产业健康有序发展良好环境，因此数据安全已成为大数据产业生态系统发展的必要条件。

数据是一门科学，有其自身发展的规律。在发明计算机之后，分为三个大的阶段，即数值计算、数据工程和数字经济。

随着海量数据的进一步集中和信息技术的进一步发展，信息安全成为大数据快速发展的瓶颈。大数据信息安全主要集中体现在多个方面，包括网络安全、系统安全、个人设备安全、供应链安全和数据安全，由此引发的数据安全事件频发。

2016 年 10 月 21 日，美国东海岸（世界最发达地区）发生世界上瘫痪面积最大（大半个美国）、时间最长（6 个多小时）的分布式拒绝服务（DDoS）攻击。

2017 年 5 月 12 日爆发的“WannaCry”的勒索病毒，通过将系统中数据信息加密，使数据变得不可用，借机勒索钱财。病毒席卷近 150 个国家，教育、交通、医疗、

能源网络成为本轮攻击的重灾区。

2018 年 8 月 3 日，台积电遭到勒索病毒入侵，几个小时之内，致使台积电在中国台湾地区的北、中、南三个重要生产基地全部停摆，造成约 2.55 亿美元的营业损失。

可信计算筑牢安全防线

针对以上这些安全威胁，国家网络安全法中指出国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

《国家网络空间安全战略》提出的战略任务“夯实网络安全基础”，强调“尽快在核心技术上取得突破，加快安全可信的产品推广应用”。

网络安全等级保护制度 2.0 标准要求全面使用安全可信的产品和服务来保障关键基础设施安全。

要实现“安全可信”，首先要认识安全的实质：设计 IT 系统不能穷尽所有逻辑组合，必定存在逻辑不全的缺陷。利用缺陷挖掘漏洞进行攻击是网络安全永远的命题。因此我们主动免疫的安全目标是确保为完成计算任务的逻辑组合不被篡改和破坏，实现正确计算。

传统的杀病毒、防火墙、入侵检测的传统“老三样”难以应对人为攻击，且容易被攻击者利用，找漏洞、打补丁的传统思路不利于整体安全。

此刻“主动免疫可信计算”也就应运而生，它是指在计算运算的同时进行安全防护，以密码为基因实施身份识别、状态度量、保密存储等功能，及时识别“自己”和“非己”成分，从而破坏与排斥进入机体的有害物质，相当于为网络信息系统培育了免疫能力。这也相当于为网络信息系统培育了免疫能力，这是安全的根本出路。

沈昌祥
国家集成电路产业发展咨询委员会委员
国家信息化专家咨询委员会委员
国家三网融合专家组成员

图 1　数据“科学”发展过程

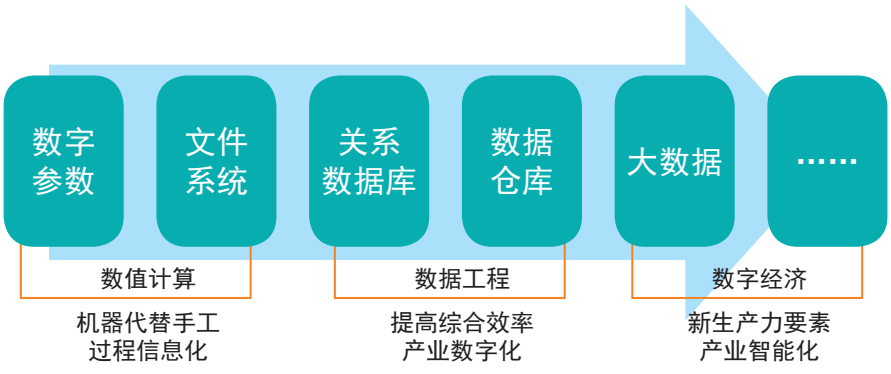
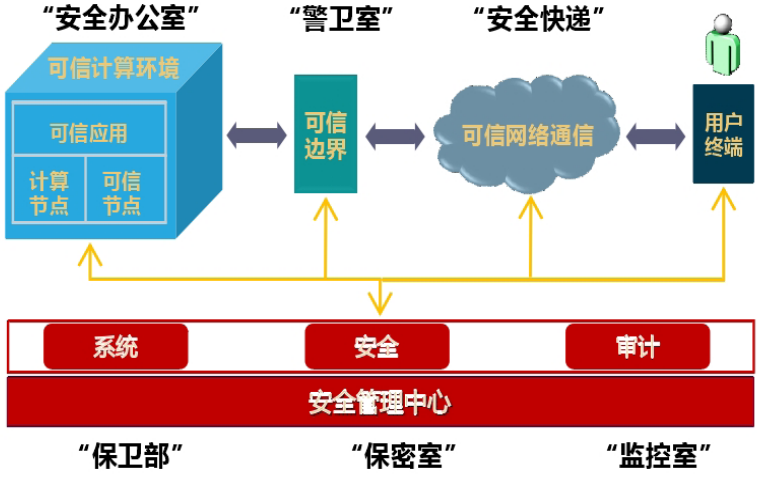


图 2　可信安全管理中心支持下的主动免疫三重防护框架



因此，在体系结构上要解决双体系结构，一边计算一边防护，必须让计算与防护部件并立。人体免疫也是这样，一边完成生活的主要部件，还有免疫系统损失的补偿。

如图 2 所示的防护部件（免疫系统），可信密码模块是“基因”，可信软件基石“抗体”，开机以后对组件进行审查，可信应用软件像白细胞一样循环在整个血液中，按照设定的安全策略进行比对、检测，这如同反腐败，在不打乱单位流程的同时，按照红头文件进行比对，发现问题及时解决、防止腐败。因此真正的主动防御是：既是免疫的，又是反腐败的，构成等级保护的三重防御体系。

具象到现实社会，安全办公室中的可信应用、计算节点及可信节点对应保卫部的人、物管理，警卫室中的可信边界对应保密室，最后一个是监控室，与审计类似，保证新型数据经济时代各种系统能做到体系结构 、资源配置、操作行为、数据存储、策略管理不被篡改、不被破坏，保持可信。最后实现的效果是：攻击者进不去、非授权者重要信息拿不到、窃取保密信息看不懂、系统和信息改不了、系统工作瘫不成、攻击行为赖不掉。

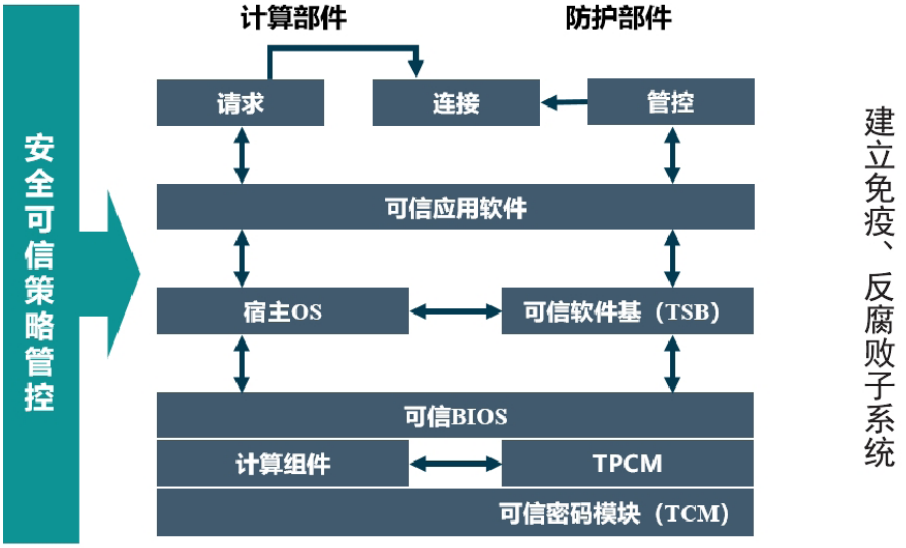
这项源于 1992 年立项研制的中国可信计算经过长期的军民融合攻关应用，已经形成了自主创新安全可信体系，开启了可信计算 3.0 时代。如今，可信计算已经广泛应用于国家重要信息系统，如增值税防伪、彩票防伪、二代居民身份证安全系统。

大数据主动免疫三重防护安全架构

对于现阶段广受关注的大数据系统，大多是基于云计算平台实现数据各种环节的梳理计算，可分为业务信息处理和系统服务保障来定安全等级，应该按（GB/T 25070-2010）进行设计安全架构。

首先是获取数据，数据采集完成后要进行打包、处理，接下来送数据处理平台（云计算平台），然后清洗数据形成有规

图 3　安全可信的计算节点双体系（计算 + 防护）结构



律的上下文语义，恢复其结构化，再进一步通过数据工程、数据库、数据挖掘这些工具，把数据变成产品，最后进行引用、处理变成商品，这就是一个完整的数字经济处理的过程。

如今我国经过 20 多年的联合攻关，已经形成了完整的产业链 / 产品链。自主可信计算平台产品设备主要有三种形态，可以方便地通过可信网络支撑平台把现有设备升级为可信计算机系统，而应用系统不用改动，便于新老设备融为一体，构成全系统安全可信。

举例来说，中央电视台的可信制播环境建设：中央电视台播出 42 个频道节目，面向全球提供中、英、西、法、俄、阿等语言电视节目，在不能与互联网物理隔离的环境下，建立了可信、可控、可管的网络制播环境，达到四级安全要求，确保节目安全播出。经受住了“永恒之蓝”勒索病毒攻击的考验，胜利完成了“一带一路”世界峰会的保障任务。

另一个更具代表性的例子是国家电网电力调度系统安全防护建设：电力可信计算密码平台已在三十四个省级以上调度控制中心使用，覆盖上千套地级以上电网调度控制系统，涉及十几万个节点，约四万座变电站和一万座发电厂，有效抵御各种网络恶意攻击，确保电力调度系统安全运行。实现了四大目标：高效处理实现实时调度、不打补丁实现免疫抗毒、不改代码实现方便实施、精练消肿实现降低成本。

面临日益严峻的国际网络空间形势，立足国情，创新驱动，弯道超车，聚全国之力用可信计算 3.0 构建网络空间安全主动免疫保障体系，筑牢网络安全防线，为把我国建设成为世界网络安全强国而努力奋斗！（**本文根据 2019 中国 IT 市场年会速记整理**）

责任编辑：卢敏
lumin@staff.ccidnet.com