网络强国系列

用可信计算3.0筑牢网络安全防线

□ 沈昌祥

Building Cyber Security Defense by Trusted Computing 3.0

Shen Changxiang

当前，网络空间已经成为继陆、海、空、天之后的第五大主权领域空间。网络安全是国际战略在军事领域的演进，对我国网络安全提出了严峻的挑战。解决信息安全核心技术设备受制于人的问题，需要创新发展主动免疫的可信防护体系。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中指出："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"。

即将实施的《中华人民共和国网络安全法》第十六条规定，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。近期发布的《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"。因此，创新发展可信计算技术，推动其产业化，是将我国建设成为"技术先进、设备领先、攻防兼备"网络强国的战略任务。

科学的网络安全观

1）网络安全是永远的主题

网络空间安全是计算科学问题、体系结构问题、计算模式问题。网络安全问题源于人们对IT认知逻辑的局限性，由于不能穷尽所有组合，只能局限于完成计算任务去设计IT系统，必定存在逻辑不全的缺陷，从而难以应对人为利用缺陷进行攻击。因此，为了安全，必须从逻辑正确验证、计算体系结构和计算模式等方面进行科学技术创新，以解决缺陷不被攻击者利用的问题，形成攻防矛盾的统一体。确保完成计算任务的逻辑组合不被篡改和破坏，实现正确计算，这就是主动免疫防御。

2）"封堵查杀"被动防护已过时

当前大部分网络安全系统主要是由防火墙、入

侵监测和病毒防范组成，称为“老三样”。“封堵查杀”难以应对利用逻辑缺陷的攻击。首先，老三样根据特征库建立防御，面对层出不穷的新漏洞与攻击方法，消极被动防不胜防；其次，老三样属于超级用户，权限过大，违背基本的安全原则；第三，老三样可以被攻击者控制，成为网络攻击的平台。例如，“棱镜门”就是利用世界著名防火墙收取情报，病毒库篡改后可以导致系统瘫痪（将正常程序作为恶意程序查杀）。因此，只有重建主动免疫可信体系才能有效抵御攻击。

3）可信免疫的计算模式与结构

可信计算是指计算运算的同时进行安全防护，计算全程可测可控，不被干扰，只有这样方能使计算结果总是与预期一样。改变只讲求计算效率，而不讲安全防护的片面计算模式。

在图 1 所示的双体系结构中，采用了一种运算和防护并存的主动免疫的新计算模式，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，相当于为计算机信息系统培育了免疫能力。

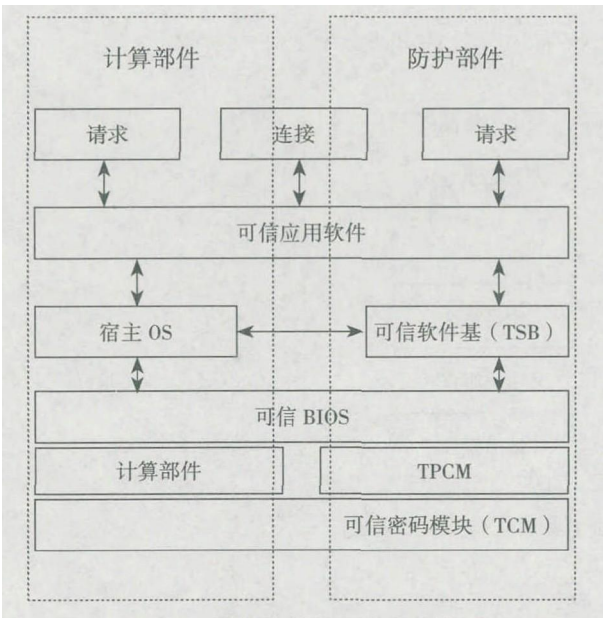

图 1　可信支持的双体系结构

4) 安全可信系统架构

网络化军事设施、云计算、大数据、工业控制、物联网等新型计算环境必须进行可信度量、识别和控制，确保体系结构可信、资源配置可信、操作行为可信、数据存储可信和策略管理可信。其系统架构如图 2 所示：

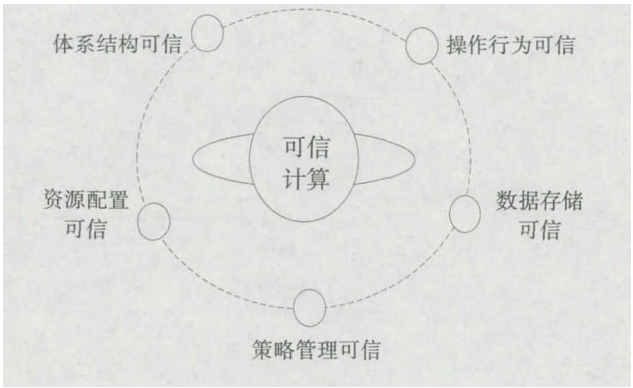

图 2　安全可信系统架构

在可信计算支撑下，将信息系统安全防护体系划分为安全计算环境、安全边界、安全通信网络 3 部分，从技术和管理 2 个方面进行安全设计，建立可信安全管理中心支持下的主动免疫三重防护框架（如图 3 所示）。实现了国家等级保护标准要求（GB/T 25070—2010），做到可信、可控、可管。

按照可信安全管理中心支持下的主动免疫三重防护框架构建积极主动的防御体系，可以达到攻击者进不去、非授权者重要信息拿不到、窃取保密信息看不懂、系统和信息篡改不了、系统工作瘫不成和攻击行为赖不掉的防护效果。“Mirai”、“黑暗力量”、“震网”、“火焰”、“心脏滴血”等将不查杀而自灭。

中国可信计算革命性创新

我国可信计算于 1992 年正式立项研究“主动免疫的综合防护系统”，经过长期攻关、军民融合，形成了自主创新的可信体系，不少已被国际可信计算组织（TCG）采纳。

2014 年以来，国内权威媒体对可信计算的创新发展进行了高度评价。《求是》发表了笔者的署名文章《用可信计算构筑网络安全》；新华社组织召开中国可信开放与网络安全高峰论坛，参考消息进行了整 2 版报道；新华社中国名牌杂志将可信计算定义为网络安全的主动防御时代；《中国信息安全》、《信息安全与通信保密》分

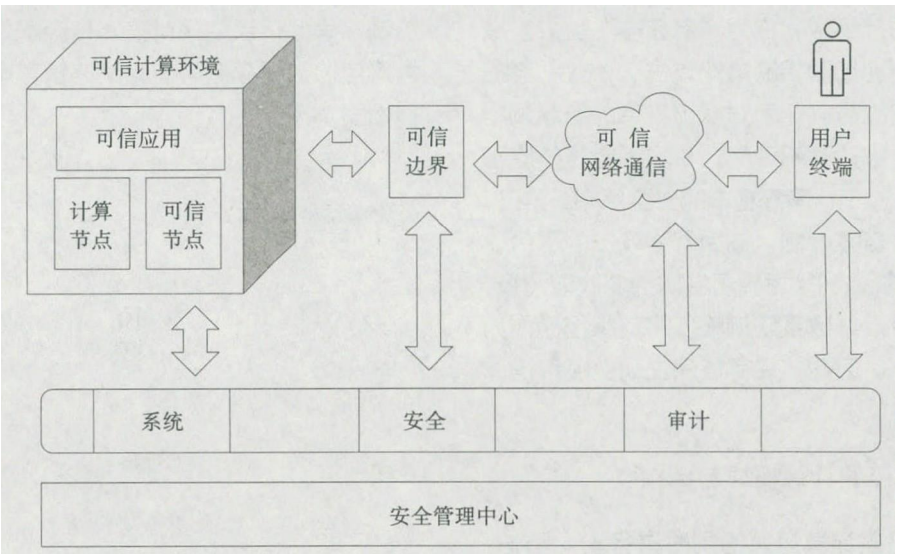

图 3 可信安全管理中心支持下的主动免疫三重防护框架

别出版了可信计算专刊。

1) 全新的可信计算体系结构

相对于国外可信计算被动调用的外挂式体系结构，中国可信计算革命性地开创了自主密码为基础、控制芯片为支柱、双融主板为平台、可信软件为核心、可信连接为纽带、策略管控成体系、安全可信保应用的可信计算体系结构，如图 4 所示：

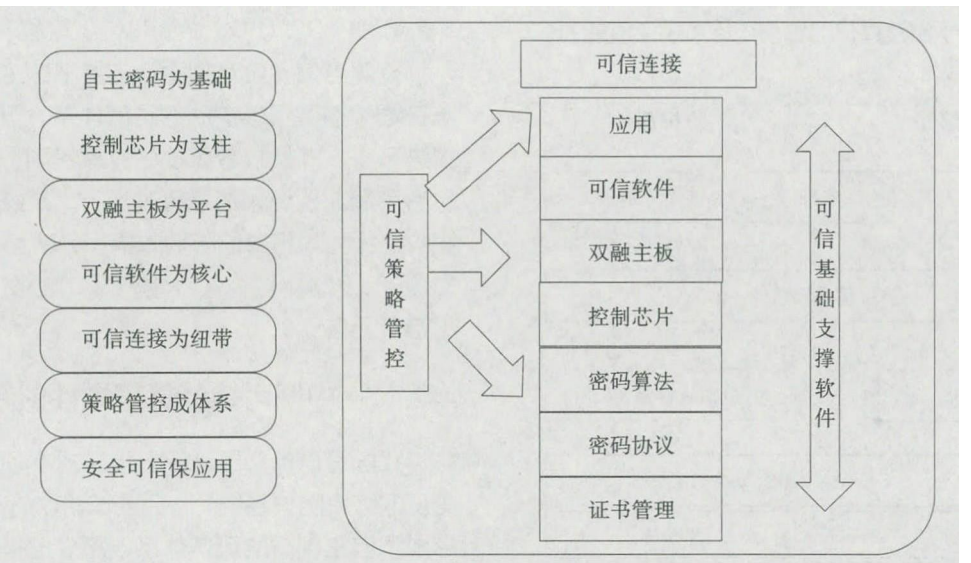

图 4 全新的可信计算体系结构

在该体系结构指引下，我国 2010 年前完成了核心的 9 部国家标准和 5 部国军标的研究起草工作。到目前为止，已发布国家标准 3 项和国军标 3 项，即将发布国家标准 2 项，已发布团体标准（中关村可信计算产业联盟标准）4 项，授权国家专利上百项。创新可信计算标准体系如图 5 所示。

2）跨越了国际可信计算组织（TCG）可信计算局限性

（1）密码体制的局限性

TCG 原版本只采用了公钥密码算法 RSA，杂凑算法只支持 SHA1 系列，回避了对称密码。由此

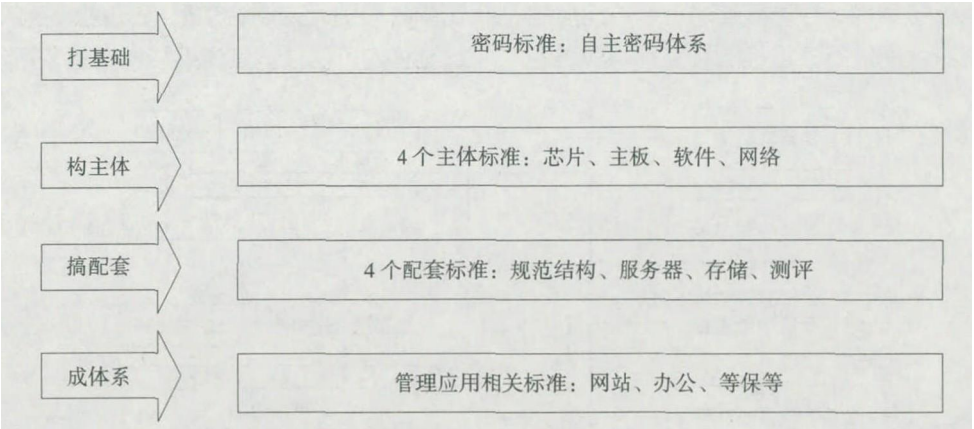

图 5 创新可信计算标准体系

导致密钥管理、密钥迁移和授权协议的设计复杂化（5类证书、7类密钥），也直接威胁着密码的安全。TPM2.0采用了我国对称非对称结合的密码体制，并申报成为了国际标准。

（2）体系结构的不合理

TCG采用外挂式结构，未从计算机体系结构上作变更，把可信平台模块（TPM）作为外部设备挂接在外总线上。软件上，可信软件栈（TSS）是TPS的子程序库，被动调用，无法动态主动度量。中国可信计算创新地采用双系统体系结构，变被动模式为主动模式，使主动免疫防御成为可能。

3）创新可信密码体系

可信计算平台密码方案的创新之处主要体现在算法、机制和证书结构3个方面：在密码算法上，全部采用国有自主设计的算法，定义了可信计算密码模块（TCM）；在密码机制上，对称密码与公钥密码相结合，提高了安全性和效率；在证书结构上，采用双证书结构，简化了证书管理，提高了可用性和可管性。密码算法和可信功能的关系如图6所示：

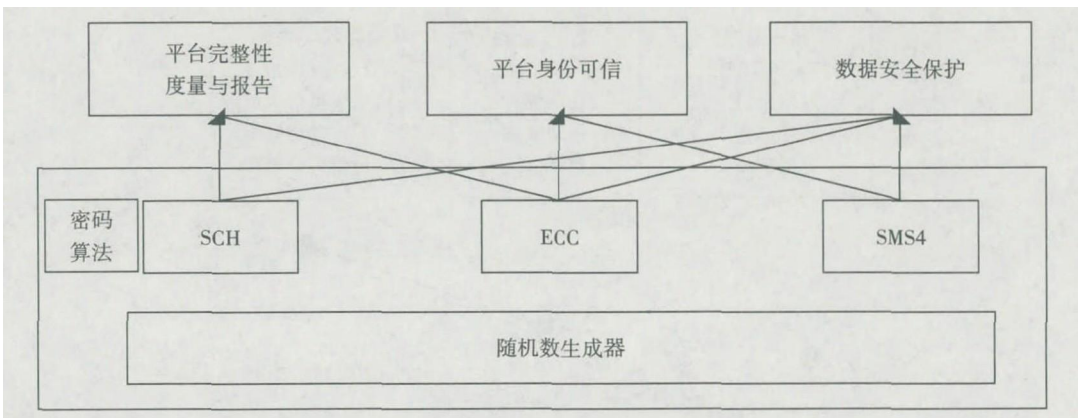

图 6 密码算法和可信功能的关系

4）创建主动免疫体系结构

主动免疫是中国可信计算革命性创新的集中体现。在双系统体系框架下，采用自主创新的对称非对称相结合的密码体制，作为免疫基因；通过主动度量控制芯片（TPCM）植入可信源根，在TCM基础上加以信任根控制功能，实现密码与控制相结合，将可信平台控制模块设计为可信计算控制节点，实现了TPCM对整个平台的主动控制；在可信平台主板中增加了可信度量节点，实现了计算和可信双节点融合；软件基础层实现宿主操作系统和可信软件基的双重系统核心，通过在操作系统核心层并接一个可信的控制软件接管系统调用，在不改变应用软件的前提下实施主动防御；网络层采用三元三

层对等的可信连接架构，在访问请求者、访问控制者和策略仲裁者之间进行三重控制和鉴别，对访问请求者和访问控制者实现统一的策略管理，提高系统整体的可信性。其体系结构如图 7 所示：

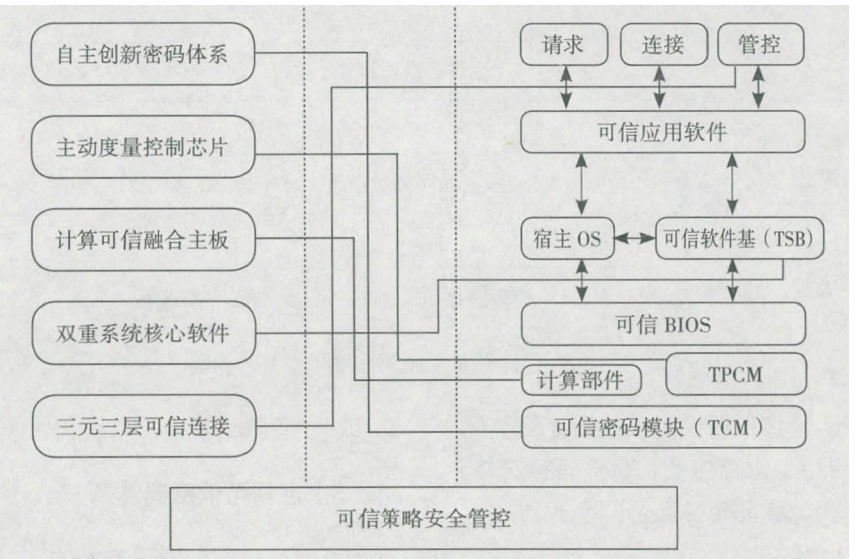

图 7 主动免疫体系结构

5）开创可信计算 3.0 新时代

可信计算 1.0 以世界容错组织为代表，主要特征是主机可靠性，通过容错算法、故障诊查实现计算机部件的冗余备份。可信计算 2.0 以 TCG 为代表，主要特征是节点安全性，通过外部挂接的 TPM 芯片实现被动度量。中国的可信计算 3.0 的主要特征是系统免疫性，其保护对象为节点虚拟动态链，通过“宿主 + 可信”双节点可信免疫架构实现对信息系统的主动免疫防护。可信计算发展路径如图 8 所示：

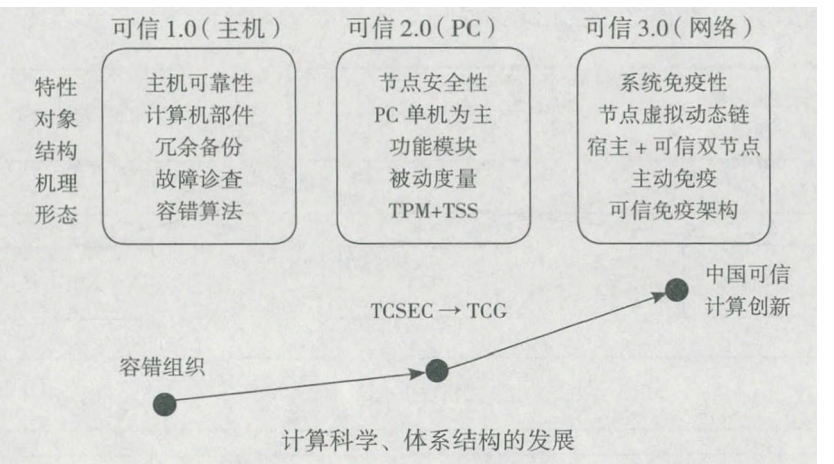

图 8 可信计算发展路径

可信计算 3.0 理论基础是计算复杂性理论以及可信验证。它针对已知流程的应用系统，根据系统的安全需求，通过“量体裁衣”的方式，针对应用和流程制定策略来适应实际安全需要，特别适合为重要生产信息系统提供安全保障，其防御特性如表 1 所示。

可信计算 3.0 是传统访问控制机制在新型信息系统环境下的创新发展，符合事物的螺旋式上升发展规律。它以密码为基因，通过主动识别、主动度量、主动保密存储，实现统一管理平台策略支撑下的数据信息处理可信和系统服务资源可信。可信计算 3.0 在攻击行为的源头判断异常行为并进行防范，其安全强度较高，可抵御未知病毒、未知漏洞的攻击，能够智能感知系统运行过程中出现的规律安全问题。

表 1　可信计算 3.0 防御特性

分　项	特　　性
理论基础	计算复杂性，可信验证
应用适应面	适用服务器、存储系统、终端、嵌入式系统
安全强度	强 / 可抵御未知病毒、未知漏洞的攻击、智能感知
保护目标	统一管理平台策略支撑下的数据信息处理可信和系统服务资源可信
技术手段	密码为基因、主动识别、主动度量、主动保密存储
防范位置	行为的源头，网络平台自动管理
成本	低，可在多核处理器内部实现可信节点
实施难度	易实施，既可适用于新系统建设也可进行旧系统改造
对业务的影响	不需要修改原应用，通过制定策略进行主动实时防护 / 业务性能影响 3% 以下

可信计算 3.0 通过独立的可信架构实现主动免疫，目前只加芯片和软件即可，对现有硬软件架构影响小。可以利用现有计算资源的冗余，也可在多核处理器内部实现可信节点，实现成本低，可靠性高。同时，可信计算 3.0 提供可信 UKey 接入、可信插卡以及可信主板改造等不同方式的产品，既可适用于新系统建设，也可用于旧系统改造；系统通过对应用透明的主动可信监控机制保障应用可信运行，不需要修改原应用程序代码，而是通过制定策略进行主动实时防护，这种防护机制对业务性能影响很小，应用实例表明系统性能影响在 3% 以下。

用可信计算 3.0 构筑网络安全

1）坚持自主可控、安全可信

《国家中长期科学技术发展纲要（2006—2020 年）》明确提出以发展高可信网络为重点开展网络安全技术及相关产品，建立网络安全技术保障体系。“十二五”规划有关工程项目都把可信计算列为发展重点，军方演示验证成果用于党政部门。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都采用可信计算 3.0 作基础支撑。

中关村可信计算产业联盟于 2014 年 4 月 16 日正式成立，经历近 3 年的运行，已有 10 多个专委会，发展迅速、成绩显著。中国可信计算已经成为保卫国家网络空间主权的战略核心技术，已在国家核心系统和关键信息基础设施得到规模化成功应用，并列为国家战略和法律要求。同时也是世界网络空间斗争的焦点，美国第 3 次“抵消战略”（对抗“下一代敌人”的“下一代技术”）把“高可信网络军事系统”等列为重点，围绕安全可信展开新的较量。

2）抢占网络空间安全核心技术战略至高点

2014 年 4 月 8 日，微软公司正式停止对 WindowsXP 的服务支持，强推可信的 Windows 8，严重挑战我国的网络安全。如果国内运行的 2 亿台终端升级为 Windows 8，不仅耗费巨资还失去了安全控制权和二次开发权。采用我国的可信计算技术对 Windows XP 进行安全增强，可避免微软停止服务所引起的安全风险，有力支撑了按习总书记批示精神政府不采购 Windows 8 的决定落实。

2014 年 10 月，微软又推出了 Windows 10，宣布停止非可信的 Windows 7。Windows 10 不仅是终端可信，而且是移动终端、服务器、云计算、大数据等全面执行可信版本，强制与硬件 TPM 芯片配置，并在网上一体化支持管理，可谓“可信全面控制，一网打尽”。推广 Windows 10 将直接威胁网络空间国家主权。

我国按照网络安全审查制度成立安全审查组，按照 WTO“尊重销售国有关法律法规和有关标准”的规则，开展对 Windows 10 的安全审查。要遵守我国《电子签名法》和《商用密码管理条例》，必须进行本土化改造，其中数字证书、可信计算、密码设备必须是国产自主的，而且我国有完整的技术、产品和服务，而且他们的主要思路来自我国的自主创新。为此，以改革开放、合作开发、互利共赢的原则成立的合资公司开始了一场新的博弈，“引进必须安全可控”。

要做到“五可一有”：可知，即对合作方开放全部源代码，要心里有数，不能盲从；可编，要基于对开源代码的理解，能自主编写代码；可重构，面向具体的应用场景和安全需求，对核心技术要素进行重构，形成定制化的新的体系结构；可信，通过可信计算技术增强自主操作系统免疫性，防范漏洞影响系统安全性，使国产化真正落地；可用，做好应用程序与操作系统的适配工作，确

保自主系统能够替代国外产品；有自主知识产权，要对最终的系统拥有自主知识产权，保护好自主创新的知识产权及其安全，坚持核心技术创新专利化、专利标准化、标准推进市场化。要走出国门，成为世界品牌。

3) 构筑主动防御、安全可信的保障体系

根据长期攻关、滚动发展，自主可信计算平台产品设备有 3 种形态：对于增量设备可采用可信芯片直接嵌入主板的方式的可信整机；对于存量设备可采用主板配插可信控制卡的方式构建免疫系统；对于不便于插卡的设备可配接 USB 可信控制模块实现可信增强。以上 3 种方式可以方便地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。

可信计算 3.0 构建主动免疫体系，通过可信安全管理平台实现系统资源、安全策略和审计追踪三权分立。科学管理再加上可信计算控制平台提供资源可信度量、数据可信存储、行为可信鉴别、主客体的可信认证，能及时发现异常行为和环境的非法

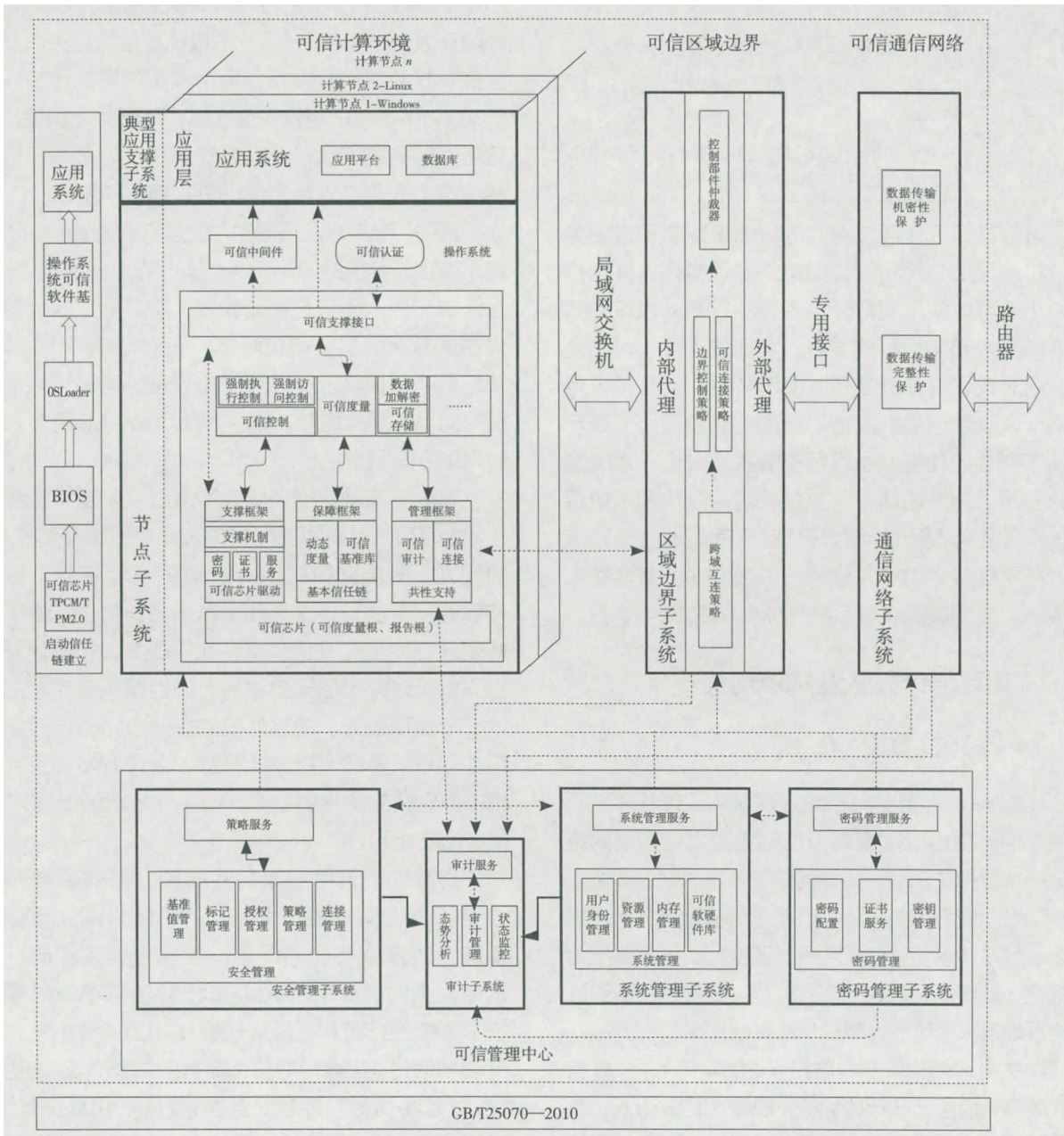

图 9 高安全等级可信防护体系

改变以及主要信息破坏，并立即采取措施，使攻击无效，实现主动免疫。即使有 BUG，也不会变成漏洞，无法攻击，保证系统安全运行。

部署可信计算 3.0 平台后，在原有信息系统建立可信免疫的主动防御安全防护体系（如图 9 所示），实现高安全等级结构化保护，改变原被动防护的局面，使等级保护制度科学实施。

基于可信计算 3.0 构建的主动免疫体系支持网络化部署方式，将主动免疫系统软件安装在安全管理平台，再通过网络分发部署到各计算节点，并实施网络化管理与控制。

4）关键信息基础设施规模化建设应用

（1）国家电网电力调度系统安全防护建设

2014 年 8 月，国家发改委印发了〔2014〕第 14 号令《电力监控系统安全防护规定》，并且同步修订了《电力监控系统安全防护总体方案》等配套技术文件。新版本的总体方案要求生产控制大区具备控制功能的系统应用可信计算技术实现计算环境和网络环境安全可信，建立对恶意代码的免疫能力，实现等级保护 4 级。图 10 是国家电网电力调度系统可信加固方案，不修改原 D5000 控制管理

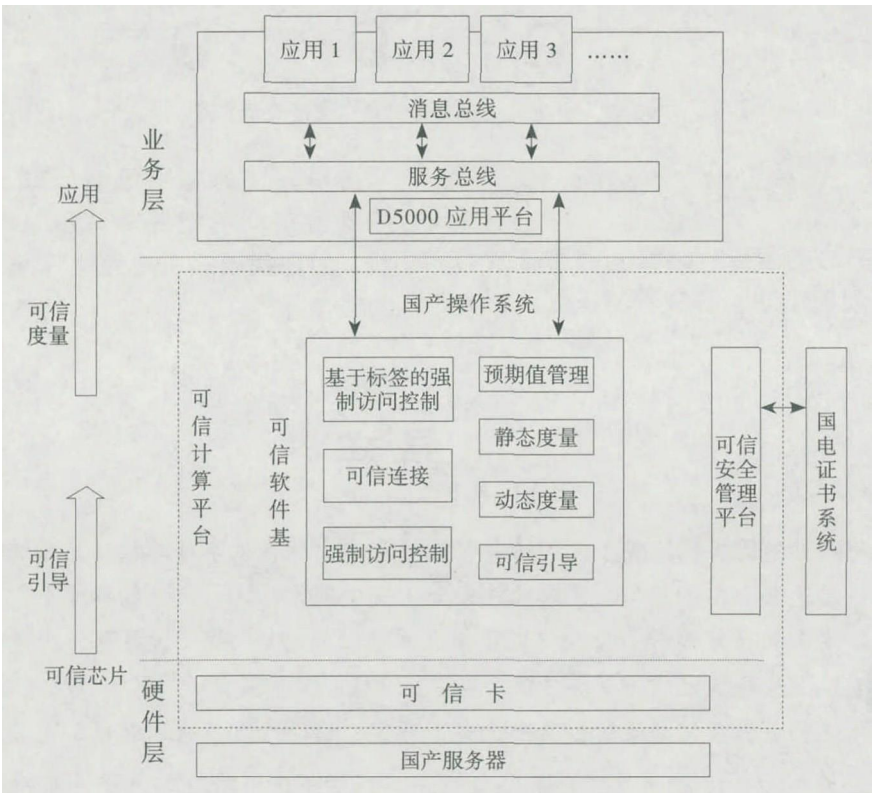

图 10　国家电网电力调度系统可信加固方案

系统代码，不加装杀毒软件和 IDS，以可信计算为核心技术，通过对系统实施逐级度量认证，实现系统的主动免疫。

电力可信计算密码平台已在 34 个省级以上调度控制中心和 59 个地级调度控制中心上线运行，覆盖了上万台服务器，运行情况良好，达到等级保护 4 级技术要求，整体系统对性能的影响小于 3%，如表 2 所示：

表 2　可信计算对性能的影响

应用	加载前 CPU 使用率 /%	加载后 CPU 使用率 /%	对 CPU 使用率影响度 /%	加载前内存使用率 /%	加载后内存使用率 /%	对内存使用率影响度 /%	加载前计算时间 /s	加载后计算时间 /s	对计算时间的影响度 /%
应用 1	2.92	2.95	1.03	11	11	0	69	69.9	1.3
应用 2	2.3	2.33	1.3	6.9	7	1.45	24.6	25.1	2.03
应用 3	2.8	2.85	1.79	7.8	7.9	1.28	18.9	19.4	2.65

（2）中央电视台可信制播环境建设

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，在没有互联网物理隔离的计算机网络环境下，构建了网络制播的可信计算安全技术体系，建立了可信、可控、可管的网络制播环境，达到4级安全要求，确保节目安全播出。中央电视台可信制播环境建设示意图如图11所示：

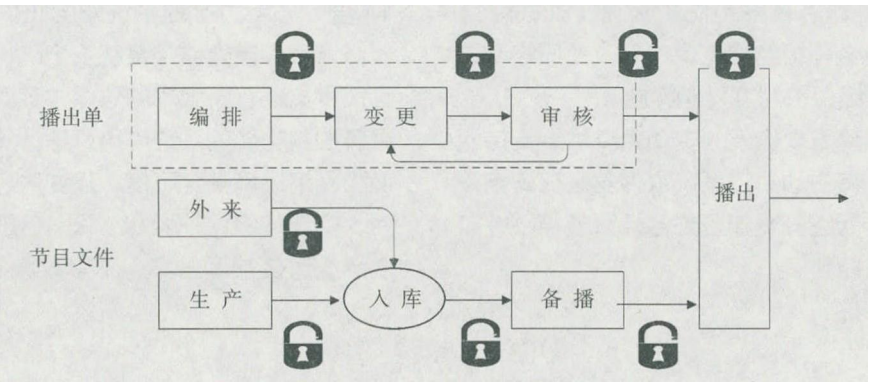

图11 中央电视台可信制播环境建设示意图

结 语

面临日益严峻的国际网络空间形势，我们要立足国情，创新驱动，解决受制于人问题。坚持纵深防御，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。

沈昌祥

中国工程院院士，1965年毕业于浙江大学，从事计算机信息系统、密码工程、信息安全体系结构、系统软件安全（安全操作系统、安全数据库等）、网络安全等方面的研究工作。先后完成了重大科研项目20多项，取得了一系列重要成果，曾获国家科技进步一等奖2项、二等奖2项、三等奖3项、军队科技进步奖10多项。这些成果在信息处理和安全技术上有重大创造性，多项达到世界先进水平，在全国全军广泛应用，取得十分显著效益，使我国信息安全保密方面取得突破性进展。在网络安全和科技创新、咨询论证和学科专业建设、人才培养等方面作出了杰出贡献。被授予“海军模范科技工作者”荣誉称号，评为国家有突出贡献中青年专家，曾当选为7届全国人大代表，1995年5月当选为中国工程院院士，1996年获军队首届专业技术重大贡献奖，2002年荣获国家第4届“光华工程科技奖”，2016年获首届中国网络安全杰出人才奖。目前担任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，国家集成电路产业发展咨询委员会委员，国家保密局专家咨询委员会主任委员，国家信息安全等级保护专家委员会主任委员，国家密码管理委员会办公室顾问，公安部“金盾工程”特邀顾问，中国人民银行信息安全顾问，国家税务总局信息技术咨询委员会委员。同时还担任北京大学、国防科技大学、浙江大学、中国科学院研究生院、上海交通大学等多所著名高校的博士生导师。

shenchx@cae.cn